Received July 29, 2019, accepted August 10, 2019, date of publication August 15, 2019, date of current version August 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2935513

Lightweight and Privacy-Preserving Data Aggregation for Mobile Multimedia Security

SUGANG MA[1,2], TIANTIAN ZHANG[3], AXIN WU[4], AND XIANGMO ZHAO[1]

[1]School of Information Engineering, Chang'an University, Xi'an 710064, China
[2]School of Computer Science and Technology, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[3]National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[4]School of Cybersecurity, Jinan University, Guangzhou 510632, China

Corresponding author: Axin Wu (waxinsec@163.com)

This work was supported in part by the Key Research and Development Program of Shaanxi under Grant 2019KW-053, in part by the Sichuan Science and Technology Program under Grant 2017GZDZX0002, and in part by the New Star Team of Xi'an University of Posts and Telecommunications under Grant 2016-02.

ABSTRACT With the continuous development of multimedia technology, a growing number of multimedia applications have emerged. The demand for multimedia services continues to grow. But the development of multimedia services is still hampered by inherent security. Privacy and integrity of multimedia data are two key issues for implementing mobile multimedia security. At present, most data privacy-preserving solutions have a trusted third party, which may become the bottleneck of the system. And, the computational efficiency of the client is inefficient. In this paper, a lightweight and privacy-preserving data aggregation for mobile multimedia is proposed. In the proposed scheme, the terminal calculation is lightweight and there is no trusted third party in our scheme. Besides, multimedia big data and personal multimedia data are balanced by creating virtual aggregation areas and the system performance is improved by adopting batch verification in our scheme. Security analysis shows that the presented scheme can guarantee the privacy, confidentiality and integrity of the personal multimedia data. The performance analysis indicates the proposed scheme is lightweight.

INDEX TERMS Mobile multimedia, security, data aggregation, privacy.

I. INTRODUCTION

With the rapid development of information technology, multimedia equipment is developing towards low power consumption and intelligent direction to support various information services [1]. For example, Facebook shares 685,000 content and Google carries out 2,000,000 video queries [2]. Multimedia data accounts for two-thirds of Internet traffic [3], [4]. The rapid development of data traffic not only leads to an increase in communication requirements, but also leads to an increase in computing requirements, which will consume a lot of resources [5], [6]. Multimedia applications, such as multimedia center online video, live broadcast, etc., are widely used in people's daily lives.

It is necessary to analyze the data of mobile multimedia to better serve users. With the timely utility of these mobile multimedia big data, the data center can make scientific decisions and improve the quality of service. Besides, these mobile multimedia big data can be used for major enterprise's decision-making and business activities [7]. However, personal multimedia data is related to personal privacy. For example, users' hobbies and habits can be inferred from personal multimedia data. If this information is mastered by malicious users, which may cause serious losses to the owner of the data. One of the problems to be solved in multimedia to balance the multimedia big data's utility and personal multimedia data. In the IoT and smart grid scenarios, to solve personal data privacy issues, many privacy protection data aggregation schemes [8]–[11] have been proposed. In these schemes, there are two basic requirements. On the one hand, the data center can get total data. On the other hand, personal data is hidden.

Homomorphic encryption (HE) [12], [13] is widely employed in the data aggregation owing to the nature of HE. However, it is imperfect to rely solely on HE [14] for data security. HE and authentication technology need to be combined. Only in this way can the confidentiality, authentication and integrity of data be guaranteed. Many data aggregation

The associate editor coordinating the review of this article and approving it for publication was Dapeng Wu.

schemes [9], [11] are based on trusted third parties, which becomes a bottleneck in the system. Besides, they can not resist the attack of internal enemies. In addition, multimedia involves a large number of multimedia devices. If the gateway sends a single data to DC, the privacy of personal multimedia data will not be protected. Certificate-based system [15] will have the problem of key escrow. And, the calculating costs of the mobile multimedia device should be also lightweight.

A. RELATED WORK

User's multimedia data is related to user's privacy, under certain circumstances personal multimedia data is obtained by malicious users which may cause serious economic consequences for data owners. Many efforts are also working to address privacy issues [16]–[18]. Zhang *et al.* proposed two fair payment schemes for outsourced data security based on the Bitcoin blockchain [19] and the Ethereum blockchain [20]. In the multimedia scenario, some data aggregation schemes [21]–[23] are proposed. Sun *et al.* [21] presented a data aggregation scheme with a trust mechanism to enhance data credibility. Wu *et al.* [22] presented a privacy protection multimedia big data aggregation scheme. Qiu *et al.* [23] presented a k-anonymous privacy-preserving scheme and corresponding data transmission strategy for participatory cognitive multimedia networks by integrating data encoding technology and message transmission strategy. However, this scheme may not be enough to protect privacy, because mobile users or customers can be re-identified by combining different types of information [24]. Zhang *et al.* [25] proposed an attribute-based encryption scheme which supports hidden access policies and can be used to realize privacy aware access control. Besides, Zhang *et al.* [26] proposed a handover authentication scheme which is suitable for all the mobile application scenarios in 5G. The security of the scheme is formally proved.

Besides, some data aggregation schemes [27]–[29] based on the Paillier encryption are proposed to protect data privacy. The gateway will receive the data sent by the user, and the data will be aggregated and sent to data center. However, in these scenarios, there is the assumption that the gateway is trusted. If the gateway sends a single data to data center, the privacy of data will not be protected. Besides, data aggregation schemes based on the Paillier encryption is inefficient.

Liu *et al.* [30] proposed a practical privacy preservation data aggregation scheme. However, there are problems in the scheme where certificate management is insufficient and bilinearity leads to inefficiency. Cui *et al.* [31] proposed an efficient certificateless aggregate signature without pairings. The scheme adopts a certificateless batch verification, which greatly improves the efficiency. Inspired by this scheme, due to the large amount of multimedia data, we applyed the batch verification to the authentication of multimedia data, which can greatly improve the authentication efficiency.

B. OUR CONTRIBUTIONS

A lightweight data aggregation scheme is presented. The main contributions of our scheme can be summarized as follows:

- Firstly, the utility of multimedia big data and personal multimedia data are balanced by creating virtual aggregation areas.
- Secondly, the certificateless batch verification technology is used to avoid the key escrow problem of a large number of multimedia terminals.
- Thirdly, the proposed scheme does not involve time-consuming bilinear pairs, which makes the calculation of multimedia terminals and data collection units lightweight. And our scheme can resist dishonest gateways.

C. ORGANIZATION

The rest of the paper is structured as follows: In section II, the preliminaries are introduced. Next, the model and design goals of our scheme are presented in section III. The concrete scheme is introduced in section IV. Correctness analysis and security analysis are introduced in section V. After that, the performance of the scheme is analyzed in section VI. Finally, in section VII, we make a conclusion.

II. PRELIMINARIES

We introduce the description of the symbols, lifted EC-ElGamal cryptosystem and certificateless signature scheme in this section.

A. NOTATIONS

We describe the symbols involved in lifted EC-ElGamal cryptosystem, certificateless signature and our scheme as shown in Table 1.

TABLE 1. Symbols used and description.

Symbol	Description
E	An elliptic curve
G	A group of prime order q
P	A generator of the group G
H_1, H_2, H_3	Three anti-collision hash functions
GK	The group public key
psk_{VID_i}	Partial secret key of V_i
psk_{ID_i}	Partial secret key of MME_i
psk'_{ID_i}	Partial secret key of DCU
(U_{pk}, U_{sk})	The public-private key pair of V_i
(MME_{pk_i}, MME_{sk_i})	The public-private key pair of MME_i
(DCU_{pk_i}, DCU_{sk_i})	The public-private key pair of DCU

B. LIFTED EC-ELGAMAL CRYPTOSYSTEM

In this part, we review the Lifted EC-ElGamal cryptosystem [32], [33], which is a HE algorithm.

- **Key generation:** The algorithm is based on the elliptic curve group $E(F_p)$ of the prime order q with a generator P. Its private and public keys are $x \in Z_q^*$ and

$Y = x \cdot P$, respectively. Besides, the public parameters of the system are $(E(F_p), q, P)$.

- **Encryption:** Generate the ciphertext $(C^a, C^b) = (r \cdot P, m \cdot P + r \cdot Y)$ about message $m \in \{0, 1, ..., K\}$, where $r \in Z_q^*$ is selected randomly and $K \ll q$.
- Decryption: The message m can be obtained from the ciphertext (C^a, C^b) by the equation $m = Dec(C^a, C^b) = log_P(C^b - xC^a)$. Owing to $K \ll q$, the time complexity of decryption is $O(\sqrt{K})$ by the Pollard's lambda algorithm [34].
- **Distributed decryption:** Suppose there are n users in a group. Private and public keys of the user U_i, $(i = 1, ..., n)$ are x_i and $Y_i = x_i P$, respectively. Let $GK = \sum_{i=1}^{n} Y_i$. Then, the ciphertext $(C^a, C^b) = (r \cdot P, m \cdot P + r \cdot GK)$ of the data m can be generated using GK. When decrypting, the decryption operator needs to interact with user U_i [34]. The decryption operator sends C^a to U_i, $(i = 1, ..., n)$, and then U_i returns D_i to the decryption operator, where $D_i = x_i C^a$. The decryption operator can recover the message m using the equation $m = log_P(C^b - \sum_{i=1}^{n} D_i)$. Distributed decryption can also be done in a subset of users within a group [30].

C. CERTIFICATELESS SIGNATURE SCHEME

In the scheme [31], aggregation and batch validation of data from n users can be realized simultaneously. In our scheme, we mainly employ the batch authentication of the scheme [31].

- **Key generation:** Cui *et al.*'s scheme [31] is based on the elliptic curve $E(F_q)$ of prime order q. Let $P_{pub} = \alpha P$ and $T_{pub} = \beta P$ be the public keys of the key generation center (KGC) and the trace authority (TRA), respectively. The public system parameters are $Params = (P, p, q, E, G, H_1, H_2, P_{pub}, T_{pub})$, where $H_1 : \{0, 1\}^* \rightarrow Z_q^*, H_2 : \{0, 1\}^* \rightarrow Z_q^*$. The private keys of KGC and TRA are $\alpha \in Z_q^*$ and $\beta \in Z_q^*$, respectively. The vehicle V_i can get part of the key $(Q_{VID_i}, psk_{VID_i}) = (d_i P, d_i + H_1(VID_i, Q_{VID_i}) \times \alpha)$ from KGC and TRA, where $d_i \in Z_q^*$. V_i chooses a random number $x_{VID_i} \in Z_q^*$ and calculates $vpk_{VID_i} = x_{VID_i} P$. Let $vsk_{VID_i} = x_{VID_i}$. Finally, V_i can get the public-private key pairs $(U_{sk}, U_{pk}) = ((psk_{VID_i}, vsk_{VID_i}), (Q_{VID_i}, vpk_{VID_i}))$.
- **Signature:** V_i chooses a random number $y_i \in Z_q^*$, calculates $R_i = y_i P$, $h_i = H_2(M_i, VID_i, vpk_{VID_i}, R_i, t_i)$ and $S_i = h_i y_i + psk_{VID_i} \mod q$, where t_i is the latest timestamp. The signature of the message M_i is $\sigma_i = (R_i, S_i)$. Finally, the message $(VID_i, U_{pk}, M_i, t_i, \sigma_i)$ is sent to the Road Site Units(RSU).
- **Individual verification:** When the data $(VID_i, U_{pk}, M_i, t_i, \sigma_i)$ from V_i is received, RSU verifies the signature by the following equation $S_i P = h_i R_i + Q_{VID_i} + h_{i.0} P_{pub}$, where $h_{i,0} = H_1(VID_i, Q_{VID_i})$ and $h_i = H_2(M_i, VID_i, vpk_{VID_i}, R_i, t_i)$. If the validation passes, the data is received.
- **Batch verification:** When the data $(VID_i, vpk_i, M_i, t_i, \sigma_i)$ from V_i is received, where $i \in [1, ..., n]$. RSU can perform batch validation by the following equation $(\sum_{i=1}^{n} v_i S_i)P = (\sum_{i=1}^{n} v_i h_i R_i) + (\sum_{i=1}^{n} v_i Q_{VID_i}) + (\sum_{i=1}^{n} v_i h_{i,0}) P_{pub}$, where $h_{i,0} = H_1(VID_i, Q_{VID_i})$ and $h_i = H_2(M_i, VID_i, vpk_{VID_i}, R_i, t_i)$. $v = (v_1, ..., v_n)$, where $v_i \in [1, 2^l]$ is a random small integer. If the validation passes, the data is received.

III. MODEL AND DEFINITION

A. SYSTEM MODEL

In this part, the system model of our scheme is introduced. The system model involves three entities: mobile multimedia entity, data collection unit and data center as shown in Figure 1.

- Mobile multimedia entity (MME): MMEs are the terminal entities of the system. MMEs are employed to collect users' mobile multimedia data and report periodically to the Data collection unit(DCU). Each user in the system is equipped with an MME. Therefore, in the paper, users and MMEs are indistinguishable.
- Data collection unit (DCU): DCU is responsible for collecting data from MMEs, aggregating them and sending them to the data center. DCU also forwards data packages between DC and MMEs.
- Data center (DC): DC is responsible for generating blinding factors for MMEs and collecting data from DCU. Through the analysis of massive multimedia data, DC can make reasonable decisions, such as preferences and behavioral habits of user group, in order to better serve users. In addition, the storage capacity of DC is unrestricted.

In the system, The transmitted data includes multimedia data types, data amounts, and other related multimedia data information. In this paper, data flow in the system is bidirectional. Close-range transmission between MMEs and DCU can be connected through wireless networks. Long-distance transmission between DCU and DC can be achieved through a LTE-A network. As a result, DC is able to obtain total users' multimedia data and do not learn personal multimedia data.

B. SECURITY MODEL AND DESIGN GOALS

Data injection attacks, DoS attacks, time synchronization attacks and other physical attacks are very common [35], [36]. In order to resist these attacks, the confidentiality, authentication and integrity of data should be guaranteed. In addition, the privacy of personal multimedia data is also very significant. The adversaries can infer the user's living habits through the user's multimedia data. DC and DCU are considered honest but curious. Both DC and DCU want to obtain the multimedia data of individual users. MMEs are legitimate users, but there will be malicious users pretending to be legitimate users.

- Privacy: The individual multimedia data of users in the system should be protected. Neither DC nor DCU knows the individual multimedia data.
- Authentication: To ensure that the data received is legitimate, the authenticity of the data should be guaran-

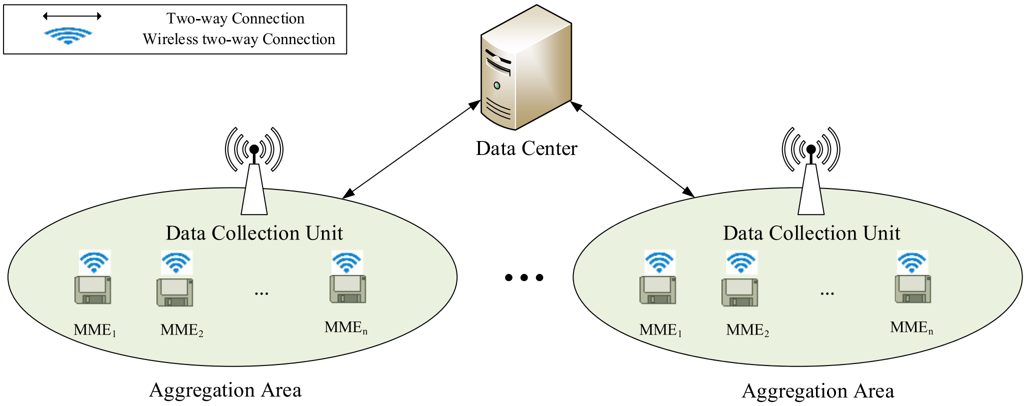


FIGURE 1. The system model.

teed. If a malicious user impersonates a legitimate user, the data should be rejected.

- Integrity: To ensure the correctness of the data during transmission, the completeness of data should be guaranteed. If the data is tampered with, the data should be found.

C. DEFINITION OF ALGORITHMS

In this section, we introduce the definition of algorithms. Our scheme consists of eight algorithms as follows.

- System setup $(1^\lambda) \to ((Y_{DC}, \alpha), PP)$: It takes a security parameter λ as input and generates its public-private key pair (Y_{DC}, α) and public parameters PP.
- Partial private key extraction $(PP) \to (Q_{ID_i}, psk_{ID_i}, Q_{A_i}, A_i, Q'_{ID_i}, psk'_{ID_i})$: It takes public parameters PP as input and generates MME's partial public-private key pair (Q_{ID_i}, psk_{ID_i}), DCU's partial public-private key pair (Q'_{ID_i}, psk'_{ID_i}) and (Q_{A_i}, A_i) which can be used to generate the aggregate area.
- Key generation $(PP) \to (MME_{pk_i}, MME_{sk_i}, DCU_{pk_i}, DCU_{sk_i})$: It takes public parameters PP as input and generates MME's public-private key pair (MME_{pk_i}, MME_{sk_i}) and DCU's public-private key pair (DCU_{pk_i}, DCU_{sk_i}).
- Aggregation area creation $(PP, ID_i, vpk_{ID_i}, Y_{DC}, Q_{A_i}, A_i) \to (GK)$: It takes public parameters PP, the identity ID_i of the MME, the partial public key vpk_{ID_i} of the MME, the public key Y_{DC} of DC and (Q_{A_i}, A_i) which can be used to generate the aggregate area as input. It outputs the group public key (GK) of the aggregation area.
- Ciphertext generation $(PP, m_i) \to (C_i^a, C_i^b, \sigma_i, t)$: It takes public parameters PP and data m_i as input and outputs the ciphertext (C_i^a, C_i^b) of the data m_i, the signature σ_i of the corresponding ciphertext and the current timestamp t.
- Ciphertext aggregation $(PP, C_i^a, C_i^b, \sigma_i) \to (C^a, C^b, \sigma_{DCU}, t_{DCU})$: It takes public parameters PP, the ciphertext (C_i^a, C_i^b) of the data m_i and the signature σ_i of the corresponding ciphertext as input and outputs the aggregated data (C^a, C^b), the aggregated ciphertext signature σ_{DCU} and the current timestamp t_{DCU}.
- Distributed decryption $(PP, ID_{DCU}, C^a, C^b, \sigma_{DCU}, t_{DCU}) \to (sum)$: It takes public parameters PP, the identity ID_{DCU} of DCU, the aggregated data (C^a, C^b), the aggregated ciphertext signature σ_{DCU} and the cuttent timestamp t_{DCU} as input and generates the total multimedia data sum.
- Track $(PP, C^a, vpk_{ID_i}, D_i) \to pass$ or $fail$: It takes public parameters PP, the aggregated data C^a, the partial public key of the MME and the signature D_i generated by the MME using its private key as input, If the verification is passed, it outputs $pass$, otherwise outputs $fail$.

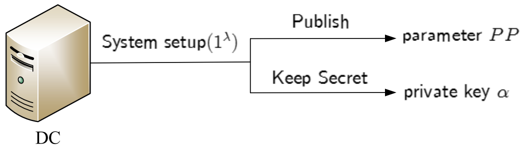


FIGURE 2. The system setup phase.

IV. THE PROPOSED SCHEME

The proposed scheme which is described below includes eight algorithms.

A. SYSTEM SETUP

The setup algorithm which is used to generate the system parameters, is run by DC as shown in Figure 2.

Given a security parameter λ, p and q are two large prime numbers. Then DC instantiates an elliptic curve

$$E : y^2 = x^3 + ax + b \ mod \ p.$$

DC generates a group G of the order q with a point P from the elliptic curve E. Then DC randomly selects $\alpha \in Z_q^*$ and calculates $Y_{DC} = \alpha P$. DC's public-private key pair is (Y_{DC}, α). DC picks random numbers $\pi_1, \pi_2, ..., \pi_n \in Z_q^*$ and calculates $\pi = \sum_{i=1}^n \pi_i$. DC secretly keeps π. There are three anti-collision hash functions $H_1 : \{0,1\}^* \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \rightarrow Z_q^*$, $H_3 : \{0,1\}^* \rightarrow G$.

Finally, DC publishes the system parameters

$$PP = (P, p, q, E, G, H_1, H_2, H_3, Y_{DC}).$$

B. PARTIAL PRIVATE KEY EXTRACTION

The partial private key extraction algorithm which is used to generate the partial private keys of MME and DCU, is run by MME, DC and DCU as shown in Figure 3.

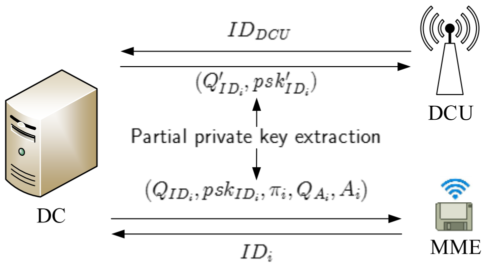

ID_{DCU}
(Q'_{ID_i}, psk'_{ID_i})
DCU
Partial private key extraction
$(Q_{ID_i}, psk_{ID_i}, \pi_i, Q_{A_i}, A_i)$
DC
MME
ID_i

FIGURE 3. The partial private key extraction phase.

MME_i randomly selects $k_i \in Z_q^*$ and then calculates $ID_i = k_i P$. Then ID_i is sent to DC through a secure channel. When DC receives the data from MME_i, it randomly chooses $d_i \in Z_q^*$ and calculates $Q_{ID_i} = d_i P$. Then, the partial secret key of MME_i is

$$psk_{ID_i} = d_i + H_1(ID_i, Q_{ID_i}) \cdot \alpha \ mod \ q.$$

DC chooses randomly $a_i \in Z_q^*$, and then calculates $Q_{A_i} = a_i P$ and $A_i = a_i + H_1(ID_i, vpk_{ID_i}) \cdot \alpha$ mod q. Finally, DC sends $(Q_{ID_i}, psk_{ID_i}, \pi_i, Q_{A_i}, A_i)$ to MME_i through a secure channel.

DCU selects $u_i \in Z_q^*$ and then calculates $ID_{DCU} = u_i P$. Then ID_{DCU} is sent to DC through a secure channel. When DC receives ID_{DCU} from DCU, it randomly selects $d'_i \in Z_q^*$ and calculates $Q'_{ID_i} = d'_i P$. Then, the partial secret key of DCU is

$$psk'_{ID_i} = d'_i + H_1(ID_{DCU}, Q_{ID'_i}) \cdot \alpha \ mod \ q.$$

Finally, DC will send (Q'_{ID_i}, psk'_{ID_i}) to DCU through a secure channel.

C. KEY GENERATION

The key generation algorithm which is used to generate the public-private key pairs of MME and DCU, is run by MME and DCU as shown in Figure 4.

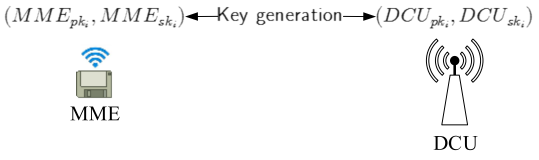


FIGURE 4. The key generation phase.

MME_i selects randomly $x_{ID_i} \in Z_q^*$ and sets $vsk_{ID_i} = x_{ID_i}$, then calculates $vpk_{ID_i} = x_{ID_i} P$. Finally, the public-private key pair of MME_i is

$$(MME_{pk_i}, MME_{sk_i}) = ((Q_{ID_i}, vpk_{ID_i}), (psk_{ID_i}, vsk_{ID_i})).$$

DCU selects randomly $x'_{ID_i} \in Z_q^*$ and sets $vsk'_{ID_i} = x'_{ID_i}$, then calculates $vpk'_{ID_i} = x'_{ID_i} P$. Finally, the public-private key pair of DCU is

$$(DCU_{pk_i}, DCU_{sk_i}) = ((Q'_{ID_i}, vpk'_{ID_i}), (psk'_{ID_i}, vsk'_{ID_i})).$$

D. AGGREGATION AREA CREATION

The aggregation area creation algorithm which is used to form an aggregation area, is run by n MMEs as shown in Figure 5.

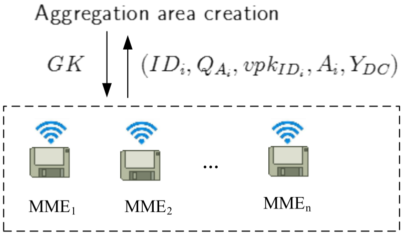

Aggregation area creation
GK
$(ID_i, Q_{A_i}, vpk_{ID_i}, A_i, Y_{DC})$
MME_1
MME_2
...
MME_n

FIGURE 5. The agregation area creation phase.

n MMEs form an aggregation area and generate a group public key of the aggregation area. MMEs form an aggregation area by broadcasting $(ID_i, Q_{A_i}, vpk_{ID_i}, A_i, Y_{DC})$. MME verifies the message sent by other multimedia entities through the following equation

$$\sum_{j=1, j\neq i}^{n} A_j P = \sum_{j=1, j\neq i}^{n} Q_{A_j} + \sum_{j=1, j\neq i}^{n} H_1(ID_j, vpk_{ID_j}) Y_{DC}. \tag{1}$$

Then, the group public key of the aggregated area is

$$GK = \sum_{i=1}^{n} vpk_{ID_i}.$$

E. CIPHERTEXT GENERATION

The ciphertext generation algorithm is run by MME to generate the ciphertext of the data and the corresponding signature as shown in Figure 6.

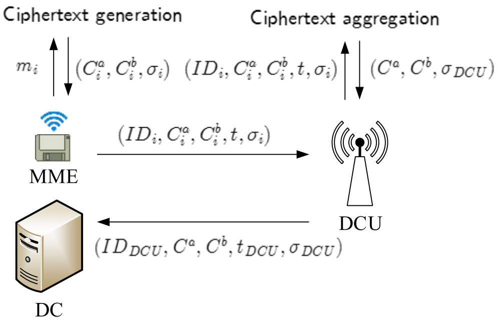

Ciphertext generation
Ciphertext aggregation
m_i
(C_i^a, C_i^b, σ_i)
$(ID_i, C_i^a, C_i^b, t, \sigma_i)$
(C^a, C^b, σ_{DCU})
$(ID_i, C_i^a, C_i^b, t, \sigma_i)$
MME
DCU
$(ID_{DCU}, C^a, C^b, t_{DCU}, \sigma_{DCU})$
DC

FIGURE 6. The ciphertext generation phase and ciphertext aggregation phase.

MME_i encrypts the collected data m_i. MME_i selects a random number $r_i \in Z_q^*$ and calculates the ciphertext

$$(C_i^a, C_i^b) = (r_i P, m_i P + r_i GK + H_3(t) \cdot \pi_i),$$

where t is the current timestamp. Then MME_i chooses a random number $y_i \in Z_q^*$, and calculates

$$\begin{aligned} R_i &= y_i P, \\ h_i &= H_2(C_i^a, C_i^b, ID_i, vpk_{ID_i}, R_i, t), \\ S_i &= h_i y_i + psk_{ID_i} \ mod \ q. \end{aligned}$$

The signature of (C_i^a, C_i^b) is $\sigma_i = (R_i, S_i)$. Finally, MME_i sends the message $(ID_i, C_i^a, C_i^b, t, \sigma_i)$ to DCU.

F. CIPHERTEXT AGGREGATION

The ciphertext aggregation algorithm which is used to generate the aggregated ciphertext and the corresponding signature, is run by DCU as shown in Figure 6.

DCU collects $(ID_i, C_i^a, C_i^b, t, \sigma_i)$ from MME_i, where $i \in [1, ..., n]$. DCU first validates the validity of data by the following equation

$$(\sum_{i=1}^{n} v_i S_i)P = (\sum_{i=1}^{n} v_i h_i R_i) + (\sum_{i=1}^{n} v_i Q_{ID_i}) + (\sum_{i=1}^{n} v_i h_{i,0}) Y_{DC}, \tag{2}$$

where

$$\begin{aligned} h_{i,0} &= H_1(ID_i, Q_{ID_i}), \\ h_i &= H_2(C_i^a, C_i^b, ID_i, vpk_{ID_i}, R_i, t), \\ v &= (v_1, ..., v_n), \end{aligned}$$

where $v_i \in [1, 2^l]$ is a random small integer. DCU aggregates data by the equation

$$\begin{aligned} (C^a, C^b) &= (\sum_{i=1}^{n} C_i^a, \sum_{i=1}^{n} C_i^b) \\ &= (r \cdot P, sum \cdot P + r \cdot GK + H_3(t)\pi), \end{aligned}$$

where $r = \sum_{i=1}^{n} r_i$ and $sum = \sum_{i=1}^{n} m_i$. Next, the aggregated ciphertext is signed by using the secret key of DCU. DCU selects a random number $r_i' \in Z_q^*$, then computes

$$\begin{aligned} R_i' &= r_i' P, \\ h_i' &= H_2(C^a, C^b, ID_{DCU}, vpk_{ID_i}', R_i', t_{DCU}), \\ S_i' &= h_i' r_i' + psk_{ID_i}', \end{aligned}$$

where t_{DCU} is the current timestamp. Then, the aggregated ciphertext signature is $\sigma_{DCU} = (R_i', S_i')$. Finally, the data $(ID_{DCU}, C^a, C^b, t_{DCU}, \sigma_{DCU})$ is sent to DC.

G. DISTRIBUTED DECRYPTION

The distributed decryption algorithm is run by DC to recover the total multimedia data as shown in Figure 7.

When the data $(ID_{DCU}, C^a, C^b, t_{DCU}, \sigma_{DCU})$ from DCU is received, DC verifies the signature by the following equation

$$S_i' P = h_i' R_i' + Q_{ID_i}' + h_{i,0}' Y_{DC}, \tag{3}$$

where

$$\begin{aligned} h_{i,0}' &= H_1(ID_{DCU}, Q_{ID}'), \\ h_i' &= H_2(C^a, C^b, ID_{DCU}, vpk_{ID_i}', R_i', t_{DCU}). \end{aligned}$$

If the validation passes, the data is received.

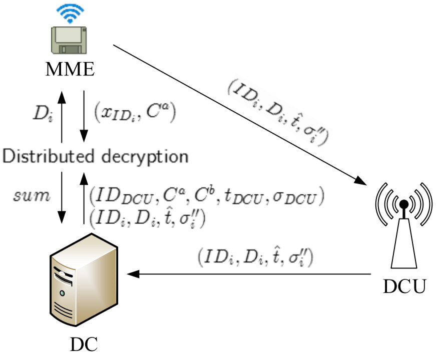

MME
D_i
(x_{ID_i}, C^a)
$(ID_i, D_i, \hat{t}, \sigma_i'')$
Distributed decryption
sum
$(ID_{DCU}, C^a, C^b, t_{DCU}, \sigma_{DCU})$
$(ID_i, D_i, \hat{t}, \sigma_i'')$
$(ID_i, D_i, \hat{t}, \sigma_i'')$
DCU
DC

FIGURE 7. The distributed decryption phase and ciphertext aggregation phase.

MME_i uses its secret key to perform the distributed decryption by the equation $D_i = x_{ID_i} C^a$, and it uses its own private key to sign it. MME_i selects randomly $y_i'' \in Z_q^*$, calculates

$$\begin{aligned} R_i'' &= y_i'' P, \\ h_i'' &= H_2(D_i, ID_i, vpk_{ID_i}, R_i, \hat{t}), \\ S_i'' &= h_i'' y_i'' + psk_{ID_i} \ mod \ q, \end{aligned}$$

where $\hat{t}$ is the current timestamp. The signature of D_i is $\sigma_i'' = (R_i'', S_i'')$.

Then the data $(ID_i, D_i, \hat{t}, \sigma_i'')$ is forwarded to DC by DCU. DC receives the data and then performs batch validation by the equation

$$(\sum_{i=1}^{n} v_i S_i'')P = (\sum_{i=1}^{n} v_i h_i'' R_i'') + (\sum_{i=1}^{n} v_i Q_{ID_i}) + (\sum_{i=1}^{n} v_i h_{i,0}) Y_{DC}, \tag{4}$$

where

$$\begin{aligned} h_{i,0} &= H_1(ID_i, Q_{ID_i}), \\ h_i'' &= H_2(D_i, ID_i, vpk_{ID_i}, R_i, \hat{t}), \\ v &= (v_1, ..., v_n), \end{aligned}$$

where $v_i \in [1, 2^l]$ is a random small integer. If the validation is passed, the total multimedia data from MMEs can be recovered by the equation

$$sum = log_P(C^b - \sum_{i=1}^{n} D_i - H_3(t)\pi).$$

H. TRACK

The track algorithm is run by DC to verify the correctness of data sent by MME during the distributed decryption phase.

If MME_i sends incorrect data during distributed decryption phase, the equation $C^a vpk_{ID_i} = D_i P$ can be used to validate it.

V. ANALYSIS

We analyze our scheme mainly from the following two aspects of this section: correctness and security.

A. CORRECTNESS ANALYSIS

We mainly consider the correctness of our scheme from the following aspects.

MME verifies the message sent by other multimedia entities through Equation 1 in the aggregation area creation phase. The correctness of the equation verified the validity of the message can be shown as follows:

$$\begin{aligned}\sum_{j=1,j\neq i}^{n} A_jP &= \sum_{j=1,j\neq i}^{n} (a_j + H_1(ID_j, vpk_{ID_j})\cdot\alpha)P\\ &= \sum_{j=1,j\neq i}^{n} Q_{A_j} + \sum_{j=1,j\neq i}^{n} H_1(ID_j, vpk_{ID_j})Y_{DC}\end{aligned}$$

In the ciphertext aggregation phase, DCU needs to validate the validity of data from MME_i by Equation 2. The correctness of the equation verified the validity of data can be shown as follows:

$$\begin{aligned}(\sum_{i=1}^{n} v_iS_i)P &= (\sum_{i=1}^{n} v_i(h_iy_i + psk_{ID_i}))P\\ &= \sum_{i=1}^{n}(v_ih_iy_iP + v_ipsk_{ID_i}P)\\ &= \sum_{i=1}^{n}(v_ih_iy_iP + v_id_iP\\ &\quad + v_iH_1(ID_i, Q_{ID_i})\cdot\alpha P)\\ &= (\sum_{i=1}^{n} v_ih_iR_i) + (\sum_{i=1}^{n} v_iQ_{ID_i})\\ &\quad + (\sum_{i=1}^{n} v_ih_{i,0})Y_{DC}\end{aligned}$$

In the distributed decryption phase, DC verifies the signature by Equation 3. The correctness of the equation verified the validity of the signature can be shown as follows:

$$\begin{aligned}S'_iP &= (h'_ir'_i + psk'_{ID_i})P\\ &= h'_ir'_iP + d'_iP + H_1(ID_{DCU}, Q_{ID'_i})\cdot\alpha P\\ &= h'_iR'_i + Q'_{ID_i} + h'_{i.0}Y_{DC}\end{aligned}$$

Besides, in the distributed decryption phase, DC performs batch validation by Equation 4. The correctness of the equation of batch validation can be shown as follows:

$$\begin{aligned}(\sum_{i=1}^{n} v_iS''_i)P &= (\sum_{i=1}^{n} v_i(h''_iy''_i + psk_{ID_i}))P\\ &= \sum_{i=1}^{n}(v_ih''_iy''_iP + v_ipsk_{ID_i}P)\\ &= \sum_{i=1}^{n}(v_ih''_iy''_iP + v_id_iP\\ &\quad + v_iH_1(ID_i, Q_{ID_i})\cdot\alpha P)\\ &= (\sum_{i=1}^{n} v_ih''_iR''_i) + (\sum_{i=1}^{n} v_iQ_{ID_i})\\ &\quad + (\sum_{i=1}^{n} v_ih_{i,0})Y_{DC}\end{aligned}$$

B. SECURITY ANALYSIS

The proposed scheme should ensure privacy, authentication and integrity of personal multimedia data.

- **Privacy:** Firstly, the privacy of personal data m_i is guaranteed by the EC-ELGamal encryption mechanism [33]. MME sends the data $(ID_i, C_i^a, C_i^b, t, \sigma_i)$ to DCU through open channels. if adversaries want to obtain m_i, the computational Diffie-Hallman (CDH) hard problem [37] needs to be solved. Specifically, if the adversary wants to get m_i from $C_i^b = m_iP + r_iGK + H_3(t)\cdot\pi_i$, he needs to calculate

$$r_iGK + H_3(t)\cdot\pi_i = x_1vpk_{ID_i} + \ldots + x_nvpk_{ID_n} + H_3(t)\cdot\pi_i.$$

However, with public parameters $(P, C_i^a, vpk_{ID_i}, \ldots, vpk_{ID_n}, t)$, it is difficult for an adversary to obtain

$$x_1vpk_{ID_i} + \ldots + x_nvpk_{ID_n} + H_3(t)\cdot\pi_i.$$

In short, m_i is secure even if the adversary obtains the message $(ID_i, C_i^a, C_i^b, t, \sigma_i)$. Secondly, our scheme can also resist collusion attack among DC, DCU and MMEs. In the worst case, MME_i $(i = 1, \ldots, n-1)$ can participate in the collusion with DC and DCU to attack MME_n. In order to deduce m_n from (C_n^a, C_n^b), the colluders need to calculate

$$\begin{aligned}r_nGK + H_3(t)\cdot\pi_n &= x_1vpk_{ID_i} + \ldots + x_nvpk_{ID_n}\\ &\quad + H_3(t)\cdot\pi_n.\end{aligned}$$

However, r_nGK cannot be recovered by the colluders without x_n and π_n. So the scheme can resist the collusion attack. Besides, DC can't obtain the total multimedia data without interacting with all MMEs [30]. Finally, for the DC, it is computationally infeasible to calculate an aggregated subset of multimedia aggregated data *sum*. Assume that the corresponding ciphertext of the data m_i is (C_i^a, C_i^b), $i \in [1, n]$. DCU may get

$$C^{b*} = sum^*P + r^*GK + H_3(t)\pi$$

and send it to DC, where

$$sum^* = \sum_{i=1}^{v} m_i, \quad r^* = \sum_{i=1}^{v} r_i, \ 1 < v < n.$$

DC wants to get sum^*, it must calculate

$$r^*GK + H_3(t)\pi = \sum_{i=1}^{n} x_{ID_i}C^{a*} + H_3(t)\pi,$$

where $C^{a*} = \sum_{i=1}^{v} C_i^a$. DC only obtains $D_i = x_{ID_i}C^a$ from MME_i. DC wants to get $x_{ID_i}C^{a*}$, and still needs to

TABLE 2. Notations about related operations and runtime.

Cryptographic operation	Time (ms)	Description
T_p	4.2110	A bilinear pairing operation
T_{em}	0.4420	A scale multiplication related to the ECC
T_{esm}	0.0138	A small scale multiplication related to the ECC

solve the CDH problem. Therefore, except for the sum of $\{m_1, m_2, m_i, \ldots, m_n\}$, the sum of any other subset of $\{m_1, m_2, m_i, \ldots, m_n\}$ cannot be obtained by DC.

- Authentication and Integrity: Suppose there are two valid signature information (σ_i, σ_i^*) generated by the MME_i with the same random element, where $\sigma_i = (R_i, S_i)$ and $\sigma_i^* = (R_i^*, S_i^*)$. Due to $S_i = h_i y_i + psk_{ID_i}$ and $S_i^* = h_i^* y_i + psk_{ID_i}$, we can get

$$\frac{h_i^* S_i - h_i S_i^*}{h_i^* - h_i} = psk_{ID_i}.$$

If the adversary tries to fake the message signature, the elliptic curve discrete logarithm problem (ECDLP) should be solved. In the process of data transmission, the certificateless signature technology is employed, which can achieve data authentication and integrity. In our scheme, all data from MMEs and DCUs are signed by using the signature technology in [31], which is based on the computational ECDLP and proved to be unforgeable against an adaptive chosen-message.

VI. PERFORMANCE EVALUATION

The performance of our scheme will be evaluated by comparing with Liu *et al.*'s scheme [30]. In our scheme and scheme [30], it is assumed that DC has strong computing power. When evaluating the computational cost, only the computational cost at terminal entities and DCU are compared. In the process of evaluation, hash operation and point addition operation on field $E(F_p)$ are neglected. Table 2 defines some symbols of related operations and tests their respective running time on the same platform [31]. Each terminal entity performs the aggregation area creation algorithm, the ciphertext generation algorithm and the distributed decryption algorithm. During the aggregation area creation phase in our scheme, the terminal entity needs to verify the correctness of the messages sent by other terminal entities and generate the group public key GK of the aggregation area. The computational overhead incurred in this phase is $2T_{em}$. While the computational overhead incurred during this phase in scheme [30] is $2T_p$. In the ciphertext generation phase of our scheme, the terminal entity needs to generate the ciphertext (C_i^a, C_i^b) of the data and the signature σ_i of the corresponding ciphertext. The computational cost is $4T_{em}$ in this phase. While the computational cost in scheme [30] is $5T_{em}$ during this phase. In the distributed decryption phase of our scheme, the terminal entity needs to calculate D_i and the corresponding signature σ_i''. The computational cost is $2T_{em}$ in this phase. While the computational cost in scheme [30] is $3T_{em}$ during this phase. The computational overhead of terminal entity at each phase is shown in Table 3. In these three phases, the total computing overhead of each terminal entity in our scheme is $8T_{em}$. While the total computing overhead of each terminal entity in scheme [30] is $2T_p + 8T_{em}$ in these three phases. DCU only involves the ciphertext aggregation phase. In the ciphertext aggregation phase of our scheme, the DCU needs to verify the correctness of the message sent by the terminal entity and generate the aggregate ciphertext (C^a, C^b) and the corresponding signature σ_{DCU}. As shown in Table 4, DCU costs $(2n+2)T_{esm} + T_{em}$ in our scheme, and costs $3T_p + (n+2)T_{em}$ in scheme [30].

TABLE 3. Terminal entity computing cost.

Scheme	Terminal entity computing cost		
	Aggregation area creation	Ciphertext aggregation	Distributed decryption
Liu et al.'s scheme	$2T_p$	$5T_{em}$	$3T_{em}$
Our scheme	$2T_{em}$	$4T_{em}$	$2T_{em}$

TABLE 4. DCU computing cost.

Scheme	DCU computing cost
	Ciphertext aggregation
Liu et al.'s scheme	$3T_p + (n+2)T_{em}$
Our scheme	$(2n+2)T_{esm} + T_{em}$

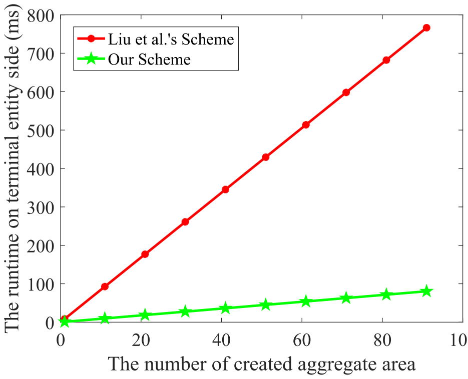


FIGURE 8. The performance comparison of terminal entity side in the aggregation area creation phase.

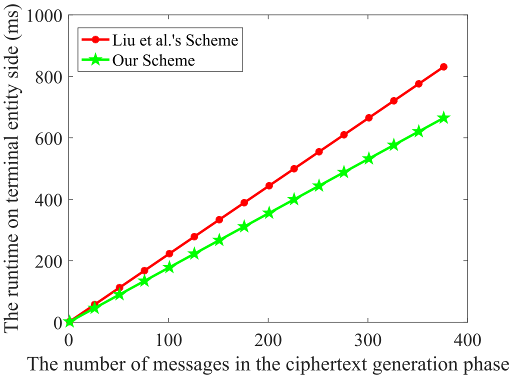


FIGURE 9. The performance comparison of terminal entity side in the ciphertext generation phase.

The following is a more intuitive performance comparison between scheme [30] and our scheme.

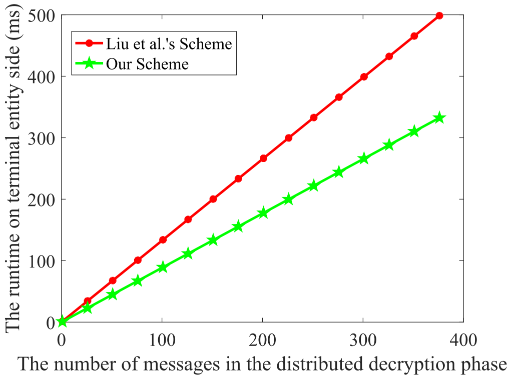


FIGURE 10. **The performance comparison of terminal entity side in the distributed decryption phase.**

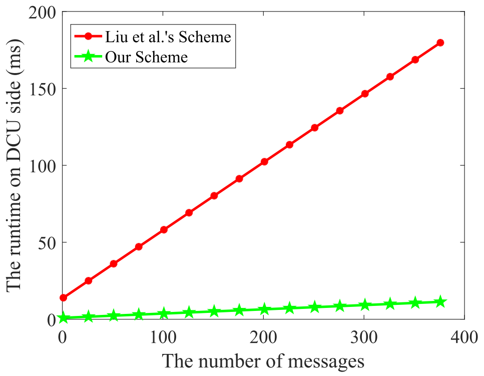


FIGURE 11. **The performance comparison of DCU side in the ciphertext aggregation phase.**

Figure 8, Figure 9 and Figure 10 compare the computing overhead of the terminal entity between scheme [30] and our scheme. In Figure 8, it can be seen that during the creation of the aggregation area phase, the computational overhead of the terminal entity increases with the increase of the number of aggregation area. However, it is obvious that the calculation of the terminal entity of scheme [30] is larger than our scheme. In Figures 9 and 10, it can be seen that in the ciphertext generation and distributed decryption phases, the computational overhead of the terminal entity increases with the increase of the amount of data. However, the calculation of the terminal entity of scheme [30] is slightly larger than our scheme. Figure 11 compare the computing overhead of the DCU between our scheme and the scheme [30]. Obviously, it can be seen that in the ciphertext generation phase, the computational cost of our scheme is lightweight. This is mainly because our scheme does not involve time-consuming bilinear pairing operations. Therefore, compared with scheme [30], our scheme has better computing performance.

VII. CONCLUSION

A lightweight and privacy-preserving data aggregation scheme for mobile multimedia security is presented to balance the utility of multimedia big data and personal multimedia data in this paper. In the proposed scheme, the privacy of the user's multimedia data can be protected, and the calculation of MMEs and DCU is lightweight. There are no certificate management issues for a large number of MMEs. Improving the communication cost of the system will be our next step.

REFERENCES

[1] Y. Kim, N. Park, and D. Won, "Privacy-enhanced adult certification method for multimedia contents on mobile RFID environments," in *Proc. IEEE Int. Symp. Consum. Electron.*, Jun. 2007, pp. 1–4.

[2] K. Zhang, X. Liang, X. Shen, and R. Lu, "Exploiting multimedia services in mobile social networks from security and privacy perspectives," *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 58–65, Mar. 2014.

[3] R. Tous, J. Torres, and E. Ayguadé, "Multimedia big data computing for in-depth event analysis," in *Proc. IEEE Int. Conf. Multimedia Big Data*, Apr. 2015, pp. 144–147.

[4] R. Tous, O. Wust, M. Gomez, J. Poveda, M. Elena, J. Torres, M. Makni, and E. Ayguadé, "User-generated content curation with deep convolutional neural networks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2016, pp. 2535–2540.

[5] D. Wu, H. Shi, H. Wang, R. Wang, and H. Fang, "A feature-based learning system for Internet of Things applications," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1928–1937, Apr. 2019.

[6] J. Chen, "Social aware edge caching in D2D enabled communication," in *Proc. Int. Conf. Artif. Intell. Commun. Netw.*, 2019, pp. 335–349.

[7] X. Li, Y. Zhu, J. Wang, Z. Liu, Y. Liu, and M. Zhang, "On the soundness and security of privacy-preserving SVM for outsourcing data classification," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 906–912, Sep./Oct. 2018.

[8] J. Xiong, J. Ren, L. Chen, Z. Yao, M. Lin, D. Wu, and B. Niu, "Enhancing privacy and availability for data clustering in intelligent electrical service of IoT," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1530–1540, Apr. 2019.

[9] A. Sun, A. Wu, X. Zheng, and F. Ren, "Efficient and privacy-preserving certificateless data aggregation in Internet of Things–enabled smart grid," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, 2019, Art. no. 1550147719842062.

[10] S. Li, K. Xue, Q. Yang, and P. Hong, "PPMA: Privacy-preserving multisubset data aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 462–471, Feb. 2018.

[11] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[12] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1999, pp. 223–238.

[13] K.-A. Shim and C.-M. Park, "A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 8, pp. 2128–2139, Aug. 2015.

[14] T. Jung, X.-Y. Li, and M. Wan, "Collusion-tolerable privacy-preserving sum and product calculation without secure channel," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 45–57, Jan. 2015.

[15] Y. Zhang, R. Deng, D. Zheng, J. Li, P. Wu, and J. Cao, "Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial iot," *IEEE Trans. Ind. Informat.*, to be published.

[16] A. Vishwa and F. K. Hussain, "A blockchain based approach for multimedia privacy protection and provenance," in *Proc. IEEE Symp. Series Comput. Intell. (SSCI)*, Nov. 2018, pp. 1941–1945.

[17] H. Li, K. Wang, X. Liu, Y. Sun, and S. Guo, "A selective privacy-preserving approach for multimedia data," *IEEE Multimedia*, vol. 24, no. 4, pp. 14–25, Oct./Nov. 2017.

[18] C.-Y. Lin, C.-C. Chang, Y.-H. Chen, and P. Prangjarote, "Multimedia privacy protection system for mobil environments," in *Proc. 7th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Oct. 2011, pp. 133–136.

[19] Y. Zhang, R. Deng, X. Liu, and D. Zheng, "Outsourcing service fair payment based on blockchain and its applications in cloud computing," *IEEE Trans. Services Comput.*, to be published.

[20] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Inf. Sci.*, vol. 462, pp. 262–277, Jun. 2018.

[21] Y. Sun, H. Luo, and S. K. Das, "A trust-based framework for fault-tolerant data aggregation in wireless multimedia sensor networks," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 6, pp. 785–797, Dec. 2012.

[22] D. Wu, B. Yang, H. Wang, C. Wang, and R. Wang, "Privacy-preserving multimedia big data aggregation in large-scale wireless sensor networks," *ACM Trans. Multimedia Comput. Commun. Appl.*, vol. 12, no. 4s, 2016, Art. no. 60.

[23] F. Qiu, F. Wu, and G. Chen, "Privacy and quality preserving multimedia data aggregation for participatory sensing systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1287–1300, Jun. 2015.

[24] J. Ni, K. Zhang, Q. Xia, X. Lin, and X. S. Shen, "Enabling strong privacy preservation and accurate task allocation for mobile crowdsensing," *IEEE Trans. Mobile Comput.*, to be published.

[25] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145, Jun. 2018.

[26] Y. Zhang, R. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5G HetNets," *IEEE Trans. Dependable Secure Comput.*, to be published.

[27] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, Sep. 2012.

[28] T. W. Chim, S.-M. Yiu, V. O. K. Li, L. C. K. Hui, and J. Zhong, "PRGA: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 85–97, Jan./Feb. 2015.

[29] H. Shen, M. Zhang, and J. Shen, "Efficient privacy-preserving cube-data aggregation scheme for smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 6, pp. 1369–1381, Jun. 2017.

[30] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1767–1774, Mar. 2019.

[31] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Inf. Sci.*, vols. 451–452, pp. 1–15, Jul. 2018.

[32] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4, pp. 469–472, Jul. 1985.

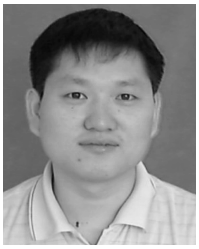
[33] Y. G. Desmedt, "Threshold cryptography," *Eur. Trans. Telecommun.*, vol. 5, no. 4, pp. 449–458, Jul. 1994.

[34] M. F. Balli, S. Uludag, A. A. Selcuk, and B. Tavli, "Distributed multi-unit privacy assured bidding (PAB) for smart grid demand response programs," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4119–4127, Sep. 2017.

[35] H. V. Singh, A. K. Singh, S. Balasubramanian, and A. Mohan, "Minimizing security threats in multimedia systems," in *Proc. 2nd Int. Conf. Distrib. Frameworks Multimedia Appl.*, pp. 1–5, May 2006.

[36] L. Yongliang, W. Gao, and S. Liu, "Multimedia security in the distributed environment," in *Proc. Conf. 10th Asia–Pacific Conf. Commun. 5th Int. Symp. Multi-Dimensional Mobile Commun.*, vol. 2, Aug./Sep. 2004, pp. 639–642.

[37] R. X. Lu and Z. F. Cao, "Simple three-party key exchange protocol," *Comput. Secur.*, vol. 26, no. 1, pp. 94–97, Feb. 2007.



SUGANG MA received the master's degree from Xidian University, in 2010. He is currently pursuing the Ph.D. degree in computer science with Chang'an University. He is currently a Senior Engineer with the Xi'an University of Posts and Telecommunications and a Senior Member of the China Communications Society. His current research interests include intelligent transportation and information system engineering.

TIANTIAN ZHANG is currently pursuing the master's degree with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. Her research interests include cloud storage security and data integrity auditing.

AXIN WU received the B.S. degree from the Zhengzhou University of Light Industry, in 2016, and the M.Eng. degree from the Xi'an University of Post and Telecommunications, in 2019. Since 2019, he has been in the Ph.D. Program with Jinan University, Guangzhou, China. His research interests include cloud security and wireless network security.

XIANGMO ZHAO was with Chang'an University for more than 20 years, where he is currently the Vice President and the Director of the Science and Technology Innovation Team of Multi-Sources Traffic Information Sensing and Fusion, Ministry of Education, and also a Professor with the School of Information Engineering, Chang'an University. He has published more than 200 peer-reviewed papers. His research interests include the Internet of Vehicles, testing of intelligent vehicles, intelligent transportation systems, and nondestructive testing for road infrastructures. He currently serves as a member of the State Council's Discipline Evaluation Committee on Transportation Engineering, and is sitting as the Academic Leader of State-Level Key Discipline of the Traffic Information Engineering and Control, Chang'an University. He received the National SciTech Progress Awards twice for his contribution on promoting the development of indoor vehicle testing technology in China. He also received the National May 1st Labor Medal of China, in 2001.