Singapore Management University
Institutional Knowledge at Singapore Management University

Research Collection School Of Information Systems School of Information Systems

4-2017

# A secure and efficient ID-based aggregate signature scheme for wireless sensor networks

Limin SHEN

Jianfeng MA

Ximeng LIU
*Singapore Management University*, xmliu@smu.edu.sg

Fushan WEI

Meixia MIAO

**DOI:** https://doi.org/10.1109/JIOT.2016.2557487

Follow this and additional works at: https://ink.library.smu.edu.sg/sis_research

Part of the Information Security Commons

## Citation

SHEN, Limin; MA, Jianfeng; LIU, Ximeng; WEI, Fushan; and MIAO, Meixia. A secure and efficient ID-based aggregate signature scheme for wireless sensor networks. (2017). *IEEE Internet of Things*. 4, (2), 546-554. Research Collection School Of Information Systems.
**Available at:** https://ink.library.smu.edu.sg/sis_research/4121

This Journal Article is brought to you for free and open access by the School of Information Systems at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Information Systems by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.

Published in IEEE Internet of Things Journal, Volume: 4, Issue: 2, April 2017, Pages 546-554
https://doi.org/10.1109/JIOT.2016.2557487

# A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks

Limin Shen, Jianfeng Ma, *Member, IEEE*, Ximeng Liu, *Member, IEEE,* Fushan Wei, and Meixia Miao

***Abstract*—Affording secure and efficient big data aggregation methods is very attractive in the field of wireless sensor networks (WSNs) research. In real settings, the WSNs have been broadly applied, such as target tracking and environment remote monitoring. However, data can be easily compromised by a vast of attacks, such as data interception and data tampering, etc. In this paper, we mainly focus on data integrity protection, give an identity-based aggregate signature (IBAS) scheme with a designated verifier for WSNs. According to the advantage of aggregate signatures, our scheme not only can keep data integrity, but also can reduce bandwidth and storage cost for WSNs. Furthermore, the security of our IBAS scheme is rigorously presented based on the computational Diffie–Hellman assumption in random oracle model.**

***Index Terms*—Aggregate signature, big data, coalition attack, data aggregation, designated verifier, identity-based (ID-based), unforgeability, wireless sensor network (WSN).**

## I. Introduction

IN BIG data era, digital universe grows in stunning speed which is produced by emerging new services, such as social network [1], [2], cloud computing [3]–[8], and Internet of things [9], [10]. Big data are gathered by omnipresent wireless sensor networks (WSNs), aerial sensory technologies, software logs, information-sensing mobile devices, microphones, cameras, etc. [11]. And the WSN is one of the highly anticipated key contributors of the big data in the future networks [12].

WSNs, with a large number of cheap, small, and highly constrained sensor nodes sense the physical world [13], has very broad application prospects [14] both in military and civilian usage, including military target tracking and surveillance [15], animal habitats monitoring [16], biomedical health monitoring [17], [18], and critical facilities tracking [19]. It can be used in some hazard environments, such as in nuclear power plants. Due to the remarkable advantages, comprehensive attention has been devoted to WSNs [20], and a number of schemes have been presented [21]–[25]. In WSNs, sensor nodes are usually resource-limited and power-constrained, they always suffer from the restricted storage and processing resources. Therefore, different from traditional networks, WSNs have their inherent resource constraints and design limitations, such as low bandwidth, short communication range, limited amount of energy, and limited processing and storage in every sensor node. Data aggregation technique is considered as a Holy Grail to reduce energy consumption for WSNs. However, the technique still has the inherent security problems, such as eavesdropping, reply attacks, data forge and data tampering, etc. Hence, designing a secure and efficient data aggregation method is very significant for WSNs.

In 1984, Shamir [26] introduced the identity-based (ID-based) cryptography, which eases the key management problem by eliminating public key certificates. In an ID-based cryptography, the user's public key is easily generated from this user's any unique identity information (e.g., the serial number, a mobile phone number, an email address, etc.), which is assumed to be publicly known. A trusted third party, called the private key generator (PKG), generates and issues secretly the corresponding private keys for all users using a master secret key. Therefore, in an ID-based signature system, verification algorithm only involves the signature pair, some public parameters and the identity information of signer, without using an additional certificate.

In 2003, Boneh *et al.* [27] introduced an aggregate signature scheme, which can compress multiple signatures generated by different users on different messages into a single short aggregate signature. The aggregate signature's validity can be equivalent to the validity of every signature which is used to generate the aggregate signature. That is to say, the aggregate signature is validity if and only if each individual signer really signed its original message, respectively. Hence, aggregation is useful technique in reducing storage cost and bandwidth, and can be a decisive building block in some settings, such as data aggregation for WSNs [22], securing border gateway protocols [28] and large scale electronic voting system [29], etc.

In this paper, combining the highlights of aggregate signature scheme and ID-based cryptography, we give an ID-based aggregate signature (IBAS) scheme for WSNs in cluster-based method (Fig. 1). The adversary in our security model has the capability to launch any coalition attacks. If an adversary can

Manuscript received January 28, 2016; revised March 16, 2016; accepted April 8, 2016. Date of publication April 21, 2016; date of current version April 28, 2017. This work was supported in part by the National High Technology Research and Development Program (863 Program) under Grant 2015AA016007, and in part by the National Nature Science Foundation of China under Grant U1405255, Grant 61170298, Grant 61502237, and Grant 61572198.

L. Shen is with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China, and also with the School of Computer Science and Technology, Nanjing Normal University, Nanjing 210023, China (e-mail: shenlimin@njnu.edu.cn).

J. Ma and M. Miao are with the School of Computer Science and Technology, Xidian University, Xi'an 710071, China.

X. Liu is with the School of Information Systems, Singapore Management University, Singapore 188065.

F. Wei is with the Department of Information Research, Zhengzhou Information Science and Technology Institute, Zhengzhou 450001, China.

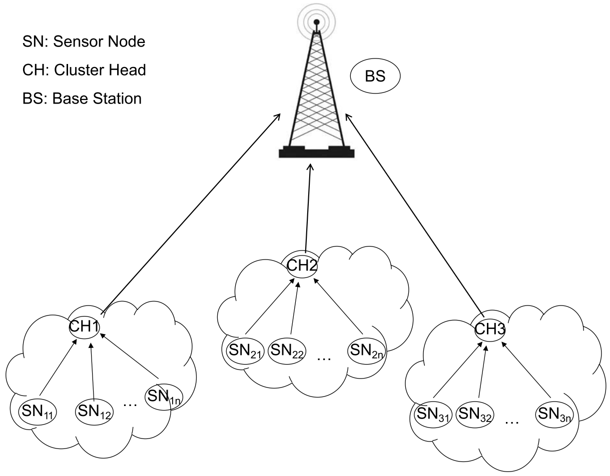


Fig. 1. Cluster-based network.

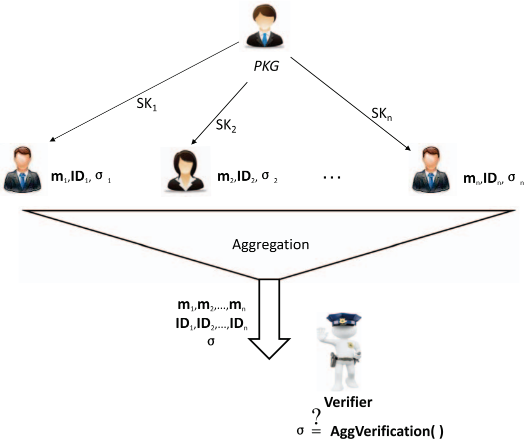


Fig. 2. IBAS scheme.

use some single signatures including invalid ones to generate a valid aggregate signature, we say that the attack is successful. In fact, our IBAS scheme not only can protect data integrity, but also can reduce bandwidth and storage cost for WSNs. The main contributions of this paper are fourfold.

1) First, we give the system model which have three components: a) data center; b) aggregator; and c) a large number of sensor nodes. Aggregator works as a cluster head, can produce the aggregate signature and send it to the data center with the messages generated by the sensor nodes. Then, through a game played with a challenger and an adversary, the security model of IBAS schemes is introduced. And in the security model, the aggregation algorithm should resist all kinds of coalition attacks.
2) Second, we give a secure IBAS scheme for WSNs with a designated verifier (data center). Our scheme is composed of six probabilistic polynomial time (PPT) algorithms: a) setup; b) KeyGeneration; c) signing; d) verification; e) aggregation; and f) AggVerification.
3) Third, the detailed security proof is given based on the computational Diffie–Hellman (CDH) assumption in random oracle model. The security proof indicates that our IBAS scheme for WSNs can ensure the integrity of the data and reduce the communication and storage cost.
4) Fourth, through the analysis of comparative performance, we demonstrate that our IBAS scheme is efficient in terms of the communication and storage overhead.

The rest of this paper is organized as follows. In the following section, we introduce some related work about aggregate signature schemes. In Section III, we give some preliminaries demanded in this paper, including bilinear pairing and complexity assumptions. Section IV presents the system model and security model of IBAS schemes. Our IBAS scheme is presented in Section V. In Section VI, we present a detailed security proof of our scheme based on the CDH assumption, and some observation of our new scheme. In Section VII, we analyze the performance of our IBAS scheme in terms of communication and computation cost. Finally, Section VIII is the conclusions.

## II. Related Work

The aggregate signature scheme can generate a compressed signature from many signatures generated by different users on different messages. Boneh *et al*. [27] introduced the concept and structure of aggregate signature schemes in 2003. After that, many aggregate signature schemes have been presented [30]–[33]. However, there still exist a lot of problems in the above schemes. In traditional public key infrastructures (PKIs), the user's public key is not related to the user's identity information, in fact, it is a "random" string. So there needs a trusted certificate authority to generate certificates which can ensure the relationship between the user and the cryptographic keys. This improves the communication overhead, computation and storage cost and would influence the efficiency of the aggregate signature scheme. ID-based cryptography [26] solved these problems. In an ID-based cryptography, the user's public key is any publicly known and unique identity information, such as the serial number, and the user no longer needs a certificate to prove its identity.

Since then, many IBAS schemes (Fig. 2) have been presented [34]–[37]. Up to now, a great many aggregate signature schemes have rapidly emerged in various settings, such as [38] and [39] in PKIs and [40]–[44] in certificateless public key cryptography, respectively. Both [43] and [45] show security drawbacks of the certificateless aggregate signature scheme in [42] by demonstrating some kinds of attacks.

Unfortunately, most of the existing aggregate signature schemes cannot resist a kind of practical and powerful attacks—coalition attacks [43], [46], [47]. Coalition attack can generate a valid aggregate signature by using some invalid single signatures with the collusion of two or more signers. If such an attack is successful, the corresponding aggregate signature will pass the validation while some single signatures used to generate it are invalid. This suggests that a valid aggregate signature may fail to prove the validity of every individual signature involved in the aggregation. This fact obviously violates the security goal for aggregate signature schemes. So, in this paper, we will mainly focus on designing the aggregate signature scheme which can resist coalition attacks.

## III. Preliminaries

The following is some basic notions required in this paper, containing the definition of bilinear pairing, the CDH complexity assumption.

### A. Bilinear Pairing

Let $G$ and $K$ denote two cyclic groups whose orders are both prime $p$. Let $P$ be a generator in $G$ and $|G| = |K|$. A map $\hat{e} : G \times G \rightarrow K$ is called a bilinear pairing if it satisfies the following properties.

1) *Bilinearity:* For all $Q_1, Q_2 \in G$ and $\tau, \upsilon \in Z_p^*$, $\hat{e}(\tau Q_1, \upsilon Q_2) = \hat{e}(Q_1, Q_2)^{\tau\upsilon}$.
2) *Nondegeneracy:* $\hat{e}(P, P) \neq 1_K$, where $1_K$ is the identity element of $K$.
3) *Computability:* For all $P_1, P_2 \in G$, there exits an efficient algorithm to compute $\hat{e}(P_1, P_2)$.

### B. Complexity Assumptions

This section revisits the CDH complexity assumption [35] needed in the following sections.

*Definition 1 (CDH Problem):* Given the elements $P, \tau P, \upsilon P \in G$, to compute $\tau\upsilon P \in G$ for unknown randomly chosen $\tau, \upsilon \in Z_p^*$.

The CDH assumption states that the CDH problem is hard. Let $\mathcal{A}$ be a CDH attacker. $\mathcal{A}$'s advantage to solve the CDH problem in $G$ is defined as

$$\mathrm{Adv}_{\mathcal{A}}^{\mathrm{CDH}} = Pr\Big[\mathcal{A}(P, \tau P, \upsilon P) = \tau\upsilon P : \tau, \upsilon \in Z_p^*\Big].$$

Here the probability is over the uniform random scalars $\tau$ and $\upsilon$ from $Z_p^*$, and the choice of $P \in G$, and the coin tosses of $\mathcal{A}$.

## IV. System Model and Security Model

### A. System Model

Security requirements in WSNs mainly are confidentiality, integrity, authenticity, scalability and flexibility, etc. In a data aggregation scheme for WSNs, it is important that no data falsify during transmissions. So we mainly focus on the data integrity protection in our system. The main consideration of our system model is to protect data integrity while reducing bandwidth and storage cost for WSNs.

Our IBAS system consists of three parts (Fig. 3): 1) data center; 2) aggregator; and 3) sensor node.

1) Data center has a strong computing power and storage space. So it can process all original big data collected by sensor nodes belong to the data center, and can provide the data information to consumers. At the beginning, every data center (as the designated verifier in our IBAS scheme) will receive its public-secret key pair $(\mathrm{PK}_{\mathrm{center}}, \mathrm{SK}_{\mathrm{center}})$, and publish the public key $\mathrm{PK}_{\mathrm{center}}$.
2) Aggregator is a special sensor node with a certain ability to calculation and communication range. It can sign messages collecting from the physical world, can get the data center's public key $\mathrm{PK}_{\mathrm{center}}$ from public channel, can generate the aggregate signature from the individual signatures signed by sensor nodes included aggregator itself, and can send the aggregate signature to the data center. We assume that the PKG generates the system parameters param, aggregator's private key $S_{\mathrm{ID}}$ corresponding to its identifier information ID, then embeds $(\mathrm{param}, S_{\mathrm{ID}})$ in aggregator when it is deployed.
3) Sensor node has limited resources in terms of computation, memory, and battery power. We assume that the PKG generates private key $S_{\mathrm{ID}_i}$ for each sensor node $\mathrm{ID}_i$. When sensor node $\mathrm{ID}_i$ is deployed, it is embedded with $(\mathrm{param}, S_{\mathrm{ID}_i})$. Every sensor node $\mathrm{ID}_i$ can use its private key $S_{\mathrm{ID}_i}$ to sign messages collecting from the physical world. In our system, each sensor node belongs to one cluster, sends messages and its signatures to their aggregator, and the messages will finally be sent to data center via aggregator.

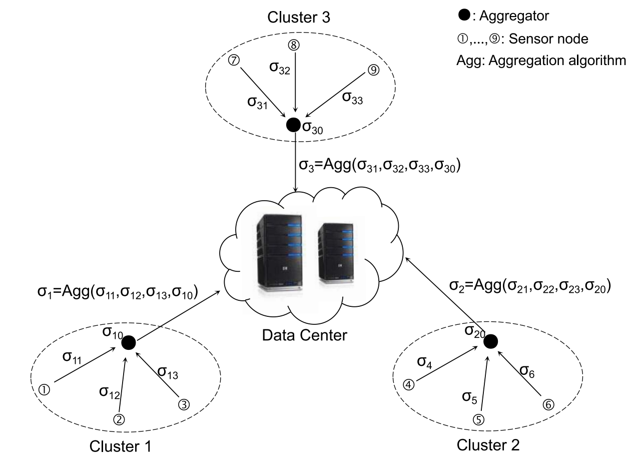


Fig. 3. Our system.

### B. Security Model of IBAS

An IBAS scheme is comprised of six PPT algorithms: 1) setup; 2) KeyGeneration; 3) signing; 4) verification; 5) aggregation; and 6) AggVerification. Please refer to [37] for the detailed instruction.

Obviously, the goal of an adversary is the existential forgery of an aggregate signature. An IBAS scheme is secure if the basic signature scheme involved is existentially unforgettable against adaptive chosen message attacks (EUF-CMA secure [48]), and the aggregation algorithm should stand up against all kinds of coalition attacks. Most of the former security models only consider the security of the basic signature scheme and the forgery of an aggregate signature, and do not consider the coalition attacks. So we mainly focus on the security of aggregation algorithm. When attacking the aggregation algorithm, the purpose of an adversary is to forge a valid aggregate signature while using some invalid individual signatures. The following is a game played with a challenger $\mathcal{B}$ and an adversary $\mathcal{A}$.

1) *Setup:* The challenger $\mathcal{B}$ runs the setup algorithm to obtain a master secret key msk and the system parameters param with a security parameter $l$. Additionally, $\mathcal{B}$ randomly generates the public-secret

key pair $(\mathrm{PK}_{\mathrm{center}}, \mathrm{SK}_{\mathrm{center}})$ of data center (designated verifier), then $\mathcal{B}$ gives param and $\mathrm{PK}_{\mathrm{center}}$ to $\mathcal{A}$.

2) *Queries:* An adversary $\mathcal{A}$ may access the oracles adaptively as follows.
   a) *KeyGeneration Query $\mathcal{O}_S(ID)$:* On receiving such a query, challenger $\mathcal{B}$ responds by running KeyGeneration algorithm to obtain the private key $S_{\mathrm{ID}}$ of the user ID, returns $S_{\mathrm{ID}}$ to $\mathcal{A}$.
   b) *Signing Query $\mathcal{O}_{\mathrm{sig}}(ID, m)$:* On receiving such a query, challenger $\mathcal{B}$ responds by running signing algorithm to obtain a signature $\sigma$ and returns $\sigma$ to $\mathcal{A}$. ($\mathcal{B}$ first runs the KeyGeneration algorithm if necessary.)
   c) *AggVerification Query $\mathcal{O}_{\mathrm{AggV}}(\{m_i, ID_i, i = 1, \ldots, n\}, \sigma)$:* On receiving such a query, challenger $\mathcal{B}$ responds whether the aggregate signature is valid for the submitting tuples by running AggVerification algorithm.

3) *Forge:* Finally, $\mathcal{A}$ outputs its forgery

$$\left(\left\{m_j, \mathrm{ID}_j, \sigma_j, j = 1, \ldots, n\right\}, \sigma^*\right).$$

$\mathcal{A}$ wins the game if the following conditions are satisfied.
   a) The aggregate signature $\sigma^*$ is valid on tuple

$$\left\{m_j, \mathrm{ID}_j, \sigma_j, j = 1, \ldots, n\right\}.$$

   b) At least one individual signature $\sigma_j (j = 1, \ldots, n)$ is invalid.

This illustrates that $\mathcal{A}$ wins the game if and only if it can forge a valid aggregate signature using a set of individual signatures which is involved at least one invalid single signature.

*Definition 2:* An IBAS scheme is $(t, \epsilon)$-secure if no $t$-time adversary can win the above game with advantage $\mathrm{Adv}_{\mathrm{AggSig}_{\mathcal{A}}} \geq \epsilon$.

## V. Our Identity-Based Aggregate Signature Scheme

In this section, we provide a secure IBAS scheme. We adopt Sakai *et al.*'s [49] signature scheme as the basis to construct our IBAS scheme. The scheme is described as follows.

### A. Setup

Assume $l$ is a security parameter, $G_1$ and $G_2$ are two cyclic groups of prime order $p$. Let $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing, and let $P$ be an arbitrary generator of $G_1$. $H_1, H_2$, and $H$ are full-domain collision resistant hash functions. $H_1, H_2 : \{0, 1\}^* \rightarrow G_1$, and $H : G_2 \rightarrow Z_p^*$. PKG chooses $x, y \in Z_p^*$ randomly and computes $P_0 = xP, \mathrm{PK}_{\mathrm{center}} = yP$. Then the system parameters are param $= \{\hat{e}, G_1, G_2, P, p, H_1, H_2, H, P_0\}$, the master secret key is msk $= x$. The data center's public-secret verification key pair is $(\mathrm{PK}_{\mathrm{center}} = yP, \mathrm{SK}_{\mathrm{center}} = y)$.

### B. KeyGeneration

Given a sensor node's identity $\mathrm{ID}_i$, compute $Q_i = H_1(\mathrm{ID}_i)$ and the sensor node's corresponding private key is $S_i = xQ_i$.

### C. Signing

To sign a message $m_i$, the sensor node $\mathrm{ID}_i$ with the corresponding private key $S_i$ generates $t_i \in Z_p^*$ randomly, and computes

$$\begin{aligned} T_i &= t_i P \\ h_i &= H_2(T_i, \mathrm{ID}_i, m_i) \\ U_i &= S_i + t_i h_i. \end{aligned}$$

The signature is $\sigma = (U_i, T_i, \mathrm{ID}_i, m_i)$.

### D. Verification

Given $(\sigma, \text{param})$, the verifier computes $Q_i = H_1(\mathrm{ID}_i)$ and $h_i = H_2(T_i, \mathrm{ID}_i, m_i)$, then accepts if the following equation holds:

$$\hat{e}(U_i, P) = \hat{e}(P_0, Q_i)\hat{e}(T_i, h_i).$$

### E. Aggregation

Given an aggregate subset of sensor nodes belong to one cluster, each sensor node with the identity $\mathrm{ID}_i$ provides a signature $\sigma_i = (U_i, T_i, \mathrm{ID}_i, m_i)$ on a message $m_i \in \{0, 1\}^*$ of its collection, $i = 1, \ldots, n$. Gained the data center's public key $\mathrm{PK}_{\mathrm{center}}$ from public channel, the aggregator computes

$$\begin{aligned} r &= H\big(\hat{e}(U_1, \mathrm{PK}_{\mathrm{center}}), \ldots, \hat{e}(U_n, \mathrm{PK}_{\mathrm{center}})\big) \\ U &= r \cdot \sum_{i=1}^{n} U_i. \end{aligned}$$

$\sigma = (U, T_1, \ldots, T_n)$ is the aggregate signature with identities $\{\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_n\}$ on messages $\{m_1, m_2, \ldots, m_n\}$, respectively.

### F. AggVerification

Given an aggregate signature $\sigma$ on the original messages $m_i \in \{0, 1\}^*$ generated by the sensor nodes belong one cluster with the identity $\mathrm{ID}_i$, $i = 1, \ldots, n$. The data center with public-secret key pair $(\mathrm{PK}_{\mathrm{center}}, \mathrm{SK}_{\mathrm{center}})$ computes $Q_i = H_1(\mathrm{ID}_i)$ and $h_i = H_2(T_i, \mathrm{ID}_i, m_i)$ and accepts if the following equation holds:

$$\hat{e}(U, P) = \Pi_{i=1}^{n} \hat{e}(P_0, Q_i)^{r'} \hat{e}(T_i, h_i)^{r'}$$

where

$$r' = H\big(\hat{e}(P_0, Q_1)^y \cdot \hat{e}(T_1, h_1)^y, \ldots, \hat{e}(P_0, Q_n)^y \cdot \hat{e}(T_n, h_n)^y\big).$$

### G. Correctness

If the following equations hold:

$$\hat{e}(U_i, P) = \hat{e}(P_0, Q_i)\hat{e}(T_i, h_i), \quad i = 1, \ldots, n.$$

Then we have

$$\hat{e}(U_i, \mathrm{PK}_{\mathrm{center}}) = \hat{e}(P_0, Q_i)^y \hat{e}(T_i, h_i)^y, \quad i = 1, \ldots, n$$

and

$$\begin{aligned} r' &= H\big(\hat{e}(P_0, Q_1)^y \hat{e}(T_1, h_1)^y, \ldots, \hat{e}(P_0, Q_n)^y \hat{e}(T_n, h_n)^y\big) \\ &= H\big(\hat{e}(U_1, \mathrm{PK}_{\mathrm{center}}), \ldots, \hat{e}(U_n, \mathrm{PK}_{\mathrm{center}})\big) \\ &= r. \end{aligned}$$

Additionally, we have

$$\begin{aligned}\hat{e}(U, P) &= \hat{e}\left(r \cdot \sum_{i=1}^{n} U_i, P\right)\\ &= \Pi_{i=1}^{n}\hat{e}(U_i, P)^r\\ &= \Pi_{i=1}^{n}\hat{e}(P_0, Q_i)^r\hat{e}(T_i, h_i)^r\\ &= \Pi_{i=1}^{n}\hat{e}(P_0, Q_i)^{r'}\hat{e}(T_i, h_i)^{r'}.\end{aligned}$$

## VI. Security Proof

In this section, first, we give security proof of the above signature scheme involved in our IBAS scheme in random oracle model, and then prove the security of the aggregate algorithm.

*Theorem 1:* Let $H_1$ and $H_2$ be random oracles and there exists an adversary $\mathcal{A}$ against our scheme with advantage $\epsilon$ when running in time $t$, making at most $d_{key}$ times KeyGeneration queries, $d_s$ times signing queries, and $d_i$ times random oracle queries to $H_i$ $(1 = 1, 2)$. Then, there exists an algorithm $\mathcal{B}$ to solve the CDH problem with probability $\epsilon' \geq \frac{1}{d_1}\epsilon$ and running in time $t' \leq t+(d_1+d_2+d_{key}+4d_s)\cdot\tau_{\text{sca}}$, where $\tau_{\text{sca}}$ denotes the time required for computing a scalar multiplication.

*Proof:* Assume $\mathcal{A}$ can break the EUF-CMA security of the scheme, then we can construct a CDH problem solver $\mathcal{B}$ who is given a random instance $(P, uP, vP)$ of the CDH problem. Next, we will show that how $\mathcal{B}$ can use $\mathcal{A}$ to obtain the value of $uvP$ in $G_1$.

At the beginning, $\mathcal{B}$ sets $P_0 = uP$ and generates system parameters param $= \{\hat{e}, G_1, G_2, P, p, H_1, H_2, P_0\}$, The hash functions $H_1$ and $H_2$ serve as random oracles controlled by $\mathcal{B}$. $\mathcal{B}$ chooses a random integer index $\lambda \in [1, d_1]$, let the $\lambda$th query to $H_1$ is on the target identity ID$^*$.

$\mathcal{B}$ responds to $\mathcal{A}$'s queries as follows. (These queries contain $H_i(i = 1, 2)$ queries, KeyGeneration queries and signing queries. All pairs of query/answer are maintained in lists.)

### A. $H_1$ Queries

$\mathcal{B}$ maintains a $H_1^{\text{list}}$ list of tuples $(\text{ID}_i, h_{1i}, Q_i)$. When receiving such an query on ID$_i$, $\mathcal{B}$ performs the following steps:

1) if $i \neq \lambda$, $\mathcal{B}$ randomly chooses $h_{1i} \in Z_q^*$, computes $Q_i = H_1(\text{ID}_i) = h_{1i}P$;
2) else if $i = \lambda$, set $h_{1\lambda} = \perp$, $Q_\lambda = vP$;
3) add the corresponding tuple to $H_1^{\text{list}}$.

We suppose that before making other related queries, $\mathcal{A}$ always makes the corresponding $H_1$ queries first.

### B. $H_2$ Queries

$\mathcal{B}$ maintains a $H_2^{\text{list}}$ list of tuples $(T_i, \text{ID}_i, m_i, h_{2i}, h_{2i}P)$. When receiving an $H_2$ query on $(T_i, \text{ID}_i, m_i)$, $\mathcal{B}$ randomly chooses $h_{2i} \in Z_q^*$, computes $H_2(T_i, \text{ID}_i, m_i) = h_{2i}P$, and add the corresponding tuple to $H_2^{\text{list}}$.

### C. KeyGeneration Queries

When receiving a KeyGeneration query on an identity ID$_i$:

1) if $i = \lambda$, $\mathcal{B}$ aborts the game;
2) else, $\mathcal{B}$ makes $H_1$ queries on ID$_i$, then searches $H_1^{\text{list}}$ for a tuple $(\text{ID}_i, h_{1i}, Q_i)$ and generates the user's private key $S_i = h_{1i}P_0$.

### D. Signing Queries

When receiving a signing query on $(\text{ID}_i, m_i)$:

1) if $i \neq \lambda$, $\mathcal{B}$ runs the signing algorithm normally to produce a signature;
2) if $i = \lambda$, $\mathcal{B}$ produces a signature in the following way.
   a) Randomly pick $t_1, t_2 \in Z_p^*$.
   b) Compute $T = t_1P_0$, $U = t_2P_0$.
   c) Set $H_2(T, \text{ID}^*, m) = t_1^{-1}(t_2P - H_1(\text{ID}^*))$.
      If there has been an tuple $(T, \text{ID}^*, m, \perp)$ in $H_2^{\text{list}}$, $\mathcal{B}$ chooses another $t_1 \in Z_p^*$ and repeat above three signature steps.
   d) The signature is $\sigma = (U, T, \text{ID}, m)$.

### E. Forge

At last, $\mathcal{A}$ generates a counterfeit $\sigma^* = (U^*, T^*, \text{ID}^*, m^*)$. If $\mathcal{A}$ forges successfully, i.e., $\sigma^*$ is valid, it should pass the verification

$$\hat{e}\big(U^*, P\big) = \hat{e}\big(P_0, Q^*\big)\hat{e}\big(T^*, h_2^*\big)$$

where

$$Q^* = H_1\big(\text{ID}^*\big) = vP, h_2^* = H_2\big(\text{ID}^*, m^*, T^*\big).$$

Search the $H_2^{\text{list}}$ for $H_2(\text{ID}^*, m^*, T^*) = h_{2\lambda}P$. Clearly, $\mathcal{B}$ can transform the above equation into

$$\hat{e}\big(U^*, P\big) = \hat{e}(uP, vP)\hat{e}\big(T^*, h_{2\lambda}P\big).$$

Then, it is easy for $\mathcal{B}$ to obtain the CDH solution

$$uvP = U^* - h_{2\lambda} \cdot T^*.$$

*1) Analysis:* It is easy for us to obtain the advantage for $\mathcal{B}$ in solving the CDH problem

$$\epsilon' \geq \frac{1}{d_1}\epsilon$$

within time

$$t' \leq t + \big(d_1 + d_2 + d_{key} + 4d_s\big) \cdot \tau_{\text{sca}}. \qquad \blacksquare$$

*Theorem 2:* In the above aggregation signature scheme, suppose $H$ is a collision resistent hash function, we can prove that the aggregate signature is valid if and only if every individual signature used in the aggregation is valid.

*Proof:* If the aggregate signature $\sigma$ is valid, then the following equation holds:

$$\hat{e}(U, P) = \Pi_{i=1}^{n}\hat{e}(P_0, Q_i)^{r'}\hat{e}(T_i, h_i)^{r'}$$

where

$$\begin{aligned}r' &= H\big(\hat{e}(P_0, Q_1)^y\hat{e}(T_1, h_1)^y, \ldots, \hat{e}(P_0, Q_n)^y\hat{e}(T_n, h_n)^y\big)\\ &= H\big(\hat{e}(U_1, \text{PK}_{\text{center}}), \ldots, \hat{e}(U_n, \text{PK}_{\text{center}})\big)\\ &= r.\end{aligned}$$

TABLE I
DEFINITION OF NOTATIONS IN SECTION VII

| Notation | Definition |
|---|---|
| $agg$ | aggregation scheme |
| $un\text{-}agg$ | un-aggregation scheme |
| $\lvert M\rvert$ | the overall length of $\{m_1, m_2, \ldots, m_n\}$ |
| $\lvert M'\rvert$ | the overall length of $\{m_1, m_2, \ldots, m_{n-1}\}$ |
| $\lvert ID\rvert$ | the overall length of $\{ID_1, ID_2, \ldots, ID_n\}$ |
| $\lvert ID'\rvert$ | the overall length of $\{ID_1, ID_2, \ldots, ID_{n-1}\}$ |
| $M_1$ | the computation cost of a scalar multiplication calculation in $G_1$ |
| $M_2$ | the computation cost of a multiplication calculation in $G_2$ |
| $exp$ | the computation cost of an exponentiation operation in $G_1$ |
| $Exp$ | the computation cost of an exponentiation operation in $G_2$ |
| $Pairing$ | the computation cost of a pairing operation in $G_2$ |

The hash function $H$'s collision resistance implies that

$$\hat{e}(U_i, \mathrm{PK}_{\mathrm{center}}) = \hat{e}(P_0, Q_i)^y \cdot \hat{e}(T_i, h_i)^y, \qquad i = 1, \ldots, n.$$

Then we can obtain

$$\hat{e}(U_i, P) = \hat{e}(P_0, Q_i) \cdot \hat{e}(T_i, h_i), \qquad i = 1, \ldots, n.$$

This illustrates that every individual signature $\sigma_i = (U_i, T_i, \mathrm{ID}_i, m_i)$ is valid.

More over, if each individual signature used to generate the aggregate signature is valid, then we have

$$\hat{e}\big(U_j, P\big) = \hat{e}\big(P_0, Q_j\big) \cdot \hat{e}\big(T_j, h_j\big), \qquad j = 1, \ldots, n.$$

Therefore

$$\hat{e}\big(U_j, \mathrm{PK}_{\mathrm{center}}\big) = \hat{e}\big(P_0, Q_j\big)^y \cdot \hat{e}\big(T_j, h_j\big)^y, \qquad j = 1, \ldots, n$$

and

$$\begin{aligned} r &= H\big(\hat{e}(U_1, \mathrm{PK}_{\mathrm{center}}), \ldots, \hat{e}(U_n, \mathrm{PK}_{\mathrm{center}})\big) \\ &= H\big(\hat{e}(P_0, Q_1)^y \hat{e}(T_1, h_1)^y, \ldots, \hat{e}(P_0, Q_n)^y \hat{e}(T_n, h_n)^y\big) \\ &= r'. \end{aligned}$$

Then we have

$$\begin{aligned} \hat{e}(U, P) &= \hat{e}\left(r \cdot \sum_{i=1}^{n} U_i, P\right) \\ &= \Pi_{i=1}^{n} \hat{e}(U_i, P)^r \\ &= \Pi_{i=1}^{n} \hat{e}(P_0, Q_i)^r \hat{e}(T_i, h_i)^r \\ &= \Pi_{i=1}^{n} \hat{e}(P_0, Q_i)^{r'} \hat{e}(T_i, h_i)^{r'}. \end{aligned}$$

This indicates that the resulting aggregate signature $\sigma$ is valid.

Furthermore

$$U = r \cdot \sum_{i=1}^{n} U_i$$

can ensure that the designated verifier (data center) cannot forge the aggregate signature, since it cannot gain the $U_i$, $i = 1, \ldots, n$. ■

The above analysis shows that an aggregate signature is valid if and only if every individual signature used in the aggregation algorithm is valid.

*2) Observation:* Through the above analysis of two theorems, we are able to draw a conclusion that our IBAS scheme for WSNs is secure and efficient. It can ensure the integrity of the data and the identity of the sender, can compress multiple signatures signed by sensor nodes into a short one, and can reduce the communication and storage cost. So it has a certain practical value in data aggregation for WSNs.

## VII. PERFORMANCE ANALYSIS

In this section, we evaluate the performance of our IBAS scheme. We give the description of some notations to be used in this section in Table I.

### *A. Comparison of Un-Aggregation and Aggregation Schemes*

We give the performance comparison of two versions of un-aggregation and aggregation schemes in this section, and un-agg and agg denote the un-aggregation and aggregation schemes, respectively. We first review the abilities of each component in our scheme. Sensor node has limited resources in terms of computation, memory, and battery power, aggregator has a certain ability to calculation and communication range and it works as a special sensor node, and data center has a strong computing power and storage space. So, our scheme's objectives are trying to reduce the communication cost and storage cost of aggregator and sensor node. Without loss of generality, we assume the aggregator's identity is $\mathrm{ID}_n$ in a cluster which has $n$ sensor nodes $\{\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_n\}$. The performance in terms of communication and computation cost is shown as follows.

*1) Communication Cost:* The comparison of communication cost (Table II) indicates that the aggregate scheme can reduce $(n-1)|G_1|$ transmission in one data aggregation process, simultaneously, can reduce $(n-1)|G_1|$ storage cost. Therefore, our scheme is an efficient data aggregation method for the WSNs.

*2) Computation Cost:* Let Pairing, $M_1, M_2$, and Exp be the computation cost of a pairing operation in $G_2$, a scalar multiplication calculation in $G_1$, a multiplication calculation in $G_2$, and an exponentiation operation in $G_2$, respectively. Notice that the verification equation

$$\hat{e}(U_i, P) = \hat{e}(P_0, Q_i)\hat{e}(T_i, h_i)$$

TABLE II
PERFORMANCE COMPARISON OF COMMUNICATION COST

| | *un-agg* | *agg* |
|---|---|---|
| Sensor node→Aggregator | $2(n-1)\cdot\lvert G_1\rvert+\lvert M'\rvert+\lvert ID'\rvert$ | $2(n-1)\cdot\lvert G_1\rvert+\lvert M'\rvert+\lvert ID'\rvert$ |
| Aggregator → Data center | $2n\cdot\lvert G_1\rvert+\lvert M\rvert+\lvert ID\rvert$ | $(n+1)\cdot\lvert G_1\rvert+\lvert M\rvert+\lvert ID\rvert$ |

TABLE III
PERFORMANCE COMPARISON OF COMPUTATION COST

| | *un-agg* | *agg* |
|---|---|---|
| Each sensor node | $2M_1$ | $2M_1$ |
| Aggregator | $0$ | $n\cdot Pairing+M_1$ |
| Data center (Verification) | $2n\cdot Pairing+n\cdot M_2$ | $(n+1)\cdot Pairing+(n+1)\cdot Exp+(2n+1)\cdot M_2$ |

TABLE IV
EFFICIENCY COMPARISON OF SOME PAIRING-BASED IBAS SCHEMES

| Scheme | | Xu et al. [34] | Gentry and Ramzan [35] | Herranz [36] | IBAS-2 in Selvi et al. [37] | Our scheme |
|---|---|---|---|---|---|---|
| Signing for each sensor node | $exp$ | 0 | 0 | 1 | 0 | 0 |
| | $M_1$ | 2 | 3 | 0 | 3 | 2 |
| AggVerification | $M_1$ | 0 | $n$ | 0 | $n$ | 0 |
| | $M_2$ | 0 | 0 | 0 | 0 | $2n+1$ |
| | $exp$ | 0 | 0 | $n$ | 0 | 0 |
| | $Exp$ | 0 | 0 | 0 | 0 | $n+1$ |
| | $Pairing$ | $n+2$ | 3 | $n$ | $n+2$ | $n+1$ |
| Coalition attack resistance | | No | No | No | No | Yes |

and the AggVerification equation

$$\begin{aligned}\hat{e}(U,P) &= \Pi_{i=1}^{n}\hat{e}(P_0,Q_i)^r\hat{e}(T_i,h_i)^r\\ &= \hat{e}\left(P_0,\sum_{i=1}^{n}Q_i\right)^r\Pi_{i=1}^{n}\big(\hat{e}(T_i,h_i)\big)^r\\ &= \left(\hat{e}\left(P_0,\sum_{i=1}^{n}Q_i\right)\cdot\left(\Pi_{i=1}^{n}\hat{e}(T_i,h_i)\right)\right)^r\end{aligned}$$

here, $\hat{e}(P_0,Q_i)$ $(i=1,\ldots,n)$ and $\hat{e}(P_0,\sum_{i=1}^{n}Q_i)$ can be precomputed. The comparison of computation cost (Table III) indicates that the aggregate scheme needs more computation cost, such as more Pairing $+M_1+(n+1)M_2+(n+1)$Exp in one data aggregation process. The experimental results of [50] show that a pairing operation cost is far more than others, in addition, data center has a strong computing power and aggregator has a certain computing ability. So our scheme is feasible because it is able to reduce $(n-1)|G_1|$ communication and storage cost during one data aggregation process.

### *B. Efficiency Comparison*

In this section, we give the efficiency comparison of our CLAS scheme with some existing pairing-based schemes (Table IV).

Our IBAS scheme and Xu *et al.*'s scheme [34] just achieve partial aggregation, then require linear number of pairings, and ours is needed more pairings in aggregation verification process. Gentry and Ramzan [35] had constant number of pairing operations during the aggregation verification, but, their scheme has some security weaknesses which have been reported in [37]. Selvi *et al.* [37] had a trivial weakness which is alike to the scheme of [35]. And the signature scheme in [36] is deterministic, that is to say, the signature generated by a user on a message remains the same.

## VIII. CONCLUSION

Due to the limited resources of sensor nodes in terms of computation, memory, and battery power, secure and energy-save data aggregation methods should be designed in WSNs to reduce the energy cost of data collection, data processing, and data transmission. In this paper, we present an IBAS scheme for WSNs, which can compress many signatures generated by sensor nodes into a short one, i.e., it can reduce the communication and storage cost. Moreover, we have proved that our IBAS scheme is secure in random oracle model based on the CDH assumption, and we also have proved that our aggregate signature can resist coalition attacks, that is to say the aggregate signature is valid if and only if every single signature used in the aggregation is valid. In our future work, we will focus on designing more efficient data aggregation schemes.

## REFERENCES

[1] I. Paik, T. Tanaka, H. Ohashi, and W. Chen, "Big data infrastructure for active situation awareness on social network services," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Santa Clara, CA, USA, 2013, pp. 411–412.

[2] E. Hargittai, "Is bigger always better? Potential biases of big data derived from social network sites," *Ann. Amer. Acad. Polit. Soc. Sci.*, vol. 659, no. 1, pp. 63–76, 2015.

[3] Z. Fu, X. Sun, Q. Liu, L. Zhou, and J. Shu, "Achieving efficient cloud search services: Multi-keyword ranked search over encrypted cloud data supporting parallel computing," *IEICE Trans. Commun.*, vol. E98-B, no. 1, pp. 190–200, Jan. 2015.

[4] I. A. T. Hashem *et al.*, "The rise of 'big data' on cloud computing: Review and open research issues," *Inf. Syst.*, vol. 47, pp. 98–115, Jan. 2015.

[5] H. Li *et al.*, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2015.2406704.

[6] H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: When QoE meets QoP," *IEEE Wireless Commun.* vol. 22, no. 4, pp. 74–80, Aug. 2015.

[7] X. Liu, B. Qin, R. Deng, and Y. Li, "An efficient privacy-preserving outsourced computation over public data," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2015.2511008.

[8] X. Liu, R. Choo, R. Deng, R. Lu, and J. Weng, "Efficient and privacy-preserving outsourced calculation of rational numbers," *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2016.2536601.

[9] H. Li *et al.*, "EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 8, pp. 2053–2064, Aug. 2014.

[10] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An efficient Merkle-tree-based authentication scheme for smart grid," *IEEE Syst. J.*, vol. 8, no. 2, pp. 655–663, Jun. 2014.

[11] C. L. P. Chen and C.-Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on big data," *Inf. Sci.*, vol. 275, no. 11, pp. 314–347, 2014.

[12] D. Takaishi, H. Nishiyama, N. Kato, and R. Miura, "Toward energy efficient big data gathering in densely distributed sensor networks," *IEEE Trans. Emerg. Topics Comput.*, vol. 2, no. 3, pp. 388–397, Sep. 2014.

[13] M. M. E. A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10, pp. 1805–1818, Oct. 2012.

[14] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[15] J. Yick, B. Mukherjee, and D. Ghosal, "Analysis of a prediction-based mobility adaptive tracking algorithm," in *Proc. IEEE 2nd Int. Conf. Broadband Netw.*, Boston, MA, USA, 2005, pp. 753–760.

[16] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring," in *Proc. WSNA*, Atlanta, GA, USA, Sep. 2002, pp. 88–97.

[17] X. Lin, R. Lu, X. Shen, Y. Nemoto, and N. Kato, "SAGE: A strong privacy-preserving scheme against global eavesdropping for eHealth systems," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 4, pp. 365–378, May 2009.

[18] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013.

[19] N. Xu *et al.*, "A wireless sensor network for structural monitoring," in *Proc. ACM Conf. Embedded Netw. Sensor Syst.*, Baltimore, MD, USA, Nov. 2004, pp. 13–24.

[20] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Comput. Netw.*, vol. 52, no. 12, pp. 2292–2330, 2008.

[21] N. Pereira, R. Gomes, B. Andersson, and E. Tovar, "Efficient aggregate computations in large-scale dense WSN," in *Proc. 15th IEEE Real Time Embedded Technol. Appl. Symp. (RTAS)*, San Francisco, CA, USA, 2009, pp. 317–326.

[22] X. Liu, H. Zhu, J. Ma, Q. Li, and J. Xiong, "Efficient attribute based sequential aggregate signature for wireless sensor networks," *Int. J. Sensor Netw.*, vol. 16, no. 3, pp. 172–184, 2014.

[23] Y. Zhang, L. Sun, H. Song, and X. Cao, "Ubiquitous WSN for healthcare: Recent advances and future prospects," *IEEE Internet Things J.*, vol. 1, no. 4, pp. 311–318, Aug. 2014.

[24] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha, "Secure data aggregation technique for wireless sensor networks in the presence of collusion attacks," *IEEE Trans. Depend. Secure Comput.*, vol. 12, no. 1, pp. 98–110, Jan./Feb. 2015.

[25] R. C. A. Alves, L. B. Gabriel, B. T. de Oliveira, C. B. Margi, and F. C. L. dos Santos, "Assisting physical (hydro) therapy with wireless sensors networks," *IEEE Internet Things J.*, vol. 2, no. 2, pp. 113–120, Apr. 2015.

[26] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO*, vol. 196. Santa Barbara, CA, USA, 1984, pp. 47–53.

[27] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in *Proc. Eurocrypt*, Warsaw, Poland, 2003, pp. 416–432.

[28] S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure border gateway protocol," *IEEE J. Sel. Areas Commun.*, vol. 18, no. 4, pp. 582–592, Apr. 2000.

[29] J.-L. Koning and D. Dubois, "Suitable properties for any electronic voting system," *Artif. Intell. Law*, vol. 14, no. 4, pp. 251–260, 2006.

[30] A. Lysyanskaya, S. Micali, L. Reyzin, and H. Shacham, "Sequential aggregate signatures from trapdoor permutations," in *Proc. EUROCRYPT*, vol. 3027. Interlaken, Switzerland, 2004, pp. 74–90.

[31] A. Boldyreva, C. Gentry, A. O'Neill, and D. H. Yum, "Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing," in *Proc. ACM Conf. Comput. Commun. Security (CCS)*, Whistler, BC, Canada, 2007, pp. 276–285.

[32] J. H. Ahn, M. Green, and S. Hohenberger, "Synchronized aggregate signatures: New definitions, constructions and applications," in *Proc. ACM Comput. Commun. Security (CCS)*, Chicago, IL, USA, 2010, pp. 473–484.

[33] Z. Shao, "Enhanced aggregate signatures from pairings," in *Proc. CISC*, vol. 3822. Beijing, China, 2005, pp. 140–149.

[34] J. Xu, Z. Zhang, and D. Feng, "ID-based aggregate signatures from bilinear pairings," in *Proc. 4th Int. Conf. CANS*, vol. 3810. Xiamen, China, 2005, pp. 110–119.

[35] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," in *Proc. Public Key Cryptography*, vol. 3958. New York, NY, USA, 2006, pp. 257–273.

[36] J. Herranz, "Deterministic identity-based signatures for partial aggregation," *Comput. J.*, vol. 49, no. 3, pp. 322–330, 2006.

[37] S. S. D. Selvi, S. S. Vivek, J. Shriram, and C. P. Rangan, "Identity based partial aggregate signature scheme without pairing," in *Proc. 35th IEEE. Sarnoff Symp. (SARNOFF)*, Newark, NJ, USA, 2012, pp. 1–6.

[38] J. Li, K. Kim, F. Zhang, and X. Chen, "Aggregate proxy signature and verifiably encrypted proxy signature," in *Proc. Int. Conf. Provable Security*, vol. 4784. Wollongong, N.S.W., Australia, 2007, pp. 208–217.

[39] Y. Wen, J. Ma, and H. Huang, "An aggregate signature scheme with specified verifier," *Chin. J. Electron.*, vol. 20, no. 2, pp. 333–336, 2011.

[40] Z. Gong, Y. Long, X. Hong, and K. Chen, "Two certificateless aggregate signatures from bilinear maps," in *Proc. IEEE SNPD*, Qingdao, China, 2007, pp. 188–193.

[41] L. Zhang, B. Qin, Q. Wu, and F. Zhang, "Efficient many-to-one authentication with certificateless aggregate signatures," *Comput. Netw.*, vol. 54, no. 14, pp. 2482–2491, 2010.

[42] H. Xiong, Z. Guan, Z. Chen, and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," *Inf. Sci.*, vol. 219, pp. 225–235, Jan. 2013.

[43] F. Zhang, L. Shen, and G. Wu, "Notes on the security of certificateless aggregate signature schemes," *Inf. Sci.*, vol. 287, pp. 32–37, Dec. 2014.

[44] S.-J. Horng *et al.*, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Inf. Sci.*, vol. 317, pp. 48–66, Oct. 2015.

[45] D. He, M. Tian, and J. Chen, "Insecurity of an efficient certificateless aggregate signature with constant pairing computations," *Inf. Sci.*, vol. 268, pp. 458–462, Jun. 2014.

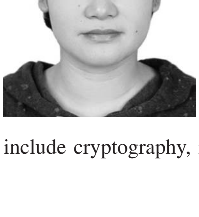
[46] K.-A. Shim, "On the security of a certificateless aggregate signature scheme," *IEEE Commun. Lett.*, vol. 15, no. 10, pp. 1136–1138, Oct. 2011.

[47] N. Q. Viet and W. Ogata, "Certificateless aggregate signature schemes with improved security," *IEICE Trans. Fundamentals Electron. Commun. Comput. Sci.*, vol. 98, no. 1, pp. 92–99, Jan. 2015.

[48] D. Xing, Z. Cao, and X. Dong, "Identity based signature scheme based on cubic residues," *Sci. China Inf. Sci.*, vol. 54, no. 10, pp. 2001–2012, 2011.

[49] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," in *Proc. Symp. Cryptography Inf. Security,* 2000, pp. 26–28.

[50] J. Shao, R. Lu, and X. Lin, "Fine-grained data sharing in cloud computing for mobile devices," in *Proc. IEEE Conf. Comput. Commun. (INFOCOM)*, Hong Kong, 2015, pp. 2677–2685.

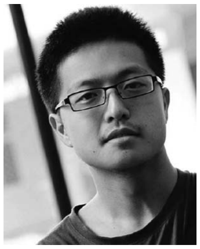


**Limin Shen** received the B.S. and M.S. degrees in mathematics from Wuhan University, Wuhan, China, in 2001 and 2004, respectively, and is currently working toward the Ph.D. degree at the School of Computer Science and Technology, Xidian University, Xi'an, China.

She is a Lecturer with the School of Computer Science and Technology, Jiangsu Engineering Research Center of Information Security and Privacy Protection Technology, Nanjing Normal University, Nanjing, China. Her current research interests include cryptography, information security, and wireless sensor networks.

**Jianfeng Ma** (M'96) received the B.S. degree in mathematics from Shaanxi Normal University, Xi'an, China, in 1985, and the M.E. and Ph.D. degrees in computer software and communications engineering from Xidian University, Xi'an, China, in 1988 and 1995, respectively.

From 1999 to 2001, he was a Research Fellow with Nanyang Technological University, Singapore. He is currently a Professor with the School of Computer Science, Xidian University. His current research interests include distributed systems, computer networks, and information and network security.



**Ximeng Liu** (S'13–M'16) received the B.S. degree in electronic engineering and Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2010 and 2015, respectively.

He was a Research Assistant with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from 2013 to 2014. He is currently a Research Fellow with the School of Information System, Singapore Management University, Singapore. His current research interests include cloud security, applied cryptography, and big data security.

**Fushan Wei** received the M.S. and Ph.D. degrees in applied mathematics from the Zhengzhou Information Science and Technology Institute, Zhengzhou, China, in 2008 and 2011, respectively.

He is currently a Lecturer with the Department of Information Research, Zhengzhou Information Science and Technology Institute. His current research interests include cryptography and information security.

**Meixia Miao** is currently working toward the Ph.D. degree at the School of Computer Science and Technology, Xidian University, Xi'an, China.

Her current research interests include cloud computing and e-commence security, cryptography, financial cryptography, and cloud computing security.