IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 17, 2022, accepted April 2, 2022, date of publication April 7, 2022, date of current version April 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3165565

CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps

CHANDRASHEKHAR MESHRAM[1], AGBOTINAME LUCKY IMOIZE[2,3], (Member, IEEE), SAJJAD SHAUKAT JAMAL[4], ADEL R. ALHARBI[5], SARITA GAJBHIYE MESHRAM[6], AND IQTADAR HUSSAIN[7,8]

[1]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, Chhindwara University, Betul, Madhya Pradesh 460001, India
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria
[3]Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University Bochum, 44801 Bochum, Germany
[4]Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia
[5]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[6]Water Resources and Applied Mathematics Research Laboratory, Nagpur 440027, India
[7]Mathematics Program, Department of Mathematics, Statistics and Physics, College of Arts and Sciences, Qatar University, Doha, Qatar
[8]Statistical Consulting Unit, College of Arts and Science, Qatar University, Doha, Qatar

Corresponding authors: Chandrashekhar Meshram (cs_meshram@rediffmail.com), Sajjad Shaukat Jamal (shussain@kku.edu.sa), and Agbotiname Lucky Imoize (aimoize@unilag.edu.ng)

This work was supported in part by the Deanship of Scientific Research, King Khalid University, through the Research Groups Program under Grant R. G. P. 1/399/42. The work of Agbotiname Lucky Imoize was supported in part by the Nigerian Petroleum Technology Development Fund (PTDF), and in part by the German Academic Exchange Service (DAAD) through the Nigerian–German Postgraduate Program under Grant 57473408.

ABSTRACT In recent years, there has been a lot of research interest in analyzing chaotic constructions and their associated cryptographic structures. Compared with the essential combination of encryption and signature, the signcryption scheme has a more realistic solution for achieving message confidentiality and authentication simultaneously. However, the security of a signcryption scheme is questionable when deployed in modern safety-critical systems, especially as billions of sensitive user information is transmitted over open communication channels. In order to address this problem, a lightweight, provably secure certificateless technique that uses Fractional Chaotic Maps (FCM) for group-oriented signcryption (CGST) is proposed. The main feature of the CGST-FCM technique is that any group signcrypter may encrypt data/information with the group manager (GM) and have it sent to the verifier seamlessly. This implies the legitimacy of the signcrypted information/data is verifiable using the public conditions of the group, but they cannot link it to the conforming signcrypter. In this scenario, valid signcrypted information/data cannot be produced by the GM or any signcrypter in that category alone. However, the GM is allowed to reveal the identity of the signcrypter when there is a legal conflict to restrict repudiation of the signature. Generally, the CGST-FCM technique is protected from the indistinguishably chosen ciphertext attack (IND-CCA). Additionally, the computationally difficult Diffie-Hellman (DH) problems have been used to build unlinkability, untraceability, unforgeability, and robustness of the projected CGST-FCM scheme. Finally, the security investigation of the presented CGST-FCM technique shows appreciable consistency and high efficiency when applied in real-time security applications.

INDEX TERMS Certificateless group signcryption scheme (CGSS), fractional chaotic maps (FCM), provably secure scheme, authentication, Diffie-Hellman (DH) problem, wireless security networks.

I. INTRODUCTION

The study of chaotic structures and their potential cryptographic designs has sparked much research interest in recent years [1]–[3]. The behaviours of certain cryptographic primitives are fundamentally similar to that of chaotic frameworks, which are represented by their sensitive reliance on random operations and initial operations in the vicinity [4]–[6]. In modern wireless communication systems, information security is essential to protect critical user information/data

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

since most people communicate over public networks [7], [8]. In order to secure sensitive information/data, it must be protected from unauthorized access, know who sent the message, protect the message from alteration, and be available to a legitimate users whenever they need the message [9]. Correspondingly, encryption techniques can guarantee secrecy, while digital signature-based approaches can guarantee honesty and authenticity [3]. In the traditional approach, the sender always had to sign the text first and then encrypt it before sending the documents to the appropriate destination. The signature then the encryption procedure is a common name for this subject. However, this approach has some inherent disadvantages, such as requiring more machine sequences and computational resources, which decreases the performance of the framework ultimately [10].

To address the flaws inherent in the traditional schemes, Zheng [11] proposed signcryption, which combines encryption and signature in a single stage. The scheme is built on the public key infrastructure (PKI) [2]. However, the procedure has certain drawbacks, such as certificate distribution, limited storage, and production issues. To address these shortcomings inherent in the scheme proposed by Zheng [11], Chen and Malone-Lee [12] came up with the identity-based signcryption (IBS), which combines the capabilities of identity-based encryption and identity-based signature into a single scheme. Several IBS techniques were implemented in [13]–[16] after the first IBS technique in the emerging literature. However, key escrow has been identified as a key challenge for several identity-based signcryption techniques.

In the pioneering work of literature, Barbosa and Farshim [17] projected a certificateless signcryption to avoid the key escrow issue, which instantaneously satisfies the properties of certificateless encryption and signature in a single phase. Following the technique in [17], another certificateless signcryption scheme (CLSC) [18] was proposed. However, the CLSC technique was used in the random oracle model. Additionally, a robust CL-PKC signcryption technique was reported by Aranha *et al.* [19] to support signatures that can be checked publicly. This scheme, which adapts the Discrete Logarithm (DL) and Computational Diffie–Hellman (CDH) principles, is quite similar to the certificateless signcryption scheme proposed by Wu and Chen [20].

In 2018, Luo and Wan [21] presented a practical and implementable CLSC scheme. In the standard model, the technique is deemed provably secure and stable. Furthermore, the technique also met indistinguishability against adaptive selective ciphertext attack and existential unforgeability. The proposed scheme achieved the known session-specific temporary information security with more robust protection and shorter ciphertext duration. Remarkably, the authors pointed out that most existing signcryption techniques in the standard model could not provide this level of security. Similarly, Rastegari *et al.* [22] examined the certificateless signcryption technique projected by Luo and Wan [21] and discovered a fundamental flaw in the construction of the scheme. In order to fill the gap in Luo and Wan, a CLSC scheme with KSSTIS was suggested in [21]. For secure communication over wireless body area networks (WBANs), a similar certificateless signcryption scheme was recently created by Guo [23]. Furthermore, Gao *et al.* [24] suggested another scheme suitable for use in WBANs. Based on the hardness of the DL and CDH problems, mathematical calculations were performed to prove the correctness of the scheme, and the results show that the technique achieves unforgeability and confidentiality in the random oracle model.

Mandal *et al.* [25] developed a three-factor certificateless signcryption-based user access control technique appropriate for IoT deployment. The scheme uses three authentication factors: a user's password, a mobile device and biometrics. Under the real-or-random (ROR) model, the AVISPA tool was used to test the security of the technique. Interestingly, the scheme outperforms the preliminary methods by a large margin. Wu *et al.* [26] present a Type I adversary attack to test the security of the scheme proposed by Shim [27]. It was discovered that the adversary could forge a legal certificateless signature on any message by replacing the public key of the signer. It is worth mentioning that the CLSC technique proposed by Wu *et al.* [26] shows an improvement over the scheme reported in [27]. The scheme was found to resist adversarial attacks in several scenarios consistently.

Previous literature works demonstrate that current certificateless signcryption schemes have varying security strengths and lower computational overheads. However, when exposed to several high-level adversarial attacks, most existing schemes show limited existential unforgeability. Additionally, the applications of the schemes in group signcryption have received inadequate treatment in the existing works of literature. Furthermore, we have not found any literature that uses Fractional Chaotic Maps (FCM) to build certificateless group signcryption schemes, which is critical to overcoming the vast limitations of existing certificateless signcryption schemes. Thus, the current paper introduces an FCM-based certificateless group signcryption technique (CGST-FCM) to address the shortcomings of the preliminary schemes.

A. CONTRIBUTIONS

The major contributions of this paper are the following: a) Using FCM, we demonstrated an effective certificateless group signcryption technique. b) In contrast to other techniques, the proposed Certificateless Group Signcryption Technique (CGST-FCM) has the lowest storage expense. c) The key innovation in our work is that, while maintaining high performance, the proposed CGST-FCM also provides high-level security. d) Comprehensive security tests of the projected scheme revealed that our new CGST-FCM is secure against Type-I and Type-II attacks from the indistinguishably chosen ciphertext attack (IND-CCA) under the Fractional Chaotic Maps-Diffie-Hellmann problem (FCM-DHP). e) The proposed CGST-FCM can be easily implemented in low-power, low-processing-power devices, such as smart cards.

TABLE 1. Symbolization and meaning.

Symbolization	Meaning
$\mathfrak{T}^{\beta}$	Fractal Chebyshev chaotic maps
p_1, q_1	Hung prime numbers
n	An integer
id_C	Identity of C client
id_{KGC}	Identity of KGC
id_{GM}	Identity of GM
m_{sk}	Master secret key
m_{pk}	Public constraint
α	A random rational number
$\mathfrak{G}_{prk}$	Groups public key
$\mathfrak{G}_{pbk}$	Groups private key
m	Message

B. ORGANIZATION

The remaining part of this article is structured as follows: The background and material are discussed in Section II. The implementation of the proposed CGST-FCM is covered in Section III. In Section IV, we demonstrated the security inquiry of the proposed CGST-FCM technique. The efficiency of the projected CGST-FCM scheme is compared in Section V. The application of the proposed technique is described in Section VI. Finally, Section VII concludes the proposed work and offers predictions for future research exploration.

II. BACKGROUND AND MATERIAL

Before going into the existing inquiry on the certificateless group signcryption approach employing fractional chaotic maps (FCM-CGST), the basic principles [28], [29] pertaining to the work are discussed in this section. This is done to describe the research gap properly. First, a Chebyshev chaotic map implementation with a short lifespan is described. A fractal Chebyshev polynomial, fractal chaotic maps utilizing the minimum approach, and other techniques employed in this work follow. The symbolization used in the paper is listed in Table 1.

A. CHEBYSHEV CHAOTIC MAPS

Two fundamental prerequisites in the evolution of cryptographic systems are ambiguity and dispersion. Chaotic frameworks are suitable for accomplishing uncertainty and diffusion possessions in cryptography because of their sensitivity to primary conditions, pseudo-randomness, and ergodicity. As a result, chaotic maps have created several symmetric and asymmetric key cryptosystems [30]–[32].

1) CHAOTIC MAP

In the variation ϑ, the CSP $\mathfrak{T}_{\mathfrak{n}}(\vartheta)$ is an $\mathfrak{n}$ -degree polynomial. Assume that $\vartheta \in [-1, 1]$ is the edition and that $\mathfrak{n}$ is a large integer. The following is what CSP entails in general [4], [33], [34]:

$$\mathfrak{T}_{\mathfrak{n}}(\vartheta) = cos\left(\mathfrak{n}\, arccos\left(\vartheta\right)\right), \quad \mathfrak{T}_0(\vartheta) = 1,\ \mathfrak{T}_1(\vartheta) = \vartheta$$

By definition, the recurrence relation of the Chebyshev polynomial assumes

$$\mathfrak{T}_{\mathfrak{n}}(\vartheta) = 2\vartheta\mathfrak{T}_{\mathfrak{n}-1}(\vartheta) - \mathfrak{T}_{\mathfrak{n}-2}(\vartheta); \quad \mathfrak{n} \geq 2$$

In this case, the functional $arccos(\vartheta)$ and $cos(\vartheta)$ are represented as $arccos : [-1, 1] \to [0, \pi]$ and $cos : \Re \to [-1, 1]$.

2) CHARACTERISTICS OF CHAOTIC MAPS

Chebyshev polynomials have the following two critical characteristics:

Chaotic characteristics: The CSP transform is defined as $\mathfrak{T}_{\mathfrak{n}} : [-1, 1] \to [-1, 1]$ is a chaotic transform accompanying the functional (invariant density) $\mathfrak{f}^*(\vartheta) = \frac{1}{\left(\pi\sqrt{1-\vartheta^2}\right)}$ for some positive Lyapunov exponent $\lambda >= \mathrm{In}\,\mathfrak{n} > 0$ with degree $\mathfrak{n} > 1$.

Semi-group characteristics: The semi-group property of the Chebyshev polynomial $\mathfrak{T}_{\mathfrak{n}}(\vartheta)$ is defined as follows:

$$\begin{aligned}\mathfrak{T}_{\mathfrak{l}}(\mathfrak{T}_{\mathfrak{l}}(\vartheta)) &= cos(\mathfrak{l}cos^{-1}(cos(\ell cos^{-1}(\vartheta))))\\ &= cos(\mathfrak{l}\ell cos^{-1}(\vartheta)) = \mathfrak{T}_{\ell\mathfrak{l}}(\vartheta) = \mathfrak{T}_{\ell}(\mathfrak{T}_{\mathfrak{l}}(\vartheta)),\end{aligned}$$

where $\mathfrak{l}$ and ℓ are positive integers and $\vartheta \in [-1, 1]$.

Public-key cryptography (PKC) based on the Chebyshev polynomial map semigroup property is not stable, according to Bergamo *et al.* [5]. Additionally, Zhang [35] demonstrated that the semigroup property holds an interval $(-\infty, +\infty)$, which can enhance the property as broached:

$$\mathfrak{T}_{\mathfrak{n}}(\vartheta) = 2\vartheta\mathfrak{T}_{\mathfrak{n}-1}(\vartheta) - \mathfrak{T}_{\mathfrak{n}-2}(\vartheta)\,(mod q_1);\ n \geq 2$$

where $\vartheta \in (-\infty, +\infty)$ and $\mathfrak{l}_1$ is a big prime. As a result, the property is: $\mathfrak{T}_{\mathfrak{l}}\left(\mathfrak{T}_{\ell}(\vartheta)\right)(mod q_1) = \mathfrak{T}_{\ell\mathfrak{l}}(\vartheta)\,(mod q_1) = \mathfrak{T}_{\ell}\left(\mathfrak{T}_{\mathfrak{l}}(\vartheta)\right)(mod q_1)$, and additionally, the semi-group characteristic is kept. Here, it is worth highlighting that extended Chebyshev polynomials commute in conformation.

3) COMPUTATIONAL PROBLEMS

Using the propositions [30], [33], [34], [36], [37], various computational challenges based on Chebyshev polynomials are explained in this segment.

4) CHAOTIC MAP-BASED DISCRETE LOGARITHM (CMDL) PROBLEM

Any polynomial time-bounded technique that discovers the integer where $\mathcal{Y} = \mathfrak{T}_{\mathfrak{l}}(\vartheta)\,(mod q_1)$ is not feasible given a random tuple $< \mathcal{Y}, \vartheta >$.

5) CHAOTIC MAP-BASED DIFFIE-HELLMAN (CMDH) PROBLEM

Any polynomial time-bounded algorithm that attempts to unravel the value $\mathfrak{T}_{\mathfrak{l}\ell}(\vartheta)\,(mod q_1)$ for a given random tuple $< \vartheta, \mathfrak{T}_{\mathfrak{l}}(\vartheta), \mathfrak{T}_{\ell}(\vartheta) >$.

B. FRACTAL CHAOTIC MAPS (FCM)

Historically, the Fractal Calculus (FC) was called a local fractional calculus [38], [39]. However, fractional calculus clinched possessions and takes precedence over the related preparation:

Assume that the formal expression for a random fractional-order $\beta\epsilon[0, 1]$ defines the fractional difference operator.

$$\xi^{\beta}\Upsilon(\mathcal{y}) = \frac{\Delta^{\beta}(\Upsilon(\mathcal{y}) - \Upsilon(\mathcal{y}_0))}{(\mathcal{y} - \mathcal{y}_0)^{\alpha}} = \Gamma(\beta + 1)(\Upsilon(\mathcal{y}) - \Upsilon(\mathcal{y}_0))$$

and the fractal integral operator is the same as this.

$$I^{\beta}\Upsilon(\mathcal{y}) = \frac{1}{\Gamma(\beta + 1)}\int_a^b \Upsilon(\mathcal{y})(d\mathcal{y})^{\beta}.$$

It can be approximated using the formula.

$$I^{\beta}\Upsilon(\mathcal{y}) = \frac{(b-a)^{\beta}}{\Gamma(\beta + 1)}\Upsilon(\mathcal{y}), \quad a \le \mathcal{y} \le b. \tag{1}$$

Using the FC definition to generalise the polynomial $\mathfrak{T}_{\mathfrak{n}}(\vartheta)$, the following construction is achieved:

$$I^{\beta}\mathfrak{T}_{\mathfrak{n}}(\vartheta) := \mathfrak{T}^{\beta}_{\mathfrak{n}}(\vartheta) = \frac{(2)^{\beta}}{\Gamma(\beta + 1)}\mathfrak{T}_{\mathfrak{n}}(\vartheta), \tag{2}$$

FCP represents the Fractal Chebyshev polynomial (see Fig.1).

1) CHARACTERISTICS OF FRACTAL CHAOTIC MAPS

Two of the soothing properties of FCP are described as follows:

Chaotic characteristic of FCM: The Fractal Chaotic Maps [39] fulfil the recurrent relations under the chaotic characteristic, i.e.,

$$\mathfrak{T}^{\beta}_{\mathfrak{n}}(\vartheta) = \frac{(2)^{\beta}}{\Gamma(\beta + 1)}(2\vartheta\mathfrak{T}_{\mathfrak{n}-1}(\vartheta) - \mathfrak{T}_{\mathfrak{n}-2}(\vartheta))(mod\ q_1).$$

When $\beta \to 0$ is employed, the usual significant effect found in Yang *et al.* [40] is elaborated clearly.

Semi-group characteristic of FCM: For FCMs operating on the interval (-∞, ∞) [31], the semi-group properties hold, i.e.,

$$\mathfrak{T}^{\beta}_{k}\left(\mathfrak{T}^{\beta}_{\mathfrak{n}}(\vartheta)\right)(mod\ q_1) = \mathfrak{T}^{\beta}_{\mathfrak{n}}\left(\mathfrak{T}^{\beta}_{k}(\vartheta)\right)(mod\ q_1) = \mathfrak{T}^{\beta}_{k\mathfrak{n}}(\vartheta).(mod\ q_1)$$

III. THE PROPOSED FRACTIONAL CHAOTIC MAPS BASED ON CERTIFICATELESS GROUP SIGNCRYPTION TECHNIQUE (CGST-FCM)

Currently, e-commerce technology is rapidly growing, and billions of online transactions are possible worldwide. As a result, employing open wireless channels for online-based commercial transactions raises several security concerns. Sophisticated security techniques are primarily desired to protect user information over these safety-critical channels.

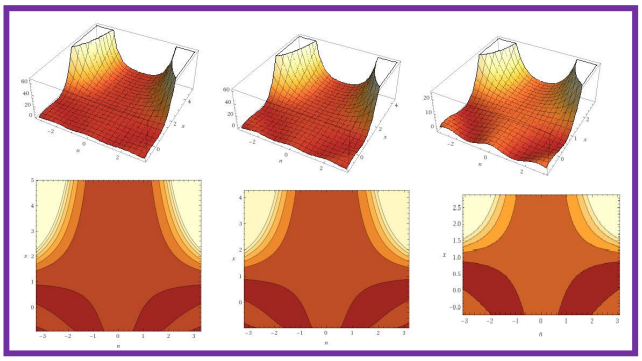

FIGURE 1. 3D-FCP when $\beta = 0$, 0.5 and 0.75 respectively.

As a result, we require an efficient certificateless group signcryption mechanism to enhance the security of e-commerce technologies. Therefore the requirement for the proposed CGST-FCM becomes critical.

The proposed CGST-FCM includes a group of clients $(SG : C_1 \ldots C_n)$, where everyone can signcrypt a message with the GM as a representative of the group and KGC. Figure 2 depicts the proposed CGST-FCM system model. The proposed CGST-FCM has six phases, which are described as follows:

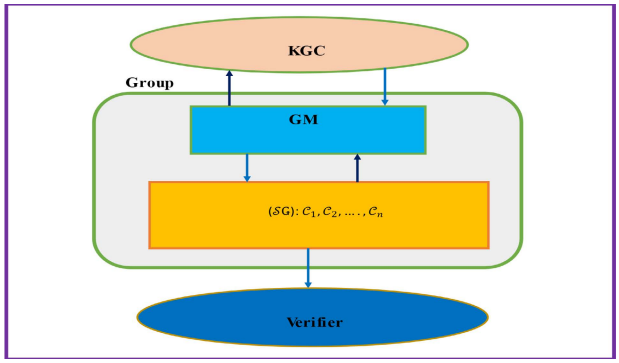

FIGURE 2. System structure of the proposed CGST-FCM.

A. SETUP

The KCG picks an integer $n = p_1 * q_1$ where p_1, q_1 are big primes consuming the secure prime techniques [41], [42]. Then, they pick g as a GF(p_1) generator. The GM is then given g and n.

B. PARTIAL PRIVATE KEY GENERATION

The KGC carries out this operation. At this point, the KGC picks a m_{sk} as its secrete factor and their identity id_{KGC}. Then, they evaluate a m_{pk} whose safety is ensured by solving extended chaotic maps. Figure 3 shows the architecture of the client key generation, verification, key generation, and signcryption framework.

$$m_{pk} = \mathfrak{T}^{\alpha}_{m_{sk}}(g)\ (mod\ n)$$

Then they deliver (m_{pk}, id_{KGC}) to the GM.

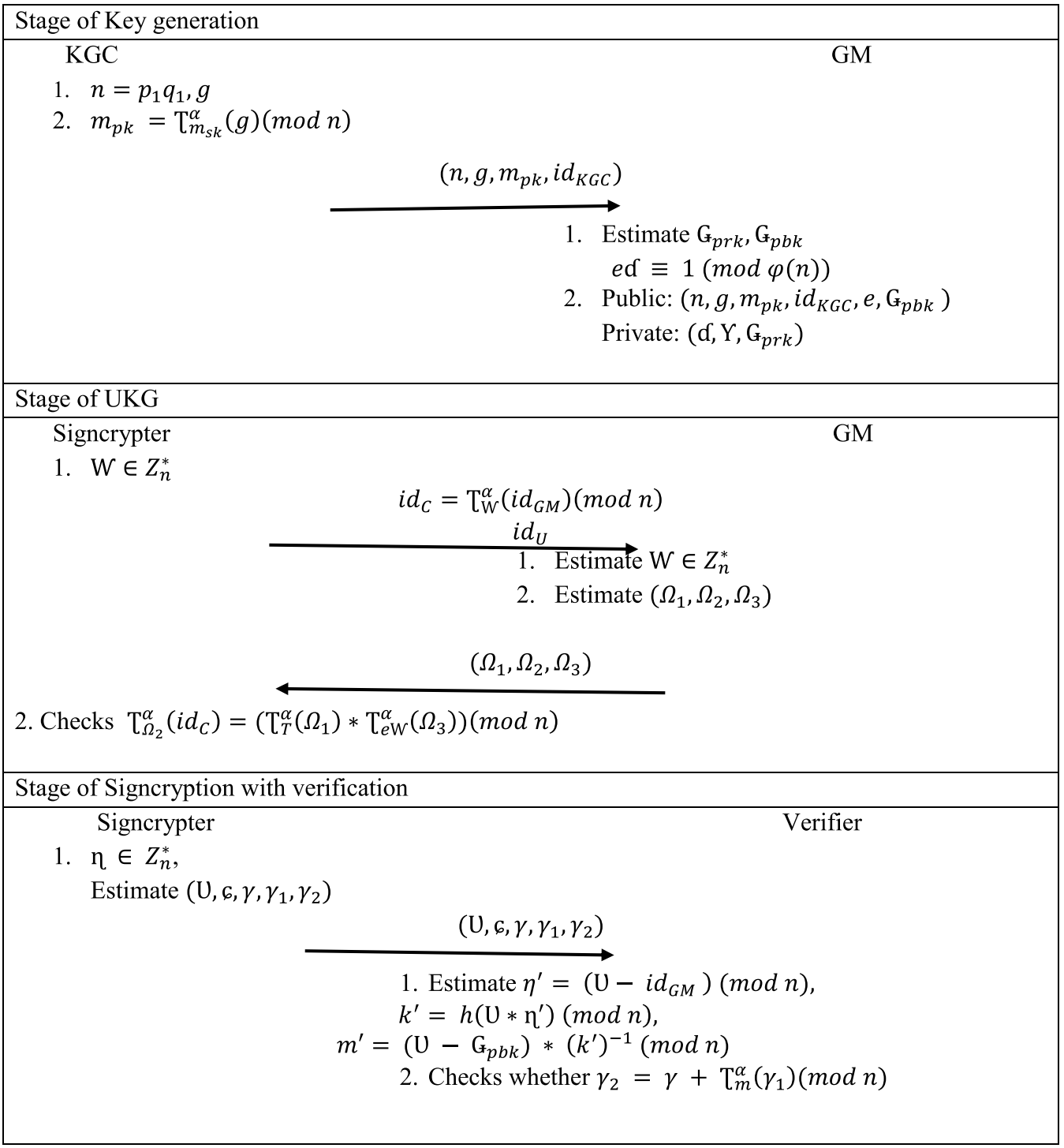

FIGURE 3. Proposed FCM-based certificateless group signcryption technique.

1) PRIVATE KEY GENERATION (PKG)

The following are the PKG metrics: The GM chooses three private exponents $\Upsilon, \mathfrak{d}$ and id_{GM}, and then determines the private and public keys of the group elucidated in the following equations.

$$\mathfrak{G}_{prk} = \Upsilon * m_{pk} + id_{KGC} * id_{GM}(mod\ n)$$
$$\mathfrak{G}_{pbk} = \Upsilon^{\alpha}_{\mathfrak{G}_{prk}}(g)\ (mod\ n)$$
$$e\mathfrak{d} \equiv 1 mod \varphi(n).$$

The GM then makes it public $(n, g, m_{pk}, id_{GM}, e, \mathfrak{G}_{prk})$ while keeping secret $(\Upsilon, \mathfrak{d}, \mathfrak{G}_{prk})$ as their secret key.

C. CLIENT'S KEY CREATION (CKC)

The GM and the signcrypter are in this stage. The following are the stages of this level.

Stage 1. Any signcrypter, after finding the public factor, chooses a private parameter $\mathrm{W} \in Z_n^*$ on behalf of the group

and determines id_C as follows:

$$id_C = \mathfrak{T}^{\alpha}_{W}(id_{GM})\,(mod\ n)$$

Then they send the id_C to the GM over a secure channel.

Stage 2. After determining the estimate of id_C, the GM picks a secrete factor $\mathfrak{a} \in Z_n^*$ and estimates $\Omega_1, \Omega_2, \Omega_3$ as follows:

$$\Omega_1 = \mathfrak{T}^{\alpha}_{\mathfrak{a}}(id_C)\,(mod\ n)$$
$$\Omega_2 = (\mathfrak{a} * T + \Omega_1)\,(mod\ n)$$
$$\Omega_3 = \mathfrak{T}^{\alpha}_{\Omega_1 * \mathfrak{d}}(id_{GM})\,(mod\ n)$$

After measuring all of the values, the GM sends $(\Omega_1, \Omega_2, \Omega_3)$ to the client.

Stage 3. The client then tests the validity of the factor using this equation.

$$\mathfrak{T}^{\alpha}_{\Omega_2}(id_C) = (\mathfrak{T}^{\alpha}_{T}(\Omega_1) * \mathfrak{T}^{\alpha}_{e\mathfrak{W}}(\Omega_3))\,(mod\ n)$$

The client will obtain three factors if this equation holds. However, the client will return the equation to the GM if it does not.

1) ACCURACY OF THE ALGORITHM

$$\begin{aligned}\mathfrak{T}^{\alpha}_{\Omega_2}(id_C) &= (\mathfrak{T}^{\alpha}_{\mathfrak{a}T}(id_C) * \mathfrak{T}^{\alpha}_{\Omega_1}(id_C))(mod\ n)\\ &= (\mathfrak{T}^{\alpha}_{T}(\Omega_1) * \mathfrak{T}^{\alpha}_{\mathfrak{W}\Omega_1}(id_{GM}))(mod\ n)\\ &= (\mathfrak{T}^{\alpha}_{T}(\Omega_1) * \mathfrak{T}^{\alpha}_{\left(\frac{\mathfrak{W}}{\mathfrak{d}}\right)}(\Omega_3))(mod\ n)\\ &= (\mathfrak{T}^{\alpha}_{T}(\Omega_1) * T^{\alpha}_{e\mathfrak{W}}(\Omega_3))\,(mod\ n)\end{aligned}$$

D. SIGNCRYPTION

The client will encrypt the information/text on behalf of the group at this argument. A client first selects a $\mathfrak{y} \in Z_n^*$ the secret factor then determines the following: Cipher ($\mathfrak{c}$) and key (k).

$$\begin{aligned}\mathfrak{U} &= \mathfrak{y} + \mathfrak{T}^{\alpha}_{\left(\frac{e}{\Omega_1}\right)}(\Omega_3)\,(mod\ n)\\ \text{Key(k)} &= h(\mathfrak{U} * \mathfrak{y})(mod\ n)\\ Cipher\ (\mathfrak{c}) &= (k * Message\ (m)) + \mathfrak{G}_{pbk}(mod\ n)\\ \gamma &= (\mathfrak{T}^{\alpha}_{\Omega_3}(\mathfrak{G}_{pbk}) * \mathfrak{T}^{\alpha}_{W}(id_{GM}))\,(mod\ n)\\ \gamma_1 &= \mathfrak{T}^{\alpha}_{\Omega_3}(g)\,(mod\ n)\\ \gamma_2 &= \gamma + T^{\alpha}_{m}(\gamma_1)\,(mod\ n)\end{aligned}$$

Then the client refers to the signcrypted text $(\mathfrak{U}, \mathfrak{c}, \gamma, \gamma_1, \gamma_2)$ to the verifier.

E. VERIFICATION

After discovering the signcrypted information, the verifier checks the legitimacy of the signcrypted information; they must first find the message. To locate a message, the verifier assesses the subsequent stages:

$$\mathfrak{y}' = (\mathfrak{U} - id_{GM})(mod\ n)$$
$$k' = h(\mathfrak{U} * \mathfrak{y}')(mod\ n) \quad (3)$$
$$m' = (\mathfrak{U} - \mathfrak{G}_{pbk}) * (k')^{-1}\,(mod\ n) \quad (4)$$

Otherwise, they would deny the message as being invalid. The verifier checks the validity of the message as soon as it is identified.

$$\gamma_2 = \gamma + \mathfrak{T}^{\alpha}_{m}(\gamma_1)\,(mod\ n)$$

The verifier will construct the signcrypted information/text of the message if this happens.

F. OPENING

If the sender has a legal dispute, the GM will identify the sender.

$$id_C = \frac{\gamma}{\mathfrak{T}^{\alpha}_{prk}(\gamma_1)}\,(mod\ n)$$

IV. SECURITY INVESTIGATIONS OF THE PROPOSED CGST-FCM TECHNIQUE

This section provides a formal security framework for the projected CGST-FCM. Consequently, two kinds of adversaries are considered, and the security examination of the projected technique is described as follows.

Theorem 1: This theorem states that the signcrypted text/information/ created by the presented CGST-FCM is correct.

Proof. This theorem exhibits the exactness characteristic of the presented CGST-FCM technique.

As a consequence of Eq. (3), we can see that

$$\begin{aligned}\mathfrak{y}' &= (\mathfrak{U} - id_{GM})(mod\ n)\\ &= \mathfrak{U} - \mathfrak{T}^{\alpha}_{e\mathfrak{d}}(id_{GM})\,(mod\ n)\\ &= \mathfrak{U} - \mathfrak{T}^{\alpha}_{(e\mathfrak{d})^{\frac{\Omega_1}{\Omega_1}}}(id_{GM})\,(mod\ n)\\ &= \mathfrak{U} - \mathfrak{T}^{\alpha}_{\left(\frac{e}{\Omega_1}\right)}(\Omega_3)\,(mod\ n)\\ &= \mathfrak{y}\end{aligned}$$

The proposed CGST-FCM scheme is seen to be correctly implemented.

Theorem 2: The projected CGST-FCM also has traceability features, such that the GM can only open the client identifier that has to sign up the signcrypted text.

Proof. We understand that the identity of a client can be obtained as $id_U = \Omega / \Omega_1^{G_{prk}}$ as a result of eq, (4).

Let

$$\begin{aligned}\frac{\gamma}{\mathfrak{T}^{\alpha}_{\mathfrak{G}_{prk}}(\gamma_1)} &= \frac{\mathfrak{T}^{\alpha}_{\Omega_3}(\mathfrak{G}_{pbk}) * \mathfrak{T}^{\alpha}_{W}(id_{GM})}{\mathfrak{T}^{\alpha}_{\Omega_3 \mathfrak{G}_{prk}}(g)}\,(mod\ n)\\ &= id_C(mod\ n)\end{aligned}$$

Consequently, the traceability assets of the presented CGST-FCM technique are fulfilled.

Theorem 3: The presented CGST-FCM can withstand Type-I and II attacks using the FCM-CDHP, as described below.

Definition 1: (Type I Attack). A foe cannot obtain the master secret key (F_1) with access to the device. However, (F_1) may substitute public keys, remove private keys and PPK, and create a signcrypted text.

Proof: The game is played among the (F_1) foe and the (ß) challenger in the Type-I attack. The communication among them is comprised of the steps mentioned as follows.

PPKG: At this point, the challenger runs the setup process to produce a KGC's (m_{sk}) and a (m_{pk}) public factor corresponding to the KGC's identity (id), then, when he asks for it, the challenger (ß) sends (m_{pk}) to the foe (F_1).

Key generation (KG): The challenger (ß) calculates a (ϒ) secret value following the GM's identity (id_{GM}), in the KG phase, then estimate the $\mathfrak{G}_{prk}$ using the secret key and PPK and sending it to the foe.

Demand public key: The foe will now appeal to the public key for any id. After getting the appeal, the challenger computes the assessment of the $\mathfrak{G}_{prk}$ and sends it to the foe.

Replace public key: After acquiring the challenger's public key, the foe generates a new Υ_1 hidden assessment and replaces the challenger's public key with their own $(\mathcal{Y}_{prk1})$.

Signcryption: The client chooses some private values for signcrypt, while a challenger message requires GM's public key and the novel text. Then, the challenger submits the signed text $S = (\mathfrak{U}, \mathfrak{c}, \gamma, \gamma_1, \gamma_2)$ on message m_1 consistent with a public key for the id of the sender to the foe compatible with the GM's public key. If the designcrypt inquiries show that Designcrypt $(m_{pk1}, id_{GM1}, \Upsilon_1, m_1, S_1)$ is equal to 1, the attacker wins the game, but the foe does not break the security because the foe cannot inquire about the signcryption on the message 1, and the foe also cannot inquire about the private key for an id_{GM1}.

Definition 2: (Type II Attack). In a Type-II attack, the foe (F_2) has retrieved the master key but cannot substitute any client's public key.

Proof. The game is played between the challenger (ß) and the foe (F_2).

PPKG: At this point, the challenger runs the setup process to produce KGC's (m_{sk}) and a (m_{pk}) public factor using the id of KGC and then sends the public key and the secret keys to a foe. The attacker would then be able to guess the PPK.

KG: The challenger (ß) then estimates a (ϒ) hidden assessment following the GM's identity (id_{GM}), determines the $\mathfrak{G}_{prk}$ with the use of a private key and PPK and sends it to the foe (F_2).

Demand public key: Following that, the challenger fixes the public key of GM and delivers it to the foe upon request.

Signcryption: Following a public key for the GM's public key and the sender's identity, the challenger can now assess a signcrypted text $S_1 = (\mathfrak{U}, \mathfrak{c}, \gamma, \gamma_1, \gamma_2)$ on m_1 message and provide it to the foe (F_2). If the designcrypt inquiries show that Designcrypt $(m_{pk1}, id_{GM1}, V_1, m_1, S_1)$ is equal to 1, the attacker wins the game, but the foe does not break the security because the foe cannot inquire about the signcryption on m_1 message and cannot inquire about the secret key for a id_{GM1}. It has also been shown that the presented system is resistant to Types-I and II attacks.

Theorem 4: The projected CGST-FCM fulfils the property of unlinkability.

Proof: After finding the group signcrypted info $(\mathfrak{U}, \mathfrak{c}, \gamma, \gamma_1, \gamma_2)$ for m, the verifier approves the signcrypted info by utilizing the group's $\mathfrak{G}_{pbk}$ public information and id_{GM} as shown in Eq. (3). If the verifier takes substitute signcrypted info $(\mathfrak{U}', \mathfrak{c}', \gamma', \gamma_1', \gamma_2')$ for the message m'. There are no similar variables in the two signcrypted info/texts $(\mathfrak{U}, \mathfrak{c}, \gamma, \gamma_1, \gamma_2)$. The verifier must check the GM to know the id of the signcrypter.

Additionally, the projected CGST-FCM has five variables, namely $(\mathfrak{a}, \mathfrak{n}, \mathfrak{U}, e, \mathfrak{W})$, to conceal the accurate assessment of the group's signcrypted text/information. Consequently, decipher the estimates of $(\mathfrak{a}, \mathfrak{n}, \mathfrak{U})$ from the signcrypted information. As a result, a foe would never connect a signcrypted information to the conforming signcrypter.

V. PERFORMANCE COMPARISON

Concerning the computational cost, we compare our approach to lately existing certificateless signcryption techniques such as that of Yu and Yang [43], Zhou [44], Lin *et al.* [45], Cao and Ge [46], and Luo and Ma [47]. Based on the communication expense, the efficiency of the presented CGST-FCM technique is assessed. Based on the output, the costs of the signcryption and verification stages are compared. It has been noted that, in comparison to the installation and extraction stages, the signcryption and verification phases require more computational resources. As a result, the comparison analysis focuses on the computational cost of the signcryption and verification stages.

Here, we used six notations of time complexity in this comparisons study, which are represented as follows: $T_e, T_{ch}, T_m, T_h, T_{ec}, T_i$, and T_p described performance time for modular exponentiation in the modular multiplication, Chebyshev chaotic map operation, elliptic curve scale multiplication, a one-way hash function, modular inverse operation, and bilinear pairing operation, respectively. The relations between $T_{ch}, T_e, T_m, T_{ec}, T_i$, and T_p with respect to $T_h (T_h = 0.32ms)$ have been established in [39], [48]–[50]. In addition, we provide the findings of our evaluation in this section. On a four-core 3.2 GHz computer with 8 GB of RAM, the results averaged 300 randomized simulation runs [51]. The studies were carried out using our MATLAB-created simulator. The following relationship exists, and the order of computational complexity of the contending metrics is given as follows: $T_{ch} \approx T_h, T_m \approx 2.5T_h, T_i \approx 7.5T_h, T_{ec} \approx 72.5T_h, T_e \approx 600T_h, T_p \approx 1550T_h$ and $T_h \approx T_{ch} < T_m < T_i < T_{ec} < T_e < T_p$. Table 2 shows the key consuming operations of the projected CGST-FCM technique and the standing techniques. There are also assessments of computational costs defined in milliseconds, as provided in Fig. 4.

The overall communication expense of the proposed certificateless group signcryption technique is the lowest, as the estimation results in Table 2 and Fig. 5 indicate. The proposed certificateless community signcryption technique outperforms the rest of the existing methods in terms of running time.

TABLE 2. Assessments with reference to major operations.

Techniques	Signcryption	Verification	Total
Yu and Yang [43]	$7T_e + 2T_p$	$T_e + 7T_p$	$8T_e + 9T_p$
Zhou [44]	$7T_e + T_p$	$5T_e + 4\,T_p$	$12T_e + 5\,T_p$
Lin et al. [45]	$5T_e$	$5T_e$	$10T_e$
Cao and Ge [46]	$7T_{ec}$	$5T_{ec}$	$12T_{ec}$
Luo and Ma [47]	$4T_{ec}$	$3T_{ec}$	$7T_{ec}$
Proposed CGST-FCM	$4T_{ch}$	$T_{ch} + T_i + 2T_m$	$5T_{ch} + T_i + 2T_m$

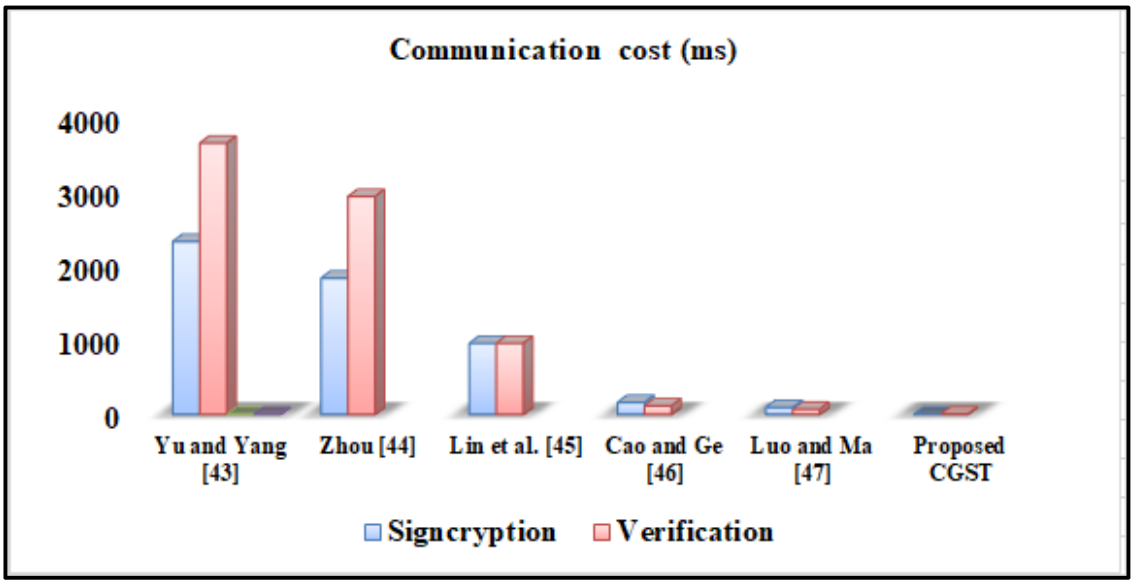

FIGURE 4. Communication cost (ms) in signcryption and verification stages.

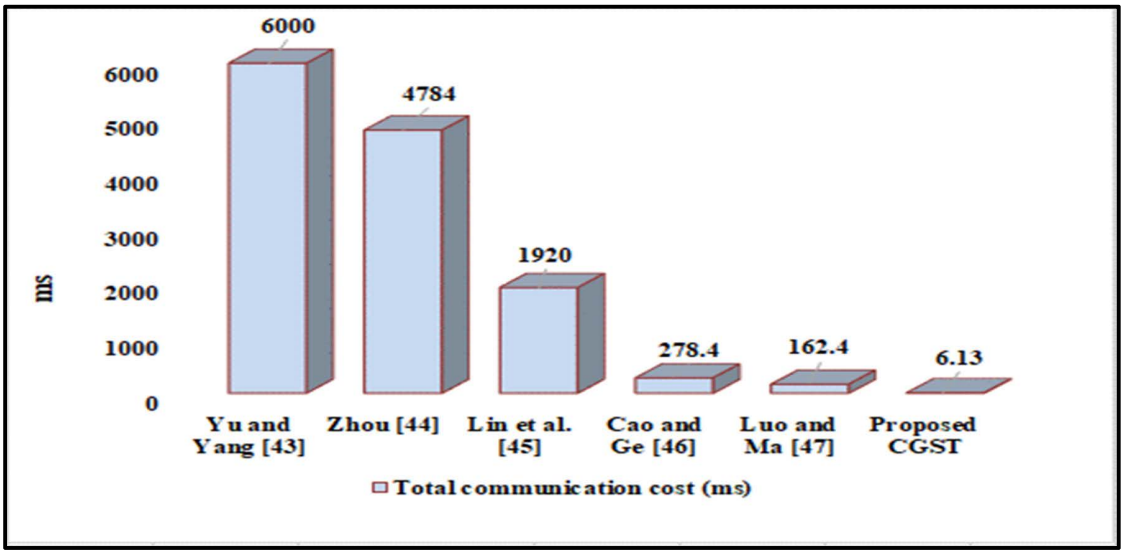

FIGURE 5. Total communication cost (ms).

VI. APPLICATION OF THE PROPOSED CGST-FCM TECHNIQUE

The proposed CGST-FCM technique would find useful applications in e-commerce, which is fast-growing globally. Nowadays, billions of online transactions are conducted in real-time seamlessly. Consequently, there are growing concerns about transmitting sensitive user information across open wireless channels. Therefore, the security of critical

user information via online transactions becomes imperative. The projected CGST-FCM scheme is well-equipped with sophisticated security features to guarantee user data authentication, security, and unforgeability over these open wireless channels. The proposed CGST-FCM scheme is ready-to-use and applicable in electronic commerce and other emerging wireless platforms.

VII. CONCLUSION

This paper projected a lightweight, provably secure certificateless group signcryption technique using FCM. The proposed CGST scheme has robust security against an IND-CCA attack in the FCM. The CGST-FCM scheme preserves all anticipated features of a certificateless signcryption procedure with a group signature technique. Additionally, the proposed technique tests the validity of the signcrypted text, anonymity of the client, and non-repudiation of the signcryption method. The complexity of solving two challenging computational problems comprising the Fractional Chaotic Maps-Discrete Logarithm Problem (FCM-DLP) and the Fractional Chaotic Maps-Diffie-Helmann Problem (FCM-DHP), guarantees the security of this technique. The proposed CGST-FCM technique can be used in various low-power devices with minimal processing power resources, such as smart cards. However, the only limitation of the fractional chaotic maps-based technique is sample selection. Therefore, future work would focus on an efficient e-cash system leveraging the proposed CGST-FCM scheme to address the envisioned sample selection issues. Finally, our future work will investigate an experimental implementation of the proposed lightweight security scheme.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers of IEEE Access for the critical comments which helped to improve the quality of this work.

REFERENCES

[1] C. Meshram, A. L. Imoize, A. Elhassouny, A. Aljaedi, A. R. Alharbi, and S. S. Jamal, "IBOOST: A lightweight provably secure identity-based online/offline signature technique based on FCM for massive devices in 5G wireless sensor networks," *IEEE Access*, vol. 9, pp. 131336–131347, 2021, doi: 10.1109/ACCESS.2021.3114287.

[2] C. Meshram, A. L. Imoize, A. Aljaedi, A. R. Alharbi, S. S. Jamal, and S. K. Barve, "A provably secure IBE transformation model for PKC using conformable Chebyshev chaotic maps under human-centered IoT environments," *Sensors*, vol. 21, no. 21, p. 7227, Oct. 2021, doi: 10.3390/s21217227.

[3] C. Meshram, M. S. Obaidat, K.-F. Hsiao, A. L. Imoize, and A. Meshram, "An effective fair off-line electronic cash protocol using extended chaotic maps with anonymity revoking trustee," in *Proc. Int. Conf. Commun., Comput., Cybersecurity, Informat. (CCCI)*, Oct. 2021, pp. 1–5, doi: 10.1109/ccci52664.2021.9583217.

[4] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, 2001, doi: 10.1109/7384.963463.

[5] P. Bergamo, P. D'Arco, A. de Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev polynomials," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 52, no. 7, pp. 1382–1393, Jul. 2005, doi: 10.1109/TCSI.2005.851701.

[6] D. Dharminder, U. Kumar, and P. Gupta, "A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services," *Complex Intell. Syst.*, vol. 7, no. 5, pp. 2531–2542, Oct. 2021, doi: 10.1007/s40747-021-00441-7.

[7] A. L. Imoize, O. Adedeji, N. Tandiya, and S. Shetty, "6G enabled smart infrastructure for sustainable society: Opportunities, challenges, and research roadmap," *Sensors*, vol. 21, no. 5, 1709, pp. 1–58, 2021, doi: 10.3390/s21051709.

[8] S. Rashid, S. Sultana, Z. Hammouch, F. Jarad, and Y. S. Hamed, "Novel aspects of discrete dynamical type inequalities within fractional operators having generalized ń-discrete Mittag–Leffler kernels and application," *Chaos, Solitons Fractals*, vol. 151, Oct. 2021, Art. no. 111204, doi: 10.1016/j.chaos.2021.111204.

[9] A. Mehmood, I. Noor-Ul-Amin, and A. I. Umar, "Public verifiable generalized authenticated encryption based on hyper elliptic curve," *J. Appl. Environ. Biol. Sci*, vol. 7, no. 12, pp. 69–73, 2017.

[10] C. Meshram, R. W. Ibrahim, S. G. Meshram, S. S. Jamal, and A. L. Imoize, "An efficient authentication with key agreement procedure using Mittag–Leffler–Chebyshev summation chaotic map under the multi-server architecture," *J. Supercomput.*, vol. 78, no. 4, pp. 4938–4959, Mar. 2022, doi: 10.1007/s11227-021-04039-1.

[11] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption)," in *Advances in Cryptology—CRYPTO '97* (Lecture Notes in Computer Science), vol. 1294, B. S. Kaliski, Ed. Berlin, Germany: Springer, 1997, doi: 10.1007/BFb0052234.

[12] L. Chen and J. Malone-Lee, "Improved identity-based signcryption," in *Public Key Cryptography—PKC 2005* (Lecture Notes in Computer Science), vol. 3386, S. Vaudenay, Ed. Berlin, Germany: Springer, 2005, doi: 10.1007/978-3-540-30580-4_25.

[13] Y. Ming and Y. Wang, "Cryptanalysis of an identity based signcryption scheme in the standard model," *Int. J. Netw. Secur.*, vol. 18, no. 1, pp. 165–171, 2016.

[14] Y. Huang and J. Yang, "A novel identity-based signcryption scheme in the standard model," *Information*, vol. 8, no. 2, p. 58, May 2017.

[15] T.-T. Tsai, S.-S. Huang, and Y.-M. Tseng, "SIBSC: Separable identity-based signcryption for resource-constrained devices," *Informatica*, vol. 28, no. 1, pp. 193–214, Jan. 2017.

[16] C. Zhou, W. Zhou, and X. Dong, "Provable certificateless generalized signcryption scheme," *Design, Codes Cryptogr.*, vol. 71, no. 2, pp. 331–346, 2014.

[17] M. Barbosa and P. Farshim, "Certificateless signcryption," *Proc. ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*, 2008, pp. 369–372, doi: 10.1145/1368310.1368364.

[18] W. Shi, N. Kumar, P. Gong, and Z. Zhang, "Cryptanalysis and improvement of a certificateless signcryption scheme without bilinear pairing," *Frontiers Comput. Sci.*, vol. 8, no. 4, pp. 656–666, 2014.

[19] D. Aranha, R. Castro, J. Lopez, and R. Dahab. (2008). *Efficient Certificateless Signcryption*. 8o Simpósio Bras. [Online]. Available: http://sbseg2008.inf.ufrgs.br/anais/data/pdf/st03_01_resumo.pdf.

[20] C. H. Wu and Z. X. Chen, "A new efficient certificateless signcryption scheme," in *Proc. Int. Symp. Inf. Sci. Eng. (ISISE)*, vol. 1, Dec. 2008, pp. 661–664, doi: 10.1109/ISISE.2008.206.

[21] M. Luo and Y. Wan, "An enhanced certificateless signcryption in the standard model," *Wireless Pers. Commun.*, vol. 98, no. 3, pp. 2693–2709, Feb. 2018, doi: 10.1007/s11277-017-4995-4.

[22] P. Rastegari, W. Susilo, and M. Dakhlalian, "Efficient certificateless signcryption in the standard model: Revisiting luo and Wan's scheme from wireless personal communications (2018)," *Comput. J.*, vol. 62, no. 8, pp. 1178–1193, Aug. 2019.

[23] Z. Guo, "Cryptanalysis of a certificateless conditional privacy-preserving authentication scheme for wireless body area networks," *Int. J. Electron. Inf. Eng.*, vol. 11, no. 1, pp. 1–8, 2019.

[24] G. Gao, X. Peng, and L. Jin, "Efficient access control scheme with certificateless signcrytion for wireless body area networks," *Int. J. Netw. Secur.*, vol. 21, no. 3, pp. 428–437, 2019, doi: 10.1109/JSEN.2016.2554625.

[25] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K. R. Choo, and Y. Park, "Certificateless-signcryption-based three-factor user access control scheme for IoT environment," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3184–3197, Apr. 2020, doi: 10.1109/JIOT.2020.2966242.

[26] C. Wu, H. Huang, K. Zhou, and C. Xu, "Cryptanalysis and improvement of a new certificateless signature scheme in the standard model," *China Commun.*, vol. 18, no. 1, pp. 151–160, Jan. 2021, doi: 10.23919/jcc.2021.01.013.

[27] K.-A. Shim, "A new certificateless signature scheme provably secure in the standard model," *IEEE Syst. J.*, vol. 13, no. 2, pp. 1421–1430, Jun. 2019, doi: 10.1109/JSYST.2018.2844809.
[28] H. Yeh, H. Sun, and T. Hwang, "Efficient three-party authentication and key agreement protocols resistant to password guessing attacks," *J. Inf. Sci. Eng.*, vol. 19, pp. 1059–1070, 2003.
[29] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," *IEE Proc. Inf. Secur.*, vol. 153, no. 1, pp. 27–39, Mar. 2006.
[30] C. Meshram, C. C. Lee, A. S. Ranadive, C. T. Li, S. G. Meshram, and J. V. Tembhurne, "A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing," *Int. J. Commun. Syst.*, vol. 33, no. 7, pp. 1–15, 2020, doi: 10.1002/dac.4307.
[31] F. A. Shamsabadi and S. B. Chehelcheshmeh, "A cloud-based mobile payment system using identity-based signature providing key revocation," *J. Supercomput.*, vol. 78, no. 2, pp. 2503–2527, Feb. 2022, doi: 10.1007/s11227-021-03830-4.
[32] J. S. Teh, M. Alawida, and Y. C. Sii, "Implementation and practical problems of chaos-based cryptography revisited," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102421, doi: 10.1016/j.jisa.2019.102421.
[33] C. Meshram, C.-C. Lee, S. G. Meshram, and C.-T. Li, "An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem," *Soft Comput.*, vol. 23, no. 16, pp. 6937–6946, Aug. 2019, doi: 10.1007/s00500-018-3332-5.
[34] C. Meshram, C.-C. Lee, S. G. Meshram, and A. Meshram, "OOS-SSS: An efficient online/offline subtree-based short signature scheme using Chebyshev chaotic maps for wireless sensor network," *IEEE Access*, vol. 8, pp. 80063–80073, 2020, doi: 10.1109/ACCESS.2020.2991348.
[35] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons Fractals*, vol. 37, no. 3, pp. 669–674, Aug. 2008, doi: 10.1016/j.chaos.2006.09.047.
[36] C. Meshram, R. W. Ibrahim, L. Deng, S. W. Shende, S. G. Meshram, and S. K. Barve, "A robust smart card and remote user password-based authentication protocol using extended chaotic maps under smart cities environment," *Soft Comput.*, vol. 25, no. 15, pp. 10037–10051, Aug. 2021, doi: 10.1007/s00500-021-05929-5.
[37] C. Meshram, M. S. Obaidat, J. V. Tembhurne, S. W. Shende, K. W. Kalare, and S. G. Meshram, "A lightweight provably secure digital short-signature technique using extended chaotic maps for human-centered IoT systems," *IEEE Syst. J.*, vol. 15, no. 4, pp. 1–9, Dec. 2020, doi: 10.1109/JSYST.2020.3043358.
[38] S. Han and E. Chang, "Chaotic map based key agreement with/out clock synchronization," *Chaos, Solitons Fractals*, vol. 39, no. 3, pp. 1283–1289, Feb. 2009, doi: 10.1016/j.chaos.2007.06.030.
[39] C. Meshram, R. W. Ibrahim, A. J. Obaid, S. G. Meshram, A. Meshram, and A. M. A. El-Latif, "Fractional chaotic maps based short signature scheme under human-centered IoT environments," *J. Adv. Res.*, vol. 32, pp. 139–148, Sep. 2021.
[40] X.-J. Yang, D. Baleanu, and H. M. Srivastava, *Local Fractional Integral Transforms and Their Applications*. New York, NY, USA: Academic, 2015.
[41] C. Meshram, P. L. Powar, M. S. Obaidat, C. Lee, and S. G. Meshram, "Efficient online/offline IBSS protocol using partial discrete logarithm for WSNs," *IET Netw.*, vol. 7, no. 6, pp. 363–367, Nov. 2018, doi: 10.1049/iet-net.2018.0019.
[42] C. Meshram, C.-C. Lee, C.-T. Li, and C.-L. Chen, "A secure key authentication scheme for cryptosystems based on GDLP and IFP," *Soft Comput.*, vol. 21, no. 24, pp. 7285–7291, Dec. 2017, doi: 10.1007/s00500-016-2440-3.
[43] H. Yu and B. Yang, "Pairing-free and secure certificateless signcryption scheme," *Comput. J.*, vol. 60, no. 8, pp. 1187–1196, Aug. 2017, doi: 10.1093/comjnl/bxx005.
[44] C. Zhou, "Certificateless signcryption scheme without random oracles," *Chin. J. Electron.*, vol. 27, no. 5, pp. 1002–1008, Sep. 2018, doi: 10.1049/cje.2018.06.002.
[45] X.-J. Lin, L. Sun, H. Qu, and D. Liu, "Cryptanalysis of a pairing-free certificateless signcryption scheme," *Comput. J.*, vol. 61, no. 4, pp. 539–544, Apr. 2018.
[46] L. Cao and W. Ge, "Analysis of certificateless signcryption schemes and construction of a secure and efficient pairing-free one based on ECC," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 9, pp. 4527–4547, Sep. 2018.
[47] W. Luo and W. Ma, "Secure and efficient data sharing scheme based on certificateless hybrid signcryption for cloud storage," *Electronics*, vol. 8, no. 5, p. 590, May 2019.
[48] C. Meshram, A. Alsanad, J. V. Tembhurne, S. W. Shende, K. W. Kalare, S. G. Meshram, M. A. Akbar, and A. Gumaei, "A provably secure lightweight subtree-based short signature scheme with fuzzy user data sharing for human-centered IoT," *IEEE Access*, vol. 9, pp. 3649–3659, 2021, doi: 10.1109/ACCESS.2020.3046367.
[49] C.-C. Lee and C.-W. Hsu, "A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps," *Nonlinear Dyn.*, vol. 71, nos. 1–2, pp. 201–211, Jan. 2013, doi: 10.1007/s11071-012-0652-3.
[50] C. C. Lee, C. T. Li, and C. W. Hsu, "A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps," *Nonlinear Dyn.*, vol. 73, no. 1, pp. 125–132, Jul. 2013, doi: 10.1007/s11071-013-0772-4.
[51] D. He, N. Kumar, J.-H. Lee, and R. S. Sherratt, "Enhanced three-factor security protocol for consumer USB mass storage devices," *IEEE Trans. Consum. Electron.*, vol. 60, no. 1, pp. 30–37, Feb. 2014.

CHANDRASHEKHAR MESHRAM received the Ph.D. degree from Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India. He is a Post-doctoral Fellow under Dr. D. S. Kothari Post-doctoral Fellowship in New Delhi, India. He is currently an Assistant Professor with the Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, Chhindwara University, Betul, Madhya Pradesh, India. His research interests include cryptography and its application, neural networks, the IoT, WSN, medical information systems, *ad-hoc* networks, number theory, fuzzy theory, time series analysis, climate change, mathematical modeling, and chaos theory. He has published over 100 scientific articles on the research fields mentioned above in international journals and conferences. He is a regular reviewer for more than 60 international journals and conferences.

AGBOTINAME LUCKY IMOIZE (Member, IEEE) received the B.Eng. degree (Hons.) in electrical and electronics engineering from Ambrose Alli University, Nigeria, in 2008, and the M.Sc. degree in electrical and electronics engineering from the University of Lagos, Nigeria, in 2012. He is a Lecturer with the Department of Electrical and Electronics Engineering, University of Lagos. Before joining the University of Lagos, he was a Lecturer with the Bells University of Technology, Nigeria. He worked as the Core Networks Products Manager at ZTE, Nigeria, from 2011 to 2012; and as a Networks Switching Subsystem Engineer at Globacom, Nigeria, from 2012 to 2017. He was awarded the Fulbright Fellowship as a Visiting Research Scholar at the Wireless@VT Laboratory, Bradley Department of Electrical and Computer Engineering, Virginia Tech, USA, where he worked under the supervision of Prof. R. Michael Buehrer, from 2017 to 2018. He is currently a Research Scholar with Ruhr University Bochum, Germany, under the Nigerian Petroleum Technology Development Fund (PTDF) and the German Academic Exchange Service (DAAD) through the Nigerian-German Postgraduate Program. He has coedited one book and coauthored over 70 papers in peer-reviewed journals and conferences. His research interests include beyond 5G and 6G wireless communications, chaotic communications, and wireless security networks. He is a Registered Engineer with the Council for the Regulation of Engineering in Nigeria (COREN) and a member of the Nigerian Society of Engineers (NSE).

SAJJAD SHAUKAT JAMAL received the Ph.D. degree in mathematics from Quaid-i-Azam University, Islamabad, Pakistan. Currently, he is working as an Assistant Professor with the Department of Mathematics, King Khalid University, Abha, Saudi Arabia. His research interests include mathematics, number theory, cryptography, digital watermarking, and steganography. He has several quality research papers in well-reputed journals on the application of mathematics in multimedia security.

ADEL R. ALHARBI received the Bachelor of Science degree in computer science from Qassim University, Saudi Arabia, in 2008, the Master of Science degrees in security engineering and computer engineering from Southern Methodist University, Dallas, TX, USA, in 2013 and 2015, respectively, and the Doctor of Philosophy degree in computer engineering from Southern Methodist University, in 2017. He has been a Faculty Staff Member with the College of Computing and Information Technology, University of Tabuk, Saudi Arabia, since 2009. He acquired several academic certificates and published several scientific papers. He is interested in research involving mobile and smart devices applications, biometrics, security, networking, and machine learning.

SARITA GAJBHIYE MESHRAM received the M.Tech. degree (Hons.) in soil and water engineering from the College of Agricultural Engineering, Jawaharlal Nehru Krishi Vishwavidyalaya, Jabalpur, Madhya Pradesh, in 2009, and the Ph.D. degree in water resource development and management from IIT Roorkee, Uttarakhand, India, in 2015. She is a Postdoctoral Fellow under Dr. D. S. Kothari Postdoctoral Fellowship in New Delhi, India. Currently, she is associated with the Water Resources and Applied Mathematics Research Laboratory, Nagpur, India. She has published over 100 research papers in refereed journals, conference and workshop proceedings, and books. Her current research interests include geographical information systems, rainfall-runoff sediment yield modelling, and SCS-CN. She is carrying out her research work in the field of rainfall-runoff, sediment yield, water quality, application of RS and GIS water networks, applied mathematics, and cryptographic protocol. She is a member of some international society and a reviewer of the reputed journal.

IQTADAR HUSSAIN received the Ph.D. degree in mathematics focused on algebraic cryptography, in 2014. He is currently an Assistant Professor with Qatar University. His H-index is 23 and i-10 index is 34. His articles have 1320 Google Scholar citations. His current research interests include the applications of mathematical concepts in the field of secure communication and cybersecurity, where he has published 63 articles in well-known journals.