





## Article

# A Multi-Message Multi-Receiver Signcryption Scheme with Edge Computing for Secure and Reliable Wireless Internet of Medical Things Communications

Insaf Ullah <sup>1</sup>, Muhammad Asghar Khan <sup>1</sup>, Ali Alkhalifah <sup>2</sup>, Rosdiadee Nordin <sup>3,\*</sup>,  
Mohammed H. Alsharif <sup>4,\*</sup>, Abdulaziz H. Alghtani <sup>5</sup> and Ayman A. Aly <sup>5</sup>

<sup>1</sup> Hamdard Institute of Engineering & Technology, Islamabad 44000, Pakistan; insafk@gmail.com (I.U.); khayyam2302@gmail.com (M.A.K.)

<sup>2</sup> Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia; a.alkhalifah@qu.edu.sa

<sup>3</sup> Department of Electrical, Electronic & Systems Engineering, Faculty of Engineering and Built Environment, Universiti Kebangsaan Malaysia, Bangi 43600, Selangor, Malaysia

<sup>4</sup> Department of Electrical Engineering, College of Electronics and Information Engineering, Sejong University, 209 Neungdong-ro, Gwangjin-gu, Seoul 05006, Korea

<sup>5</sup> Department of Mechanical Engineering, College of Engineering, Taif University, Taif 21944, Saudi Arabia; a.ghtani@tu.edu.sa (A.H.A.); aymanaly@tu.edu.sa (A.A.A.)

\* Correspondence: adee@ukm.edu.my (R.N.); malsharif@sejong.ac.kr (M.H.A.)



**Citation:** Ullah, I.; Khan, M.A.; Alkhalifah, A.; Nordin, R.; Alsharif, M.H.; Alghtani, A.H.; Aly, A.A. A Multi-Message Multi-Receiver Signcryption Scheme with Edge Computing for Secure and Reliable Wireless Internet of Medical Things Communications. *Sustainability* **2021**, *13*, 13184. <https://doi.org/10.3390/su132313184>

Academic Editor: Manuel Fernandez-Veiga

Received: 11 October 2021  
Accepted: 25 November 2021  
Published: 28 November 2021

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Abstract:** Thanks to recent advancements in biomedical sensors, wireless networking technologies, and information networks, traditional healthcare methods are evolving into a new healthcare infrastructure known as the Internet of Medical Things (IoMT). It enables patients in remote areas to obtain preventative or proactive healthcare services at a cheaper cost through the ease of time-independent interaction. Despite the many benefits of IoMT, the ubiquitously linked devices offer significant security and privacy concerns for patient data. In the literature, several multi-message and multi-receiver signcryption schemes have been proposed that use traditional public-key cryptography, identity-based cryptography, or certificateless cryptography methods to securely transfer patient health-related data from a variety of biomedical sensors to healthcare professionals. However, certificate management, key escrow, and key distribution are all complications with these methods. Furthermore, in terms of IoMT performance and privacy requirements, they are impractical. This article aims to include edge computing into an IoMT with secure deployment employing a multi-message and multi-receiver signcryption scheme to address these issues. In the proposed method, certificate-based signcryption and hyperelliptic curve cryptography (HECC) have been coupled for excellent performance and security. The cost study confirms that the proposed scheme is better than the existing schemes in terms of computational and communication costs.

**Keywords:** Internet of Things; hyperelliptic curve; multi-message and multi-receiver signcryption; certificate-based cryptography; edge computing; IoMT; 5G

## 1. Introduction

The Internet of Medical Things (IoMT) is an emerging paradigm in the IoT marketplace that can group all medical devices and applications over the Internet to collect, examine, and exchange physiological data of patients [1]. Figure 1 depicts the general architecture of the IoMT system, which includes a number of biomedical sensors, special embedded devices and wireless technologies. The biomedical sensors are used in IoMT settings to collect patient data such as breathing rate, blood pressure, chest noise, body temperature, breathing rate, electrocardiogram (ECG), and patient location, etc. Likewise, patient data can then be examined through special embedded devices such as computers, smartphones, and smartwatches, etc. [2]. Short-range wireless technologies

such as Bluetooth Low Energy (BLE), Wi-Fi, and Zigbee, among others, can be used to communicate collected and examined data. The special embedded devices (controllers) can be further linked to cloud servers using the Fifth Generation (5G) wireless connection for high storage and intense data processing. The collected data from the patient monitoring sensors are usually too large to be handled by the local server. It requires a high level of storage and computational capabilities. Fortunately, the emerging 5G mobile networking architecture includes a Multiaccess Edge Computing (MEC) facility. When MEC is used in an IoMT system, it provides high storage and intense processing capabilities. The healthcare professionals can access the cloud server to review the health information and provide the patient with the appropriate assistance. In addition, when any medical indicators of the patient appear irregular, healthcare professionals will immediately contact the patient to provide guidance and medical examinations [3–6]. Furthermore, patient data can be stored in the health information system as electronic health records, which are accessible to medical practitioners when patients visit the hospital.

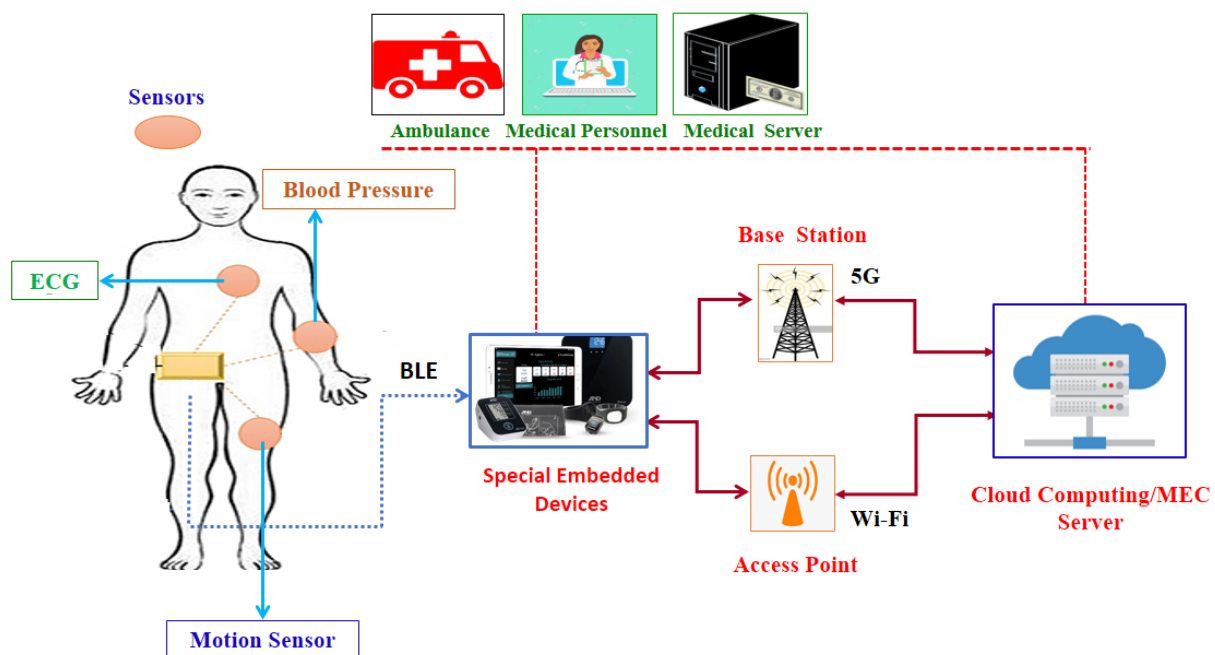


Figure 1. General architecture of the IoMT system.

On the one hand, the IoMT system provides several benefits, but on the other hand, the widespread use of linked devices over an open wireless channel raises significant security and privacy concerns [7–10]. In addition, most biomedical devices have limited computational resources and, as a result, fail to perform conventional cryptographic operations. To address these flaws, an integrated scheme known as "signcryption" can be employed [11–13]. Signcryption is a public key cryptographic scheme that performs both encryption and digital signature operations at the same time. It is much more efficient and cost-effective than any of the alternates, i.e., performing the encryption and digital signature individually. In addition, the Multi-message and Multi-receiver Signcryption (MMSC) method is an extension of the signcryption scheme in which multiple messages are transmitted in one ciphertext to multiple receivers [14]. The use of the multicast channel will speed up the communication process; however, the basic security features such as confidentiality, unforgeability and anonymity should be maintained.

To find the solution for the aforementioned security attributes, several Multi-message and Multi-receiver Signcryption (MMSC) schemes [15–21] have been proposed by using the Public Key Infrastructure (PKI)-based cryptography [22], Identity (ID)-based cryptography [23] or Certificateless (CL)-based cryptography [24]. However, the conventional PKI-based MMSC schemes suggested in [15,16] suffer from a heavy burden of certificate

management. In addition, the ID-based MMSC scheme introduced in [17] imposes the key escrow issue, while the heterogeneous ID-based and CL-based MMSC schemes implemented in [18,19] pose the key distribution problem. The CL-based MMSC schemes introduced in [20,21] bring about the key distribution problem. The schemes proposed in [15–21] either have poor performance in terms of computation cost or failure to meet the security requirements. In general, the proposed schemes are based on mathematical models that employ bilinear pairing or Elliptic Curve Cryptography (ECC), both of which have been proven to impose significant computational and communication burdens. In contrast to these two methods, Hyper Elliptic Curve Cryptography (HECC) is a lightweight cryptosystem, which provides the same level of security as opposed to ECC and bilinear pairing with a lower key size. In HECC, the key size is 80 bits, whereas ECC requires a key size of 160 bits.

### 1.1. Contributions

This article proposes a Multi-message Multi-receiver Signcryption (MMSC) scheme in a certificate-based setting. The proposed scheme is based on the concept of HECC, which is an enhanced version of the ECC that provides the same level of security as ECC and bilinear pairing with a smaller key size. Some of the key features that distinguish the contributions of our research in this work are as follows:

- Firstly, for an IoMT system, a multi-message and multi-receiver signcryption scheme has been proposed. In multicast channels under the Random Oracle Model (ROM), the proposed scheme guarantees confidentiality, unforgeability, and receiver anonymity.
- Secondly, for encryption and signature authentication, the proposed scheme makes use of hyperelliptic curve cryptography.
- Thirdly, we introduce a 5G architecture for IoMT with an edge computing facility.
- Finally, a thorough comparative analysis is performed to assess the performance of the proposed scheme. The findings show that the proposed scheme is efficient in terms of computation and communication costs from its counterpart schemes.

### 1.2. Organization of the Paper

The article is structured as follows. The related work is discussed in Section 2. The preliminaries are clarified in Section 3. The network model, threat model and syntax are provided in Section 4. The proposed scheme is provided in Section 5. Security analysis is carried out in Section 6. In Section 7, a performance comparison is carried out. Finally, the concluding ideas are included in Section 8.

## 2. Related Work

In this section, we examine and evaluate current MMSC schemes in terms of their research aims, security requirements, and computational and communication overheads.

In 2017, a heterogeneous MMSC scheme for ad hoc networks was proposed by Wang et al. [25]. In heterogeneous forms, the suggested scheme achieves a two-way signcryption that can move between PKI cryptography and IBC. Wang et al.'s [25] scheme uses PKI and IBC and thus creates an unavoidable key escrow issue as well as PKI certificate management burdens. Additionally, bilinear pairing is inefficient in terms of computation and communication costs due to the costly pairing operations. Niu et al. [18] implemented a heterogeneous MMSC signature later in the same year that can move from IBC under the ROM to certificateless cryptography. Unfortunately, Niu et al.'s scheme suffers from the problems such as private key distribution and key escrow. Furthermore, the scheme efficiency is based on bilinear pairing, which is not suitable for IoMT systems due to the high computation cost.

Gao et al. [20] proposed an efficient and practical certificateless signcryption scheme for wireless body area networks. The scheme is based exclusively on the widely used RSA cryptosystem and does not involve bilinear pairing. RSA is not suitable for IoMT because, like bilinear pairing, it is computationally costly. Pang et al. [26] constructed an

anonymous MMSC scheme under the ROM. The proposed scheme aimed to remove the issue encountered during the distribution of the partial private key. However, the efficiency of the given scheme is again based on ECC, which is comparatively inefficient in terms of computation cost as opposed to HECC.

In 2019, Pang et al. [27] proposed an anonymous and efficient certificateless MMSC scheme. The authors aimed to eliminate the key escrow problem, which is commonly linked with IBC, as well as the certificate management problem, which is associated with PKI-based cryptography. However, the given scheme needs a secure channel for the distribution of partial private keys and therefore suffers from partial private key distribution problems. In 2019, Peng et al. [21] suggested a certificateless MMSC scheme using ECC. However, for the delivery of partial private keys, the scheme needs a secure channel. Finally, in 2020, Ming et al. [28] proposed an efficient anonymous certificate-based MMSC scheme for healthcare Internet of Things. The proposed method is based on ECC and employs certificate-based cryptography. It eliminates certificate management, key escrow, and key distribution issues, but, owing to ECC, it incurs high computational cost.

All of the schemes discussed above are based on computationally complex problems of ECC and bilinear pairing. In this paper, we propose a lightweight and secure security scheme termed MMSC in a certificate-based setting using HECC. The HECC approach is suitable for the IoMT system since it facilitates small keys.

### 3. Preliminaries

This section includes some explanations about HEC and formal definitions as well as the notions used in the proposed scheme, which are illustrated in Table 1.

**Table 1.** Notations used in the proposed scheme.

S. No	Symbol	Explanation
1	$CA$	Certificate authority
2	$\mathcal{T}$	global parameter
3	$\delta$	secret key of CA
4	$Y$	public key of CA
5	$H\xi$	hyper elliptic curve
6	$\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$	one way hash functions
7	$D$	divisor of $H\xi$
8	$ID_s, ID_i$	identity of sender and multi receiver respectively
9	$\alpha_s, \alpha_i$	private key of sender and receivers
10	$\beta_s, \beta_i$	public key of sender and receivers
11	$CR_s, CR_i$	certificate of sender and receivers
12	$C_i, m_i$	multi-cipher text and multi-plaintext
13	$E_{\theta_i}, D_{\theta_i}$	encryption and decryption
14	$\theta_i$	multi-encryption and multi-decryption key

- Hyper Elliptic Curve

Suppose  $f$  represents a non-finite field and  $f^*$  is an algebraic closure of  $f$ . The following equation represents hyper elliptic curve ( $H\xi$ ) over  $f$  considering its solutions  $(\zeta, \iota)$  belong to  $f \times f$ , while  $g \geq 1$  is the genus.  $H\xi: \iota^2 + h(\zeta)\iota = F(\zeta)$ .

Therefore,  $h(\zeta)$  : a polynomial and belongs to  $f(\zeta)$  having degree at most  $g$ .  $F(\zeta)$  : represents a monic polynomial having degree is equal to  $2g + 1$ . The points on  $H\xi$  further form a set called Jacobian, which is the quotient group  $\mathcal{J} = \mathcal{D}^0 / \mathcal{P}$ , where  $\mathcal{D}^0$  represents zero-degree devisors and  $\mathcal{P}$  rational function-oriented devisors. Furthermore, each element of the Jacobian is represented as  $\mathcal{J}_{H\xi}(f)$  and can be denoted individually through a divisor  $D = \sum m_i P_i$ , and  $m_i$  represents a formal sum of points of  $f^*$ .

- Hyper Elliptic Curve Discrete Logarithm Problem (HECDLP)

Suppose given two devisors  $D_1$  and  $D_2$  belonging to  $\mathcal{J}_{H\xi}(f)$ , finding integer  $\rho$ , such that  $D_2 = \rho \cdot D_1$  is called HECDLP.

- Hyper Elliptic Curve Deffi–Helman Problem (HECDHP)

Suppose given two divisors  $D_1$  and  $D_2$  belonging to  $\mathcal{J}_{H_e}(f)$ , finding integer  $\rho$  and  $\omega$  such that  $D_2 = \omega \cdot \rho \cdot D_1$  is called HECDHP.

#### 4. Network Model, Threat Model and Syntax

In this section, we will define the network model, threat model and syntax of the proposed scheme.

##### 4.1. Network Model

The network model of the proposed certificate-based MMSC scheme consists of biomedical sensors, special embedded devices, ambulance, medical personal, medical server, cloud computing/MEC server and wireless technologies (BLE, Wi-Fi and 5G), as shown in Figure 1. Biomedical sensors can monitor and extract patient physiological data, which can further analyze with special embedded devices, such as smartphones, smartwatches or even a special embedded unit. Each of the biomedical sensors and the special embedded devices is wirelessly linked through short range communication technology known as BLE.

Special embedded devices can be further linked to the cloud computing/MEC server via Wi-Fi and 5G mobile communication to provide access. In addition, the medical server claims to be a local computer-attached administrator, where hospital professionals can view electronic health records (HERs) of patients. For future consultations, the HER is kept safely on the storage server.

##### 4.2. Threat Model

The threat model includes three games, which will be played among a malicious agent/forgery ( $\mathcal{MA}/\mathcal{MF}$ ) and a challenger  $\zeta$  [29]. The first game is played for confidentiality regarding indistinguishability in contradiction of adaptive chosen multi-ciphertext attacks (IND-CBMMS-CCA). In this game,  $\mathcal{MA}$  with non-ignorable advantages  $\epsilon$ , wants to break IND-CBMMS-CCA of a proposed CBMMS.  $\zeta$  selects a random number  $\delta$  and  $Y$ , then makes  $\mathcal{T}$  available to  $\mathcal{MA}$ . Furthermore,  $\mathcal{MA}$  selects  $ID_s^*$  as a sender identity,  $ID_i^*$  as receivers group identities, and two different natures but the same length set of messages ( $m^x_i, m^y_i$ ). Further,  $\zeta$  chooses  $\rho \in \{0, 1\}$ , to investigate which set of messages will be multi-signcryption. For this game  $\mathcal{MA}$  asks the queries such as  $\mathcal{H}_j(m_j)$ , Create Entity ( $ID_e$ ), Corrupt Entity ( $ID_e$ ), and multi-message multi-receiver signcryption, respectively.

The second game is played for unforgeability regarding existential forgeability against adaptive chosen multi-message attacks (EUF-CBMMS-CMA). In this game  $\mathcal{MF}$  with  $\epsilon$  can solve HECDLP with the help of  $\zeta$ .  $\zeta$  selects a random number  $\delta$  and  $Y$ , then makes  $\mathcal{T}$  available to  $\mathcal{MF}$ . Furthermore,  $\mathcal{MF}$  selects  $ID_s^*$  as a sender identity,  $ID_i^*$  as receivers group identities. For this game,  $\mathcal{MF}$  asks the queries such as  $\mathcal{H}_j(m_j)$ , Create Entity ( $ID_e$ ), Corrupt Entity ( $ID_e$ ), Multi-Message Multi-receiver Signcryption, and Multi-Message-Multi-receiver Un-signcryption, respectively.  $\mathcal{MF}$  can win this game if it is making the solution for HECDLP.

The third game is about anonymity property, e.g., anonymous indistinguishability beneath the taken multi-ciphertext attack (ANON-CBMMS-CCA). In this game,  $\mathcal{MA}$  with non-ignorable advantages  $\epsilon$  wants to break ANON-CBMMS-CCA of a proposed CBMMS.  $\zeta$  selects a random number  $\delta$  and  $Y$ , then makes  $\mathcal{T}$  available to  $\mathcal{MA}$ . Furthermore,  $\mathcal{MA}$  selects a target identity set TGL and two different natures but with the same set length of messages ( $m^x_i, m^y_i$ ). Further,  $\zeta$  chooses  $\rho \in \{0, 1\}$  to investigate which set of messages will be multi signcryption. For this game  $\mathcal{MA}$  ask the queries such as  $\mathcal{H}_j(m_j)$ , Create Entity ( $ID_e$ ), Corrupt Entity ( $ID_e$ ), and multi-message multi-receiver signcryption, respectively.

Note that the queries, such as  $\mathcal{H}_j(m_j)$ , Create Entity ( $ID_e$ ), Corrupt Entity ( $ID_e$ ), multi-message multi-receiver signcryption, and multi-message multi-receiver Un-signcryption, are defined clearly in Theorem1, Theorem 2, and Theorem 3 of the security analysis section.

### 4.3. Syntax

The following six steps the comprise syntax for the proposed CBMMS [24]:

1. **Setup:** A global parameter set  $\mathcal{T}$  is created by CA, then, CA selects  $\delta$  and computes  $\Upsilon$ , and sets  $\Upsilon$  and  $\delta$  is a public and private key.
2. **Set-Public-Variant:** An entity with identity  $ID_e$  chooses a random number  $v_e$ , computes  $\varphi_e$ , and sends a tuple  $(\varphi_e, ID_e)$  to CA.
3. **Set-Certificate:** For an entity with identity  $ID_e$ , CA selects a random number  $\chi_e$ , calculates  $\gamma_e$ , computes a certificate  $CR_e$ , calculates  $W_e$  and sends a tuple  $(W_e, CR_e)$  to CA.
4. **Set-Public-and-Private-Key:** An entity with identity  $ID_e$  computes  $\alpha_e$  as a private key and computes his/her public key as  $\beta_e$ .
5. **Multi-message-Multi-receiver Signcryption:** A sender with identity  $(ID_s)$  can take  $(ID_s, CR_s, \beta_s, m_i)$  as an in input and make a Multi-Message-Multi-receiver signcryption tuple  $\psi$ .
6. **Multi-message-Multi-receiver Un-signcryption:** Each recipient with identity  $(ID_i)$  can take the tuple  $\psi$  for verification of a multi-signature and for recovering multi-encryption data.

### 5. Proposed Scheme

The proposed scheme is described in detail in this section, which is made from the following six computational steps:

1. **Setup:** A global parameter set  $\mathcal{T} = \{H\xi, D, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3\}$  is created by CA, where  $\mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3$  are the one-way hash functions,  $H\xi$  is a hyper elliptic curve, and  $D$  is the divisor. Then, CA computes  $Y = \delta.D$ , where  $\delta \in \{1, 2, 3, 4, \dots, n-1\}$ , and set  $Y$  and  $\delta$  is a public and private key.
2. **Set-Public-Variant:** An entity with identity  $ID_e$  chooses  $\mathcal{V}_e \in \{1, 2, 3, 4, \dots, n-1\}$ , computes  $\varphi_e = \mathcal{V}_e.D$ , and sends a tuple  $(\varphi_e, ID_e)$  to CA.
3. **Set-Certificate:** For an entity with identity  $ID_e$ , CA selects  $\mathcal{X}_e \in \{1, 2, 3, 4, \dots, n-1\}$ , calculates  $\gamma_e = \mathcal{X}_e.D$ , computes  $CR_e = \gamma_e + \varphi_e$ , calculates  $\mathcal{W}_e = \mathcal{H}_1(CR_e, ID_e) \cdot \mathcal{X}_e + \delta$  and sends a tuple  $(\mathcal{W}_e, CR_e)$  to CA.
4. **Set-Public-and-Private-Key:** An entity with identity  $ID_e$  computes  $\alpha_e = \mathcal{H}_1(CR_e, ID_e) \cdot \mathcal{V}_e + \mathcal{W}_e$  as a private key and computes his/her public key as  $\beta_e = \alpha_e.D$ .
5. **Multi-message-Multi-receiver Signcryption:** A sender with identity  $(ID_s)$  can perform the following steps for generation of Multi-Message-Multi-receiver signcryption data.
  - Choose  $\phi_i \in \{1, 2, 3, 4, \dots, n-1\}$  and multiply with divisor as:  $\mu_i = \phi_i.D$ .
  - Compute  $\vartheta_i = \mathcal{H}_2(\phi_i \cdot \beta_i)$ , where  $i = \{1, 2, 3, \dots, n\}$
  - Make a Ciphertext as  $\mathcal{C}_i = E_{\vartheta_i}(CR_s, \beta_s, m_i)$  and make a non-reversible hash value  $\mathcal{J}_i = \mathcal{H}_3(ID_s, CR_s, \beta_s, m_i)$
  - Compute a multi signature as  $\mathcal{G}_i = \phi_i - \mathcal{J}_i \cdot \alpha_s$  and send Multi-message-Multi-receiver signcryption  $\psi = (\mathcal{C}_i, \mathcal{J}_i, \mathcal{G}_i)$  to the recipient group.
6. **Multi-message-Multi-receiver Un-signcryption:** each recipient with identity  $(ID_i)$  can perform the following steps for verification of multi-signature and recovering multi-encryption data.
  - Calculate  $\mu_i = \mathcal{G}_i.D + \mathcal{J}_i \cdot \beta_s$  and  $\vartheta_i = \mathcal{H}_2(\mu_i \cdot \alpha_i)$
  - Compute  $(ID_s, CR_s, \beta_s, m_i) = D_{\vartheta_i}(\mathcal{C}_i)$ .

#### Correctness Analysis

The recipient with identity  $(ID_i)$  computes

$$\begin{aligned}
 \mu_i &= \mathcal{G}_i.D + \mathcal{J}_i \cdot \beta_s \\
 &= \mathcal{G}_i.D + \mathcal{J}_i \cdot \beta_s = (\phi_i - \mathcal{J}_i \cdot \alpha_s).D + \mathcal{J}_i \cdot \alpha_s.D \text{ where } \mathcal{G}_i = \phi_i - \mathcal{J}_i \cdot \alpha_s \text{ and } \beta_s = \alpha_s.D \\
 &= D(\phi_i - \mathcal{J}_i \cdot \alpha_s + \mathcal{J}_i \cdot \alpha_s) = D(\phi_i) = \phi_i.D = \mu_i
 \end{aligned} \tag{1}$$

Then it calculates

$$\begin{aligned} \vartheta_i &= \mathcal{H}_3(\mu_i, \alpha_i) \\ \vartheta_i &= \mathcal{H}_3(\mu_i, \alpha_i) = (\mathcal{G}_i \cdot D + \mathcal{J}_i \cdot \beta_s) \cdot \alpha_i = ((\phi_i - \mathcal{J}_i \cdot \alpha_s) \cdot D + \mathcal{J}_i \cdot \beta_s) \cdot \alpha_i \\ &= ((\phi_i \cdot D - \mathcal{J}_i \cdot \alpha_s \cdot D) + \mathcal{J}_i \cdot \beta_s) \cdot \alpha_i \\ &= ((\phi_i \cdot D - \mathcal{J}_i \cdot \beta_s) + \mathcal{J}_i \cdot \beta_s) \cdot \alpha_i = (\phi_i \cdot D) \cdot \alpha_i = (\mu_i) \cdot \alpha_i \end{aligned} \quad (2)$$

## 6. Security Analysis

This section contains the following three theorems for proving the three games, which are discussed in the threat model.

**Theorem 1.** Suppose a malicious agent ( $\mathcal{MA}$ ) with non-ignorable advantages  $\epsilon$ , wants to break IND-CBMMS-CCA of a proposed CBMMS. Further, the challenger  $\zeta$  serves is a subroutine for finding the solution of a hyper elliptic curve Diffie–Hellman problem (HECDHP) for  $\mathcal{MA}$ . Assume  $\varsigma = \rho \cdot D$ ,  $\sigma = \omega \cdot D$  where  $\rho, \omega \in \{1, 2, 3, 4, \dots, n-1\}$  then we must say the HECDHP instance will be  $\varsigma$  and  $\sigma$ . Therefore,  $\zeta$  computes  $Y = \delta \cdot D$ , where  $\delta \in \{1, 2, 3, 4, \dots, n-1\}$ , and sends  $Y$  and  $\mathcal{T} = \{H\xi, D, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3\}$  to  $\mathcal{MA}$ . Furthermore,  $\mathcal{MA}$  selects  $ID_s^*$  as a sender identity,  $ID_i^*$  as receivers group identities, and two different natures but the same set length of messages ( $m^x_i, m^y_i$ ). Further,  $\zeta$  chooses  $q \in \{0, 1\}$  to investigate which set of messages will be multi-signcryption and, in the user list  $L_{usr}$ , divorces the identity data associated with  $ID_s^*$ . It fixed  $\varsigma = \beta_i^*$ . Therefore, for the determination of multi-cipher text, it set  $\mu_i = \delta$ . Then,  $\zeta$  generates some value for  $\mathcal{J}_i$  and chooses  $\mathcal{C}_i, \mathcal{G}_i$  from  $\{1, 2, 3, 4, \dots, n-1\}$ . Further, its stores the corresponding values in the user list that are  $L_{\mathcal{H}_3}$  and  $L_{\mathcal{H}_4}$ . Finally,  $\zeta$  sends a triple  $(\mathcal{J}_i, \mathcal{C}_i, \mathcal{G}_i)$  to  $\mathcal{MA}$ . Consequently, the  $\mathcal{MA}$  can ensue with the following queries, which are answered through  $\zeta$ .

1.  **$\mathcal{H}_j$  ( $m_j$ ):**  $\zeta$  maintains a list  $L_{\mathcal{H}_j}$  and initially stores  $m_j$  and  $\mathcal{J}_j$ . Note that, for the hash of  $m_j$ , the result is obtained as  $\mathcal{J}_j$  where  $(j = 1, 2, 3)$ . If the requested value is not existing in  $L_{\mathcal{H}_j}$ , then  $\zeta$  generates a new hash value for  $\mathcal{MA}$ . The  $\mathcal{MA}$  has access to  $L_{\mathcal{H}_j}$ .
2. **Create Entity ( $ID_e$ ):** if  $ID_e = ID_i^*$ , then  $\varsigma = \beta_i^*$  and chooses a random number for  $CR_i^*$ . Further, it adds  $(CR_i^*, \Psi, ID_i^*, \beta_i^*)$  into  $L_{usr}$  and  $(CR_i^*, \Psi, ID_i^*)$  into  $L_{\mathcal{H}_1}$ . If  $ID_e$  is not previously added in  $L_{usr}$ ,  $\zeta$  computes  $CR_e = \ell \cdot D$ , where  $\ell$  belongs to  $\{1, 2, 3, 4, \dots, n-1\}$ , then selects  $\alpha_e$  from  $\{1, 2, 3, 4, \dots, n-1\}$ , calculates  $\mathcal{W}_e = (\alpha_e + \delta) / \ell$ , sets  $\beta_e = \alpha_e \cdot D$ , and includes  $\mathcal{W}_e$  into  $L_{\mathcal{H}_1}$ . Furthermore, the values such as  $ID_e, CR_e, \beta_e$ , and  $\alpha_e$  are included to  $L_{usr}$ .
3. **Corrupt Entity ( $ID_e$ ):** If the requested value for  $ID_e$  does not belong to  $L_{usr}$ ,  $\zeta$  calls the Create Entity ( $ID_e$ ) query for generating  $\alpha_e$  and dispatches it to  $\mathcal{MA}$ .
4. **Multi-message-Multi-receiver Signcryption: Multi-Message-Multi-receiver Signcryption:**  $\zeta$  will stop further processing, if  $ID_e = ID_i^*$  or  $ID_e = ID_s^*$ , otherwise  $\zeta$  search in  $L_{usr}$ , if the entry exists for  $ID_i$  and  $ID_s$ . If such entry is not existing in  $L_{usr}$ , then it calls Create Entity ( $ID_e$ ) and generates  $(\mathcal{J}_i, \mathcal{C}_i, \mathcal{G}_i)$ .

When the above query is finished successfully, then  $\mathcal{MA}$  is decided upon  $\varrho$ . When  $\zeta$  is able to find the solution for a hyper elliptic curve discrete logarithm problem and determines  $E_{\vartheta_i}(ID_s, CR_s, \beta_s, m_i)$  from  $L_{\mathcal{H}_2}$ , then  $\mathcal{MA}$  will able with  $\epsilon$  to win this game. Therefore, the  $\mathcal{MA}$  can solve HECDHP with the following probability and events:

$E_1$ :  $\mathcal{MA}$  wins in creating an entity query ( $Q_{CE}$ ), and its probability is  $\frac{\epsilon}{Q_{CE}}$ .

$E_2$ :  $\mathcal{MA}$  wins in the Multi-message-Multi-receiver Signcryption query ( $Q_{MMS}$ ), and its probability is  $\frac{Q_{MMS}}{2^k}$ .

$E_3$ :  $\mathcal{MA}$  processes the  **$\mathcal{H}_2$  query ( $Q_{\mathcal{H}_2}$ ) without any hurdles** and its probability is  $\frac{1}{Q_{\mathcal{H}_2}}$ .

Therefore, the breaching probability will be  $\epsilon' \geq \left( \frac{\epsilon}{Q_{CE}} \cdot \frac{Q_{MMS}}{2^k} \cdot \frac{1}{Q_{\mathcal{H}_2}} \right)$ , which means that our proposed scheme provides IND- CBMMS-CCA security regarding confidentiality.

**Theorem 2.** Assume a malicious forger ( $\mathcal{MF}$ ) with non-ignorable advantages  $\epsilon$  wants to break EUF-CBMMS-CMA of a proposed CBMMS. Further, the challenger  $\zeta$  serves as a subroutine for

finding the solution of the hyper elliptic curve discrete logarithm problem (HECDLP) for  $\mathcal{MF}$ . Assume  $\zeta = \rho.D$  where  $\rho \in \{1, 2, 3, 4, \dots, n-1\}$  then we must say the HECDLP instance will be  $\rho$ . Therefore,  $\zeta$  computes  $Y = \delta.D$ , where  $\delta \in \{1, 2, 3, 4, \dots, n-1\}$  and sends  $Y$  and  $\mathcal{T} = \{H\xi, D, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3\}$  to  $\mathcal{MA}$ . Furthermore,  $\mathcal{MA}$  selects  $ID_s^*$  as a sender identity and  $ID_i^*$  as receiver group identities. Consequently, the  $\mathcal{MA}$  can ensue with the following queries, which are answered through  $\zeta$ .

1.  **$\mathcal{H}_j(m_j)$ :**  $\zeta$  maintains a list  $L_{\mathcal{H}_j}$  and initially stored  $m_j$  and  $\mathcal{J}_j$ . Note that, for the hash of  $m_j$ , the result is obtained as  $\mathcal{J}_j$  where  $(j = 1, 2, 3)$ . If the requested value is not existing in  $L_{\mathcal{H}_j}$ , then  $\zeta$  generates a new hash value for  $\mathcal{MF}$ . The  $\mathcal{MF}$  has access to  $L_{\mathcal{H}_j}$ .
2. **Create Entity ( $ID_e$ ):** If  $ID_e$  is not previously added in  $L_{usr}$ , then we define two conditions, which are: the first condition is if  $ID_e = ID_i^*$ , then  $\zeta = \beta_i^*$  and chooses a random number for  $CR_i^*$ . Further, it adds  $(CR_i^*, \psi, ID_i^*, \beta_i^*)$  into  $L_{usr}$  and  $(CR_i^*, \psi, ID_i^*)$  into  $L_{\mathcal{H}_1}$ . The second condition is if  $ID_e$  is not equal to  $ID_i^*$ , then  $\zeta$  computes  $CR_e = \ell.D$ , where  $\ell$  belongs to  $\{1, 2, 3, 4, \dots, n-1\}$ , then selects  $\alpha_e$  from  $\{1, 2, 3, 4, \dots, n-1\}$ , calculates  $\mathcal{W}_e = (\alpha_e + \delta)/\ell$ , sets  $\beta_e = \alpha_e.D$ , and includes  $\mathcal{W}_e$  into  $L_{\mathcal{H}_1}$ . Furthermore, the values such as  $ID_e, CR_e, \beta_e$ , and  $\alpha_e$  are included to  $L_{usr}$ .
3. **Corrupt Entity ( $ID_e$ ):** If the requested value for  $ID_e$  does not belong to  $L_{usr}$ ,  $\zeta$  calls the Create Entity ( $ID_e$ ) query to generate  $\alpha_e$  and dispatches it to  $\mathcal{MF}$ .
4. **Multi-message-Multi-receiver Signcryption:**  $\zeta$  will stop further processing, if  $ID_e = ID_i^*$  or  $ID_e = ID_s^*$ , otherwise  $\zeta$  searches in  $L_{usr}$ , if the entry exists for  $ID_i$  and  $ID_s$ . If such entry does not exist in  $L_{usr}$ , then it calls Create Entity ( $ID_e$ ) and generates  $(\mathcal{J}_i, \mathcal{C}_i, \mathcal{G}_i)$ .
5. **Multi-message-Multi-receiver Un-signcryption:**  $\zeta$  can check the validity of multi-ciphertext, which is basically generated by  $ID_s$  for  $ID_i$  and then it recovers the multi-plaintext.

When the above query is finished successfully, then  $\mathcal{MF}$  and  $\zeta$  will create their respective Multi-message-Multi-receiver Signcryption triples, which are  $(\mathcal{J}_i, \mathcal{C}_i, \mathcal{G}_i)$  and  $(\mathcal{J}_i^*, \mathcal{G}_i^*, \mathcal{C}_i)$ . Therefore, we can obtain the following results [24]:

$$\begin{aligned}
 & \mathcal{G}_i.D + \mathcal{J}_i.\beta_i = \mathcal{G}_i^*.D + \mathcal{J}_i^*.\beta_i \\
 = & \mathcal{G}_i.D - \mathcal{G}_i^*.D = \mathcal{J}_i^*.\beta_i - \mathcal{J}_i.\beta_i = (\mathcal{G}_i - \mathcal{G}_i^*).D = (\mathcal{J}_i^* - \mathcal{J}_i).\beta_i \\
 = & (\mathcal{G}_i - \mathcal{G}_i^*).D = (\mathcal{J}_i^* - \mathcal{J}_i).\rho.D \\
 = & (\mathcal{G}_i - \mathcal{G}_i^*) = (\mathcal{J}_i^* - \mathcal{J}_i).\rho
 \end{aligned} \tag{3}$$

$(\mathcal{G}_i - \mathcal{G}_i^*)/(\mathcal{J}_i^* - \mathcal{J}_i) = \rho$  will be the solution of HECDLP.

The  $\mathcal{MF}$  can solve HECDLP with the probability of  $\frac{\epsilon}{Q_{\mathcal{H}_3}}$ , and this means that our proposed scheme provides EUF-CBMMS-CMA security regarding unforgeability.

**Theorem 3.** Here, the malicious agent ( $\mathcal{MA}$ ), having advantage  $\epsilon$ , wants to break ANON-CBMMS-CCA of a proposed CBMMS. Further, the challenger  $\zeta$  serves is a subroutine for finding the solution of HECDHP for  $\mathcal{MA}$ . Adopt  $\zeta = \rho.D$ ,  $\sigma = \omega.D$  where  $\rho, \omega \in \{1, 2, 3, 4, \dots, n-1\}$ , then we must say the HECDHP instance will be  $\zeta$  and  $\sigma$ . Therefore,  $\zeta$  computes  $Y = \delta.D$ , where  $\delta \in \{1, 2, 3, 4, \dots, n-1\}$ , and sends  $Y$  and  $\mathcal{T} = \{H\xi, D, \mathcal{H}_1, \mathcal{H}_2, \mathcal{H}_3\}$  to  $\mathcal{MA}$ . Furthermore,  $\mathcal{MA}$  selects a target identity set  $TGL = \{ID_1^*, ID_2^*, \dots, ID_n^*\}$  and two different natures but with the same set length of messages  $(m^x_i, m^y_i)$ . Further,  $\zeta$  chooses  $q \in \{0, 1\}$  to investigate which set of messages will be multi-signcryption, and in the user list,  $L_{usr}$  divorces the identity associated data with  $ID_s^*$ . It fixed  $\zeta = \beta_i^*$ . Therefore, for the determination of multi-cipher text, it sets  $\mu_i = \delta$ . Then,  $\zeta$  generate some value for  $\mathcal{J}_i$  and chooses  $\mathcal{C}_i, \mathcal{G}_i$  from  $\{1, 2, 3, 4, \dots, n-1\}$ . Further, it stores the corresponding values in the user list, which are  $L_{\mathcal{H}_3}$  and  $L_{\mathcal{H}_4}$ . Finally,  $\zeta$  sends a triple  $(\mathcal{J}_i, \mathcal{C}_i, \mathcal{G}_i)$  to  $\mathcal{MA}$ . Consequently, the  $\mathcal{MA}$  can ensue with the following queries, which are answered through  $\zeta$ .

1.  **$\mathcal{H}_j(m_j)$ :**  $\zeta$  maintains a list  $L_{\mathcal{H}_j}$  and initially stores  $m_j$  and  $\mathcal{J}_j$ . Note that for the hash of  $m_j$ , the result obtained as  $\mathcal{J}_j$  where  $(j = 1, 2, 3)$ . If the requested value does not exist in  $L_{\mathcal{H}_j}$ , then  $\zeta$  generates a new hash value for  $\mathcal{MA}$ . The  $\mathcal{MA}$  has access to  $L_{\mathcal{H}_j}$ .



2. **Create Entity ( $ID_e$ ):** If  $ID_e = ID_i^*$ , then  $\zeta = \beta_i^*$  and chooses a random number for  $CR_i^*$ . Further, it adds  $(CR_i^*, \Psi, ID_i^*, \beta_i^*)$  into  $L_{usr}$  and  $(CR_i^*, \Psi, ID_i^*)$  into  $L_{\mathcal{H}_1}$ . If  $ID_e$  is not previously added in  $L_{usr}$ ,  $\zeta$  computes  $CR_e = \ell.D$ , where  $\ell$  belongs to  $\{1, 2, 3, 4, \dots, n - 1\}$ , then selects  $\alpha_e$  from  $\{1, 2, 3, 4, \dots, n - 1\}$ , calculates  $\mathcal{W}_e = (\alpha_e + \delta)/\ell$ , sets  $\beta_e = \alpha_e.D$ , and includes  $\mathcal{W}_e$  into  $L_{\mathcal{H}_1}$ . Furthermore, the values such as  $ID_e, CR_e, \beta_e$ , and  $\alpha_e$  are included to  $L_{usr}$ .
3. **Corrupt Entity ( $ID_e$ ):** If the requested value for  $ID_e$  does not belong to  $L_{usr}$ ,  $\zeta$  calls the *Create Entity ( $ID_e$ )* query to generate  $\alpha_e$  and dispatches it to  $\mathcal{MA}$ .
4. **Multi-message-Multi-receiver Signcryption:**  $\zeta$  will stop further processing if  $ID_e = ID_i^*$  or  $ID_e = ID_s^*$ ; otherwise,  $\zeta$  searches in  $L_{usr}$ , if the entry exists for  $ID_i$  and  $ID_s$ . If such entry does not exist in  $L_{usr}$ , then it calls *Create Entity ( $ID_e$ )* and generates  $(\mathcal{J}_i, \mathcal{C}_i, \mathcal{G}_i)$ .

When the above query is finished successfully, then  $\mathcal{MA}$  is decided upon  $\varrho$ . When  $\zeta$  is able to find the solution for the hyper elliptic curve discrete logarithm problem and determines  $E_{\theta_i}(ID_s, CR_s, \beta_s, m_i)$  from  $L_{\mathcal{H}_2}$ , then  $\mathcal{MA}$  will able with  $\epsilon$  to win this game. Therefore, the  $\mathcal{MA}$  can solve *HECDHP* with the probability of  $\frac{\epsilon}{Q_{\mathcal{H}_2}}$  and this means that our proposed scheme provides *IND-CBMMs-CCA* security regarding confidentiality.

### 7. Performance Comparison

In this section, we compare our scheme’s communication and computation costs with the corresponding current three existing schemes, i.e., Pang et al. [20], Peng et al. [21] and Ming et al. [28], on the basis of expensive mathematical operations used such as Scalar Elliptic curve point Multiplication (SEM) and Scalar HyperElliptic curve divisor Multiplication (SHEM) to show the efficiency, security and superiority. While the operation, such as addition, division, subtraction, hashing, encryption and decryption, is neglected because of its minimum numerical length. We consider the following kinds of operations for our comparative study.

Scalar Elliptic curve point Multiplication (SEM): The number of total point multiplication required on an elliptic curve.

Scalar HyperElliptic curve divisor Multiplication (SHEM): The total number of divisor points required on a hyperelliptic curve.

q = 160 bits

Number of messages =  $mi$

Number of receivers=  $\Pi$

Size of single message ( $m$ ) = 1024 bits

The SEM and SHEM values are shown in Table 2. To calculate the efficiency of the proposed solution, the Multi-precision Integer and Rational Arithmetic C Library (MIRACL) [30] is used to test the runtime of simple cryptographic operations up to 1000 times.

**Table 2.** Computational time of major operations in milliseconds.

Name of Operation	SEM	SHEM
Time in milliseconds (ms)	0.97 ms	0.48 ms

The following specs are observed on a workstation: Intel Core i7- 4510U Processor<sup>@</sup> 2.0 GHz, 8 GB RAM and Windows 7 Home Standard 64-bit Operating System [31]. We compared our scheme with Pang et al. [20], Peng et al. [21] and Ming et al. [28] by considering the same settings, and the findings are shown in Tables 3–5. The time required for SHEM is 0.48 ms [32,33].

Moreover, the results of a comparative study with current equivalents suggest that, as seen in Figures 2 and 3, the new scheme is defined by the lowest cost of computation. In comparison, from the related existing schemes, as shown in Figure 4, the ciphertext size is comparatively less in our proposed scheme.

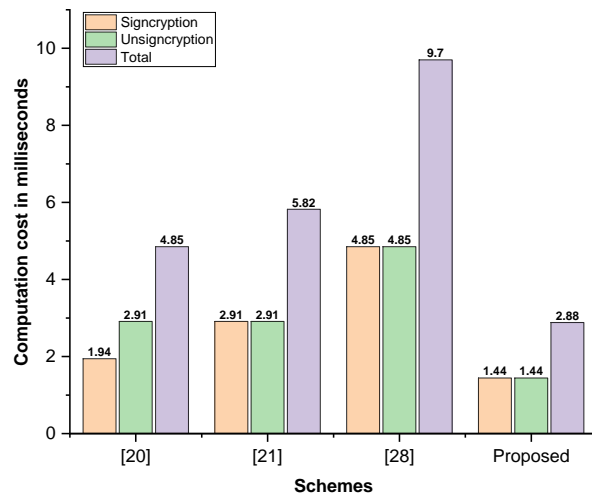


Figure 2. Computation cost comparison in milliseconds for a single node.

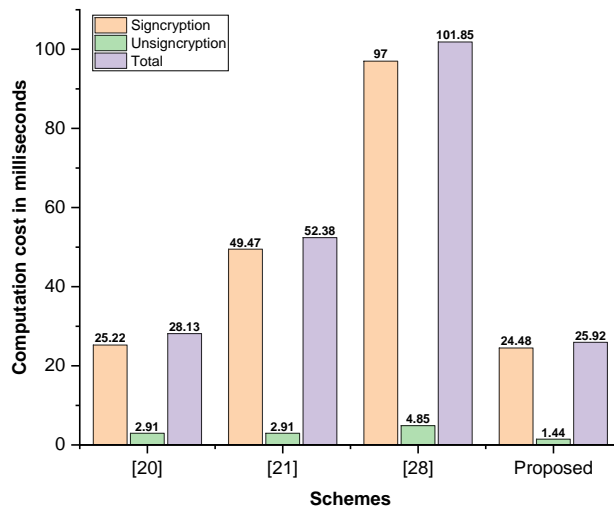


Figure 3. Computation cost comparison in milliseconds for fifteen nodes.

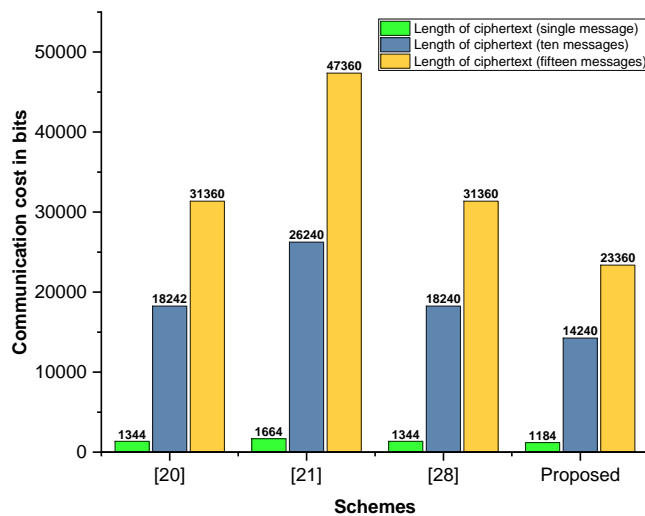


Figure 4. Communication cost comparison in bits.

**Table 3.** Computation and communication cost comparison for single node and single message.

Schemes	Signcryption	Unsigncryption	Length of Ciphertext
Pang et al. [20]	$(\Pi + 1) \text{ SEM} = (1 + 1) \times 0.97 = 1.94$	$3 \text{ SEM} = 3 \times (0.97) = 2.91$	$ m_i  + \Pi  2q  =  1024  + 1  2(160)  = 1344$
Peng et al. [21]	$(2 \Pi + 1) \text{ SEM} = (2 \times 1 + 1) \times 0.97 = 2.91$	$3 \text{ SEM} = 3 \times (0.97) = 2.91$	$ m_i  + \Pi  4q  =  1024  + 1  4(160)  = 1664$
Ming et al. [28]	$(4 \Pi + 1) \text{ SEM} = (4 \times 1 + 1) \times 0.97 = 4.85$	$5 \text{ SEM} = 5 \times (0.97) = 4.85$	$ m_i  + \Pi  2q  =  1024  + 1  2(160)  = 1344$
Proposed	$(2 \Pi + 1) \text{ SHEM} = (2 \times 1 + 1) \times 0.48 = 1.44$	$3 \text{ SHEM} = 3 \times (0.48) = 1.44$	$ m_i  + \Pi  2n  =  1024  + 1  2(80)  = 1184$

**Table 4.** Computation and communication cost comparison for twenty-five nodes and ten messages.

Schemes	Signcryption	Unsigncryption	Length of Ciphertext
Pang et al. [20]	$(\Pi + 1) \text{ SEM} = (25 + 1) \times 0.97 = 25.22$	$3 \text{ SEM} = 3 \times (0.97) = 2.91$	$ m_i  + \Pi  2q  = 10  1024  + 25  2(160)  = 18,240$
Peng et al. [21]	$(2 \Pi + 1) \text{ SEM} = (2 \times 25 + 1) \times 0.97 = 49.47$	$3 \text{ SEM} = 3 \times (0.97) = 2.91$	$ m_i  + \Pi  4q  = 10  1024  + 25  4(160)  = 26,240$
Ming et al. [28]	$(4 \Pi + 1) \text{ SEM} = (4 \times 25 + 1) \times 0.97 = 97$	$5 \text{ SEM} = 5 \times (0.97) = 4.85$	$ m_i  + \Pi  2q  = 10  1024  + 25  2(160)  = 18,240$
Proposed	$(2 \Pi + 1) \text{ SHEM} = (2 \times 25 + 1) \times 0.48 = 24.48$	$3 \text{ SHEM} = 3 \times (0.48) = 1.44$	$ m_i  + \Pi  2n  = 10  1024  + 25  2(80)  = 14,240$

**Table 5.** Computation and communication cost comparison for fifty nodes and fifteen messages.

Schemes	Signcryption	Unsigncryption	Length of Ciphertext
Pang et al. [20]	$(\Pi + 1) \text{ SEM} = (50 + 1) \times 0.97 = 49.47$	$3 \text{ SEM} = 3 \times (0.97) = 2.91$	$ m_i  + \Pi  2q  = 15  1024  + 50  2(160)  = 31,360$
Peng et al. [21]	$(2 \Pi + 1) \text{ SEM} = (2 \times 50 + 1) \times 0.97 = 97.97$	$3 \text{ SEM} = 3 \times (0.97) = 2.91$	$ m_i  + \Pi  4q  = 15  1024  + 50  4(160)  = 47,360$
Ming et al. [28]	$(4 \Pi + 1) \text{ SEM} = (4 \times 50 + 1) \times 0.97 = 194.97$	$5 \text{ SEM} = 5 \times (0.97) = 4.85$	$ m_i  + \Pi  2q  = 15  1024  + 50  2(160)  = 31,360$
Proposed	$(2 \Pi + 1) \text{ SHEM} = (2 \times 50 + 1) \times 0.48 = 48.48$	$3 \text{ SHEM} = 3 \times (0.48) = 1.44$	$ m_i  + \Pi  2n  = 15  1024  + 50  2(80)  = 23,360$

## 8. Conclusions

In the remote sharing of patient data, such as monitoring, treatment progression, diagnosis and consultation, the Internet of Medical Things (IoMT) plays a major role. Multiple biomedical sensors are ubiquitously linked with the Internet in IoMT, thereby offering seamless communication with effective usage of resources. However, because of the resource-constrained biomedical devices, traditional cryptographic approaches are not practical for the majority of IoMT implementations. Fortunately, the envisioned 5G mobile communication architecture includes an edge computing facility that can provide on-demand processing, computation, and storage. In this paper, we proposed a lightweight security scheme, using the hyperelliptic curve (HEC) principle together with a certificate-based cryptography called a Multi-message and Multi-receiver Signcryption. The HEC solution is a reliable technique due to the small key size and therefore has huge potential for future IoMT applications. The formal security analysis using ROM confirms confidentiality, unforgeability, and receiver anonymity by the proposed scheme. Furthermore, after a comparative comparison with the key existing schemes, the proposed scheme proved to be effective in terms of both the cost of computation and communication.

**Author Contributions:** Conceptualization, I.U. and M.A.K.; formal analysis, I.U. and M.A.K.; methodology I.U., M.H.A. and M.A.K.; resources I.U., M.H.A. and M.A.K.; software, I.U., M.H.A. and M.A.K.; supervision, R.N.; writing—original draft, I.U., M.H.A., R.N. and M.A.K.; writing—review and editing, A.A., A.A.A., A.H.A., and R.N.; validation, A.A.; investigation, A.A.; funding, R.N. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the Air Force Office of Scientific Research: FA2386-20-1-4045 (UKM Ref: KK-2020-007); and also by the Taif University Researchers Supporting Project through Taif University, Taif, Saudi Arabia, under Grant TURSP-2020/349.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

- Alsharif, M.H.; Kelechi, A.H.; Albreem, M.A.; Chaudhry, S.A.; Zia, M.S.; Kim, S. Sixth Generation (6G) Wireless Networks: Vision, Research Activities, Challenges and Potential Solutions. *Symmetry* **2020**, *12*, 676. [CrossRef]
- Islam, S.M.R.; Kwak, D.; Kabir, H.; Hossain, M.; Kwak, K.-S. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
- Ullah, I.; AlOmari, A.; Amin, N.U.; Khan, M.A.; Khattak, H. An Energy Efficient and Formally Secured Certificate-Based Signcryption for Wireless Body Area Networks with the Internet of Things. *Electronics* **2019**, *8*, 1171. [CrossRef]
- Kumar, A.; Albreem, M.A.; Gupta, M.; Alsharif, M.H.; Kim, S. Future 5G Network Based Smart Hospitals: Hybrid Detection Technique for Latency Improvement. *IEEE Access* **2020**, *8*, 153240–153249. [CrossRef]
- Yin, Y.; Zeng, Y.; Chen, X.; Fan, Y. The internet of things in healthcare: An overview. *J. Ind. Inf. Integr.* **2016**, *1*, 3–13. [CrossRef]
- Woo, M.W.; Lee, J.; Park, K. A reliable IoT system for Personal Healthcare Devices. *Futur. Gener. Comput. Syst.* **2018**, *78*, 626–640. [CrossRef]
- Ullah, I.; Amin, N.U.; Khan, M.A.; Khattak, H.; Kumari, S. An Efficient and Provable Secure Certificate-Based Combined Signature, Encryption and Signcryption Scheme for Internet of Things (IoT) in Mobile Health (M-Health) System. *J. Med. Syst.* **2021**, *45*, 4. [CrossRef]
- Islam, S.H.; Khan, M.K.; Al-Khouri, A.M. Anonymous and provably secure certificateless multireceiver encryption without bilinear pairing. *Secur. Commun. Netw.* **2014**, *8*, 2214–2231. [CrossRef]
- Amin, R.; Hafizul Islam, S.K.; Biswas, G.P.; Khan, M.K.; Kumar, N. A robust and anonymous patient monitoring system using wireless medical sensor networks. *Future Gener. Comput. Syst.* **2018**, *80*, 483–495. [CrossRef]
- Mahmood, K.; Akram, W.; Shafiq, A.; Altaf, I.; Lodhi, M.A.; Islam, S.H. An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments. *Comput. Electr. Eng.* **2020**, *88*, 106888. [CrossRef]
- Zheng, Y. Digital signcryption or how to achieve  $\text{cost}(\text{signature} \ \& \ \text{encryption}) \ll \text{cost}(\text{signature}) + \text{cost}(\text{encryption})$ . In Proceedings of the Smart Card Research and Advanced Applications, Santa Barbara, CA, USA, 17–21 August 1997; Springer: Berlin, Germany, 1997; pp. 165–179.
- Islam, S.H.; Li, F. Leakage-Free and Provably Secure Certificateless Signcryption Scheme Using Bilinear Pairings. *Comput. J.* **2015**, *58*, 2636–2648. [CrossRef]
- Karati, A.; Hafizul Islam, S.K.; Biswas, G.P.; Bhuiyan, M.Z.A.; Vijayakumar, P.; Karuppiyah, M. Provably Secure Identity-based Signcryption Scheme for Crowdsourced Industrial Internet of Things Environments. *IEEE Internet Things J.* **2018**, *14*, 3701–3711.
- He, D.; Wang, H.; Wang, L.; Shen, J.; Yang, X. Efficient certificateless anonymous multi-receiver encryption scheme for mobile devices. *Soft Comput.* **2016**, *21*, 6801–6810. [CrossRef]
- Seo, M.; Kim, K. Electronic funds transfer protocol using domain-verifiable signcryption scheme. In *Lecture Notes in Computer Science*; Springer: Berlin, Germany, 2000; pp. 269–277.
- Han, Y.; Gui, X. Adaptive secure multicast in wireless networks. *Int. J. Commun. Syst.* **2009**, *22*, 1213–1239. [CrossRef]
- Qiu, J.; Bai, J.; Song, X.; Hou, S. Secure and efficient multi-message and multi-receiver ID-based signcryption for rekeying in ad hoc networks. *J. Chongqing Univ. (Engl. Ed.)* **2013**, *2*, 91–96.
- Niu, S.; Niu, L.; Yang, X.; Wang, C.; Jia, X. Heterogeneous hybrid signcryption for multi-message and multi-receiver. *PLoS ONE* **2017**, *12*, e0184407. [CrossRef] [PubMed]
- Qiu, J.; Fan, K.; Zhang, K.; Pan, Q.; Li, H.; Yang, Y.T. An Efficient Multi-Message and Multi-Receiver Signcryption Scheme for Heterogeneous Smart Mobile IoT. *IEEE Access* **2019**, *7*, 180205–180217. [CrossRef]
- Gao, G.; Peng, X.; Jin, L. Efficient access control scheme with certificateless signcryption for wireless body area networks. *Int. J. Netw. Secur.* **2019**, *21*, 428–437.
- Peng, C.; Chen, J.; Obaidat, M.S.; Vijayakumar, P.; He, D. Efficient and provably secure multi-receiver signcryption scheme for multicast communication in edge computing. *IEEE Internet Things J.* **2019**, *7*, 6056–6068. [CrossRef]
- Diffie, W.; Hellman, M.E. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
- Shamir, A. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology*; Springer: Berlin, Germany, 2000; pp. 47–53.
- Al-Riyami, S.S.; Paterson, K.G. Certificateless public key cryptography. In *Requirements Engineering: Foundation for Software Quality*; Springer: Berlin, Germany, 2003; pp. 452–473.
- Wang, C.; Liu, C.; Li, Y.; Qiao, H.; Chen, L. Multi-message and multi-receiver heterogeneous signcryption scheme for ad-hoc networks. *Inf. Secur. J. Glob. Perspect.* **2017**, *26*, 136–152. [CrossRef]
- Pang, L.; Kou, M.; Wei, M.; Li, H. Anonymous Certificateless Multi-Receiver Signcryption Scheme Without Secure Channel. *IEEE Access* **2019**, *7*, 84091–84106. [CrossRef]
- Pang, L.; Wei, M.; Li, H. Efficient and Anonymous Certificateless Multi-Message and Multi-Receiver Signcryption Scheme Based on ECC. *IEEE Access* **2019**, *7*, 24511–24526. [CrossRef]
- Ming, Y.; Yu, X.; Shen, X. Efficient anonymous certificate-based multi-message and multi-receiver signcryption scheme for healthcare Internet of things. *IEEE Access* **2020**, *8*, 153561–153576. [CrossRef]
- Patonico, S.; Shabisha, P.; Braeken, A.; Touhafi, A.; Steenhaut, K. Elliptic curve-based proxy re-signcryption scheme for secure data storage on the cloud. *Concurr. Comput. Pr. Exp.* **2020**, *32*, e5657. [CrossRef]
- Shamus Software Ltd. Miracl Library. Available online: <http://github.com/miracl/MIRACL> (accessed on 24 November 2021).

31. Zhou, C.; Zhao, Z.; Zhou, W.; Mei, Y. Certificateless key insulated generalized signcryption scheme without bilinear pair-ings. *Secur. Commun. Netw.* **2017**, *2017*, 8405879. [[CrossRef](#)]
32. Khan, M.A.; Ullah, I.; Kumar, N.; Oubbati, O.S.; Qureshi, I.M.; Noor, F.; Khanzada, F.U. An Efficient and Secure Certificate-Based Access Control and Key Agreement Scheme for Flying Ad-Hoc Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 4839–4851. [[CrossRef](#)]
33. Khan, M.A.; Ullah, I.; Nisar, S.; Noor, F.; Qureshi, I.M.; Khanzada, F.; Khattak, H.; Aziz, M.A. Multiaccess Edge Computing Empowered Flying Ad Hoc Networks with Secure Deployment Using Identity-Based Generalized Signcryption. *Mob. Inf. Syst.* **2020**, *2020*, 8861947. [[CrossRef](#)]