IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 28, 2020, accepted August 18, 2020, date of publication August 21, 2020, date of current version September 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3018488

Efficient Anonymous Certificate-Based Multi-Message and Multi-Receiver Signcryption Scheme for Healthcare Internet of Things

YANG MING[1], (Member, IEEE), XIAOPENG YU[1], AND XIAOQIN SHEN[2]
[1]School of Information Engineering, Chang'an University, Xi'an 710064, China
[2]School of Sciences, Xi'an University of Technology, Xi'an 710054, China

Corresponding author: Yang Ming (yangming@chd.edu.cn)

This work was supported in part by the Natural Science Foundation of Shaanxi Province under Grant 2018JM6081, and in part by the Fundamental Research Funds for the Central Universities, CHD, under Grant 300102249204.

ABSTRACT Healthcare Internet of Things (IoT) is an emerging paradigm, which can provide comprehensive and different types of health services and enable various types of medical sensors to monitor patient's health conditions. In the healthcare IoT, patient is deployed with a variety of medical sensors, which continuously monitors and collects patient's sensitive health data that needs specially protection for preventing privacy leakage. To safely send multiple different health data monitored by multiple different medical sensors to multiple corresponding healthcare professionals in one data report, several multi-message and multi-receiver signcryption schemes have been introduced by employing the traditional public key cryptography, identity-based cryptography or certificateless cryptography. However, these schemes suffer from the certificate management, key escrow and key distribution problem. Besides, due to the resource-constraint property of medical sensors, they are unsuitable for healthcare IoT in terms of both performance and privacy requirements. To solve these issues, this paper introduces an efficient anonymous certificate-based multi-message and multi-receiver signcryption scheme for healthcare IoT, where the certificate-based cryptography and elliptic curve cryptography are combined to simplify the certificate management problem, eliminate the key escrow problem, solve the key distribution problem and ensure the privacy-preserving. Furthermore, the security analysis suggests that the proposed scheme is able to achieve the confidentiality, unforgeability, receiver anonymity, sender anonymity and decryption fairness; the performance evaluation indicates that the proposed scheme brings to the lower computation cost and communication cost in comparison to the existing schemes.

INDEX TERMS Certificate-based cryptography, elliptic curve cryptography, multi-message and multi-receiver signcryption, healthcare Internet of Things.

I. INTRODUCTION

Healthcare IoT [1] has been introduced as a promising paradigm to provide comprehensive and different types of health services and greatly improve the quality of health care. A typical healthcare IoT architecture [2], [3] is illustrated in Figure 1, which consists of medical sensors, patient, healthcare professionals, gateway and cloud server. In healthcare IoT system, a variety of medical sensors are deployed for patient to monitor health data of patient, such as temperature, heart rate, brain wave, blood pressure etc [4]. To share the monitored IoT medical sensors health data with the corresponding healthcare professionals, these health data need to be uploaded the cloud server via the gateway. After that, the healthcare professionals can access the cloud to analyze the health data and provide necessary assistance to the patient, for example, the healthcare professionals will immediately contact the patient to provide advices and arrange medical examinations when certain medical indicators of the patient are abnormal. It is worth noting that the medical sensors have normally a very limited communication and computational capabilities, so operations in the healthcare IoT should be lightweight [5]. Furthermore, there are risks of information leakage during the health data transmission [6], such as an

The associate editor coordinating the review of this manuscript and approving it for publication was Kuo-Hui Yeh.

FIGURE 1. A typical healthcare IoT architecture.

adversary may attempt to eavesdrop the wireless communication, so it is advisable to protect the health data during transmission.

In order to securely and efficiently send monitored health data to multiple corresponding healthcare professionals in the healthcare IoT system, the multicast communication [7] has received considerable attention recently, which is an essential one-to-many communication architecture. It is worth noting that data reports are transmitted via open wireless networks, so they are vulnerable to various attacks [8]. To achieve secure multicast communication, several multi-receiver encryption (ME) schemes [9]–[28] and multi-receiver signcryption (MSC) schemes [29]–[42] have been introduced. However, existing schemes [9]–[42] cannot send multiple different health data monitored by multiple different medical sensors to multiple corresponding healthcare professionals in one data report. To find a solution to the issue, several multi-message and multi-receiver signcryption (MMSC) schemes [43]–[49] have been introduced by using the public key infrastructure (PKI)-based cryptography [50], identity (ID)-based cryptography [51] or certificateless (CL)-based cryptography [52]. However, the traditional PKI-based MMSC schemes [43], [44] suffers from the heavy certificate management burden, the ID-based MMSC scheme [45] brings the key escrow issue, the ID-based and CL-based Heterogeneous MMSC schemes [46], [47] exist the key escrow and key distribution problem, the CL-based MMSC schemes [48], [49] cause the key distribution problem. Furthermore, the schemes [43]–[49] either have a poor performance or fail to satisfy the security requirements.

To solve the aforementioned problems, based on the certificate-based (CB) cryptography [53] and the elliptic curve cryptography (ECC) [54], [55], this paper proposes an efficient anonymous certificate-based MMSC scheme for healthcare IoT. The main contributions of this paper are able to be summarized as follows:

- Firstly, based on the certificate-based cryptography and ECC, an efficient anonymous certificate-based MMSC scheme is proposed, which avoids the problem of certificate management, key escrow and key distribution.
- Secondly, through comprehensive security analysis, the proposed certificate-based MMSC scheme satisfies the confidentiality, unforgeability, receiver anonymity, sender anonymity and decryption fairness.
- Finally, the performances evaluation results illustrates that the proposed certificate-based MMSC scheme brings the lower communication and computation cost compared with existing MMSC schemes.

This paper is organized as follows. Section 2 surveys the related work. In Section 3, the background was introduced. Section 4 presents the concrete scheme. The security proof and analysis are performed in Section 5. Section 6 makes the performance evaluation. The paper is summaried in Section 7.

II. RELATED WORK

Some MMSC schemes [43]–[49] closely related to this paper are roughly divided into four categories: the PKI-based MMSC schemes [43], [44], the ID-based MMSC scheme [45], the heterogeneous hybrid MMSC schemes [46], [47] and the CL-based MMSC schemes [48], [49].

In the PKI-based MMSC schemes, Seo and Kim [43] presented the first MMSC scheme based on the PKI-based cryptography, in which only predetermined users within the domain could obtain their own corresponding messages. Based on the PKI-based cryptography, Han and Gui [44] introduced a MMSC framework to achieve secure multicast communication, but it is inefficiency due to using the bilinear pairing. However, the PKI-based MMSC schemes requires large amounts of storage and computing resources to manage the certificate of users, which leads to the heavy the certificate management burden.

In order to overcome the certificate management problem in the PKI-based MMSC schemes, based on the ID-based cryptography, Qiu *et al.* [45] presented a secure ID-based MMSC scheme for key update, which has a poor performance due to employing bilinear pairing. In the ID-based MMSC scheme, user uses the identity as the public key and obtains the private key from private key generator (PKG). Therefore, the ID-based MMSC scheme avoids the certificate management problem in traditional PKC-based MMSC schemes. However, the ID-based MMSC scheme [45] causes the key escrow issue, namely, PKG has the ability to know the private key of user.

In order to solve the key escrow issue of the receiver in ID-based MMSC scheme, based on the ID-based cryptography and CL-based cryptography, Niu *et al.* [46] presented a heterogeneous hybrid MMSC scheme, which allows a sender in ID-based cryptography to send different multiple messages to different multiple receivers in CL-based cryptography, achieves confidentiality, unforgeability and conditional identity privacy preservation. In heterogeneous hybrid MMSC scheme, the private key of receiver is produced by integrating the partial private key from key generator center (KGC) and the secret value from receiver itself. Therefore, KGC does not have the ability to know the private key of receiver. Qiu *et al.* [47] introduces an efficient secure

heterogeneous MMSC scheme for the distributed mobile IoT based on the ID-based cryptography, the CL-based cryptography and ECC. However, the heterogeneous hybrid MMSC schemes [46,47] exist the key escrow issue of the sender in ID-based cryptography and key distribution issue of the receiver in CL-based cryptography.

In order to resolve the key escrow issue in ID-based MMSC scheme and heterogeneous hybrid MMSC schemes, based on the CL-based cryptography, Pang *et al.* [48] introduced an efficient anonymous CL-based MMSC scheme. In the CL-based MMSC scheme, the private key of the user (receiver and sender) is generated by combining the partial private key from KGC and the secret value from user itself. Therefore, KGC does not have the ability to know the private key of the user. Peng *et al.* [49] illustrated that Pang *et al.*'s scheme [48] is unable to realize the confidentiality and unforgeability since the attacker is able to fake user's legal private key and public key, and introduced a CL-based MMSC scheme for secure multicast communication by employing the CL-based cryptography and ECC. However, the CL-based MMSC schemes [48], [49] bring the key distribution problem, that is, a secure channel is required during the private key generation process of the user.

III. BACKGROUND

A. SYSTEM MODEL

The system model of the proposed certificate-based MMSC scheme is shown in Figure 2, which consists of three entities: key generation center (KGC), patient U_s, and healthcare professionals $\{U_{r_1}, U_{r_2}, \cdots, U_{r_n}\}$. For readability, we display the definitions of symbols in Table 1.

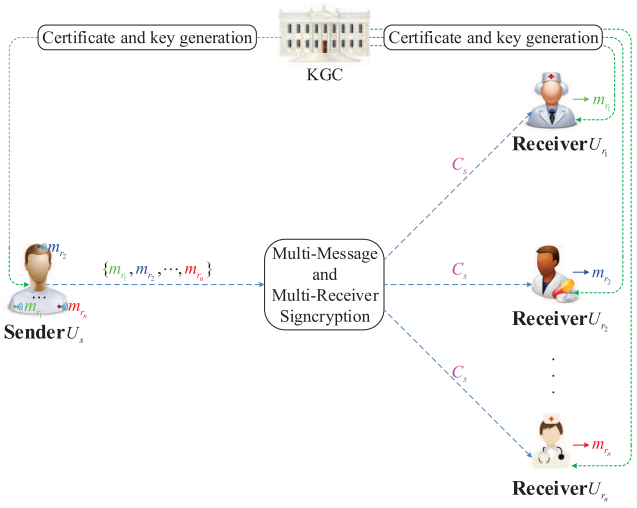

FIGURE 2. System model.

KGC: It is an honest-but-curious entity responsible for the generation of system parameters and registration of patient and healthcare professionals.

U_s: It is a sender and deployed with various smart sensors monitoring the physical condition. Besides, it can signcrypt the health data $\{m_{r_1}, m_{r_2}, \cdots, m_{r_n}\}$ to obtain the data report C_s, and send it to multiple corresponding healthcare professionals.

U_{r_i}: It is a receiver and may obtain the monitored health data m_{r_i} from the patient's data report C_s. Besides, different healthcare professionals are able to obtain different health data from the same data report.

TABLE 1. Notations.

Symbols	Definitions
KGC	Key generation center
s	Master key
P_{pub}	KGC's public key
$params$	System parameters
U_s	The patient
id_s	U_s's real identity
ID_s	U_s's pseudo identity
x_s	U_s's private key
$\{X_s, R_s\}$	U_s's public key
$cert_s$	U_s's certificate
U_{r_i}	The i-th healthcare professional
id_{r_i}	U_{r_i}'s real identity
ID_{r_i}	U_{r_i}'s pseudo identity
x_{r_i}	U_{r_i}'s private key
$\{X_{r_i}, R_{r_i}\}$	U_{r_i}'s public key
$cert_{r_i}$	U_{r_i}'s certificate
n	The number of healthcare professionals
m_{r_i}	The health data that patient U_s sends to healthcare professional U_{r_i}
C_s	The data report
H_i	Five hash functions $H_i : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $i = 0, 1, 2, 3, 4$.

B. DEFINITION OF ANONYMOUS CERTIFICATE-BASED MMSC

The definition of anonymous certificate-based MMSC comprises of the following four algorithms.

- $Setup\{\lambda\} \rightarrow \{s, params\}$: This algorithm is run by the KGC. It takes a security parameter λ as input and outputs the master key s and system parameters $params$. KGC keeps s secretly and publishes $params$.
- $Certificate\ and\ key\ generation\{id_i, s, params\} \rightarrow \{ID_i, x_i, \{X_i, R_i\}, cert_i\}$: This algorithm is run by the user (sender and receiver) and KGC. It takes user's real identity id_i, master key s and system parameters $params$ as input and outputs the pseudo identity ID_i, private key x_i, public key $\{X_i, R_i\}$ and certificate $cert_i$.
- $Signcryption\{\{m_{r_1}, m_{r_2}, \cdots, m_{r_n}\}, \{ID_{r_1}, ID_{r_2}, \cdots, ID_{r_n}\}, \{\{X_{r_1}, R_{r_1}\}, \{X_{r_2}, R_{r_2}\}, \cdots, \{X_{r_n}, R_{r_n}\}\}, ID_s, x_s, \{X_s, R_s\}, cert_s, params\} \rightarrow \{C_s\}$: This algorithm is run by the sender. It takes the messages $\{m_{r_1}, m_{r_2}, \cdots, m_{r_n}\}$, receivers' pseudo identity $\{ID_{r_1}, ID_{r_2}, \cdots, ID_{r_n}\}$, receivers' public key $\{\{X_{r_1}, R_{r_1}\}, \{X_{r_2}, R_{r_2}\}, \cdots, \{X_{r_n}, R_{r_n}\}\}$, sender's pseudo identity ID_s, sender's private key x_s, sender's public key $\{X_s, R_s\}$, sender's certificate $cert_s$ and system parameters $params$ as input and outputs the ciphertext C_s.
- $Unsigncryption\{C_s, ID_{r_i}, x_{r_i}, \{X_{r_i}, R_{r_i}\}, cert_{r_i}, ID_s, \{X_s, R_s\}, params\} \rightarrow \{m_{r_i}\}$: This algorithm is run by the receiver. It takes the ciphertext C_s, receiver's pseudo

identity ID_{r_i}, receiver's private key x_{r_i}, receiver's public key $\{X_{r_i}, R_{r_i}\}$, receiver's certificate c_{r_i}, sender's pseudo identity ID_s, sender's public key $\{X_s, R_s\}$ and system parameters *params* as input and outputs the message m_{r_i}.

C. SECURITY REQUIREMENTS

1) CONFIDENTIALITY

Only authorized healthcare professionals are able to obtain the monitored health data from patient's data report.

2) UNFORGEABILITY

Any attacker cannot forge the patient's legal data report; moreover, any modification of data reports can be detected.

3) RECEIVER ANONYMITY

For any data report, authorized healthcare professional has ability to know whether he/she is a legal receiver of the data report but cannot judge whether other users are the legitimate receivers of the data report.

4) SENDER ANONYMITY

Any attacker should not reveal the patient's real identity by analysing the received data report.

5) DECRYPTION FAIRNESS

All authorized healthcare professionals have the same ability to unsigncrypt patient's data report to obtain health data.

D. SECURITY ASSUMPTION

The elliptic curve E over finite field F_p formed by a set of points (x, y) meeting $y^2 = x^3 + ax + b \bmod p$, where p is a prime number, $4a^3 + 27b^2 \neq 0$ and $a, b \in F_p$ [54], [55]. All points on E and infinity point O form an additive cyclic group $\mathbb{G}$ with generator P and prime order q. The scalar multiplication calculation over $\mathbb{G}$ is defined as $kP = P + P + \cdots + P$ (k times), where $k \in \mathbb{Z}_q^*$ and $P \in \mathbb{G}$.

The security of the proposed certificate-based MMSC scheme depends on the hardness of DDH problem and ECDL problem, which are summarized as follows.

1) DECISIONAL DIFFIE-HELLMAN (DDH) ASSUMPTION [56]

Let $\mathbb{G}$ is an additive group with prime order q. For any probabilistic polynomial time (PPT) adversary, given $P, aP, bP, Z \in \mathbb{G}$, where $a, b \in \mathbb{Z}_q^*$, it is hard to decide whether $Z = abP$ holds.

2) ELLIPTIC CURVE DISCRETE LOGARITHM (ECDL) ASSUMPTION [57], [58]

Let $\mathbb{G}$ is an additive group with prime order q. For any PPT adversary, given $P, xP \in \mathbb{G}$, where $x \in \mathbb{Z}_q^*$, it is hard to compute x.

E. SECURITY MODEL

The security of certificate-based MMSC scheme should meet the confidentiality, unforgeability and receiver anonymity. According to certificate-based cryptography [59], Type I adversary $\mathcal{A}_I$ and Type II adversary $\mathcal{A}_{II}$ are considered in the security model. $\mathcal{A}_I$ serves as malicious user and models an outside adversary, $\mathcal{A}_{II}$ acts as malicious-but-passive KGC and models an inside adversary.

- $\mathcal{A}_I$: It may not access the master key, but may replace the public key of user.
- $\mathcal{A}_{II}$: It may access the master key, but may not replace the public key of user.

The security model of the proposed certificate-based MMSC scheme is defined by the interaction between the challenger $\mathcal{C}$ and adversary $\mathcal{A}_I$ ($\mathcal{A}_{II}$). The following queries are able to be issued by $\mathcal{A}_I$ and $\mathcal{A}_{II}$.

- **Hash query**: Receiving the hash query, $\mathcal{C}$ returns a random value.
- **Create user query**: Receiving the create user query on ID_i, $\mathcal{C}$ returns the public key $\{X_i, R_i\}$.
- **Private key query**: Receiving the private key query on ID_i, $\mathcal{C}$ returns the private key x_i.
- **Certificate query**: Receiving the certificate query on ID_i, $\mathcal{C}$ returns the certificate $cert_i$.
- **Public key replacement query**: Receiving the query on ID_i with $\{X_i', R_i'\}$, $\mathcal{C}$ replaces the public key $\{X_i, R_i\}$ with $\{X_i', R_i'\}$.
- **Signcryption query**: Receiving the signcryption query on the messages $\{m_{r_1}, m_{r_2}, \cdots, m_{r_n}\}$ under the sender ID_s and the receivers $\{ID_{r_1}, ID_{r_2}, \cdots, ID_{r_n}\}$, $\mathcal{C}$ returns the ciphertext C_s.
- **Undesigncryption query**: Receiving the unsigncryption query on the ciphertext C_s under the sender ID_s and the receiver ID_{r_i}, $\mathcal{C}$ returns the corresponding message m_{r_i}.

Definition 1 (Confidentiality): A certificate-based MMSC scheme is IND-CCA (indistinguishability under the chosen ciphertext attack) secure that if any PPT adversary has at most a negligible advantage in Game 1 *and Game 2.*

Game 1 (IND-CCA-I): It is the interactive game between $\mathcal{C}$ and $\mathcal{A}_I$.

Initialization: $\mathcal{A}_I$ selects the challenging identities $ID_r^* = \{ID_{r_1}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$ as the receivers, and sends them to $\mathcal{C}$.

Setup: $\mathcal{C}$ produces the system parameters, and outputs them to $\mathcal{A}_I$.

Phase 1: $\mathcal{A}_I$ adaptively issues polynomial bounded times hash, create user, private key, certificate, public key replacement, signcryption and unsigncryption queries.

Challenge: $\mathcal{A}_I$ selects two messages $m_0^* = \{m_{0,r_1}^*, m_{0,r_2}^*, \cdots, m_{0,r_n}^*\}$ and $m_1^* = \{m_{1,r_1}^*, m_{1,r_2}^*, \cdots, m_{1,r_n}^*\}$ of equal length and the sender ID_s^*, and then sends them to $\mathcal{C}$. $\mathcal{C}$ randomly selects $\beta \in \{0, 1\}$ and generates the ciphertext C_s^* on $m_\beta^* = \{m_{\beta,r_1}^*, m_{\beta,r_2}^*, \cdots, m_{\beta,r_n}^*\}$ under ID_s^* and ID_r^*. Finally, $\mathcal{C}$ sends C_s^* to $\mathcal{A}_I$.

Phase 2: $\mathcal{A}_I$ adaptively issues the query in Phase 1 except that it cannot issue the certificate query on $ID_{r_i}^*(i = 1, 2, \cdots, n)$, the signcryption query on m_β^* under ID_s^* and ID_r^*, and the unsigncryption query on C_s^* under ID_s^* and ID_r^*.

Guess: $\mathcal{A}_I$ outputs $\beta' \in \{0, 1\}$ as its guess and wins the game if $\beta' = \beta$.

$\mathcal{A}_I$'s advantage is defined as

$$Adv_{\mathcal{A}_I}^{IND-CCA} = |\Pr[\beta' = \beta] - \frac{1}{2}|.$$

Game 2 (IND-CCA-II): It is the interactive game between $\mathcal{C}$ and $\mathcal{A}_{II}$.

Initialization: $\mathcal{A}_{II}$ selects the challenging identities $ID_r^* = \{ID_{r_1}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$ as the receivers, and sends them to $\mathcal{C}$.

Setup: $\mathcal{C}$ produces the master key and system parameters, and outputs them to $\mathcal{A}_{II}$.

Phase 1: $\mathcal{A}_{II}$ adaptively issues polynomial bounded times hash, create user, private key, signcryption and unsigncryption queries.

Challenge: $\mathcal{A}_{II}$ selects two messages $m_0^* = \{m_{0,r_1}^*, m_{0,r_2}^*, \cdots, m_{0,r_n}^*\}$ and $m_1^* = \{m_{1,r_1}^*, m_{1,r_2}^*, \cdots, m_{1,r_n}^*\}$ of equal length and the sender ID_s^*, and then sends them to $\mathcal{C}$. $\mathcal{C}$ randomly selects $\beta \in \{0, 1\}$ and generates the ciphertext C_s^* on $m_\beta^* = \{m_{\beta,r_1}^*, m_{\beta,r_2}^*, \cdots, m_{\beta,r_n}^*\}$ under ID_s^* and ID_r^*. Finally, $\mathcal{C}$ sends C_s^* to $\mathcal{A}_{II}$.

Phase 2: $\mathcal{A}_{II}$ adaptively issues the query in Phase 1 except that it cannot issue the private key query on $ID_{r_i}^*(i = 1, 2, \cdots, n)$, the signcryption query on m_β^* under ID_s^* and ID_r^*, and the unsigncryption query on C_s^* under ID_s^* and ID_r^*.

Guess: $\mathcal{A}_{II}$ outputs $\beta' \in \{0, 1\}$ as its guess and wins the game if $\beta' = \beta$.

$\mathcal{A}_{II}$'s advantage is defined as

$$Adv_{\mathcal{A}_{II}}^{IND-CCA} = |\Pr[\beta' = \beta] - \frac{1}{2}|.$$

Definition 2 (Unforgeability): A certificate-based MMSC scheme is EUF-CMA (existential unforgeability under the chosen message attack) secure that if any PPT adversary has at most a negligible advantage in Game 3 and Game 4.

Game 3 (EUF-CMA-I): It is the interactive game between $\mathcal{C}$ and $\mathcal{A}_I$.

Initialization: $\mathcal{A}_I$ selects the challenging identity ID_s^* as the sender, and sends it to $\mathcal{C}$.

Setup: $\mathcal{C}$ produces the system parameters, and outputs them to $\mathcal{A}_I$.

Query: $\mathcal{A}_I$ adaptively issues polynomial bounded times hash, create user, private key, certificate, public key replacement, signcryption and unsigncryption queries.

Forgery: $\mathcal{C}$ outputs a ciphertext C_s^* on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $ID_r^* = \{ID_{r_1}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$, such that

- C_s^* is valid.
- $\mathcal{A}_I$ has never issues the certificate query on ID_s^*.
- $\mathcal{A}_I$ has never issues the signcryption query on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and ID_r^*.

$\mathcal{A}_I$'s advantage is defined as

$$Adv_{\mathcal{A}_I}^{EUF-CMA} = |\Pr[\textit{The success probability of } \mathcal{A}_I]|.$$

Game 4 (EUF-CMA-II): It is the interactive game between $\mathcal{C}$ and $\mathcal{A}_{II}$.

Initialization: $\mathcal{A}_{II}$ selects the challenging identity ID_s^* as the sender, and sends it to $\mathcal{C}$.

Setup: $\mathcal{C}$ produces the master key and system parameters, and outputs them to $\mathcal{A}_{II}$.

Query: $\mathcal{A}_{II}$ adaptively issues polynomial bounded times hash, create user, private key, signcryption and unsigncryption queries.

Forgery: $\mathcal{C}$ outputs a ciphertext C_s^* on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $ID_r^* = \{ID_{r_1}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$, such that

- C_s^* is valid.
- $\mathcal{A}_{II}$ has never issues the private key query on ID_s^*.
- $\mathcal{A}_{II}$ has never issues the signcryption query on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and ID_r^*.

$\mathcal{A}_{II}$'s advantage is defined as

$$Adv_{\mathcal{A}_{II}}^{EUF-CMA} = |\Pr[\textit{The success probability of } \mathcal{A}_{II}]|.$$

Definition 3 (Receiver anonymity): A certificate-based MMSC scheme is ANON-IND-CCA (anonymous indistinguishability under the chosen ciphertext attack) secure that if any PPT adversary has at most a negligible advantage in Game 5 and Game 6.

Game 5 (ANON-IND-CCA-I): It is the interactive game between $\mathcal{C}$ and $\mathcal{A}_I$.

Initialization: $\mathcal{A}_I$ selects the challenging identities $\{ID_{r_0}^*, ID_{r_1}^*\}$ as the receivers, and sends them to $\mathcal{C}$.

Setup: $\mathcal{C}$ produces the system parameters, and outputs them to $\mathcal{A}_I$.

Phase 1: $\mathcal{A}_I$ adaptively issues polynomial bounded times hash, create user, private key, certificate, public key replacement, signcryption and unsigncryption queries.

Challenge: $\mathcal{A}_I$ selects the messages $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$, the sender ID_s^* and the receivers $\{ID_{r_2}^*, ID_{r_3}^*, \cdots, ID_{r_n}^*\}$, and then sends them to $\mathcal{C}$. $\mathcal{C}$ randomly selects $\beta \in \{0, 1\}$ and generates the ciphertext C_s^* on $\{m_r^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$. Finally, $\mathcal{C}$ sends C_s^* to $\mathcal{A}_I$.

Phase 2: $\mathcal{A}_I$ adaptively issues the query in Phase 1 except that it cannot issue the certificate query on $ID_{r_i}^*(i = 0, 1)$, the signcryption query on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$, and the unsigncryption query on C_s^* under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$.

Guess: $\mathcal{A}_I$ outputs $\beta' \in \{0, 1\}$ as its guess and wins the game if $\beta' = \beta$.

$\mathcal{A}_I$'s advantage is defined as

$$Adv_{\mathcal{A}_I}^{ANON-IND-CCA} = |\Pr[\beta' = \beta] - \frac{1}{2}|.$$

Game 6 (ANON-IND-CCA-II): It is the interactive game between $\mathcal{C}$ and $\mathcal{A}_{II}$.

Initialization: $\mathcal{A}_{II}$ selects the challenging identities $\{ID_{r_0}^*, ID_{r_1}^*\}$ as the receivers, and sends them to $\mathcal{C}$.

Setup: $\mathcal{C}$ produces the master key and system parameters, and outputs them to $\mathcal{A}_{II}$.

Phase 1: $\mathcal{A}_{II}$ adaptively issues polynomial bounded times hash, create user, private key, signcryption and unsigncryption queries.

Challenge: $\mathcal{A}_{II}$ selects the messages $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$, the sender ID_s^* and the receiver $\{ID_{r_2}^*, ID_{r_3}^*, \cdots, ID_{r_n}^*\}$, and then sends them to $\mathcal{C}$. $\mathcal{C}$ randomly selects $\beta \in \{0, 1\}$ and

generates the ciphertext C_s^* on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$. Finally, $\mathcal{C}$ sends C_s^* to $\mathcal{A}_{II}$.

Phase 2: $\mathcal{A}_{II}$ adaptively issues the query in Phase 1 except that it cannot issue the private key query on $ID_{r_i}^*(i = 0, 1)$, the signcryption query on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$, and the unsigncryption query on C_s^* under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$.

Guess: $\mathcal{A}_{II}$ outputs $\beta' \in \{0, 1\}$ as its guess and wins the game if $\beta' = \beta$.

$\mathcal{A}_{II}$'s advantage is defined as

$$Adv_{\mathcal{A}_{II}}^{ANON-IND-CCA} = |\Pr[\beta' = \beta] - \frac{1}{2}|.$$

IV. THE PROPOSED SCHEME

In the section, we proposes an efficient anonymous certificate-based MMSC scheme for healthcare IoT. Specifically, it includes setup, certificate and key generation, signcryption and unsigncryption phases.

A. SETUP

KGC generates the system parameters by means of performing the following steps.

(1) KGC selects a non-singular elliptic curve E formed by $y^2 = x^3 + ax + b \bmod p$, where p is a prime number.
(2) KGC chooses a group $\mathbb{G}$ with generator P and prime order q.
(3) KGC randomly selects the master key $s \in \mathbb{Z}_q^*$ and calculates the system public key $P_{pub}{=}s \cdot P$.
(4) KGC selects five hash functions $H_i : \{0, 1\}^* \to \mathbb{Z}_q^*$, $i = 0, 1, 2, 3, 4$.
(5) KGC publishes the system parameters $params = \{q, p, P, \mathbb{G}, P_{pub}, H_0, H_1, H_2, H_3, H_4\}$.

B. CERTIFICATE AND KEY GENERATION

The user U_i with real identity id_i registers with KGC to produce the pseudo identity ID_i, public key $\{X_i, R_i\}$, private key x_i and certificate $cert_i$ through performing the following steps.

(1) U_i randomly selects the private key $\xi_i, x_i \in \mathbb{Z}_q^*$ and calculates

$$ID_i = H_0(id_i, \xi_i),$$
$$X_i = x_i \cdot P,$$

and then sends the pseudo identity ID_i and partial public key X_i to the KGC.

(2) Receiving the ID_i and X_i, KGC randomly selects $r_i \in \mathbb{Z}_q^*$ and calculates

$$R_i = r_i \cdot P,$$
$$cert_i = r_i + s \cdot H_1(ID_i, X_i, R_i, P_{pub}),$$

and then sends the public key $\{X_i, R_i\}$ and the certificate $cert_i$ to U_i via public channel.

(3) U_i can verify the certificate $cert_i$ by the following equation

$$cert_i \cdot P = R_i + H_1(ID_i, X_i, R_i, P_{pub}) \cdot P_{pub}.$$

C. SIGNCRYPTION

Given the health data $\{m_{r_1}, m_{r_2}, \cdots, m_{r_n}\}$, the healthcare professionals' identity $\{ID_{r_1}, ID_{r_2}, \cdots, ID_{r_n}\}$ and public key $< \{X_{r_1}, R_{r_1}\}, \{X_{r_2}, R_{r_2}\}, \cdots, \{X_{r_n}, R_{r_n}\} >$, the patient U_s could generates the data report C_s through performing the following steps.

(1) U_s randomly selects $l_s \in \mathbb{Z}_q^*$ and calculates

$$L_s = l_s \cdot P.$$

(2) U_s calculates

$$c_{r_i} = H_1(ID_{r_i}, X_{r_i}, R_{r_i}, P_{pub}),$$
$$E_{r_i} = l_s \cdot (X_{r_i} + R_{r_i} + c_{r_i} \cdot P_{pub}),$$
$$e_{r_i} = H_2(E_{r_i}), \text{ for each } i = 1, 2, \cdots, n,$$

and then calculates

$$f(x) = \prod_{i=1, i\neq 1}^{n} \frac{(x - e_{r_i})}{(e_{r_1} - e_{r_i})} m_{r_1} + \prod_{i=1, i\neq 2}^{n} \frac{(x - e_{r_i})}{(e_{r_2} - e_{r_i})} m_{r_2} + \cdots + \prod_{i=1, i\neq n}^{n} \frac{(x - e_{r_i})}{(e_{r_n} - e_{r_i})} m_{r_n}$$
$$= g_{n-1}x^{n-1} + \cdots + g_1 x + g_0 (\text{mod} p),$$

and sets $G_s = (g_{n-1}, \cdots, g_1, g_0)$.

(3) U_s calculates

$$f_s = H_3(ID_s, X_s, R_s, G_s),$$
$$h_s = H_4(ID_s, X_s, R_s, L_s),$$
$$\sigma_s = x_s \cdot f_s + cert_s + l_s \cdot h_s.$$

(4) U_s sends the data report $C_s = \{L_s, G_s, \sigma_s\}$ towards the corresponding healthcare professionals.

D. UNSIGNCRYPTION

Receiving the data report $C_s = \{L_s, G_s, \sigma_s\}$, U_{r_i} could unsigncrypt C_s to obtain the health data m_{r_i} through performing the following steps.

(1) U_{r_i} calculates

$$c_s = H_1(ID_s, X_s, R_s, P_{pub}),$$
$$f_s = H_3(ID_s, X_s, R_s, G_s),$$
$$h_s = H_4(ID_s, X_s, R_s, L_s).$$

(2) U_{r_i} checks whether the following equation holds

$$\sigma_s \cdot P = f_s \cdot X_s + R_s + c_s \cdot P_{pub} + h_s \cdot L_s.$$

If it does hold, U_{r_i} calculates

$$E_{r_i} = (x_{r_i} + cert_{r_i}) \cdot L_s,$$
$$e_{r_i} = H_2(E_{r_i}),$$
$$f(e_{r_i}) = g_{n-1}e_{r_i}^{n-1} + \cdots + g_1 e_{r_i} + g_0 = m_{r_i}.$$

V. SECURITY

Security proof and analysis between existing MMSC schemes [43]–[49] and the proposed certificate-based MMSC scheme is conducted.

A. SECURITY PROOF

Theorem 1: The proposed certificate-based MMSC scheme is IND-CCA secure in ROM under DDH assumption.

Proof: Theorem 1 is able to be proved by the Lemma 1 and Lemma 2.

Lemma 1: The proposed MMSC scheme is IND-CCA-I secure in ROM under DDH assumption.

Proof: Assuming that $\mathcal{A}_I$ wins the Game 1 with probability ε in time t, we can build an algorithm $\mathcal{B}$ to break DDH assumption with probability ε' in time t'. Given an instance (P, aP, bP, Z) of DDH assumption, $\mathcal{B}$'s goal is to decide whether $Z = abP$ holds.

Initialization: $\mathcal{A}_I$ selects the challenging identities $ID_r^* = \{ID_{r_1}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$ as the receivers, and sends them to $\mathcal{B}$.

Setup: $\mathcal{B}$ sets $P_{pub} = aP$, and returns $params = \{q, p, P, \mathbb{G}, P_{pub}, H_0, H_1, H_2, H_3, H_4\}$ to $\mathcal{A}_I$.

In order to maintain the quick response and consistency, $\mathcal{B}$ keeps the following lists:

- L_{H_0}: It consists of tuples (id_i, ξ_i, τ_i).
- L_{H_1}: It consists of tuples $(ID_i, X_i, R_i, P_{pub}, c_i)$.
- L_{H_2}: It consists of tuples (E_i, e_i).
- L_{H_3}: It consists of tuples $(ID_i, X_i, R_i, G_i, f_i)$.
- L_{H_4}: It consists of tuples $(ID_i, X_i, R_i, L_i, h_i)$.
- L_{U_i}: It consists of tuples $(ID_i, x_i, X_i, r_i, R_i, cert_i)$.

Phase 1: $\mathcal{A}_I$ adaptively issues the following polynomial bounded times queries.

H_0 **query**: $\mathcal{A}_I$ issues a query on (id_i, ξ_i), $\mathcal{B}$ checks the L_{H_0} and performs as follows:

- If the L_{H_0} contains (id_i, ξ_i, τ_i). $\mathcal{B}$ returns $\tau_i = H_0(id_i, \xi_i)$ to $\mathcal{A}_I$.
- If the L_{H_0} does not contain (id_i, ξ_i, τ_i), $\mathcal{B}$ randomly selects $\tau_i \in \mathbb{Z}_q^*$, adds (id_i, ξ_i, τ_i) into the L_{H_0} and returns τ_i to $\mathcal{A}_I$.

H_1 **query**: $\mathcal{A}_I$ issues a query on $(ID_i, X_i, R_i, P_{pub})$, $\mathcal{B}$ checks the L_{H_1} and performs as follows:

- If the L_{H_1} contains $(ID_i, X_i, R_i, P_{pub}, c_i)$, $\mathcal{B}$ returns $c_i = H_1(ID_i, X_i, R_i, P_{pub})$ to $\mathcal{A}_I$.
- If the L_{H_1} does not contain $(ID_i, X_i, R_i, P_{pub}, c_i)$, $\mathcal{B}$ randomly selects $c_i \in \mathbb{Z}_q^*$, adds $(ID_i, X_i, R_i, P_{pub}, c_i)$ into the L_{H_1} and returns c_i to $\mathcal{A}_I$.

H_2 **query**: $\mathcal{A}_I$ issues a query on E_i, $\mathcal{B}$ checks the L_{H_2} and performs as follows:

- If the L_{H_2} contains (E_i, e_i), $\mathcal{B}$ returns $e_i = H_2(E_i)$ to $\mathcal{A}_I$.
- If the L_{H_2} does not contain (E_i, e_i), $\mathcal{B}$ randomly selects $e_i \in \mathbb{Z}_q^*$, adds (E_i, e_i) into the L_{H_2} and returns e_i to $\mathcal{A}_I$.

H_3 **query**: $\mathcal{A}_I$ issues a query on (ID_i, X_i, R_i, G_i), $\mathcal{B}$ checks the L_{H_3} and performs as follows:

- If the L_{H_3} contains $(ID_i, X_i, R_i, G_i, f_i)$, $\mathcal{B}$ returns $f_i = H_3(ID_i, X_i, R_i, G_i)$ to $\mathcal{A}_I$.
- If the L_{H_3} does not contain $(ID_i, X_i, R_i, G_i, f_i)$, $\mathcal{B}$ randomly selects $f_i \in \mathbb{Z}_q^*$, adds $(ID_i, X_i, R_i, G_i, f_i)$ into the L_{H_3} and returns f_i to $\mathcal{A}_I$.

H_4 **query**: $\mathcal{A}_I$ issues a query on (ID_i, X_i, R_i, L_i), $\mathcal{B}$ checks the L_{H_4} and performs as follows:

- If the L_{H_4} contains $(ID_i, X_i, R_i, L_i, h_i)$, $\mathcal{B}$ returns $h_i = H_4(ID_i, X_i, R_i, L_i)$ to $\mathcal{A}_I$.
- If the L_{H_4} does not contain $(ID_i, X_i, R_i, L_i, h_i)$, $\mathcal{B}$ randomly selects $h_i \in \mathbb{Z}_q^*$, adds $(ID_i, X_i, R_i, L_i, h_i)$ into the L_{H_4} and returns h_i to $\mathcal{A}_I$.

Create user query: $\mathcal{A}_I$ issues a create user query on ID_i, $\mathcal{B}$ checks the L_{U_i}. If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_I$. Otherwise, $\mathcal{B}$ performs as follows:

- If $ID_i \in ID_r^*$, $\mathcal{B}$ randomly selects x_i, $r_i \in \mathbb{Z}_q^*$ and computes $X_i = x_iP$, $R_i = r_iP$, Then, $\mathcal{B}$ adds $(ID_i, x_i, X_i, r_i, R_i, \perp)$ into the L_{U_i}. Finally, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_I$.
- If $ID_i \notin ID_r^*$, $\mathcal{B}$ randomly selects x_i, $cert_i$, $c_i \in \mathbb{Z}_q^*$ and computes $X_i = x_iP$, $R_i = cert_iP - c_iP_{pub}$. If c_i already appear in the L_{H_1}, $\mathcal{B}$ randomly selects $cert_i \in \mathbb{Z}_q^*$ and tries again. Then, $\mathcal{B}$ adds $(ID_i, x_i, X_i, \perp, R_i, cert_i)$ and $(ID_i, X_i, R_i, P_{pub}, c_i)$ into the L_{U_i} and the L_{H_1}, respectively. Finally, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_I$.

Private key query: $\mathcal{A}_I$ issues a query on ID_i, $\mathcal{B}$ checks the L_{U_i} and performs as follows:

- If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ returns x_i to $\mathcal{A}_I$.
- If the L_{U_i} does not contain $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ performs the create user query on ID_i and returns x_i to $\mathcal{A}_I$.

Certificate query: $\mathcal{A}_I$ issues a certificate query on ID_i, $\mathcal{B}$ performs as follows:

- If $ID_i \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_i \notin ID_r^*$, $\mathcal{B}$ checks the L_{U_i} and performs as follows:
  - If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ returns $cert_i$ to $\mathcal{A}_I$.
  - If the L_{U_i} does not contain $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ performs the create user query on ID_i and returns $cert_i$ to $\mathcal{A}_I$.

Public key replacement query: $\mathcal{A}_I$ issues a query on ID_i with $\{X_i', R_i'\}$, $\mathcal{B}$ checks the L_{U_i} and performs as follows:

- If $ID_i \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_i \notin ID_r^*$, $\mathcal{B}$ performs as follows:
  - If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ sets $X_i = X_i'$, $R_i = R_i'$, $x_i = \perp$, $r_i = \perp$, $cert_i = \perp$, and adds $(ID_i, \perp, X_i', \perp, R_i', \perp)$ into the L_{U_i}.
  - If the L_{U_i} does not contain $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ performs the create user query on ID_i, and sets $X_i = X_i'$, $R_i = R_i'$, $x_i = \perp$, $r_i = \perp$, $cert_i = \perp$, and adds $(ID_i, \perp, X_i', \perp, R_i', \perp)$ into the L_{U_i}.

Signcryption query: $\mathcal{A}_I$ issues a query on the messages $\{m_{r_1}, m_{r_2}, \cdots, m_{r_n}\}$ under the sender ID_s and the receivers $\{ID_{r_1}, ID_{r_2}, \cdots, ID_{r_n}\}$. $\mathcal{B}$ performs as follows:

- If $ID_s \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_s \notin ID_r^*$, $\mathcal{B}$ performs the private key query on ID_s to obtain x_s, the certificate query on ID_s to obtain $cert_s$, and the create user query on ID_{r_i} to obtain $\{X_{r_i}, R_{r_i}\}(i = 1, 2, \cdots, n)$. Finally, $\mathcal{B}$ generates the ciphertext $C_s = \{L_s, G_s, \sigma_s\}$ according to the proposed certificate-based MMSC scheme, and returns the ciphertext C_s to $\mathcal{A}_I$.

Unsigncryption query: $\mathcal{A}_I$ issues an unsigncryption query on $C_s = \{L_s, G_s, \sigma_s\}$ under ID_s and ID_{r_i}. $\mathcal{B}$ performs as follows:

- If $ID_{r_i} \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_{r_i} \notin ID_r^*$, $\mathcal{B}$ performs the private key query on ID_{r_i} to obtain x_{r_i} and the certificate query on ID_{r_i} to obtain $cert_{r_i}$. Then, $\mathcal{B}$ unsigncrypts C_s according to the proposed certificate-based MMSC scheme, and returns the message m_{r_i} to $\mathcal{A}_I$.

Challenge: $\mathcal{A}_I$ randomly selects two messages $m_0^* = \{m_{0,r_1}^*, m_{0,r_2}^*, \cdots, m_{0,r_n}^*\}$ and $m_1^* = \{m_{1,r_1}^*, m_{1,r_2}^*, \cdots, m_{1,r_n}^*\}$ of equal length, and then sends them to $\mathcal{B}$. $\mathcal{B}$ randomly selects $\beta \in \{0, 1\}$ and generates the ciphertext C_s^* on $m_\beta^* = \{m_{\beta,r_1}^*, m_{\beta,r_2}^*, \cdots, m_{\beta,r_n}^*\}$ under ID_s^* and ID_r^* as follows:

- If $ID_s^* \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_s^* \notin ID_r^*$, $\mathcal{B}$ performs the create user query on $ID_{r_i}^*$ to obtain $(ID_{r_i}^*, x_{r_i}^*, X_{r_i}^*, r_{r_i}^*, R_{r_i}^*, \perp)$, the H_1 query on $(ID_{r_i}^*, X_{r_i}^*, R_{r_i}^*, P_{pub})$ to obtain $c_{r_i}^*$, the private key query on ID_s^* to obtain x_s^*, and the certificate query on ID_s^* to obtain $cert_s^*$. Then, $\mathcal{B}$ computes $L_s^* = bP, E_{r_i}^* = x_{r_i}^* bP + r_{r_i}^* bP + c_{r_i}^* Z$, and performs the H_2 query on $E_{r_i}^*$ to obtain $e_{r_i}^*$, where $i = 1, 2, \cdots, n$. Finally, $\mathcal{B}$ generates G_s^* and σ_s^* according to the proposed certificate-based MMSC scheme, and returns the ciphertext $C_s^* = \{L_s^*, G_s^*, \sigma_s^*\}$ to $\mathcal{A}_I$.

Phase 2: $\mathcal{A}_I$ adaptively issues the query in Phase 1 except that it cannot issue the certificate query on $ID_{r_i}^*(i = 1, 2, \cdots, n)$, the signcryption query on m_β^* under ID_s^* and ID_r^*, and the unsigncryption query on C_s^* under ID_s^* and ID_r^*.

Guess: $\mathcal{A}_I$ outputs $\beta' \in \{0, 1\}$ as its guess. If $\beta = \beta'$ holds, $\mathcal{B}$ outputs 1 indicating that $Z = abP$. Otherwise, $\mathcal{B}$ outputs 0.

Probability analysis: Supposing $\mathcal{A}_I$ can issue at most q_{H_i} hash $H_i(i = 0, 1, 2, 3, 4)$ queries, q_c create user queries, q_{pri} private key queries, q_{cert} certificate queries, q_{pub} public key replacement queries, q_s signcryption queries and q_u unsigncryption queries. The following two events are defined:

- E_1: $\mathcal{B}$ does not abort in the create user query, certificate query, public key replacement query, signcryption query and unsigncryption query.
- E_2: $\mathcal{B}$ correctly outputs β.

In accordance with the above simulation, we are able to get $\Pr[E_1] \geq (1 - \frac{q_{H_1}}{q})^{q_c}(1 - \frac{1}{q_{H_1}})^{q_{cert}+q_{pub}+q_s+q_u}$, $\Pr[E_2|E_1] \geq \varepsilon$, so the success probability of $\mathcal{B}$ is displayed as:

$$\begin{aligned}\varepsilon' &= \Pr[E_1 \wedge E_2] \\ &\geq \Pr[E_1]\Pr[E_2|E_1] \\ &\geq (1 - \frac{q_{H_1}}{q})^{q_c}(1 - \frac{1}{q_{H_1}})^{q_{cert}+q_{pub}+q_s+q_u}\varepsilon.\end{aligned}$$

By the above analysis, we get conclusion that $\mathcal{B}$ breaks the IND-CCA-I secure with non-negligible advantage $\varepsilon' \geq (1 - \frac{q_{H_1}}{q})^{q_c}(1 - \frac{1}{q_{H_1}})^{q_{cert}+q_{pub}+q_s+q_u}\varepsilon$ in time $t' \leq t + (3q_c + (2n + 1)q_s + 5q_u)t_{sm}$, where t_{sm} is the runtime of scalar multiplication calculation on ECC. This conflicts with the DDH assumption, therefore, the proposed certificate-based MMSC scheme meets the confidentiality.

Lemma 2: The proposed certificate-based MMSC scheme is IND-CCA-II secure in ROM under DDH assumption.

Proof: Assuming that $\mathcal{A}_{II}$ wins the Game 2 with probability ε in time t, we can build an algorithm $\mathcal{B}$ to break DDH assumption with probability ε' in time t'. Given an instance (P, aP, bP, Z) of DDH assumption, $\mathcal{B}$'s goal is to decide whether $Z = abP$ holds.

Initialization: $\mathcal{A}_{II}$ selects the challenging identities $ID_r^* = \{ID_{r_1}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$ as the receivers, and sends them to $\mathcal{B}$.

Setup: $\mathcal{B}$ randomly selects $s \in \mathbb{Z}_q^*$ as master key and calculates $P_{pub} = sP$. Then, $\mathcal{B}$ returns s and $params = \{q, p, P, \mathbb{G}, P_{pub}, H_0, H_1, H_2, H_3, H_4\}$ to $\mathcal{A}_{II}$.

Phase 1: $\mathcal{A}_{II}$ adaptively issues the following polynomial bounded times queries.

$H_i(i = 0, 1, 2, 3, 4)$ **query**: It is the same as Lemma 1.

Create user query: $\mathcal{A}_{II}$ issues a create user query on ID_i, $\mathcal{B}$ checks the L_{U_i}. If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_{II}$. Otherwise, $\mathcal{B}$ performs as follows:

- If $ID_i \in ID_r^*$, $\mathcal{B}$ randomly selects x_i, r_i, $c_i \in \mathbb{Z}_q^*$ and computes $X_i = x_i aP, R_i = r_i P, cert_i = r_i + s \cdot c_i$. Then, $\mathcal{B}$ adds $(ID_i, x_i, X_i, r_i, R_i, cert_i)$ and $(ID_i, X_i, R_i, P_{pub}, c_i)$ into the L_{U_i} and the L_{H_1}, respectively. Finally, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_{II}$.
- If $ID_i \notin ID_r^*$, $\mathcal{B}$ produces $(ID_i, x_i, X_i, r_i, R_i, cert_i)$ according to the proposed certificate-based MMSC scheme, and returns $\{X_i, R_i\}$ to $\mathcal{A}_{II}$.

Private key query: $\mathcal{A}_{II}$ issues a query on ID_i, $\mathcal{B}$ performs as follows:

- If $ID_{r_i} \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_{r_i} \notin ID_r^*$, $\mathcal{B}$ checks the L_{U_i} and performs as follows:
  - If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ returns x_i to $\mathcal{A}_{II}$.
  - If the L_{U_i} does not contain $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ performs the create user query on ID_i and returns x_i to $\mathcal{A}_{II}$.

Signcryption query: $\mathcal{A}_I$ issues a query on the messages $\{m_{r_1}, m_{r_2}, \cdots, m_{r_n}\}$ under the sender ID_s and the receivers $\{ID_{r_1}, ID_{r_2}, \cdots, ID_{r_n}\}$. $\mathcal{B}$ performs as follows:

- If $ID_s \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_s \notin ID_r^*$, $\mathcal{B}$ performs the private key query on ID_s to obtain x_s and the create user query on ID_{r_i} to obtain $\{X_{r_i}, R_{r_i}\}(i = 1, 2, \cdots, n)$. Finally, $\mathcal{B}$ generates the ciphertext $C_s = \{L_s, G_s, \sigma_s\}$ according to the proposed certificate-based MMSC scheme, and returns the ciphertext C_s to $\mathcal{A}_I$.

Unsigncryption query: $\mathcal{A}_{II}$ issues an unsigncryption query on $C_s = \{L_s, G_s, \sigma_s\}$ under ID_s and ID_{r_i}. $\mathcal{B}$ performs as follows:

- If $ID_{r_i} \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_{r_i} \notin ID_r^*$, $\mathcal{B}$ performs the private key query on ID_{r_i} to obtain x_{r_i}. Then, $\mathcal{B}$ unsigncrypts C_s according to the proposed certificate-based MMSC scheme, and returns m_{r_i} to $\mathcal{A}_{II}$.

Challenge: $\mathcal{A}_{II}$ randomly selects two messages $m_0^* = \{m_{0,r_1}^*, m_{0,r_2}^*, \cdots, m_{0,r_n}^*\}$ and $m_1^* = \{m_{1,r_1}^*, m_{1,r_2}^*, \cdots, m_{1,r_n}^*\}$

of equal length, and then sends them to $\mathcal{B}$. $\mathcal{B}$ randomly selects $\beta \in \{0, 1\}$ and computes the ciphertext C_s^* on $m_\beta^* = \{m_{\beta,r_1}^*, m_{\beta,r_2}^*, \cdots, m_{\beta,r_n}^*\}$ under ID_s^* and ID_r^* as follows:

- If $ID_s^* \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_s^* \notin ID_r^*$, $\mathcal{B}$ performs the create user query on $ID_{r_i}^*$ to obtain $(ID_{r_i}^*, x_{r_i}^*, X_{r_i}^*, r_{r_i}^*, R_{r_i}^*, cert_{r_i}^*)$, the H_1 query on $(ID_{r_i}^*, X_{r_i}^*, R_{r_i}^*, P_{pub})$ to obtain $c_{r_i}^*$, and the private key query on ID_s^* to obtain x_s^*. Then, $\mathcal{B}$ computes $L_s^* = bP$, $E_{r_i}^* = x_{r_i}^* Z + r_{r_i}^* bP + c_{r_i}^* sbP$, and performs the H_2 query on $E_{r_i}^*$ to obtain $e_{r_i}^*$, where $i = 1, 2, \cdots, n$. Finally, $\mathcal{B}$ produces G_s^* and σ_s^* according to the proposed certificate-based MMSC scheme, and returns the ciphertext $C_s^* = \{L_s^*, G_s^*, \sigma_s^*\}$ to $\mathcal{A}_{II}$.

Phase 2: $\mathcal{A}_{II}$ adaptively issues the query in Phase 1 except that it is unable to issue the private key query on $ID_{r_i}^*(i = 1, 2, \cdots, n)$, the signcryption query on m_β^* under ID_s^* and ID_r^*, and the unsigncryption query on C_s^* under ID_s^* and ID_r^*.

Guess: $\mathcal{A}_{II}$ outputs $\beta' \in \{0, 1\}$ as its guess. If $\beta = \beta'$ holds, $\mathcal{B}$ outputs 1 indicating that $Z = abP$. Otherwise, $\mathcal{B}$ outputs 0.

Probability analysis: Supposing $\mathcal{A}_{II}$ can issue at most q_{H_i} hash $H_i(i = 0, 1, 2, 3, 4)$ queries, q_c create user queries, q_{pri} private key queries, q_s signcryption queries and q_u unsigncryption queries. The following two events are defined:

- E_1: $\mathcal{B}$ does not abort in the private key query, signcryption query and unsigncryption query.
- E_2: $\mathcal{B}$ correctly outputs β.

In accordance with the above simulation, we are able to get $\Pr[E_1] \geq (1 - \frac{1}{q_{H_1}})^{q_{pri}+q_s+q_u}$, $\Pr[E_2|E_1] \geq \varepsilon$, so the success probability of $\mathcal{B}$ is displayed as:

$$\begin{aligned}\varepsilon' &= \Pr[E_1 \wedge E_2] \\ &\geq \Pr[E_1]\Pr[E_2|E_1] \\ &\geq (1 - \frac{1}{q_{H_1}})^{q_{pri}+q_s+q_u}\varepsilon.\end{aligned}$$

By the above analysis, we get conclusion that $\mathcal{B}$ breaks the IND-CCA-II secure with non-negligible advantage $\varepsilon' \geq (1 - \frac{1}{q_{H_1}})^{q_{pri}+q_s+q_u}\varepsilon$ in time $t' \leq t + (2q_c + (2n + 1)q_s + 5q_u)t_{sm}$. This conflicts with the DDH assumption, therefore, the proposed certificate-based MMSC scheme meets the confidentiality.

Theorem 2: The proposed certificate-based MMSC scheme is EUF-CMA secure in ROM under ECDL assumption.

Proof: Theorem 2 is able to be proved by the Lemma 3 and Lemma 4.

Lemma 3: The proposed certificate-based MMSC scheme is EUF-CMA-I secure in ROM under ECDL assumption.

Proof: Assuming that $\mathcal{A}_I$ wins the Game 3 with probability ε in time t, we can build an algorithm $\mathcal{B}$ to break ECDL assumption with probability ε' in time t'. Given an instance (P, aP) of ECDL assumption, $\mathcal{B}$'s goal is to compute a.

Initialization: $\mathcal{A}_I$ selects the challenging identity ID_s^* as the sender, and sends it to $\mathcal{B}$.

Setup: $\mathcal{B}$ sets $P_{pub} = aP$, and returns $params = \{q, p, P, \mathbb{G}, P_{pub}, H_0, H_1, H_2, H_3, H_4\}$ to $\mathcal{A}_I$.

Query: $\mathcal{A}_I$ adaptively issues the following polynomial bounded times queries.

$H_i(i = 0, 1, 2, 3, 4)$ **query**: It is the same as Lemma 1.

Create user query: $\mathcal{A}_I$ issues a create user query on ID_i, $\mathcal{B}$ checks the L_{U_i}. If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_I$. Otherwise, $\mathcal{B}$ performs as follows:

- If $ID_i = ID_s^*$, $\mathcal{B}$ randomly selects x_i, $r_i \in \mathbb{Z}_q^*$ and computes $X_i = x_i P$, $R_i = r_i P$. Then, $\mathcal{B}$ adds $(ID_i, x_i, X_i, r_i, R_i, \perp)$ into the L_{U_i}. Finally, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_I$.
- If $ID_i \neq ID_s^*$, $\mathcal{B}$ randomly selects x_i, $cert_i$, $c_i \in \mathbb{Z}_q^*$ and computes $X_i = x_i P$, $R_i = cert_i P - c_i P_{pub}$. If c_i already appear in the L_{H_1}, $\mathcal{B}$ randomly selects another $cert_i \in \mathbb{Z}_q^*$ and tries again. Then, $\mathcal{B}$ adds $(ID_i, x_i, X_i, \perp, R_i, cert_i)$ and $(ID_i, X_i, R_i, P_{pub}, c_i)$ into the L_{U_i} and the L_{H_1}, respectively. Finally, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_I$.

Private key query: It is the same as Lemma 1.

Certificate query: $\mathcal{A}_I$ issues a certificate query on ID_i, $\mathcal{B}$ performs as follows:

- If $ID_i = ID_s^*$, $\mathcal{B}$ aborts the game.
- If $ID_i \neq ID_s^*$, $\mathcal{B}$ checks the L_{U_i} and performs as follows:
  - If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ returns $cert_i$ to $\mathcal{A}_I$.
  - If the L_{U_i} does not contain $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ performs the create user query on ID_i and returns $cert_i$ to $\mathcal{A}_I$.

Public key replacement query: $\mathcal{A}_I$ issues a query on ID_i with $\{X_i', R_i'\}$, $\mathcal{B}$ checks the L_{U_i} and performs as follows:

- If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ sets $X_i = X_i'$, $R_i = R_i'$, $x_i = \perp$, $r_i = \perp$, $cert_i = \perp$, and adds $(ID_i, \perp, X_i', \perp, R_i', \perp)$ into the L_{U_i}.
- If the L_{U_i} does not contain $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ performs the create user query on ID_i, and sets $X_i = X_i'$, $R_i = R_i'$, $x_i = \perp$, $r_i = \perp$, $cert_i = \perp$, and adds $(ID_i, \perp, X_i', \perp, R_i', \perp)$ into the L_{U_i}.

Signcryption query: $\mathcal{A}_I$ issues a query on the messages $\{m_{r_1}, m_{r_2}, \cdots, m_{r_n}\}$ under the sender ID_s and the receivers $\{ID_{r_1}, ID_{r_2}, \cdots, ID_{r_n}\}$, $\mathcal{B}$ performs as follows:

- If $ID_s = ID_s^*$, $\mathcal{B}$ performs the create user query on ID_s to obtain $\{X_s, R_s\}$, and the H_1 query on $(ID_s, X_s, R_s, P_{pub})$ to obtain c_s. Then, $\mathcal{B}$ randomly selects $f_s, h_s, \sigma_s \in \mathbb{Z}_q^*$ and computes $L_s = (h_s)^{-1}(\sigma_s P - f_s X_s - R_s - c_s aP)$. If the h_s already appears in the L_{H_4}, $\mathcal{B}$ randomly selects another $\sigma_s \in \mathbb{Z}_q^*$ and tries again. $\mathcal{B}$ adds $(ID_s, X_s, R_s, G_s, f_s)$ and $(ID_s, X_s, R_s, L_s, h_s)$ into the L_{H_3} and the L_{H_4}, respectively. Finally, $\mathcal{B}$ produces G_s according to the proposed certificate-based MMSC scheme, and returns the ciphertext $C_s = \{L_s, G_s, \sigma_s\}$ to $\mathcal{A}_I$.
- If $ID_s \neq ID_s^*$, $\mathcal{B}$ performs the private key query on ID_s to obtain x_s, the certificate query on ID_s to obtain $cert_s$, and the create user query on ID_{r_i} to obtain $\{X_{r_i}, R_{r_i}\}(i = 1, 2, \cdots, n)$. Then, $\mathcal{B}$ produces the ciphertext $C_s = \{L_s, G_s, \sigma_s\}$ according to the proposed certificate-based MMSC scheme, and returns C_s to $\mathcal{A}_I$.

Unsigncryption query: $\mathcal{A}_I$ issues an unsigncryption query on $C_s = \{L_s, G_s, \sigma_s\}$ under ID_s and ID_{r_i}. $\mathcal{B}$ performs the private key query on ID_{r_i} to obtain x_{r_i}, and the certificate query on ID_{r_i} to obtain $cert_{r_i}$. Then, $\mathcal{B}$ unsigncrypts C_s according to the proposed certificate-based MMSC scheme, and returns m_{r_i} to $\mathcal{A}_I$.

Forgery: $\mathcal{A}_I$ outputs a forged ciphertexts $C_s^* = \{L_s^*, G_s^*, \sigma_s^*\}$ on the messages $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under the sender ID_s^* and the receivers $\{ID_{r_1}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$. Based on the forking lemma [60], $\mathcal{B}$ produces another valid ciphertext $C_s^{*'} = \{L_s^*, G_s^*, \sigma_s^{*'}\}$ by choosing different H_1. Due to both ciphertexts are valid, the following two equations are able to be obtain:

$$\sigma_s^* P = f_s^* X_s^* + R_s^* + c_s^* aP + h_s^* L_s^*,$$
$$\sigma_s^{*'} P = f_s^* X_s^* + R_s^* + c_s^{*'} aP + h_s^* L_s^*.$$

We can obtain the equation:

$$(\sigma_s^* - \sigma_s^{*'})P = (c_s^* - c_s^{*'})aP.$$

$\mathcal{B}$ outputs $a = (\sigma_s^* - \sigma_s^{*'})(c_s^* - c_s^{*'})^{-1}$ as a solution to the given ECDL problem.

Probability analysis: Supposing $\mathcal{A}_I$ can issue at most q_{H_i} hash $H_i(i = 0, 1, 2, 3, 4)$ queries, q_c create user queries, q_{pri} private key queries, q_{cert} certificate queries, q_{pub} public key replacement queries, q_s signcryption queries and q_u unsigncryption queries. The following three events are defined:

- E_1: $\mathcal{B}$ never aborts the create user query, certificate query and signcryption query.
- E_2: $\mathcal{B}$ outputs a valid ciphertext.
- E_3: $ID_i = ID_s^*$.

In accordance with the above simulation, we are able to get $\Pr[E_1] \geq (1 - \frac{q_{H_1}}{q})^{q_c}(1 - \frac{1}{q_{H_1}})^{q_{cert}}(1 - \frac{q_{H_4}}{q})^{q_s}$, $\Pr[E_2|E_1] \geq \varepsilon$, $\Pr[E_3|E_1 \wedge E_2] \geq \frac{1}{q_{H_1}}$, so the probability that $\mathcal{B}$ solves the ECDL problem is displayed as:

$$\begin{aligned}\varepsilon' &= \Pr[E_1 \wedge E_2 \wedge E_3] \\ &\geq \Pr[E_1]\Pr[E_2|E_1]\Pr[E_3|E_1 \wedge E_2] \\ &\geq \frac{1}{q_{H_1}}(1 - \frac{q_{H_1}}{q})^{q_c}(1 - \frac{1}{q_{H_1}})^{q_{cert}}(1 - \frac{q_{H_4}}{q})^{q_s}\varepsilon.\end{aligned}$$

By the above analysis, we get conclusion that $\mathcal{B}$ breaks the ECDL problem with non-negligible advantage $\varepsilon' \geq \frac{1}{q_{H_1}}(1 - \frac{q_{H_1}}{q})^{q_c}(1 - \frac{1}{q_{H_1}})^{q_{cert}}(1 - \frac{q_{H_4}}{q})^{q_s}\varepsilon$ in time $t' \leq t + (3q_c + (2n + 3)q_s + 5q_u)t_{sm}$. This conflicts with the ECDL assumption, therefore, the proposed certificate-based MMSC scheme meets the unforgeability.

Lemma 4: The proposed certificate-based MMSC scheme is EUF-CMA-II secure in ROM under ECDL assumption.

Proof: Assuming that $\mathcal{A}_{II}$ wins the Game 4 with probability ε in time t, we can build an algorithm $\mathcal{B}$ to break ECDL assumption with probability ε' in time t'. Given an instance (P, aP) of ECDL assumption, $\mathcal{B}$'s goal is to compute a.

Initialization: $\mathcal{A}_{II}$ selects the challenging identity ID_s^* as the sender, and sends it to $\mathcal{B}$.

Setup: $\mathcal{B}$ randomly selects $s \in \mathbb{Z}_q^*$ as master key and calculates $P_{pub} = sP$. Then, $\mathcal{B}$ returns s and $params = \{q, p, P, \mathbb{G}, P_{pub}, H_0, H_1, H_2, H_3, H_4\}$ to $\mathcal{A}_{II}$.

Query: $\mathcal{A}_{II}$ adaptively issues the following polynomial bounded times queries.

$H_i(i = 0, 1, 2, 3, 4)$ **query**: It is the same as Lemma 1.

Create user query: $\mathcal{A}_{II}$ issues a create user query on ID_i, $\mathcal{B}$ checks the L_{U_i}. If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_{II}$. Otherwise, $\mathcal{B}$ performs as follows:

- If $ID_i = ID_s^*$, $\mathcal{B}$ randomly selects r_i, $c_i \in \mathbb{Z}_q^*$ and computes $X_i = aP$, $R_i = r_i P$, $cert_i = r_i + s \cdot c_i$. Then, $\mathcal{B}$ adds $(ID_i, \perp, X_i, r_i, R_i, cert_i)$ into the L_{U_i}. Finally, $\mathcal{B}$ returns $\{X_i, R_i\}$ to $\mathcal{A}_{II}$.
- If $ID_i \neq ID_s^*$, $\mathcal{B}$ produces $(ID_i, x_i, X_i, r_i, R_i, cert_i)$ according to the proposed certificate-based MMSC scheme, and returns $\{X_i, R_i\}$ to $\mathcal{A}_{II}$.

Private key query: $\mathcal{A}_{II}$ issues a query on ID_i, $\mathcal{B}$ performs as follows:

- If $ID_i = ID_s^*$, $\mathcal{B}$ aborts the game.
- If $ID_i \neq ID_s^*$, $\mathcal{B}$ checks the L_{U_i} and performs as follows:
  - If the L_{U_i} contains $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ returns x_i to $\mathcal{A}_{II}$.
  - If the L_{U_i} does not contain $(ID_i, x_i, X_i, r_i, R_i, cert_i)$, $\mathcal{B}$ performs the create user query on ID_i and returns x_i to $\mathcal{A}_{II}$.

Signcryption query: $\mathcal{A}_{II}$ issues a query on the messages $\{m_{r_1}, m_{r_2}, \cdots, m_{r_n}\}$ under the sender ID_s and the receivers $\{ID_{r_1}, ID_{r_2}, \cdots, ID_{r_n}\}$, $\mathcal{B}$ performs as follows:

- If $ID_s = ID_s^*$, $\mathcal{B}$ performs the create user query on ID_s to obtain $\{X_s, R_s\}$, and the H_1 query on $(ID_s, X_s, R_s, P_{pub})$ to obtain c_s. Then, $\mathcal{B}$ randomly selects f_s, h_s, $\sigma_s \in \mathbb{Z}_q^*$ and computes $L_s = (h_s)^{-1}(\sigma_s P - f_s aP - R_s - c_s P_{pub})$. If the h_s already appears in the L_{H_4}, $\mathcal{B}$ randomly selects another $\sigma_s \in \mathbb{Z}_q^*$ and tries again. $\mathcal{B}$ adds $(ID_s, X_s, R_s, G_s, f_s)$ and $(ID_s, X_s, R_s, L_s, h_s)$ into the L_{H_3} and the L_{H_4}, respectively. Finally, $\mathcal{B}$ produces G_s according to the proposed certificate-based MMSC scheme, and returns the ciphertext $C_s = \{L_s, G_s, \sigma_s\}$ to $\mathcal{A}_{II}$.
- If $ID_s \neq ID_s^*$, $\mathcal{B}$ performs the private key query on ID_s to obtain x_s, and the create user query on ID_{r_i} to obtain $\{X_{r_i}, R_{r_i}\}(i = 1, 2, \cdots, n)$. Then, $\mathcal{B}$ produces the ciphertext $C_s = \{L_s, G_s, \sigma_s\}$ according to the proposed certificate-based MMSC scheme, and returns C_s to $\mathcal{A}_{II}$.

Unsigncryption query: $\mathcal{A}_{II}$ issues an unsigncryption query on $C_s = \{L_s, G_s, \sigma_s\}$ under ID_s and $\{ID_{r_1}, ID_{r_2}, \cdots, ID_{r_n}\}$. $\mathcal{B}$ performs the private key query on ID_{r_i} to obtain x_{r_i}. Then, $\mathcal{B}$ unsigncrypts C_s according to the proposed certificate-based MMSC scheme, and returns m_{r_i} to $\mathcal{A}_{II}$.

Forgery: $\mathcal{A}_{II}$ outputs a forged ciphertexts $C_s^* = \{L_s^*, G_s^*, \sigma_s^*\}$ on the messages $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under the sender ID_s^* and the receivers $\{ID_{r_1}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$. Based on the forking lemma [60], $\mathcal{B}$ produces another valid ciphertext $C_s^{*'} = \{L_s^*, G_s^*, \sigma_s^{*'}\}$ by choosing a different H_3. Due to both ciphertexts are valid, the following two equations are able to

be obtain:

$$\sigma_s^* P = f_s^* aP + R_s^* + c_s^* P_{pub} + h_s^* L_s^*,$$
$$\sigma_s^{*'} P = f_s^{*'} aP + R_s^* + c_s^* P_{pub} + h_s^* L_s^*.$$

We can obtain the equation:

$$(\sigma_s^* - \sigma_s^{*'})P = (f_s^* - f_s^{*'})aP.$$

$\mathcal{B}$ outputs $a = (\sigma_s^* - \sigma_s^{*'})(f_s^* - f_s^{*'})^{-1}$ as a solution to the given ECDL problem.

Probability analysis: Supposing $\mathcal{A}_{II}$ can issue at most q_{H_i} hash $H_i (i = 0, 1, 2, 3, 4)$ queries, q_c create user queries, q_{pri} private key queries, q_s signcryption queries and q_u unsigncryption queries. The following three events are defined:

- E_1: $\mathcal{B}$ never aborts the private key query and signcryption query.
- E_2: $\mathcal{B}$ outputs a valid ciphertext.
- E_3: $ID_i = ID_s^*$.

In accordance with the above simulation, we are able to get $\Pr[E_1] \geq (1 - \frac{1}{q_{H_1}})^{q_{pri}}(1 - \frac{q_{H_4}}{q})^{q_s}$, $\Pr[E_2|E_1] \geq \varepsilon$, $\Pr[E_3|E_1 \wedge E_2] \geq \frac{1}{q_{H_1}}$, so the probability that $\mathcal{B}$ solves the ECDL problem is displayed as:

$$\begin{aligned}\varepsilon' &= \Pr[E_1 \wedge E_2 \wedge E_3] \\ &\geq \Pr[E_1]\Pr[E_2|E_1]\Pr[E_3|E_1 \wedge E_2] \\ &\geq \frac{1}{q_{H_1}}(1 - \frac{1}{q_{H_1}})^{q_{pri}}(1 - \frac{q_{H_4}}{q})^{q_s}\varepsilon.\end{aligned}$$

By the above analysis, we get conclusion that $\mathcal{B}$ breaks the ECDL problem with non-negligible advantage $\varepsilon' \geq \frac{1}{q_{H_2}}(1 - \frac{1}{q_{H_1}})^{q_{pri}}(1 - \frac{q_{H_4}}{q})^{q_s}\varepsilon$ in time $t' \leq t + (2q_c + (2n + 4)q_s + 5q_u)t_{sm}$. This conflicts with the ECDL assumption, therefore, the proposed certificate-based MMSC scheme meets the unforgeability.

Theorem 3: The proposed certificate-based MMSC scheme is ANON-IND-CCA secure in ROM under DDH assumption.

Proof: Theorem 3 is able to be proved by the Lemma 5 and Lemma 6.

Lemma 5: The proposed certificate-based MMSC scheme is ANON-IND-CCA-I secure in ROM under DDH assumption.

Proof. Assuming that $\mathcal{A}_I$ wins the Game 5 with probability ε in time t, we can build an algorithm $\mathcal{B}$ to break DDH assumption with probability ε' in time t'. Given an instance (P, aP, bP, Z) of DDH assumption, $\mathcal{B}$'s goal is to decide whether $Z = abP$ holds.

Initialization: $\mathcal{A}_I$ selects the challenging identities $ID_r^* = \{ID_{r_0}^*, ID_{r_1}^*\}$, and sends them to $\mathcal{B}$.

Setup: $\mathcal{B}$ sets $P_{pub} = aP$, and returns $params = \{q, p, P, \mathbb{G}, P_{pub}, H_0, H_1, H_2, H_3, H_4\}$ to $\mathcal{A}_I$.

Phase 1: It is the same as Lemma 1.

Challenge: $\mathcal{A}_I$ selects the messages $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$, the sender ID_s^* and the receivers $\{ID_{r_2}^*, ID_{r_3}^*, \cdots, ID_{r_n}^*\}$, and then sends them to $\mathcal{B}$. $\mathcal{B}$ randomly selects $\beta \in \{0, 1\}$ and generates the ciphertext C_s^* on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$ as follows:

- If $ID_s^* \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_s^* \notin ID_r^*$, $\mathcal{B}$ performs the create user query on $ID_{r_i}^*$ to obtain $(ID_{r_i}^*, x_{r_i}^*, X_{r_i}^*, r_{r_i}^*, R_{r_i}^*, \perp)$, the H_1 query on $(ID_{r_i}^*, X_{r_i}^*, R_{r_i}^*, P_{pub})$ to obtain $c_{r_i}^*$, the private key query on ID_s^* to obtain x_s^*, and the certificate query on ID_s^* to obtain $cert_s^*$. Then, $\mathcal{B}$ computes $L_s^* = bP$, $E_{r_i}^* = x_{r_i}^* bP + r_{r_i}^* bP + c_{r_i}^* Z$, and performs the H_2 query on $E_{r_i}^*$ to obtain $e_{r_i}^*$, where $i = \beta, 2, \cdots, n$. Finally, $\mathcal{B}$ produces G_s^* and σ_s^* according to the proposed certificate-based MMSC scheme, and returns the ciphertext $C_s^* = \{L_s^*, G_s^*, \sigma_s^*\}$ to $\mathcal{A}_I$.

Phase 2: $\mathcal{A}_I$ adaptively issues the query in Phase 1 except that it cannot issue the certificate query on $ID_{r_\beta}^*$, the signcryption query on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$, and the unsigncryption query on C_s^* under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$.

Guess: $\mathcal{A}_I$ outputs $\beta' \in \{0, 1\}$ as its guess. If $\beta = \beta'$ holds, $\mathcal{B}$ outputs 1 indicating that $Z = abP$. Otherwise, $\mathcal{B}$ outputs 0.

Probability analysis: It is the same as Lemma 1.

We get conclusion that $\mathcal{B}$ breaks the ANON-IND-CCA-I secure with non-negligible advantage $\varepsilon' \geq (1 - \frac{q_{H_1}}{q})^{q_c}(1 - \frac{1}{q_{H_1}})^{q_{cert}+q_{pub}+q_s+q_u}\varepsilon$ in time $t' \leq t + (3q_c + (2n+1)q_s + 5q_u)t_{sm}$. This conflicts with the DDH assumption, therefore, the proposed certificate-based MMSC scheme meets the receiver anonymity.

Lemma 6: The proposed certificate-based MMSC scheme is ANON-IND-CCA-II secure in ROM under DDH assumption.

Proof: Assuming that $\mathcal{A}_{II}$ wins the Game 6 with probability ε in time t, we can build an algorithm $\mathcal{B}$ to break DDH assumption with probability ε' in time t'. Given an instance (P, aP, bP, Z) of DDH assumption, $\mathcal{B}$'s goal is to decide whether $Z = abP$ holds.

Initialization: $\mathcal{A}_{II}$ selects the challenging identities $ID_r^* = \{ID_{r_0}^*, ID_{r_1}^*\}$, and sends them to $\mathcal{B}$.

Setup: $\mathcal{B}$ randomly selects $s \in \mathbb{Z}_q^*$ as master key and calculates $P_{pub} = sP$. Then, $\mathcal{B}$ returns s and $params = \{q, p, P, \mathbb{G}, P_{pub}, H_0, H_1, H_2, H_3, H_4\}$ to $\mathcal{A}_{II}$.

Phase 1: It is the same as Lemma 2.

Challenge: $\mathcal{A}_{II}$ selects the messages $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$, the sender ID_s^* and the receivers $\{ID_{r_2}^*, ID_{r_3}^*, \cdots, ID_{r_n}^*\}$, and then sends them to $\mathcal{B}$. $\mathcal{B}$ randomly selects $\beta \in \{0, 1\}$ and generates the ciphertext C_s^* on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$ as follows:

- If $ID_s^* \in ID_r^*$, $\mathcal{B}$ aborts the game.
- If $ID_s^* \notin ID_r^*$, $\mathcal{B}$ performs the create user query on $ID_{r_i}^*$ to obtain $(ID_{r_i}^*, x_{r_i}^*, X_{r_i}^*, r_{r_i}^*, R_{r_i}^*, cert_{r_i}^*)$, the H_1 query on $(ID_{r_i}^*, X_{r_i}^*, R_{r_i}^*, P_{pub})$ to obtain $c_{r_i}^*$, and the private key query on ID_s^* to obtain x_s^*. Then, $\mathcal{B}$ computes $L_s^* = bP$, $E_{r_i}^* = x_{r_i}^* Z + r_{r_i}^* bP + c_{r_i}^* sbP$, and performs the H_2 query on $E_{r_i}^*$ to obtain $e_{r_i}^*$, where $i = \beta, 2, \cdots, n$. Finally, $\mathcal{B}$ produces G_s^* and σ_s^* according to the proposed

TABLE 2. Security comparisons.

Scheme	Seo *et al.*'s scheme [43]	Han *et al.*'s scheme [44]	Qiu *et al.*'s scheme [45]	Niu *et al.*'s scheme [46]	Qiu *et al.*'s scheme [47]	Pang *et al.*'s scheme [48]	Peng *et al.*'s scheme [49]	The proposed scheme
Public key setting	PKI	PKI	ID	ID and CL	ID and CL	CL	CL	CB
Confidentiality	√	√	√	√	√	×	√	√
Unforgeability	×	×	√	√	√	×	√	√
Receiver anonymity	√	√	√	√	√	√	√	√
Sender anonymity	×	×	×	√	×	×	×	√
Decryption fairness	√	√	×	×	×	√	×	√
No certificate management burden	×	×	√	√	√	√	√	√
Key escrow freeness	√	√	×	×	√	√	√	√
Public channel	×	×	×	×	√	×	×	√

certificate-based MMSC scheme, and returns the ciphertext $C_s^* = \{L_s^*, G_s^*, \sigma_s^*\}$ to $\mathcal{A}_{II}$.

Phase 2: $\mathcal{A}_{II}$ adaptively issues the query in Phase 1 except that it is unable to issue the private key query on $ID_{r_\beta}^*$, the signcryption query on $\{m_{r_1}^*, m_{r_2}^*, \cdots, m_{r_n}^*\}$ under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$, and the unsigncryption query on C_s^* under ID_s^* and $\{ID_{r_\beta}^*, ID_{r_2}^*, \cdots, ID_{r_n}^*\}$.

Guess: $\mathcal{A}_{II}$ outputs $\beta' \in \{0, 1\}$ as its guess. If $\beta = \beta'$ holds, $\mathcal{B}$ outputs 1 indicating that $Z = abP$. Otherwise, $\mathcal{B}$ outputs 0.

Probability analysis: It is the same as Lemma 2.

We get conclusion that $\mathcal{B}$ breaks the ANON-IND-CCA-II secure with non-negligible advantage $\varepsilon' \geq (1 - \frac{1}{q_{H_1}})^{q_{pri}+q_s+q_u}\varepsilon$ in time $t' \leq t + (2q_c + (2n + 1)q_s + 5q_u)t_{sm}$. This conflicts with the DDH assumption, therefore, the proposed certificate-based MMSC scheme meets the receiver anonymity.

B. SECURITY ANALYSIS

1) CONFIDENTIALITY

In accordance with Theorem 1, any PPT adversary is not able to calculate patient's health data due to the DDH assumption, therefore, the confidentiality could be achieved in the proposed certificate-based MMSC scheme.

2) UNFORGEABILITY

According to Theorem 2, no PPT adversary can forge a valid data report due to difficulty of the ECDL problem, hence the unforgeability could be provided in the proposed certificate-based MMSC scheme.

3) RECEIVER ANONYMITY

Based on Theorem 3, for any data report, any healthcare professionals cannot judge whether others are receivers of the data report, and hence the receiver anonymity can be achieved in the proposed certificate-based MMSC scheme.

4) SENDER ANONYMITY

According to the proposed MMSC scheme, the patient's real identity id_s is only contained in the random pseudo identity $ID_s = H_0(id_s, \xi_s)$. Due to the collision resistance of the hash function H_0, for any PPT adversary, it is impossible to extract patient's real identity id_s from the pseudo identity ID_s, and thus the sender anonymity could be met in the proposed certificate-based MMSC scheme.

5) DECRYPTION FAIRNESS

From the equation $f(e_{r_i}) = g_{n-1}e_{r_i}^{n-1} + \cdots + g_1 e_{r_i} + g_0 = m_{r_i}$, any authorized healthcare professional has the same ability to achieve his/her own corresponding health data m_{r_i} by making use of e_{r_i}, thus the decryption fairness can be provided in the proposed certificate-based MMSC scheme.

Security comparisons between the MMSC schemes [43]–[49] and the proposed certificate-based MMSC scheme are illustrated in Table 2, in which "√" represents "meet" and "×" denotes "not meet".

In accordance with Table 2, Seo *et al.*'s scheme [43] and Han *et al.*'s scheme [44] are not able to provide unforgeability, sender anonymity and decryption fairness. Furthermore, them exist certificate management problem and need secure channel as a result of the use of the PKI-based cryptography. Qiu *et al.*'s scheme [45] is not able to satisfy sender anonymity and decryption fairness. Moreover, it suffers key escrow issue and needs secure channel due to utilizing the ID-based cryptography. Niu *et al.*'s scheme [46] is unable to achieve decryption fairness. In addition, it exists key escrow issue and needs secure channel because of using the ID-based cryptography and CL-based cryptography. Qiu *et al.*'s scheme [47] is not able to satisfy the sender anonymity and decryption fairness. Pang *et al.*'s scheme [48] is unable to meet confidentiality, unforgeability and sender anonymity. Peng *et al.*'s scheme [49] could not achieve sender anonymity and decryption fairness. Besides, the existing MMSC schemes [48], [49] require of the secure channel owing to using the CL-based cryptography. By the contrast, the proposed certificate-based MMSC scheme is able to provide all security requirements.

VI. PERFORMANCE EVALUATION

A. COMPUTATION COST

Analysis and comparison of the computation costs between the MMSC schemes [43]–[49] and the proposed certificate-based MMSC scheme are displayed in this subsection.

To realize fair comparison, the MMSC schemes [43]–[49] and the proposed certificate-based MMSC scheme are compared under the 80-bit security level. With regard to the pairing-based MMSC schemes [43]–[46], we select the bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, where $\mathbb{G}_1$ is the additive group formed by super singular elliptic curve $E : y^2 = x^3 + x \bmod p$, p is 512-bit random primer number, q is 160-bit random Solinas prime number and $q \cdot 12 \cdot r = p + 1$. For the

MMSC schemes [47]–[49] and the proposed certificate-based MMSC scheme, we choose the additive group $\mathbb{G}$ formed by elliptic curve $E : y^2 = x^3 + ax + b \bmod p$, p are 160-bits random prime number, $a = -3$ and b is 160-bits prime number.

The runtime of cryptographic operations are able to be obtained by means of the MIRACL Crypto SDK [61]. The test could be run on the 64-bit Windows 7 system with i7 CPU, 1.8 GHz-4.9 GHz and 8 GB memory. The average runtime of cryptographic operations running 10000 times are listed in Table 3.

TABLE 3. Runtime of cryptographic operations (millisecond).

Notations	Descriptions	Runtime
T_{m-ecc}	Scalar multiplication operation in ECC	0.3851
T_e	Scalar exponentiation operation in $\mathbb{G}_1$	1.4202
T_h	Map to point hash operation	3.5819
T_{pe}	Pairing-based exponentiation operation	0.5203
T_p	Bilinear pairing operation	10.3092
T_{se}	Symmetric encryption (AES)	0.0024
T_{sd}	Symmetric decryption (AES)	0.0028

Computation cost between the proposed certificate-based MMSC scheme and existing MMSC schemes [43]–[49] are compared in Table 4.

For the computation cost of signcryption, Seo *et al.*'s scheme [43] requires to run $n + 1$ scalar exponentiation operations in $\mathbb{G}_1$ and n symmetric encryption, the total time thus is $1.4226n+1.4202$ ms. Han *et al.*'s scheme [44] requires to run $3n + 1$ scalar exponentiation operations in $\mathbb{G}_1$ and n map to point hash operations, therefore the total time is $7.8425n + 1.4202$ ms. Qiu *et al.*'s scheme [45] requires to run one scalar exponentiation operation in $\mathbb{G}_1$, $n + 1$ map to point hash operations and n bilinear pairing operations, and hence the total time is $13.8911n + 5.0021$ ms. Niu *et al.*'s scheme [46] requires to run $2n + 2$ scalar exponentiation operations in $\mathbb{G}_1$, $2n$ pairing-based exponentiation operations and one symmetric encryption, hence the total time thus is $3.8810n + 2.8428$ ms. Qiu *et al.*'s scheme [47] requires to run $2n + 2$ scalar multiplication operations in ECC and one symmetric encryption, so the total time is $0.7702n + 0.7726$ ms. Pang *et al.*'s scheme [48] requires to run $2n + 1$ scalar multiplication operations in ECC and one symmetric encryption, thence the total time is $0.7702n + 0.7726$ ms. Peng *et al.*'s scheme [49] requires to run $2n+1$ scalar multiplication operations in ECC and n symmetric encryption, and then the total time thus is $0.7726n + 0.3851$ ms. In the single-receiver signcryption scheme, sending a message to one receiver requires to run three scalar multiplication operations in ECC, sending n messages to n receivers requires to run $3n$ scalar multiplication operations in ECC. Hence, the total time is $1.1553n$ ms. The proposed certificate-based MMSC scheme requires to run $2n+1$ scalar multiplication operations in ECC, therefore the total time thus is $0.7702n + 0.3851$ ms.

For the computation cost of unsigncryption, Seo *et al.*'s scheme [43] requires to run three exponentiation operations in $\mathbb{G}_1$ and one symmetric decryption, the total time thus is 4.2634 ms. Han *et al.*'s scheme [44] requires to run one scalar exponentiation operation in $\mathbb{G}_1$, one map to point hash and two bilinear pairing operations, therefore the total time is 25.6205 ms. Qiu *et al.*'s scheme [45] requires to run two scalar exponentiation operations in $\mathbb{G}_1$, one map to point hash and one bilinear pairing operation, and hence the total time is 16.7315 ms. Niu *et al.*'s scheme [46] requires to run one scalar exponentiation operation in $\mathbb{G}_1$, four bilinear pairing operations and one symmetric decryption, hence the total time is 42.6598 ms. Qiu *et al.*'s scheme [47] requires to run five scalar multiplication operations in ECC and one symmetric encryption, so the total time is 1.9283 ms. Pang *et al.*'s scheme [48] requires to four scalar multiplication operations in ECC and one symmetric encryption, thence the total time is 1.5432 ms. Peng *et al.*'s scheme [49] requires to run four scalar multiplication operations in ECC and one symmetric encryption, and then the total time is 1.5432 ms. The single-receiver signcryption scheme requires to run five scalar multiplication operations in ECC, therefore the total time thus is 1.9255 ms. The proposed certificate-based MMSC scheme requires to run five scalar multiplication operations in ECC, therefore the total time thus is 1.9255 ms.

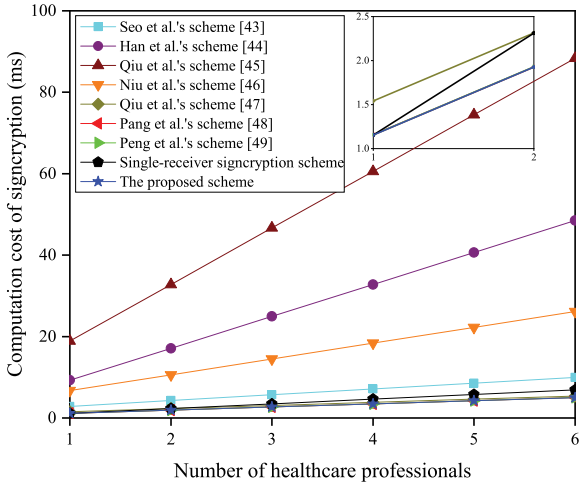

FIGURE 3. Computation costs of signcryption.

From Figure 3, we could know that computation cost of signcryption increases linearly with the growth of healthcare professionals, the proposed certificate-based MMSC scheme has the lowest slope and smallest computation cost compared with the MMSC schemes [43]–[49] and the single-receiver signcryption scheme.

As displayed in Figure 4, the computation cost of unsigncryption in the proposed certificate-based MMSC scheme is the smallest than the MMSC schemes [43]–[47]; the computation cost of unsigncryption are 1.9255 ms in the proposed certificate-based MMSC scheme, which is reduced by 54.8%, 92.5%, 88.5%, 95.5% and 0.2% compared with the MMSC schemes [43]–[47], respectively; the computation cost of unsigncryption in the MMSC schemes [48], [49] is the smaller compared with the proposed certificate-based MMSC scheme, but Peng *et al.*'s scheme [49] declared that

TABLE 4. Comparison of computation cost.

Schemes	Signcryption	Unsigncryption
Seo *et al.*'s scheme [43]	$(n+1)T_e + nT_{se}$ $= 1.4226n + 1.4202$ ms	$3T_e + T_{sd}$ $= 4.2634$ ms
Han *et al.*'s scheme [44]	$(3n+1)T_e + nT_h$ $= 7.8425n + 1.4202$ ms	$T_e + T_h + 2T_p$ $= 25.6205$ ms
Qiu *et al.*'s scheme [45]	$T_e + (n+1)T_h + nT_p$ $= 13.8911n + 5.0021$ ms	$2T_e + T_h + T_p$ $= 16.7315$ ms
Niu *et al.*'s scheme [46]	$(2n+2)T_e + 2nT_{pe} + T_{se}$ $= 3.8810n + 2.8428$ ms	$T_e + 4T_p + T_{sd}$ $= 42.6598$ ms
Qiu *et al.*'s scheme [47]	$(2n+2)T_{m-ecc} + T_{se}$ $= 0.7702n + 0.7726$ ms	$5T_{m-ecc} + T_{sd}$ $= 1.9283$ ms
Pang *et al.*'s scheme [48]	$(2n+1)T_{m-ecc} + T_{se}$ $= 0.7702n + 0.3875$ ms	$4T_{m-ecc} + T_{sd}$ $= 1.5432$ ms
Peng *et al.*'s scheme [49]	$(2n+1)T_{m-ecc} + nT_{se}$ $= 0.7726n + 0.3851$ ms	$4T_{m-ecc} + T_{sd}$ $= 1.5432$ ms
Single-receiver signcryption scheme	$3nT_{m-ecc}$ $= 1.1553n$ ms	$5T_{m-ecc}$ $= 1.9255$ ms
The proposed scheme	$(2n+1)T_{m-ecc}$ $= 0.7702n + 0.3851$ ms	$5T_{m-ecc}$ $= 1.9255$ ms

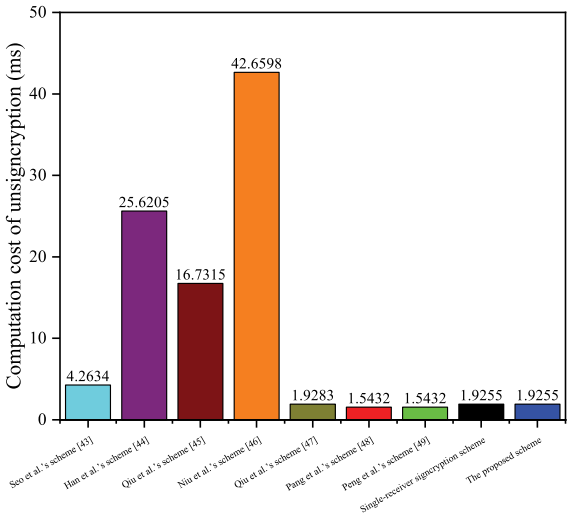

FIGURE 4. Computation costs of unsigncryption.

Pang *et al.*'s scheme [48] fails to satisfy the unforgeability and confidentiality. Besides, Peng *et al.*'s scheme [49] is unable to not satisfy the sender anonymity and decryption fairness; the computation cost of unsigncryption in the single-receiver signcryption scheme is the same as the proposed certificate-based MMSC scheme.

B. COMMUNICATION COST

Communication cost of the proposed certificate-based MMSC scheme and existing MMSC schemes [43]–[49] are evaluated in this subsection. According to the above analysis, the length of elements in $\mathbb{G}_1$, $\mathbb{G}$ and $\mathbb{Z}_q^*$ are 64 bytes, 20 bytes and 20 bytes, respectively. Comparison result of communication cost is demonstrated in Table 5.

TABLE 5. Comparison result of communication cost.

Schemes	Data report size
Seo *et al.*'s scheme [43]	$128n + 20$ bytes
Han *et al.*'s scheme [44]	$64n + 64$ bytes
Qiu *et al.*'s scheme [45]	$64n + 148$ bytes
Niu *et al.*'s scheme [46]	$128n + 192$ bytes
Qiu *et al.*'s scheme [47]	$20n + 80$ bytes
Pang *et al.*'s scheme [48]	$20n + 80$ bytes
Peng *et al.*'s scheme [49]	$20n + 40$ bytes
Single-receiver signcryption scheme	$60n$ bytes
The proposed scheme	$20n + 40$ bytes

In the Seo *et al.*'s scheme [43], the data report size is

$$|c_1| + |c_2| + \cdots + |c_n| + |r_1| + |r_2| + \cdots + |r_n| + |s| = n|\mathbb{G}_1| + n|\mathbb{G}_1| + |\mathbb{Z}_q^*| = 128n + 20 \ bytes.$$

In the Han *et al.*'s scheme [44], the data report size is

$$|U| + |Z_1| + |Z_2| + \cdots + |Z_n| = n|\mathbb{G}_1| + n|\mathbb{G}_1| = 64n + 64 \ bytes.$$

In the Qiu *et al.*'s scheme [45], the data report size is

$$|c| + |r| + |w| + |V| = |\mathbb{G}_1| + |\mathbb{G}_1| + n|\mathbb{G}_1| + |\mathbb{Z}_q^*| = 64n + 148 \ bytes.$$

In the Niu *et al.*'s scheme [46], the data report size is

$$|C| + |U_1| + |U_2| + |S| + |\varphi| = |\mathbb{G}_1| + |\mathbb{G}_1| + |\mathbb{G}_1| + n|\mathbb{G}_1| + n|\mathbb{G}_1| = 128n + 192 \ bytes.$$

In the Qiu *et al.*'s scheme [47], the data report size is

$$|S| + |R_2| + |v| + |h| + |A| = |\mathbb{G}| + |\mathbb{G}| + |\mathbb{Z}_q^*| + |\mathbb{Z}_q^*| + n|\mathbb{Z}_q^*| = 20n + 80 \ bytes.$$

In the Pang *et al.*'s scheme [48], the data report size is

$$|c_0| + |c_1| + \cdots + |c_{n-1}| + |R| + |V| + |w| + |z| = n|\mathbb{Z}_q^*| + |\mathbb{G}| + |\mathbb{G}| + |\mathbb{Z}_q^*| + |\mathbb{Z}_q^*| = 20n + 80 \ bytes.$$

In the Peng *et al.*'s scheme [49], the data report size is

$$|C| + |e| + |f| = n|\mathbb{G}| + |\mathbb{Z}_q^*| + |\mathbb{Z}_q^*| = 20n + 40 \ bytes.$$

In the single-receiver signcryption scheme, the data report size of sending a message to one receiver is $|L_s|+|C_s|+|\sigma_s| = |\mathbb{G}| + |\mathbb{Z}_q^*| + |\mathbb{Z}_q^*| = 60$ *bytes*; the data report size of sending n messages to n receivers is

$$n(|L_s| + |C_s| + |\sigma_s|) = n(|\mathbb{G}| + |\mathbb{Z}_q^*| + |\mathbb{Z}_q^*|) = 60n \ bytes.$$

In the proposed certificate-based MMSC scheme, the data report size is

$$|L_s| + |G_s| + |\sigma_s| = |\mathbb{G}| + n|\mathbb{Z}_q^*| + |\mathbb{Z}_q^*| = 20n + 40 \ bytes.$$

As shown in Figure 5, the communication cost increases linearly with the growth of healthcare professionals, the proposed certificate-based MMSC scheme has the lowest slope and smallest communication cost compared with the MMSC schemes [43]–[48] and single-receiver encryption scheme; the communication cost in the proposed certificate-based MMSC scheme is the same as that in the Peng *et al.*'s scheme [49], but Peng *et al.*'s scheme [49] could not provide the sender anonymity and decryption fairness.

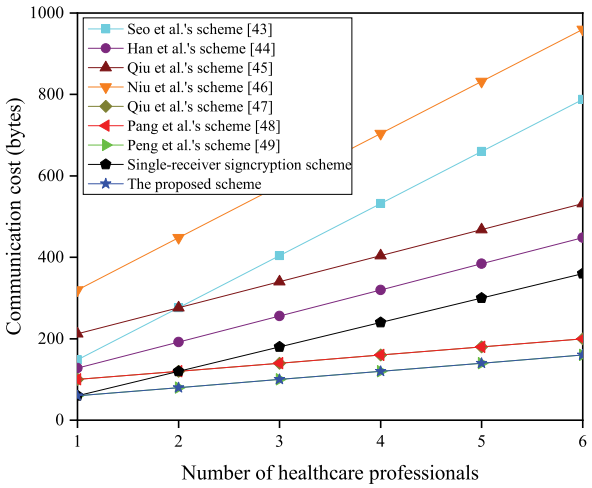

FIGURE 5. Comparison of communication.

VII. CONCLUSION

In this paper, an efficient anonymous certificate-based MMSC scheme for healthcare IoT is first presented by utilizing the certificate-based cryptography and the ECC, it avoids the problem of certificate management, key escrow and key distribution. Furthermore, the analysis of security displays that it could satisfy the confidentiality, unforgeability, receiver anonymity, sender anonymity and decryption fairness, with the performance evaluation indicating that it is the more effective in terms of computation and communication cost.

REFERENCES

[1] S. Xu, Y. Li, R. H. Deng, Y. Zhang, X. Luo, and X. Liu, "Lightweight and expressive fine-grained access control for healthcare Internet-of-Things," *IEEE Trans. Cloud Comput.*, early access, Aug. 20, 2019, doi: 10.1109/TCC.2019.2936481.

[2] G. Yang, L. Xie, M. Mäntysalo, X. Zhou, Z. Pang, L. D. Xu, S. Kao-Walter, Q. Chen, and L.-R. Zheng, "A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2180–2191, Nov. 2014.

[3] N. B. Gayathri, G. Thumbur, P. R. Kumar, M. Z. U. Rahman, P. V. Reddy, and A. Lay-Ekuakille, "Efficient and secure pairing-free certificateless aggregate signature scheme for healthcare wireless medical sensor networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 9064–9075, Oct. 2019.

[4] C. C. Chang and C. H. Li, "Algebraic secret sharing using privacy homomorphisms for IoT-based healthcare systems," *Math. Biosci. Eng.*, vol. 16, no. 5, pp. 3367–3381, 2019.

[5] Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare Internet-of-Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3610–3617, Aug. 2018.

[6] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured data collection with hardware-based ciphers for IoT-based healthcare," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 410–420, Feb. 2019.

[7] P. Porambage, A. Braeken, C. Schmitt, A. Gurtov, M. Ylianttila, and B. Stiller, "Group key establishment for enabling secure multicast communication in wireless sensor networks deployed for IoT applications," *IEEE Access*, vol. 3, pp. 1503–1511, 2015.

[8] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proc. IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[9] M. Bellare, A. Boldyreva, and S. Micali, "Public-key encryption in a multi-user setting: Security proofs and improvements," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2000, pp. 259–274.

[10] L. Lu and L. Hu, "Pairing-based multi-recipient public key encryption," in *Proc. Int. Conf. Secur. Manage.* Berlin, Germany: Springer, 2006, pp. 159–165.

[11] J. Baek, R. Safavi-Naini, and W. Susilo, "Efficient multi-receiver identity-based encryption and its application to broadcast encryption," in *Proc. Int. Workshop Public Key Cryptogr.* Berlin, Germany: Springer, 2005, pp. 380–397.

[12] C.-I. Fan, L.-Y. Huang, and P.-H. Ho, "Anonymous multireceiver identity-based encryption," *IEEE Trans. Comput.*, vol. 59, no. 9, pp. 1239–1249, Sep. 2010.

[13] H. Wang, Y. Zhang, H. Xiong, and B. Qin, "Cryptanalysis and improvements of an anonymous multi-receiver identity-based encryption scheme," *IET Inf. Secur.*, vol. 6, no. 1, pp. 20–27, 2012.

[14] H.-Y. Chien, "Improved anonymous multi-receiver identity-based encryption," *Comput. J.*, vol. 55, no. 4, pp. 439–446, Apr. 2012.

[15] Y.-M. Tseng, Y.-H. Huang, and H.-J. Chang, "Privacy-preserving multireceiver ID-based encryption with provable security," *Int. J. Commun. Syst.*, vol. 27, no. 7, pp. 1034–1050, Jul. 2014.

[16] J. Zhang and J. Mao, "An improved anonymous multi-receiver identity-based encryption scheme," *Int. J. Commun. Syst.*, vol. 28, no. 4, pp. 645–658, Mar. 2015.

[17] S. H. Islam, M. K. Khan, and A. M. Al-Khouri, "Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing," *Secur. Commun. Netw.*, vol. 8, no. 13, pp. 2214–2231, Sep. 2015.

[18] Y.-H. Hung, S.-S. Huang, Y.-M. Tseng, and T.-T. Tsai, "Efficient anonymous multireceiver certificateless encryption," *IEEE Syst. J.*, vol. 11, no. 4, pp. 2602–2613, Dec. 2017.

[19] D. He, H. Wang, L. Wang, J. Shen, and X. Yang, "Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices," *Soft Comput.*, vol. 21, no. 22, pp. 6801–6810, Nov. 2017.

[20] E. K. Win, T. Yoshihisa, Y. Ishi, T. Kawakami, Y. Teranishi, and S. Shimojo, "A lightweight multi-receiver encryption scheme with mutual authentication," in *Proc. IEEE 41st Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2017, pp. 491–497.

[21] Y. F. Tseng and C.-I. Fan, "Provably CCA-secure anonymous multi-receiver certificateless authenticated encryption," *J. Inf. Sci. Eng.*, vol. 34, no. 6, pp. 1517–1541, Nov. 2018.

[22] R. Gao, J. Zeng, and L. Deng, "Efficient certificateless anonymous multi-receiver encryption scheme without bilinear parings," *Math. Problems Eng.*, vol. 2018, pp. 1–13, Jul. 2018.

[23] C. Sur, C. D. Jung, and K. H. Rhee, "Multi-receiver certificate-based encryption and application to public key broadcast encryption," in *Proc. ECSIS Symp. Bio-Inspired, Learn., Intell. Syst. Secur.*, Aug. 2007, pp. 35–40.
[24] C.-I. Fan, P.-J. Tsai, J.-J. Huang, and W.-T. Chen, "Anonymous multi-receiver certificate-based encryption," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Oct. 2013, pp. 19–26.
[25] J. Li, L. Chen, Y. Lu, and Y. Zhang, "Anonymous certificate-based broadcast encryption with constant decryption cost," *Inf. Sci.*, vols. 454–455, pp. 110–127, Jul. 2018.
[26] L. Chen, J. Li, and Y. Zhang, "Anonymous certificate-based broadcast encryption with personalized messages," *IEEE Trans. Broadcast.*, early access, Apr. 27, 2020, doi: 10.1109/TBC.2020.2984974.
[27] L. Chen, J. Li, Y. Lu, and Y. Zhang, "Adaptively secure certificate-based broadcast encryption and its application to cloud storage service," *Inf. Sci.*, vol. 538, pp. 273–289, Oct. 2020.
[28] Y. Lu, J. Li, and Y. Zhang, "Privacy-preserving and pairing-free multirecipient certificateless encryption with keyword search for cloud-assisted IIoT," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2553–2562, Apr. 2020.
[29] Y. Han and X. Gui, "Multi-recipient signcryption for secure group communication," in *Proc. 4th IEEE Conf. Ind. Electron. Appl.*, May 2009, pp. 161–165.
[30] S. Duan and Z. Cao, "Efficient and provably secure multi-receiver identity-based signcryption," in *Proc. Australas. Conf. Inf. Secur. Privacy*. Berlin, Germany: Springer, 2006, pp. 195–206.
[31] S. Narayan and P. Udaya, "A probably secure multi-receiver identity-based signcryption using bilinear maps," in *Proc. Int. Conf. Secur. Cryptogr.* Berlin, Germany: Springer, 2007, pp. 305–308.
[32] Y. Yu, B. Yang, X. Huang, and M. Zhang, "Efficient identity-based signcryption scheme for multiple receivers," in *Proc. Int. Conf. Autonomic Trusted Comput.* Berlin, Germany: Springer, 2007, pp. 13–21.
[33] C.-H. Tan, "On the security of provably secure multi-receiver ID-based signcryption scheme," *IEICE Trans. Fundamentals Electron., Commun. Comput. Sci.*, vol. E91-A, no. 7, pp. 1836–1838, Jul. 2008.
[34] F. Li, H. Xiong, and X. Nie, "A new multi-receiver ID-based signcryption scheme for group communications," in *Proc. Int. Conf. Commun., Circuits Syst.*, Jul. 2009, pp. 296–300.
[35] Y. Ming, X. Zhao, and Y. Wang, "Multi-receiver identity-based signcryption scheme in the standard model," in *Proc. Int. Conf. Inf. Comput. Appl.* Berlin, Germany: Springer, 2010, pp. 487–494.
[36] B. Zhang and Q. Xu, "An ID-based anonymous signcryption scheme for multiple receivers secure in the standard model," in *Proc. Int. Conf. Adv. Comput. Sci. Inf. Technol.* Berlin, Germany: Springer, 2010, pp. 15–27.
[37] L. Wu, "An ID-based multi-receiver signcryption scheme in manet," *J. Theor. Appl. Inf. Technol.*, vol. 46, no. 1, pp. 120–124, 2012.
[38] L. Pang, H. Li, and Y. Wang, "nMIBAS: A novel multi-receiver ID-based anonymous signcryption with decryption fairness," *Comput. Informat.*, vol. 32, no. 3, pp. 441–460, 2013.
[39] C. Zhou, "Provably secure and efficient multi-receiver identity-based generalized signcryption scheme," in *Proc. 9th Asia Joint Conf. Inf. Secur.*, Sep. 2014, pp. 82–88.
[40] S. S. D. Selvi, S. S. Vivek, D. Shukla, and P. R. Chandrasekaran, "Efficient and provably secure certificateless multi-receiver signcryption," in *Proc. Int. Conf. Provable Secur.* Berlin, Germany: Springer, 2008, pp. 52–67.
[41] S. Miao, F. Zhang, and L. Zhang, "Cryptanalysis of a certificateless multi-receiver signcryption scheme," in *Proc. Int. Conf. Multimedia Inf. Netw. Secur.*, 2010, pp. 593–597.
[42] S. Ullah, L. Marcenaro, and B. Rinner, "Secure smart cameras by aggregate-signcryption with decryption fairness for multi-receiver IoT applications," *Sensors*, vol. 19, no. 327, pp. 1–22, 2019.
[43] M. Seo and K. Kim, "Electronic funds transfer protocol using domain-verifiable signcryption scheme," in *Proc. Int. Conf. Inf. Secur. Cryptol.* Berlin, Germany: Springer, 1999, pp. 269–277.
[44] Y. Han and X. Gui, "Adaptive secure multicast in wireless networks," *Int. J. Commun. Syst.*, vol. 22, no. 9, pp. 1213–1239, Sep. 2009.
[45] J. Qiu, J. Bai, X. Song, and S. Hou, "Secure and effcient multi-message and multi-receiver ID-based signcryption for rekeying in ad hoc networks," *J. Chongqing Univ. (English Edition)*, vol. 12, no. 2, pp. 91–96, 2013.
[46] S. Niu, L. Niu, X. Yang, C. Wang, and X. Jia, "Heterogeneous hybrid signcryption for multi-message and multi-receiver," *PLoS ONE*, vol. 12, no. 9, pp. 1–13, 2017.
[47] J. Qiu, K. Fan, K. Zhang, Q. Pan, H. Li, and Y. Yang, "An efficient multi-message and multi-receiver signcryption scheme for heterogeneous smart mobile IoT," *IEEE Access*, vol. 7, pp. 180205–180217, 2019.
[48] L. Pang, M. Wei, and H. Li, "Efficient and anonymous certificateless multi-message and multi-receiver signcryption scheme based on ECC," *IEEE Access*, vol. 7, pp. 24511–24526, 2019.
[49] C. Peng, J. Chen, M. S. Obaidat, P. Vijayakumar, and D. He, "Efficient and provably secure multi-receiver signcryption scheme for multicast communication in edge computing," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6056–6068, Jul. 2019.
[50] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.
[51] A. Shamir, "Identity-based cryptosystem and signature scheme," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 1985, pp. 120–126.
[52] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2003, pp. 452–473.
[53] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2003, pp. 272–293.
[54] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 1985, pp. 417–426.
[55] N. Koblitz, "Elliptic curve cryptosystem," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[56] J. Li, X. Huang, M. Hong, and Y. Zhang, "Certificate-based signcryption with enhanced security features," *Comput. Math. Appl.*, vol. 64, no. 6, pp. 1587–1601, Sep. 2012.
[57] Y. Ming and H. Cheng, "Efficient certificateless conditional privacy-preserving authentication scheme in VANETs," *Mobile Inf. Syst.*, vol. 2019, Feb. 2019, Art. no. 7593138.
[58] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2690, Aug. 2015.
[59] G. K. Verma, B. B. Singh, N. Kumar, O. Kaiwartya, and M. S. Obaidat, "PFCBAS: Pairing free and provable certificate-based aggregate signature scheme for the e-healthcare monitoring system," *IEEE Syst. J.*, vol. 14, no. 2, pp. 1704–1715, Jun. 2019.
[60] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 1996, pp. 387–398.
[61] Shamus Software Ltd. *Multi Precision Integer and Rational Arithmetic Cryptographic Library (MIRACL)*. Accessed: Jul. 1, 2020. [Online]. Available: http://www.certivox.com/miracl/

YANG MING (Member, IEEE) received the B.S. and M.S. degrees in mathematics from the Xi'an University of Technology, in 2002 and 2005, respectively, and the Ph.D. degree in cryptography from Xidian University, in 2008. He is currently a Professor with Chang'an University. His main research interests include cryptography and wireless network security.

XIAOPENG YU received the B.S. degree from Chang'an University, Xi'an, in 2017, where he is currently pursuing the master's degree. His main research interests include cryptography and wireless network security.

XIAOQIN SHEN received the B.S. degree in mathematics from the Xi'an University of Technology, in 2002, and the Ph.D. degree from Xi'an Jiaotong University, in 2007. She is currently a Professor with the Xi'an University of Technology. Her main research interests include cryptography and wireless network security.