sensors

MDPI

Article

An Efficient Electronic Cash System Based on Certificateless Group Signcryption Scheme Using Conformable Chaotic Maps

Chandrashekhar Meshram [1], Agbotiname Lucky Imoize [2,3,*], Amer Aljaedi [4], Adel R. Alharbi [4], Sajjad Shaukat Jamal [5] and Sharad Kumar Barve [6]

1 Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Govt. Post-Graduation College, College of Chhindwara University, Betul 460001, India; cs_meshram@rediffmail.com
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, 44801 Bochum, Germany
4 College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia; aaljaedi@ut.edu.sa (A.A.); aalharbi@ut.edu.sa (A.R.A.)
5 Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia; shussain@kku.edu.sa
6 Water Resources and Applied Mathematics Research Lab, Nagpur 440027, India; drshardbarve@rediffmail.com
* Correspondence: aimoize@unilag.edu.ng

Abstract: Signcryption schemes leveraging chaotic constructions have garnered significant research interest in recent years. These schemes have proffered practical solutions towards addressing the vast security vulnerabilities in Electronic Cash Systems (ECS). The schemes can seamlessly perform message confidentiality and authentication simultaneously. Still, their applications in emerging electronic cash platforms require a higher degree of complexity in design and robustness, especially as billions of online transactions are conducted globally. Consequently, several security issues arise from using open wireless channels for online business transactions. In order to guarantee the security of user information over these safety-limited channels, sophisticated security schemes are solely desired. However, the existing signcryption schemes cannot provide the required confidentiality and authentication for user information on these online platforms. Therefore, the need for certificateless group signcryption schemes (CGSS) becomes imperative. This paper presents an efficient electronic cash system based on CGSS using conformable chaotic maps (CCM). In our design, any group signcrypter would encrypt information/data with the group manager (GM) and send it to the verifier, who confirms the authenticity of the signcrypted information/data using the public criteria of the group. Additionally, the traceability, unforgeability, unlinkability, and robust security of the proposed CGSS-CCM ECS scheme have been built leveraging computationally difficult problems. Performance evaluation of the proposed CGSS-CCM ECS scheme shows that it is secure from the Indistinguishably Chosen Ciphertext Attack. Finally, the security analysis of the proposed technique shows high efficiency in security-vulnerable applications. Overall, the scheme gave superior security features compared to the existing methods in the preliminaries.

Keywords: certificateless group signcryption scheme (CGSS); conformable chaotic maps (CCM); electronic cash system (ECS); signcrypter; provably secure schemes; authentication; E-commerce channels

Citation: Meshram, C.; Imoize, A.L.; Aljaedi, A.; Alharbi, A.R.; Jamal, S.S.; Barve, S.K. An Efficient Electronic Cash System Based on Certificateless Group Signcryption Scheme Using Conformable Chaotic Maps. *Sensors* **2021**, *21*, 7039. https://doi.org/10.3390/s21217039

Academic Editor: Jiankun Hu

Received: 17 September 2021
Accepted: 21 October 2021
Published: 23 October 2021

1. Introduction

In modern electronic commerce, digital signatures play a significant role due to integrity and authentication requirements. Integrity is a vital property that helps to monitor the received messages from being modified by an adversary, while the authentication property helps protect the sender from impersonation [1]. Currently, group signcryption schemes are gaining entrance into the e-commerce space. For example, Chaum and van

Heyst [2] introduced a group signature scheme that allows a signature from any group member to represent the group. However, several limitations of group signature schemes have been identified [3–5]. Only group members are eligible to sign, and the message receiver cannot know the signer, among others. In practice, a signcryption scheme should be designed to meet specific security attributes such as public verifiability, ciphertext authentication, public ciphertext authentication, and ciphertext anonymity [3–7]. Under favorable conditions, these should be designed with extremely hard assumptions. However, if an adversary can solve the hardness assumption of a given signcryption scheme, they can conveniently process the private keys of each user in the system [8]. The ability of the foe to solve the hardness assumption poses a severe security threat in electronic commerce channels, and the need to address such security vulnerabilities is not negotiable. In order to address this problem, this paper presents an efficient electronic commerce system based on a certificateless group signcryption scheme (CGSS) using conformable chaotic maps (CCM).

1.1. Contributions

The contributions of the paper are outlined as follows. First, we give comprehensive literature on the electronic commerce system based on certificateless group signcryption schemes. To ensure consumers' anonymity in e-commerce platforms, we merged the valuable features of a certificateless signature scheme (CSS) with a group signcryption scheme (GSS) in the projected CGSS-CCM scheme for the electronic cash system (ECS). This study proposed a new efficient certificateless group signcryption scheme and electronic cash system (ECS). For the electronic cash system development, we used certificateless group signcryption schemes, and for the development of certificateless group signcryption schemes, we used conformable chaotic maps. A group signcrypter, with the help of the group manager (GM), encrypts a communication on behalf of the group in our design. In this scenario, any group signcrypter would encrypt information/data with the GM and have it sent to the verifier, who then approves the authenticity of the signcrypted information/data using the public criteria of the group. We further examined the proposed scheme's security to confirm that neither the GM nor any other group member can yield a legal signcrypted text. Additionally, we carried out a performance analysis of the proposed CGSS-CCM scheme and demonstrated its indistinguishably under the chosen ciphertext attack. The traceability, unforgeability, unlinkability, and robust security of the proposed CGSS-CCM ECS scheme were verified using computationally difficult problems. Finally, we compared the security features of the proposed CGSS-CCM ECS scheme with the existing techniques using several standard metrics.

1.2. Paper Organization

The organization of the paper is as follows. Section 2 covers the related works. Section 3 presents the background and material. Section 4 covers the proposed certificateless group signcryption scheme using conformable chaotic maps; this section also captures the setup, partial private key generation, private key generation. user key generation, signcryption, verification, and opening. Section 5 gives a detailed security investigation of the proposed CGSS-CCM ECS scheme. In Section 6, the proposed electronic cash system based on CGSS using conformable chaotic maps is detailed. The scheme comprises the initialization, joining, withdrawal, payment, deposit, and identity revocation phases. In Section 7, the security analysis comprising unforgeability and anonymity of the proposed ECS scheme is highlighted, and the efficiency of the scheme is demonstrated. Section 8 focuses on the performance comparison of the proposed CGSS-CCM with other related schemes. Finally, Section 9 provides a concise conclusion to the paper.

2. Related Works

Conformable chaotic maps (CCM) are used to generate public and secret parameters of the proposed CGSS. CCM and pairing are different; the development of CCM depends

on the Chebyshev polynomial, but pairing depends on the bilinear pairing operation of the function. Pairing operations cover more computation costs than chaotic maps or CCM. Therefore, CCM or chaotic maps play a significant role in developing the lightweight cryptographic scheme compared to pairing operation.

In the existing literature, Shamir [3] reported an identity-based cryptographic scheme, whose idea motivated an identity-based multi-signcryption scheme [4], and a certificateless signature without pairing [5]. Similarly, Park et al. [6] reported an identity-based group signature, which allows verification of the group signature by examining the identities of the group members. However, if a change in the group structure occurs, previous group signatures provided by other group members become invalid. But this limitation is undesirable in practical e-commerce systems. Tseng and Jan [7] presented a related ID-based scheme that addresses most of the flaws identified in Park et al. [6]. In several works of literature, the key escrow problem has been named one of the main flaws of ID-based cryptosystems. Al-Riyami and Paterson [8] reported an encryption scheme that does not need a public key to address this issue. Similarly, Ma, Ao, and He [9] proposed a certificateless group signature to address the key escrow problem in ID-based group signature schemes.

In recent years, public-key cryptosystems are fast gaining widespread popularity in guaranteeing message confidentiality, non-repudiation, and more. Firstly, the message that has the private key of the sender is signed, and the message signature pair is encrypted using a temporal session key [10,11]. Consequently, the receiver's public key can be used to encrypt the session key before transmission, and the session key retrieved by the receiver recovers sent messages using his private key. This procedure is carried out after both the random session key and the receiver get the encrypted message-signature pair [12]. Afterwards, the receiver decrypts the encrypted message-signature pair using the session key. In this case, the authenticity and integrity of the message are confirmed by the receiver by verifying the signature using the sender's public key. However, the traditional signature and then encryption technique is cost-prohibitive and computationally intensive. In order to decrease the cost and processing time of this scheme, the idea of signcryption that combines the features of digital signature and encryption is presented by Zheng [13].

The signcryption scheme reported by Zheng uses the discrete logarithm (DL) problem over a finite field. Interestingly, an enhanced form of Zheng's scheme had been reported by Zheng and Imai [14] to tackle the inherent public verifiability issues discovered in the scheme reported by Zheng [13]. In the same vein, Bao and Deng's [15] modification to Zheng's scheme allows public verifiability. However, public verifiability is undesirable in practical applications requiring firewall filtering [16].

Gamage et al. [17] reported a robust signcryption scheme that maintains the public ciphertext authentication property. The scheme allows a seamless signature verification without an external entity based on the computationally Diffie–Hellman (CDH) protocol [18]. However, the CDH-based protocol cannot perform ciphertext anonymity. Consequently, a foe can conduct random checks to decipher the message's originality [19]. In practice, this is not desirable in e-commerce, where there is a need to adequately preserve the sender's information from any adversary. However, the schemes mentioned above did not address the forward secrecy property, which is crucial in e-commerce. Motivated by this gap in the literature, Chow et al. [19] offered a forward secure signcryption scheme that allows public ciphertext authentication. However, the scheme uses bilinear pairing, which increases the computational complexity [20].

Han et al. [21] have provided a forward secrecy scheme that does not use bilinear pairing. The scheme shows better efficiency than Chow et al. [19]. A forward secure proxy signcryption scheme with public verifiability was presented by Elkamchouchi, Nasr, and Ismail [22]. Though this scheme aggregates hard problems, it showed limited efficiency, perhaps due to composite modulus design, and cannot perform ciphertext authentication. Additionally, Iqbal and Afzal [23] have reported a related construction with forward secrecy and public ciphertext authentication for several applications. In a related study,

Chaudhry et al. [24] offered a signcryption scheme tailored for an e-commerce system. Still, the protocol cannot support forward secrecy and public verifiability, which are candidate requirements in e-cash systems [25,26].

The security of electronic cash systems is a significant issue contending the rapid development of e-commerce. Several security schemes have been presented to tackle this issue [27,28]. Specifically, Wang, Cao and Zhang [27] offer a novel scheme for untraceable electronic cash transactions based on discrete logarithm assumption and the cut-and-choose approach. Here, the bank is not involved in any payment between a user and a receiver.

In [28], the authors utilized the concept of a group signature scheme to design a robust ECS. However, the security issues threatening e-commerce channels remain, especially as the business community is growing exponentially. Thus, the security of e-commerce platforms is ripe for comprehensive research exploitation.

Following the preceding security schemes deployed in electronic cash systems, several electronic cash protocols leveraging cryptographic constructions have been reported [29–34]. In particular, Lee, Choi, and Rhee [29] proposed a robust security scheme to address the problem of double-spending in secure electronic cash systems. In work, due to Nishide and Sakurai [30], a security scheme has been offered to secure offline anonymous electronic cash systems. The goal is to preserve sensitive user information from being compromised by insiders. Kutubi, Alam, and Morimoto [31] proposed an offline electronic payment scheme that satisfies essential security requirements of e-payment platforms was proposed. The scheme offers simple computations, and the merchant can verify the spent e-coin leveraging Schnorr's blind signature. Additionally, the scheme enables trusted authorities to identify the dishonest spender if multiple spending occurs with ease.

Additionally, Islam [32] reported a provably secure pairingless identity-based signature scheme for use in an e-cash system. Recently, an exchange centre-based digital cash payment solution was reported by Xu and Li [33] to address several security issues proliferating the e-commerce domain. Lastly, Alidadi et al. [34] offered an identity-based signature with key revocation functions for a cloud-enabled mobile payment system.

It is evident, based on the previous research, that no work has implemented the certificateless group signcryption scheme based on conformable chaotic maps in an electronic cash system as in our proposed work.

3. Background and Materials

This segment reviews the various underlying concepts relating to the work before delving into the current investigation on certificateless group signcryption schemes using conformable chaotic maps (CGSS-CCM). First, a short-lived Chebyshev chaotic map implementation is presented. This is followed by a Chebyshev polynomial, conformable chaotic maps using the minimal method, and delineated a list of other techniques used in this development. A list of symbols used in the paper is provided in Table 1.

Table 1. List of symbols.

Symbol	Meaning
T^{a}	Conformable Chebyshev chaotic maps
$\mathfrak{n}$	Large integer
p_1, p_2	Large prime numbers
$\mathfrak{TD}_{\mathrm{KGC}}$	Identity of KGC
$\mathfrak{TD}_{\mathrm{GM}}$	Identity of GM
$\mathfrak{TD}_{C}$	Identity of C client
a	An arbitrary rational number
$\mathfrak{m}_{sk}$	Master secret key
$\mathcal{G}_{prk}$	Group's public key
$\mathcal{G}_{pbk}$	Group's private key
$\mathfrak{c}$	Cipher
$\mathfrak{fi}$	Hash function
$\mathfrak{m}_{pk}$	Public constraint
$\mathfrak{m}$	Message
$\mathfrak{k}$	Key

3.1. Chebyshev Chaotic Polynomials

The operatory of Chebyshev sequential polynomials (CSP) is investigated (see [35]). In the $\mathfrak{z}$ variation, CSP $T_{\mathfrak{y}}(\mathfrak{z})$ is a $\mathfrak{y}$-degree polynomial. Let the arrangement be $\mathfrak{z} \in [-1, 1]$, and $\mathfrak{y}$ be an integer. In general, CSP reported the following:

$$\begin{gathered} \mathrm{T}_{\mathfrak{y}}(\mathfrak{z}) = \cos(\mathfrak{y} \times arc\ \cos(\mathfrak{z})), \\ \mathrm{T}_0(\mathfrak{z}) = 1,\ \mathrm{T}_1(\mathfrak{z}) = \mathfrak{z}, \\ \mathrm{T}_{\mathfrak{y}}(\mathfrak{z}) = 2\mathfrak{z}\mathrm{T}_{\mathfrak{y}-1}(\mathfrak{z}) - \mathrm{T}_{\mathfrak{y}-2}(\mathfrak{z});\ \mathfrak{y} \geq 2 \end{gathered}$$

Under these conditions, the functional $arc\ \cos(\mathfrak{z})$ and $\cos(\mathfrak{z})$ denoted as $arc\ \cos: [-1,\ 1] \to [0,\ \pi]$ and $\cos: \mathrm{R} \to [-1,\ 1]$.

CSP has two fundamental properties: chaotic and semi-group properties [36–40].

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

(2) Semi-group property: The possessions of a semi-group meet the following criteria:

$$\begin{aligned} \mathrm{T}_{\ell}(\mathrm{T}_{w}(\mathfrak{z})) = \cos\ & (\ell arc\cos((\cos(warc\cos(\mathfrak{z}))))) \\ & = \cos(\ell arc\cos(\mathfrak{z})) \\ & = \mathrm{T}_{w\ell}(\mathfrak{z}) \\ & = T_{w}(\mathrm{T}_{\ell}(\mathfrak{z})), \end{aligned}$$

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

Zhang [40] showed that the semi-group property preserves the interval $(-\infty, +\infty)$, which may be utilized to improve the property as tracks:

$$\mathrm{T}_{\mathfrak{y}}(\mathfrak{z}) = 2\mathfrak{z}\mathrm{T}_{\mathfrak{y}-1}(\mathfrak{z}) - \mathrm{T}_{\mathfrak{y}-2}(\mathfrak{z});\ \mathrm{n} \geq 2$$

where $\mathfrak{z} \in (-\infty, +\infty)$ and q_1 is a large and safe prime. As a result, the property is:

$$\mathrm{T}_{\ell}(\mathrm{T}_{w}(\mathfrak{z}))(mod q_1) = \mathrm{T}_{w\ell}(\mathfrak{z})(mod q_1) = \mathrm{T}_{w}(\mathrm{T}_{\ell}(\mathfrak{z}))(mod q_1)$$

In addition, the semi-group property is retained. It is worth noting that extended Chebyshev polynomials commute under confirmation as well.

There are two assessments for Chebyshev polynomials (CP) that consider handling in polynomial time:

(1) The discrete log's (DL) task is to invent an integer ℓ with the end goal $T_\ell(\mathfrak{z}) = v$ given two items $\mathfrak{z}$ and v.
(2) The Diffie–Hellman problem (DHP) task is to measure the $T_{\ell w}(\mathfrak{z})$ element due to three elements $\mathfrak{z}$, $T_\ell(\mathfrak{z})$, and $T_w(\mathfrak{z})$.

3.2. Conformable Chebyshev Chaotic Maps (CCCM)

Previously, the conformable calculus (CC) was known as the conformable fractional calculus (CFC) [41]. However, it puts a burden on the known properties of fractional calculus (derivatives of non-integer power). CC, in essence, is responsible for future preparation.

Assume that u is a fractional (arbitrary) number between 0 and 1. An operator u is conformable differential if and only if α^0 is the self-operator and α^1 is the usual difference operational. For differentiable utility, α^u is clearly conformable if and only if $\beta = \beta(y)$.

$$\alpha^0\beta(y) = \beta(y), \ \alpha^1\beta(y) = \beta'(y).$$

Anderson et al. [41] have proposed a new formulation of CC derived from control theory to describe the performance of a proportional-differentiation controller that conforms to the error function. The following is the structure of the instruction.

Definition 1. If $u \in [0, 1]$ is true, then CC has in the following documentation.

$$\alpha^u\beta(y) = \eta_1(u,y)\beta(y) + \eta_0(u,y)\beta'(y),$$

where the η_1 and η_0 functions reach the limits

$$\lim_{u\to 0}\eta_1(u,y) = 1, \quad \lim_{u\to 1}\eta_1(u,y) = 0,$$
$$\lim_{u\to 0}\eta_0(u,y) = 0, \quad \lim_{u\to 1}\eta_0(u,y) = 1.$$

In order to get the overhead description, we shall deliberate $\eta_1(u,y) = (1-u)y^u$ and $\eta_0(u,y) = uy^{1-u}$, or $\eta_1(u,y) = \frac{(1-u)}{\Gamma(1+u)}$ and $\eta_0(u,y) = \frac{u}{\Gamma(1+u)}$ where $\alpha^u\beta(y)$ is the name of the $\beta(y)$ function's conformable differential operator. As a result, the fractional tuning connections of the function and its derivative, η_1, η_0 are always dependably.

We obtain the resulting structure by applying the notion of CC to express the polynomial $T_\mathfrak{y}(y)$:

Since $T'_\mathfrak{y}(y) = 2\mathfrak{y}T_{\mathfrak{y}-1}(y)$, then $\alpha^u T_\mathfrak{y}(y)$ has the subsequent formal relationship (1)

$$T^u_\mathfrak{y}(y) := \alpha^u T_\mathfrak{y}(y) = \eta_1(u,y)T_\mathfrak{y}(y) + \eta_0(u,y)T'_\mathfrak{y}(y) \tag{1}$$

The Formula (1) can be replaced by (2)

$$T^u_\mathfrak{y}(y) = \eta_1(u,y)T_\mathfrak{y}(y) + 2\mathfrak{y}\eta_0(u,y) \times \omega(y)T_{\mathfrak{y}-1}(y), \tag{2}$$

where $\omega(y) = 1 + 2y + \left(4y^2 - 1\right) + \ldots + \left(\mathfrak{y} - 1\right)$-times. The conformable Chebyshev polynomials (CCP) are defined by Equation (2) (See Figure 1 [42]).

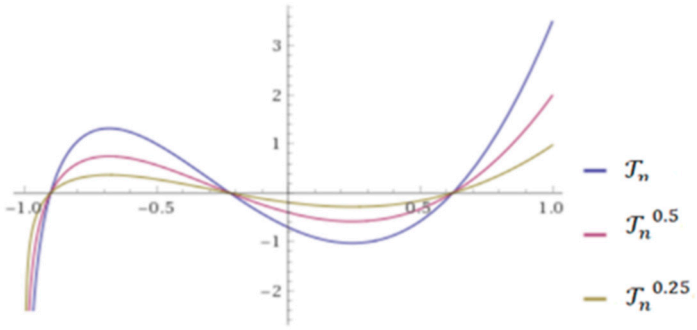

Figure 1. CCP for different values of $u = 0.25,\ 0.5,\ 1$ with $\eta_1(u,y) = \frac{(1-u)}{\Gamma(1+u)}$ and $\eta_0(u,y) = \frac{u}{\Gamma(1+u)}$.

Properties of CCCM: The CCCM possesses the following two exciting features:

Definition 2. *(Chaotic properties of CCCM).* The CCCM satisfies recurrent relations under the chaotic property [42] i.e.,

$$\mathrm{T}^u_{\mathfrak{y}}(y) = [2y\,\eta_1(\alpha,y) + 2\mathfrak{y}\,\eta_0\,(u,y) \times \omega(y)]\ \ \mathrm{T}_{\mathfrak{y}_{-1}}(y) - \eta_1(u,y)\mathrm{T}_{\mathfrak{y}_{-2}}(y)$$

Definition 3. (Semi-group properties of CCCM). The semi-group properties look for CCCMs located on the interval $(-\infty, \infty)$ [42], i.e., $\mathrm{T}^u_k\left(\mathrm{T}^u_{\mathfrak{y}}(y)\right) = \mathrm{T}^u_{\mathfrak{y}}(\mathrm{T}^u_k(y)) = \mathrm{T}^u_{k\mathfrak{y}}(y)$

It is worth noting that when we use $u \to 0$, we get the original instance from [40].

At this point, we note that the DL and assignments for the CCP are approximately DHP occur.

4. The Proposed Certificateless Group Signcryption Scheme Based on Conformable Chaotic Maps

In this section, we introduced an efficient CGSS using conformable chaotic maps. A group of signcrypters $(\mathcal{SG}: C_1, C_2, \ldots, C_{\mathfrak{n}})$ is included in the proposed CGSS-CCM, and anyone can signcrypt a message using the GM on behalf of a KGC and the group. The proposed CGSS-CCM is divided into six phases, as follows:

4.1. Setup

Using the safe prime techniques [43,44], the KCG chooses an integer $n = p_1 \times p_2$ where p_1, p_2 are enormous primes. After that, they choose g as a GF (p_1) generator and pick the $a \in [0,1]$ rational number. Then they give $\mathfrak{n}$ and g to the GM.

4.2. Partial Private Key Generation (PPKG)

The KGC is in charge of this operation. As it secretes factor and their identification $\mathfrak{TD}_{\mathrm{KGC}}$, the KGC selects a master secret key $\mathfrak{m}_{sk}$ at this point. Then they assess $\mathfrak{m}_{pk}$, a public constraint whose security is guaranteed by solving conformable chaotic maps.

$$\mathfrak{m}_{pk} = \mathrm{T}^a_{\mathfrak{m}_{sk}}(g)(mod\ \mathfrak{n})$$

Then they hand over $\left(\mathfrak{m}_{pk},\ \mathfrak{TD}_{\mathrm{KGC}}\right)$ to the GM.

4.3. Private Key Generation (PKG)

The PKG measurements are as follows: the GM selects three private variables λ, d and $\mathfrak{TD}_{\mathrm{GM}}$, and then calculates the group's public and private keys as follows.

$$\mathcal{G}_{prk} = \lambda \times \mathfrak{m}_{pk} + \mathfrak{TD}_{\mathrm{KGC}} \times \mathfrak{TD}_{\mathrm{GM}} (mod\ \mathfrak{n})$$

$$\mathcal{G}_{pbk} = \mathrm{T}^{a}_{\mathcal{G}_{prk}}(g)(mod\ \mathfrak{n})$$

$$ed \equiv 1\ mod\ \phi(\mathfrak{n}).$$

The GM then makes $\left(\mathfrak{n}, g, \mathfrak{m}_{pk}, \mathfrak{TD}_{\mathrm{GM}}, e, \mathcal{G}_{prk}\right)$ variables public while keeping them $\left(\lambda,\ e,\ \mathcal{G}_{prk}\right)$ secret as their private key.

4.4. User Key Generation (UKG)

The signcrypter and the GM are in this phase. This level's steps are listed below.

Step 1. After determining the public factor, any signcrypter picks a secret parameter $W \in \mathbb{Z}^{*}_{\mathfrak{n}}$ on behalf of the party and calculates $\mathfrak{TD}_C$ as follows:

$$\mathfrak{TD}_C = \mathrm{T}^{a}_{W}(\mathfrak{TD}_{\mathrm{GM}})(mod\ \mathfrak{n})$$

The $\mathfrak{TD}_C$ is then sent to the GM through a private channel.

Step 2. Following the estimation of $\mathfrak{TD}_C$, the GM selects a secrete parameter $\alpha \in \mathbb{Z}^{*}_{\mathfrak{n}}$ and estimates $\omega_1,\ \omega_2,\ \omega_3$ as follows:

$$\omega_1 = \mathrm{T}^{a}_{\alpha}(\mathfrak{TD}_C)(mod\ \mathfrak{n})$$

$$\omega_2 = (\alpha \times \mathcal{T} + \omega_1)(mod\ \mathfrak{n})$$

$$\omega_3 = \mathrm{T}^{a}_{\omega_1 \times d}(\mathfrak{TD}_{\mathrm{GM}})(mod\ \mathfrak{n})$$

The GM sends $(\omega_1,\ \omega_2,\ \omega_3)$ to the signcrypter after measuring all of the values.

Step 3. The signcrypter then uses this equation to check the parameter's authenticity.

$$\mathrm{T}^{a}_{\omega_2}(\mathfrak{TD}_C) = (\mathrm{T}^{a}_{\mathcal{T}}(\omega_1) \times \mathrm{T}^{a}_{eW}(\omega_3))(mod\ \mathfrak{n})$$

If this equation holds true, the client will receive three factors; if it does not, the client will return it to the GM.

Correctness.

$$\begin{aligned}
\mathrm{T}^{a}_{\omega_2}(\mathfrak{TD}_C) &= \left(\mathrm{T}^{a}_{\alpha \mathrm{T}}(\mathfrak{TD}_C) \times \mathrm{T}^{a}_{\omega_1}(\mathfrak{TD}_C)\right)(mod\ \mathfrak{n}) \\
&= \left(\mathrm{T}^{a}_{\mathcal{T}}(\omega_1) \times \mathrm{T}^{a}_{W\omega_1}(\mathfrak{TD}_{\mathrm{GM}})\right)(mod\ \mathfrak{n}) \\
&= (\mathrm{T}^{a}_{\mathcal{T}}(\omega_1) \times \mathrm{T}^{a}_{(\frac{W}{d})}(\omega_3))(mod\ \mathfrak{n}) \\
&= (\mathrm{T}^{a}_{\mathcal{T}}(\omega_1) \times \mathrm{T}^{a}_{eW}(\omega_3))(mod\ \mathfrak{n})
\end{aligned}$$

4.5. Signcryption

The client will signcrypt the text on behalf of the party at this point. The client initially chooses a $\mathfrak{y} \in \mathbb{Z}^{*}_{\mathfrak{n}}$ private factor, after which he/she determines the following: Key ($\mathfrak{k}$) and cipher ($\mathfrak{c}$).

$$U = \mathfrak{y} + \mathrm{T}^{a}_{(\frac{e}{\omega_1})}(\omega_3)(mod\ \mathfrak{n})$$

$$\mathrm{Key}(\mathfrak{k}) = \mathfrak{h}\left(U \times \mathfrak{y}\right)(mod\ \mathfrak{n})$$

$$Cipher\ (\mathfrak{c}) = (\mathfrak{k} \times Message(\mathfrak{m})) + \mathcal{G}_{pbk}(mod\ \mathfrak{n})$$

$$\lambda = \left(\mathrm{T}^{a}_{\omega_3}\left(\mathcal{G}_{pbk}\right) \times \mathrm{T}^{a}_{W}(\mathfrak{TD}_{\mathrm{GM}})\right)(mod\ \mathfrak{n}) \tag{3}$$

$$\lambda_1 = \mathrm{T}^{a}_{\omega_3}(g)(mod\ \mathfrak{n}) \tag{4}$$

$$\lambda_2 = \lambda + \mathrm{T}^{a}_{\mathfrak{m}}(\lambda_1)(mod\ \mathfrak{n}) \tag{5}$$

The client then refers the verifier to the signcrypted text $(U,\ \mathfrak{c},\ \lambda, \lambda_1, \lambda_2)$.

4.6. Verification

The verifier confirms the legitimacy of the signcrypted information after discovering it, but first, they must locate the message. The verifier evaluates the following processes to locate a message:

$$\mathfrak{y} = (U - \mathfrak{TD}_{\mathrm{GM}}) \ (mod\ \mathfrak{n})$$

$$\mathfrak{k}' = \mathfrak{h}\left(U \times \mathfrak{y}'\right) \ (mod\ \mathfrak{n}) \tag{6}$$

$$\mathfrak{m}' = \left(U - \mathcal{G}_{pbk}\right) \times \left(\mathfrak{k}'\right)^{-1} (mod\ \mathfrak{n}) \tag{7}$$

Otherwise, they would dismiss the communication as illegitimate. As soon as the message is identified, the verifier verifies its legitimacy.

$$\lambda_2 = \lambda + \mathrm{T}^a_{\mathfrak{m}}(\lambda_1) (mod\ \mathfrak{n}) \tag{8}$$

If this occurs, the verifier will create the signcrypted text on the message.

4.7. Opening

The GM will identify the sender if the sender is involved in a legal issue.

$$\mathfrak{TD}_C = \frac{\lambda}{\mathrm{T}^a_{prk}(\lambda_1)} (mod\ \mathfrak{n}) \tag{9}$$

5. Security Investigation of the Proposed CGSS-CCM ECS Scheme

The proposed CGSS-CCM scheme is given a formal security foundation in this section. As a result, two types of adversaries are studied, and the proposed technique's security assessment is detailed as follows.

Theorem 1. The CGSS-CCM generated signcrypted text that is correct.

Proof. This theorem demonstrates the correctness property of the projected CGSS-CCM scheme. □

We can observe, as a result of Equation (5), that

$$\begin{aligned}
\mathfrak{y}' &= (U - \mathfrak{TD}_{\mathrm{GM}})(mod\ \mathfrak{n}) \\
&= U - \mathrm{T}^a_{\mathfrak{e}d}(\mathfrak{TD}_{\mathrm{GM}})(mod\ \mathfrak{n}) \\
&= U - \mathrm{T}^a_{(\mathfrak{e}d)^{\frac{\omega_1}{\omega_3}}}(\mathfrak{TD}_{\mathrm{GM}})(mod\ \mathfrak{n}) \\
&= U - \mathrm{T}^a_{(\frac{\mathfrak{e}}{\omega_1})}(\omega_3)(mod\ \mathfrak{n}) \\
&= \mathfrak{y}
\end{aligned}$$

The suggested CGSS-CCM scheme appears to be implemented appropriately.

Theorem 2. The CGSS-CCM is expected to have traceability capabilities, such as the ability for the GM only to open the signcrypter identification that has signed the signcrypted document.

Proof. As a result of Equation (7), we realize that a signcrypter's identity can be retrieved as $\mathfrak{TD}_U = \omega / {\omega_1}^{\mathcal{G}_{prk}}$. □

Let

$$\frac{\lambda}{\mathrm{T}^a_{\mathcal{G}_{prk}}(\lambda_1)} = \frac{\mathrm{T}^a_{\omega_3}\left(\mathcal{G}_{pbk}\right) \times \mathrm{T}^a_W(\mathfrak{TD}_{\mathrm{GM}})}{\mathrm{T}^a_{\omega_3 \mathcal{G}_{prk}}(g)} (mod\ \mathfrak{n}) = \mathfrak{TD}_C (mod\ \mathfrak{n})$$

As a result, the traceability properties of the proposed CGSS-CCM approach are fulfilled.

Theorem 3. Using the CCM-CDHP, the given CGSS-CCM can withstand Type-II and Type-I attacks, as stated below.

Definition 4. (Type I Attack). A foe (F_1) having access to the device will be unable to gain the master secret key. However, F_1 can generate a signcrypted text by substituting public keys, removing private and partial private keys.

Proof. The game is played among the challenger (c) and the foe $\left(\mathrm{F}_1\right)$ and the challenger (c) in the Type-I attack. The steps outlined below are used to communicate between them. □

PPKG: When the challenger (c) requests it, the challenger (c) conducts the setup procedure to generate a KGC's master private key and a public factor $\left(\mathfrak{m}_{pk}\right)$ corresponding to the KGC's identification ($\mathfrak{TD}$), then transmits $\left(\mathfrak{m}_{pk}\right)$ to the foe $\left(\mathrm{F}_1\right)$.

Key generation (KG): In the KG stage, the challenger (c) evaluates a (λ) private value after learning the GM's identification ($\mathfrak{TD}_{\mathrm{GM}}$), then uses the private key and partial secrete key to estimate the GM's private key $\left(\mathcal{G}_{prk}\right)$ and communicate it to the foe.

Request public key: For any identification, the adversary will now turn to the public key. The challenger calculates the value of the GM's public key $\left(\mathcal{G}_{prk}\right)$ and delivers it to the foe after getting the appeal.

Replace public key: The foe creates a novel λ_1 private value and substitutes the challenger's public key with their own public key $\left(\mathcal{G}_{prk1}\right)$ after obtaining the challenger's public key.

Signcryption: For signcrypt, the client chooses specific secret values, but for a challenger message, the GM's public key and the original text are required. The challenger then sends the signed text $S = (U,\ c, \lambda,\ \lambda_1,\ \lambda_2)$ on message m_1 to the foe using a public key for the sender's identity that matches the GM's public key. The foe wins the game if Designcrypt $\left(\mathfrak{m}_{pk1},\ \mathfrak{TD}_{\mathrm{GM1}},\ \lambda_1,\ \mathfrak{m}_1,\ S_1\right)$ equals 1, but the adversary does not breach the security since the foe cannot enquire about the signcryption on the message $\mathfrak{m}_1$ and the private key for an $\mathfrak{TD}_{\mathrm{GM1}}$.

Definition 5. (Type II Attack). The foe $\left(\mathrm{F}_2\right)$ has retrieved the master key via a Type-II attack but cannot substitute any client's public key.

Proof. The challenger (c) and the foe $\left(\mathrm{F}_2\right)$ compete in this game. □

PPKG: The challenger then uses the setup method to generate a KGC's master private key and an $\left(\mathfrak{m}_{pk}\right)$ public factor based on the KGC's identity ($\mathfrak{TD}$), and then delivers the public and private keys to the foe. After that, the adversary would be able to estimate the partial private key.

Key generation: Following the GMs identify ($\mathfrak{TD}_{\mathrm{GM}}$), the challenger ($c$) estimates a (λ) hidden value, calculates the GM's private key $\left(\mathcal{G}_{prk}\right)$ using the partial private key and secret key and delivers it to the foe $\left(\mathrm{F}_2\right)$.

Request public key: The challenger then determines the GM's following public key and, upon request, provides it to the foe.

Signcryption: The challenger can now estimate a signcrypted text $S_1 = (U,\ c, \lambda,\ \lambda_1,\ \lambda_2)$ on message $\mathfrak{m}_1$ and give it to the foe $\left(\mathrm{F}_2\right)$ using a public key for the sender's identity and the GM's public key. The foe wins the game if Designcrypt $\left(\mathfrak{m}_{pk1},\ \mathfrak{TD}_{\mathrm{GM}\,1},\ \lambda_1,\ \mathfrak{m}_1,\ S_1\right)$ equals 1, but the adversary does not breach the security since the foe cannot request the

signcryption on the message $\mathfrak{m}_1$ and the private key for an $\mathfrak{TD}_{\mathrm{GM}1}$. The presented system has also been proved to be resistant to Type-II and Type-I attacks.

Theorem 4. The proposed CGSS-CCM satisfies the unlinkability property.

Proof. The verifier confirms the signcrypted info by using the group's $\mathcal{G}_{pbk}$ public info and $\mathfrak{TD}_{\mathrm{GM}}$ as exposed in Equation (6) after discovering the group signcrypted info $(U, c, \lambda, \lambda_1, \lambda_2)$ for $\mathfrak{m}$ message . If the verifier receives alternative signcrypted information $(U', c', \lambda', \lambda_1', \lambda_2')$ for the message $\mathfrak{m}'$. In the two signcrypted info $(U, c, \lambda, \lambda_1, \lambda_2)$, there are no identical variables. When the verifier wishes to know the signcrypter's identity $(\mathfrak{TD})$, they must consult the GM. The projected CGSS-CCM also comprises five variables, namely $\left(\alpha, \mathfrak{y}, U, W, \mathfrak{e}\right)$, to hide the precise estimate of the group's signcrypted info/text. As a result, it is impossible to decode the estimates of $\left(\alpha, \mathfrak{y}, U\right)$ from the signcrypted data. As a result, an adversary would never be able to link signed data to the compliant signcrypter. □

6. Proposed Electronic Cash System Based on CGSS Using Conformable Chaotic Maps

This section proposes a new efficient electronic cash system based on CGSS using conformable chaotic maps. A consumer, a GM of that customer group (CG), a bank and a merchant participate in an ECS consisting of a series of protocols. In sum, an electronic cash system comprises the following six distinct phases, and Figure 2 depicts the planned E-cash scheme's configuration.

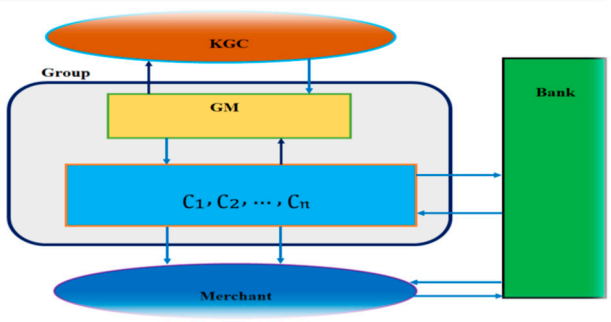

Figure 2. A model of the proposed electronic cash system (ECS).

6.1. Initialization

This stage is handled by a trusted third-party key generation center (KGC) and the GM because our projected method is a certificateless scheme. With KGC, the group's GM establishes a public and private key for the group.

Step 1. The KCG selects an integer $\mathfrak{n} = p_1 \times p_2$ where p_1, p_2 are huge primes using the secure prime schemes. Then they select g as a GF (p_1) generator and select a random $a \in [0, 1]$ rational number. Then they give g and $\mathfrak{n}$ to the GM.

Step 2. The KGC selects two secret parameters $\mathfrak{m}_{sk}'$ and $\mathfrak{TD}_{\mathrm{KGC}}' \in \mathbb{Z}_{\mathfrak{n}}^*$ at random and computes a public parameter $\mathfrak{m}_{pk}'$ as a result.

$$\mathfrak{m}_{pk}' = \mathrm{T}_{\mathfrak{m}_{sk}'}^{a}(g)(mod\ \mathfrak{n}) \tag{10}$$

Then, on a secret channel, they send $\left(\mathfrak{n}, \mathfrak{m}_{pk}', g\right)$ to the GM.

Step 3. The GM first selects a secret parameter $\lambda' \in \mathbb{Z}_{\mathfrak{n}}^*$ and their identification as $\mathfrak{TD}_{\mathrm{GM}}'$ after obtaining the parameter from the KGC, and then calculates the group's public and private key as

$$\mathcal{G}'_{prk} = \lambda' \times \mathfrak{m}'_{pk} + \mathfrak{TD}'_{\mathrm{KGC}} \times \mathfrak{TD}'_{\mathrm{GM}}\ (mod\ \mathfrak{n})$$
$$\mathcal{G}'_{Pbk} = \mathrm{T}^{a}_{\mathcal{G}'_{prk}}(g)(mod\ \mathfrak{n})$$
$$\mathfrak{e} \equiv 1\ mod\ \phi(\mathfrak{n}).$$

The GM then makes $(\mathfrak{n},\ g, \mathfrak{TD}'_{\mathrm{GM}},\ \mathfrak{e},\ \mathcal{G}'_{Pbk})$ public to everybody while keeping $\left(\ \mathfrak{e},\ \lambda', \mathcal{G}'_{prk}\right)$ private.

6.2. Joining Phase

Each customer $\mathfrak{C}_i$ wishes to join the CG in this step. Thus they engage with the GM as in Step 1. Initial, each customer $\mathfrak{C}_i$ selects a secret parameter $W' \in \mathbb{Z}^*_{\mathfrak{n}}$ at random and calculates the subsequent:

$$\mathfrak{TD}_{\mathfrak{C}_i} = \mathrm{T}^{a}_{w'}\left(\mathfrak{TD}'_{\mathrm{GM}}\right)(mod\ \mathfrak{n}) \tag{11}$$

They then send it to the GM.

GM produces a membership certificate for each customer after determining their identification.

$$\mathfrak{m}_{\mathfrak{C}_i} = \mathrm{T}^{a}_{W\prime}\left(\mathfrak{TD}_{\mathfrak{C}_i}\right)(mod\ \mathfrak{n}) \tag{12}$$

After, the GM adds a new record for customer identification with the membership certificate as $\left(\mathfrak{m}_{\mathfrak{C}_i},\ d\right)$.

6.3. Withdrawal Phase

The customer approaches the bank and requests a coin. The bank demands identity confirmation from the customer; thus, the customer must complete the promise stage before the procedure can be signcrypted.

Step 1. In this stage, each customer selects two secret parameters at random: $\alpha', \mathfrak{y}' \in \mathbb{Z}^*_{\mathfrak{n}}$, and calculates the signcrypted text as follows:

$$\omega_{11} = \mathrm{T}^{a}_{\alpha'}\left(\mathfrak{T}D_{\mathfrak{C}_i}\right)(mod\ \mathfrak{n})$$

$$\omega_{21} = \alpha' \times \mathcal{T} + \omega_{11}(mod\ \mathfrak{n})$$

where $\mathcal{T}$ is the time and date concatenation.

$$\omega_{31} = \mathrm{T}^{a}_{\omega_{11} \times e}\left(\mathfrak{m}_{\mathfrak{C}_i}\right)(mod\ \mathfrak{n})$$

$$U' = \mathfrak{y}' + \mathfrak{TD}'_{\mathrm{GM}}(mod\ \mathfrak{n})$$
$$\mathrm{Key}\left(\mathfrak{k}'\right) = \mathfrak{fi}\left(U' \times n'\right)(mod\ \mathfrak{n})$$
$$\mathfrak{C}' = \mathfrak{k}' \times \mathfrak{m}' + \mathcal{G}'_{Pbk}(mod\ \mathfrak{n})$$

Step 2. The bank verifies the text's legitimacy after discovering the signcrypted text from the customer.

$$\mathrm{T}^{a}_{\omega_{21}}\left(\mathfrak{TD}_{\mathfrak{C}_i}\right) = \mathrm{T}^{a}_{\mathcal{T}}(\omega_{11}) \times \omega_{31}(mod\ \mathfrak{n})$$

Correctness.

$$\mathrm{T}^{a}_{\omega_{21}}\left(\mathfrak{TD}_{\mathfrak{C}_i}\right) = \mathrm{T}^{a}_{\alpha' \times \mathcal{T} + \omega_{11}}\left(\mathfrak{TD}_{\mathfrak{C}_i}\right)(mod\ \mathfrak{n})$$
$$= \mathrm{T}^{a}_{\alpha' \times \mathcal{T}}\left(\mathfrak{TD}_{\mathfrak{C}_i}\right) \times \mathrm{T}^{a}_{\omega_{11}}\left(\mathfrak{TD}_{\mathfrak{C}_i}\right)(mod\ \mathfrak{n})$$
$$= \mathrm{T}^{a}_{\mathrm{T}}(\omega_{11}) \times \mathrm{T}^{a}_{\omega_{11}/d}\left(\mathfrak{m}_{\mathfrak{C}_i}\right)(mod\ \mathfrak{n})$$
$$= \mathrm{T}^{a}_{\mathrm{T}}(\omega_{11}) \times \mathrm{T}^{a}_{\omega_{11} \times e}\left(\mathfrak{m}_{\mathfrak{C}_i}\right)(mod\ \mathfrak{n})$$

$$= \mathrm{T}^{a}_{\omega_{21}}\left(\mathfrak{TD}_{\mathfrak{C}_i}\right) = \mathrm{T}^{a}_{\mathcal{T}}(\omega_{11}) \times \omega_{31}(mod\ \mathfrak{n})$$

If this equation is true, the bank calculates

$$\xi' = \mathrm{T}^{a}_{\omega_{31}}\left(\mathcal{G}'_{Pbk}\right) \times \mathfrak{TD}_{\mathfrak{C}_i}(mod\ \mathfrak{n})$$
$$\xi'_1 = \mathrm{T}^{a}_{\omega_{31}}(g)(mod\ \mathfrak{n})$$

The bank then sends the consumer these two parameters $\left(\xi',\ \xi'_1\right)$ as their bank identification.
Step 3. The customer calculates another secret parameter after obtaining the secret parameter from the bank.

$$\xi'_3 = \mathrm{T}^{a}_{\mathfrak{n}'}\left(\xi'_2\right)(mod\ \mathfrak{n})$$

where $\xi'_2 = \left(\xi' + \xi'_1\right)$ and stores the coin as $\left(\xi'_3, \mathbb{k}',\ \mathfrak{C}',\ U'\right)$

6.4. Payment Phase

The interaction between the merchant and the customer takes place during this phase.
Step 1. The customer delivers the coin $\left(\xi'_2,\ \xi'_3, \mathbb{k}',\ \mathfrak{C}',\ U'\right)$ to the merchant for payment. After locating the coin, the merchant first validates its legitimacy, which requires them to compute.

$$\mathfrak{y}' = U' - \mathfrak{TD}'_{\mathrm{GM}}(mod\ \mathfrak{n}).$$

Then they determine if the condition's value is met or not.

$$\mathfrak{fi}\left(U' \times \mathfrak{y}'\right) = \mathbb{k}'(mod\ \mathfrak{n}),$$

If yes, the merchant proceeds to the next step; otherwise, the customer is notified.

$$\mathbb{F} = \mathfrak{C}' - \mathcal{G}'_{Pbk}(mod\ \mathfrak{n})$$

and F's value is sent to the consumer.
Step 2. The customer then generates a new parameter as follows:

$$\mathbb{F}' = \left(\mathbb{F}/\mathfrak{m}'\right)\ (mod\ \mathfrak{n})$$

and $\mathbb{F}'$ value is sent to the merchant. If $\mathbb{F}' = \mathbb{k}'$, the merchant accepts the coin.

6.5. Deposit Phase

The interaction between the bank and the merchant is described in this phase.
Step 1. The merchant transmits this signcrypted text $\left(\xi'_2,\ \xi'_3,\ \mathbb{k}',\ \mathfrak{C}',\ U'\right)$ and the coin $(\mathbb{F}', \mathbb{F})$ to the bank after accepting the coin.
Step 2. The bank checks whether $\mathfrak{fi}\left(U' \times \mathfrak{y}'\right) = \mathbb{k}'(mod\ \mathfrak{n})$ if the coin exists, otherwise it sends an incorrect message.
The bank stores the coin $(\mathbb{F}',\ \mathbb{F})$ in the placed table if it is valid.

6.6. Identity Revocation Phase

In the event of a dispute, the bank will submit the signcrypted document to the GM, who will then identify the dishonest customer.

$$\mathfrak{TD}_{\mathfrak{C}_i} = \xi'/\mathrm{T}^{a}_{\mathcal{G}'_{prk}}\left(\xi'_1\right)\ (mod\ \mathfrak{n}) \tag{13}$$

7. Security Analysis of the Proposed CGSS-CCM ECS Scheme

This section details some of the security and effectiveness features of our ECS scheme. We demonstrate that our offline ECS scheme is secure from threats, such as forgery and anonymity.

7.1. Unforgeability

In the suggested approach, a fraudulent customer cannot falsify the coin because, in the event of blackmail or a legal disagreement, the bank notifies the GM of that client group. The GM can then use the equation $\mathfrak{TD}_{\mathfrak{C}_i} = \xi' / \mathrm{T}^{a}_{\mathcal{G}'_{prk}}(\xi'_1)(mod\ \mathfrak{n})$ to identify the customer's identification, and only the user who is the account owner in the withdrawal protocol can withdraw an e-coin.

7.2. Anonymity

The projected technique allows the user to make an anonymous payment to the merchant because the retailer is unaware of the customer's identity. They can only accept a coin from the user and check the correctness of the signcrypted document, but the merchant has no way of knowing who the customer is. As a result, the suggested system is unaffected by the anonymity attribute.

8. Performance Comparison

In this section, we compare our technique to recently contributed electronic cash systems [45–49] in terms of communication cost. The efficiency of the provided electronic cash system is evaluated based on communication costs. The output is compared based on the cost of the withdrawal and payment phases. In contrast to the installation, joining, deposit, and identity revocation stages, the withdrawal and payment phases need additional computational resources. As a result, the computation cost for the withdrawal and payment phases is used to perform the comparison analysis. In this part of the comparisons study, we utilized the following six notations of this complexity: $\dagger_h, \dagger_m, \dagger_{ch}, \dagger_e, \dagger_{sy}, \dagger_{ec}$ and $\dagger_p$ reported performance time for a one-way hash function modular multiplication, Chebyshev chaotic map operation, modular exponentiation in the group, symmetric encryption operation, elliptic curve scale multiplication, and bilinear pairing operations. The relations among $\dagger_h, \dagger_m, \dagger_{ch}, \dagger_e, \dagger_{sy}, \dagger_{ec}$ and $\dagger_p$ with respect to $\dagger_h$ ($\dagger_h = 0.32$ ms and $a = 1/2$ since $a \in [0,1]$ [46]) have been established in [38,50–53]. The following illustration depicts the relationship and order of computational complexity between the metrics: $\dagger_{ch} \approx \dagger_h, \dagger_m \approx 2.5\,\dagger_h, \dagger_{sy} \approx \dagger_h, \dagger_{ec} \approx 72.5\dagger_h, \dagger_e \approx 600\dagger_h, \dagger_p \approx 1550\dagger_h$ and $\dagger_h \approx \dagger_{ch} \approx \dagger_{sy} < \dagger_m < \dagger_{ec} < \dagger_e < \dagger_p$. Table 1 depicts the predicted electronic cash system's primary consuming operations as well as existing techniques. There are additional comparisons of computing costs in milliseconds (ms) in Figure 3. The evaluation results in Table 2 and Figure 4 show that the suggested electronic cash system has the lowest overall communication expense. In terms of running time, the proposed electronic cash system outperforms the other methods. The proposed CGSS-CCM ECS scheme would find useful applications in emerging wireless communication systems in the 6G era and beyond [54].

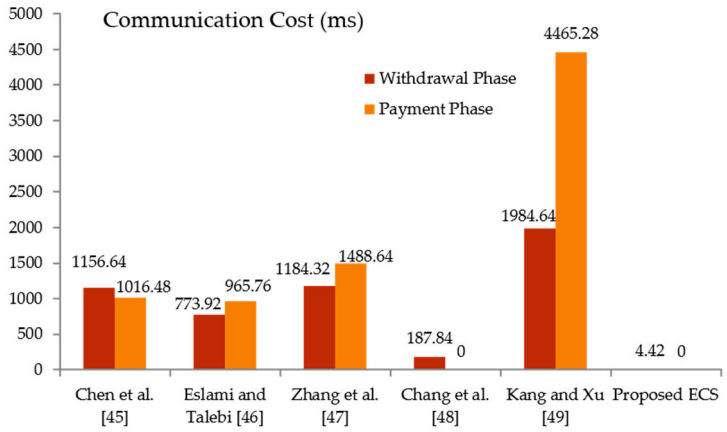

Figure 3. Communication cost (ms) in withdrawal and payment phases.

Table 2. Assessments of important operations with reverence techniques.

Techniques	Withdrawal Phase	Payment Phase	Total
Chen et al. [45]	$3\dagger_h + 3\dagger_p + 4\dagger_{sy} + 7\dagger_{ec}$	$2\dagger_h + 3\dagger_p + 2\dagger_{sy} + \dagger_{ec}$	$5\dagger_h + 6\dagger_p + 6\dagger_{sy} + 8\dagger_{ec}$
Eslami and Talebi [46]	$4\dagger_e + 7\dagger_m + \dagger_h$	$5\dagger_e + 6\dagger_m + 3\dagger_h$	$9\dagger_e + 13\dagger_m + 4\dagger_h$
Zhang et al. [47]	$2\dagger_h + 2\dagger_p + \dagger_e$	$2\dagger_h + 3\dagger_p$	$4\dagger_h + 5\dagger_p + \dagger_e$
Chang et al. [48]	$3\dagger_h + 4\dagger_{sy} + 8\dagger_{ec}$	0	$3\dagger_h + 4\dagger_{sy} + 8\dagger_{ec}$
Kang and Xu [49]	$2\dagger_h + 4\dagger_p$	$4\dagger_h + 9\dagger_p$	$6\dagger_h + 13\dagger_p$
Proposed ECS	$3\dagger_{ch} + \dagger_h + 3\dagger_m$	0	$3\dagger_{ch} + \dagger_h + 3\dagger_m$

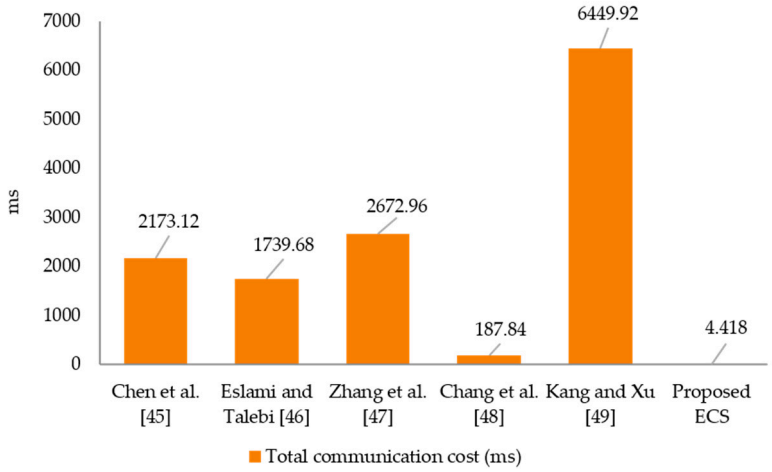

Figure 4. Total communication cost (ms).

9. Conclusions

This paper proposed an efficient and effective ECS based on the concept of CGSS-CCM, which is secure against an IND-CCA attack in conformable chaotic maps. In order to demonstrate the strengths of our CGSS-CCM enabled scheme, we performed standard security examinations. We found that it meets the requirements for anonymity and unforgeability in a well-designed and secure electronic cash payment system. Additionally, we compared the computational costs of our scheme with five other schemes, and the results showed that our ECS had lower costs than the other five schemes. Finally, our scheme can be helpful in many real-life applications, such as online auctions, e-banking, and electronic voting systems. Future work could extend the proposed CGSS-CCM assisted scheme to ease its applicability in emerging wireless application scenarios.

Author Contributions: C.M. and A.L.I. were responsible for the conceptualization of the topic; article gathering and sorting were carried out by C.M., A.L.I., A.A., A.R.A., S.S.J. and S.K.B.; manuscript writing and original drafting and formal analysis were carried out by C.M. and A.L.I.; writing of reviews and editing were carried out by A.L.I., A.A., A.R.A., S.S.J. and S.K.B.; C.M. and A.L.I. led the overall research activity. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing is not applicable to this article.

Acknowledgments: The authors would like to thank the Deanship of Scientific Research at King Khalid University for funding this work through the research groups program under grant number R. G. P. 1/72/42. The work of Agbotiname Lucky Imoize is supported by the Nigerian Petroleum Technology Development Fund (PTDF) and the German Academic Exchange Service (DAAD) through the Nigerian-German Postgraduate Program under Grant 57473408.

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

References

1. Zhang, J.; Wu, Q.; Wang, Y. A new efficient group signature with forward security. *Informatica* **2005**, *29*, 321–325.
2. Chaum, D.; van Heyst, E. Advances in Cryptology—EUROCRYPT '91. *Trans. Comput. Sci. XI* **1991**, *547*, 257–265. [CrossRef]
3. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In *Advances in Cryptology*; Springer: Amsterdam, The Netherlands, 2000; pp. 47–53.
4. Zhang, J.; Mao, J. A novel identity-based multi-signcryption scheme. *Comput. Commun.* **2009**, *32*, 14–18. [CrossRef]
5. Wan, Z.; Weng, J.; Li, J. Security Mediated Certificateless Signatures Without Pairing. *J. Comput.* **2010**, *5*, 1862–1869. [CrossRef]
6. Park, S.; Kim, S.; Won, D. ID-based group signature. *Electron. Lett.* **1997**, *33*, 1616–1617. [CrossRef]
7. Tseng, Y.-M.; Jan, J.-K. A novel ID-based group signature. *Inf. Sci.* **1999**, *120*, 131–141. [CrossRef]
8. Al-Riyami, S.S.; Paterson, K.G. Certificateless Public Key Cryptography. In *Advances in Autonomous Robotics*; Springer: Amsterdam, The Netherlands, 2003; Volume 2003, pp. 452–473.
9. Ma, C.; Ao, F.; He, D. Certificateless group inside signature. In Proceedings of the Autonomous Decentralized Systems, 2005. ISADS 2005, Chengdu, China, 4–8 April 2005; IEEE: Manhattan, NY, USA, 2005; pp. 194–200.
10. Li, F.; Shirase, M.; Takagi, T. Certificateless Hybrid Signcryption. *Adv. Knowl. Discov. Data Min.* **2009**, *2009*, 112–123. [CrossRef]
11. Rastegari, P.; Susilo, W.; Dakhlalian, M. Efficient Certificateless Signcryption in the Standard Model: Revisiting Luo and Wan's Scheme from Wireless Personal Communications (2018). *Comput. J.* **2019**, *62*, 1178–1193. [CrossRef]
12. Lee, T.-F. Provably Secure Anonymous Single-Sign-On Authentication Mechanisms Using Extended Chebyshev Chaotic Maps for Distributed Computer Networks. *IEEE Syst. J.* **2018**, *12*, 1499–1505. [CrossRef]
13. Zheng, Y. Digital signcryption or how to achieve cost (signature & encryption). In *Advances in Cryptology—CRYPTO '97*; Springer: Amsterdam, The Netherlands, 1997; pp. 165–179.
14. Zheng, Y.; Imai, H. How to construct efficient signcryption schemes on elliptic curves. *Inf. Process. Lett.* **1998**, *68*, 227–233. [CrossRef]
15. Bao, F.; Deng, R.H. A signcryption scheme with signature directly verifiable by public key. *Comput. Vis.* **1998**, 55–59. [CrossRef]
16. Daniel, R.; Rajsingh, E.B.; Silas, S. A forward secure signcryption scheme with ciphertext authentication for e-payment systems using conic curve cryptography. *J. King Saud Univ. Comput. Inf. Sci.* **2021**, *33*, 86–98. [CrossRef]
17. Gamage, C.; Leiwo, J.; Zheng, Y. Encrypted Message Authentication by Firewalls. In *Public Key Cryptography*; Springer: Berlin/Heidelberg, Germany, 1999; pp. 69–81.
18. Diffie, W.; Hellman, M.E. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
19. Chow, S.S.M.; Yiu, S.M.; Hui, L.C.K.; Chow, K.P. Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity. In *Information Security and Cryptology—ICISC 2003*; Springer: Amsterdam, The Netherlands, 2004; pp. 352–369.
20. Ullah, I.; Alkhalifah, A.; Rehman, S.U.; Kumar, N.; Khan, M.A. An Anonymous Certificateless Signcryption Scheme for Internet of Health Things. *IEEE Access* **2021**, *9*, 101207–101216. [CrossRef]
21. Han, Y.; Yang, X.; Hu, Y. Signcryption based on elliptic curve and its multi-party schemes. In Proceedings of the 3rd International Conference on Information Security, Shanghai, China, 14–16 November 2004; ACM: New York, NY, USA, 2004; pp. 216–217.
22. Elkamchouchi, H.; Nasr, M.; Ismail, R. A new efficient strong proxy signcryption scheme based on a combination of hard problems. In Proceedings of the 2009 IEEE International Conference on Systems, Man and Cybernetics, San Antonio, TX, USA, 11–14 October 2009; IEEE: Manhattan, NY, USA, 2009; pp. 5123–5127.
23. Iqbal, W.; Afzal, M.; Ahmad, F. An efficient elliptic curve based signcryption scheme for firewalls. In Proceedings of the 2013 2nd National Conference on Information Assurance (NCIA), Rawalpindi, Pakistan, 11–12 December 2013; IEEE: Manhattan, NY, USA, 2013; pp. 67–72.
24. Chaudhry, S.A.; Farash, M.S.; Naqvi, H.; Sher, M. A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. *Electron. Commer. Res.* **2016**, *16*, 113–139. [CrossRef]
25. Ahmed, F.; Bashir, F.; Masood, A. A Publicly Verifiable Low Cost Signcryption Scheme Ensuring Confidentiality. In Proceedings of the 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, Wuhan, China, 24–25 April 2010; IEEE: Manhattan, NY, USA, 2010; Volume 1, pp. 232–235.
26. Gutub, A.; Aljuaid, N.; Khan, E. Counting-based secret sharing technique for multimedia applications. *Multimed. Tools Appl.* **2019**, *78*, 5591–5619. [CrossRef]
27. Wang, H.; Cao, J.; Zhang, Y. Untraceable Electronic Cash System in the Internet of Things. In *Access Control Management in Cloud Environments*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 43–63. [CrossRef]
28. Maitland, G.; Boyd, C. Fair Electronic Cash Based on a Group Signature Scheme. *Comput. Vis.* **2001**, 461–465. [CrossRef]
29. Lee, H.J.; Choi, M.S.; Rhee, C.S. Traceability of double spending in secure electronic cash system. In Proceedings of the 2003 International Conference on Computer Networks and Mobile Computing, 2003. ICCNMC 2003, Shanghai, China, 20–23 October 2003; IEEE: Manhattan, NY, USA, 2004; pp. 330–333.
30. Nishide, T.; Sakurai, K. Security of Offline Anonymous Electronic Cash Systems against Insider Attacks by Untrusted Authorities Revisited. In Proceedings of the 2011 Third International Conference on Intelligent Networking and Collaborative Systems, Fukuoka, Japan, 30 November–2 December 2011; IEEE: Manhattan, NY, USA, 2011; pp. 656–661.

31. Kutubi, M.A.A.R.; Alam, K.M.R.; Morimoto, Y. A Simplified Scheme for Secure Offline Electronic Payment Systems. *High-Confid. Comput.* **2021**, *1*, 100031. [CrossRef]
32. Islam, S.H.; Amin, R.; Biswas, G.P.; Obaidat, M.S.; Khan, M.K. Provably Secure Pairing-Free Identity-Based Partially Blind Signature Scheme and Its Application in Online E-cash System. *Arab. J. Sci. Eng.* **2016**, *41*, 3163–3176. [CrossRef]
33. Xu, Y.; Li, J. An Exchange Center Based Digital Cash Payment Solution. In *Advances in Intelligent Systems and Computing*; Springer: Amsterdam, The Netherlands, 2021; pp. 265–274.
34. Shamsabadi, F.A.; Chehelcheshmeh, S.B. A cloud-based mobile payment system using identity-based signature providing key revocation. *J. Supercomput.* **2021**, 1–25. [CrossRef]
35. Mason, J.C.; Handscomb, D.C. *Chebyshev Polynomials*; Chapman & Hall/CRC: Boca Raton, FL, USA, 2003.
36. Meshram, C.; Li, C.-T.; Meshram, S.G. An efficient online/offline ID-based short signature procedure using extended chaotic maps. *Soft Comput.* **2019**, *23*, 747–753. [CrossRef]
37. Meshram, C.; Lee, C.-C.; Ranadive, A.S.; Li, C.-T.; Meshram, S.G.; Tembhurne, J.V. A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing. *Int. J. Commun. Syst.* **2020**, *33*, e4307. [CrossRef]
38. Meshram, C.; Ibrahim, R.W.; Obaid, A.J.; Meshram, S.G.; Meshram, A.; El-Latif, A.M.A. Fractional chaotic maps based short signature scheme under human-centered IoT environments. *J. Adv. Res.* **2020**, *32*, 139–148. [CrossRef]
39. Meshram, C.; Lee, C.-C.; Meshram, S.G.; Meshram, A. OOS-SSS: An Efficient Online/Offline Subtree-Based Short Signature Scheme Using Chebyshev Chaotic Maps for Wireless Sensor Network. *IEEE Access* **2020**, *8*, 80063–80073. [CrossRef]
40. Zhang, L. Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos Solitons Fractals* **2008**, *37*, 669–674. [CrossRef]
41. Anderson, D.; Camrud, E.; Ulness, D.J. On the nature of the conformable derivative and its applications to physics. *arXiv* **2018**, arXiv:1810.02005.
42. Meshram, C.; Ibrahim, R.W.; Obaidat, M.S.; Sadoun, B.; Meshram, S.G.; Tembhurne, J.V. An effective mobile-healthcare emerging emergency medical system using conformable chaotic maps. *Soft Comput.* **2021**, *25*, 8905–8920. [CrossRef]
43. Meshram, C.; Powar, P.L.; Obaidat, M.S.; Lee, C.; Meshram, S.G. Efficient online/offline IBSS protocol using partial discrete logarithm for WSNs. *IET Networks* **2018**, *7*, 363–367. [CrossRef]
44. Meshram, C.; Lee, C.-C.; Li, C.-T.; Chen, C.-L. A secure key authentication scheme for cryptosystems based on GDLP and IFP. *Soft Comput.* **2017**, *21*, 7285–7291. [CrossRef]
45. Chen, Y.; Chou, J.-S.; Sun, H.-M.; Cho, M.-H. A novel electronic cash system with trustee-based anonymity revocation from pairing. *Electron. Commer. Res. Appl.* **2011**, *10*, 673–682. [CrossRef]
46. Eslami, Z.; Talebi, M. A new untraceable off-line electronic cash system. *Electron. Commer. Res. Appl.* **2011**, *10*, 59–66. [CrossRef]
47. Zhang, L.; Zhang, F.; Qin, B.; Liu, S. Provably-secure electronic cash based on certificateless partially-blind signatures. *Electron. Commer. Res. Appl.* **2011**, *10*, 545–552. [CrossRef]
48. Chang, C.-C.; Chen, W.-Y.; Chang, S.-C. A highly efficient and secure electronic cash system based on secure sharing in cloud environment. *Secur. Commun. Netw.* **2016**, *9*, 2476–2483. [CrossRef]
49. Kang, B.; Xu, D. Secure Electronic Cash Scheme with Anonymity Revocation. *Mob. Inf. Syst.* **2016**, *2016*, 1–10. [CrossRef]
50. Meshram, C.; AlSanad, A.; Tembhurne, J.V.; Shende, S.W.; Kalare, K.W.; Meshram, S.G.; Akbar, M.A.; Gumaei, A. A Provably Secure Lightweight Subtree-Based Short Signature Scheme with Fuzzy User Data Sharing for Human-Centered IoT. *IEEE Access* **2021**, *9*, 3649–3659. [CrossRef]
51. Lee, C.-C.; Hsu, C.-W. A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. *Nonlinear Dyn.* **2012**, *71*, 201–211. [CrossRef]
52. Lee, C.-C.; Li, C.-T.; Hsu, C.-W. A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps. *Nonlinear Dyn.* **2013**, *73*, 125–132. [CrossRef]
53. Mohanty, S.; Majhi, B.; Das, S. A secure electronic cash based on a certificateless group signcryption scheme. *Math. Comput. Model.* **2013**, *58*, 186–195. [CrossRef]
54. Imoize, A.; Adedeji, O.; Tandiya, N.; Shetty, S. 6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap. *Sensors* **2021**, *21*, 1709. [CrossRef]