Computers, Materials & Continua
DOI:10.32604/cmc.2022.022642
Article

Tech Science Press

SBOOSP for Massive Devices in 5G WSNs Using Conformable Chaotic Maps

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

[1]Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, 460001, M.P., India
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, 100213, Lagos, Nigeria
[3]Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801, Bochum, Germany
[4]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia
[5]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
*Corresponding Author: Chandrashekhar Meshram. Email: cs_meshram@rediffmail.com
Received: 13 August 2021; Accepted: 15 October 2021

Abstract: The commercialization of the fifth-generation (5G) wireless network has begun. Massive devices are being integrated into 5G-enabled wireless sensor networks (5G WSNs) to deliver a variety of valuable services to network users. However, there are rising fears that 5G WSNs will expose sensitive user data to new security vulnerabilities. For secure end-to-end communication, key agreement and user authentication have been proposed. However, when billions of massive devices are networked to collect and analyze complex user data, more stringent security approaches are required. Data integrity, non-repudiation, and authentication necessitate special-purpose subtree-based signature mechanisms that are pretty difficult to create in practice. To address this issue, this work provides an efficient, provably secure, lightweight subtree-based online/offline signature procedure (SBOOSP) and its aggregation (Agg-SBOOSP) for massive devices in 5G WSNs using conformable chaotic maps. The SBOOSP enables multi-time offline storage access while reducing processing time. As a result, the signer can utilize the pre-stored offline information in polynomial time. This feature distinguishes our presented SBOOSP from previous online/offline-signing procedures that only allow for one signature. Furthermore, the new procedure supports a secret key during the pre-registration process, but no secret key is necessary during the offline stage. The suggested SBOOSP is secure in the logic of unforgeability on the chosen message attack in the random oracle. Additionally, SBOOSP and Agg-SBOOSP had the lowest computing costs compared to other contending schemes. Overall, the suggested SBOOSP outperforms several preliminary security schemes in terms of performance and computational overhead.

Keywords: Subtree-based online/offline signature procedure (SBOOSP); 5G WSNs; provably secure scheme; massive devices; conformable chaotic maps

1 Introduction

Massive access configuration enables the sharing of radio spectrum amongst an enormous number of devices. Massive access presents a potential risk of information leakage because one device in the network setting can receive a signal from other devices in the network. In order to address this access security problem, upper layer encryption techniques have been deployed [1]. However, wireless communication technology is fast evolving, and eavesdropping nodes are gaining significant intrusion capabilities. As a result, the traditional encryption techniques need to be significantly enhanced to guarantee the security of user information. In recent times, massive devices are gaining widespread adoption in 5G and beyond 5G wireless communications. Massive devices are designed using cost-effective nodes, and they have limited computational processing power. Therefore, they are not able to satisfy the high complexity requirements of advanced encryption techniques.

The commercialization of fifth-generation (5G) wireless networks has facilitated advanced technologies to address the proliferating issues in 4G LTE wireless networks [2]. In recent times, 5G wireless networks have witnessed the massive deployment of radio access networks to support several applications, including wireless sensor networks (WSNs) [3,4]. Practically, sensor nodes in WSNs can be configured and integrated into billions of massive machine-type communication (MTC) devices (MD) in 5G wireless networks to facilitate user data transmission over WSN-assisted channels [5–7]. However, there are growing concerns that the security of these channels is grossly limited, and the need to secure sensitive user data being transmitted over these channels is not negotiable [8]. Toward this end, efficient, provably secure, and lightweight subtree-based online/offline signature procedures are currently being exploited to address this problem.

1.1 Motivation and Contribution

This paper presents a comprehensive overview of efficient, provably secure, lightweight subtree-based online/offline signature procedures. Most schemes are designed based on hard problems that are relatively difficult to solve in practice from the literature review. Such schemes require high computing resources and prohibitive communication costs. Moreover, most of these schemes cannot be tested entirely using AVISPA, Scyther, and other security validation tools. Therefore, deploying such schemes in small devices with limited computational resources can be detrimental and pose serious reliability issues. In order to address this problem, the need to exploit efficient, provably secure, lightweight subtree-based online/offline signature procedure (SBOOSP) to boost the security and extends the processing capabilities of resource-limited massive devices in 5G WSNs is not out of place. Thus, we present an efficient, provably secure, lightweight subtree-based online/offline signature procedure (SBOOSP) for massive devices in 5G WSNs. It is worth mentioning that the proposed SBOOSP lowers the computational and communications costs drastically.

Additionally, the current study is motivated by using conformable chaotic maps to design the SBOOSP scheme for application in massive devices in 5G WSNs. The proposed SBOOSP demonstrates appreciable security in random oracle unforgeability of subtree-based signature (STBS) under chosen message attack. Furthermore, we present an extension to the proposed SBOOSP to facilitate the registration and implementation of different messages in 5G WSNs. Additionally, our SBOOSP was tested and compared with several schemes using standard metrics. Finally, our SBOOSP offers robust and superior security characteristics to the preliminary schemes applied to resource-limited and low-powered devices in 5G WSNs.

1.2 Paper Organization

The rest of this work is arranged in the following manner. Section 2 gives a brief literature review. Section 3 presents the preliminary background to conformable chaotic maps and notations associated with subtree. Section 4 offers the proposed efficient, provably secure, lightweight subtree-based online/offline signature procedure for massive devices in 5G WSNs using conformable chaotic maps. In Section 5, the security examinations and helpful discussions are reported. The aggregation of the proposed SBOOSP scheme for massive devices in 5G WSNs is highlighted in Section 6. Section 7 discusses the performance analysis of SBOOSP and Agg-SBOOSP. The primary setting of the SBOOSP technique for massive devices in 5G WSNs is presented in Section 8. Finally, a concise conclusion to the paper is specified in Section 9.

2 Related Works

The traditional encryption schemes depend on secure key distribution that may not find practical applications in massive devices such as grant-free random access in 5G and beyond 5G wireless networks. Thus, there is a need to deploy physical layer security schemes to complement the conventional encryption schemes to guarantee secured massive access in 5G WSNs [9]. The physical layer security ensures that the eavesdropping channel capacity is less than the information transmission percentage of the link being considered. Consequently, it becomes challenging for the eavesdropper to decode the intercepted signal accurately [10,11]. In order to improve the secrecy performance of physical layer security, there is a need to degrade the quality of the eavesdropping signal while enhancing the quality of the desired signal significantly. Thus, multiple-antenna schemes have been employed to provide physical-layer security [12]. By transmitting the desired signal in the null space of the eavesdropping channel matrix, it becomes extremely difficult for the legitimate signal to be intercepted by the eavesdropper [13,14]. However, the high spatial resolution of large-scale antenna arrays in 5G wireless networks can be exploited to guarantee secure access for massive devices in 5G WSNs [15,16].

In the existing literature, Even et al. [17] proposed online/offline signature to address some of the highlighted security vulnerability issues. Part of the signature process is carried out online, and the other part was done offline. The offline-signing process consumes considerable time and is more costly in terms of computational resources. Additionally, the online signing phase is much faster, lightweight, and efficient. In Even et al. [17], a general construction suitable for transforming a digital signature technique to its online/offline signature equivalent is presented. One major limitation of this generalized construction is the extension of each signature in a quadratic time. Interestingly, Shamir et al. [18] address this fundamental limitation using the hash-sign-switch scheme that converts any signature type. Also, some special purpose schemes have been proposed [19] to enhance the Shamir and Tauman scheme.

Kurosawa et al. [20], proposed online/offline signature procedures independent of the random oracle. Additionally, short signatures [21] and efficient online/offline schemes [22] without the random oracle have been proposed. For low-power devices, the online/offline signature procedures reported in [23] are prospective. Also, lattice-based online/offline signature procedures are given in [24]. Furthermore, Xu et al. [25] presented an identity-based online/offline multi-purpose signatures procedure. Though the scheme found practical applications in IoTs and WSNs, several limitations have been reported. Li et al. [26] noticed that the scheme [25] could not restrain forgery attacks. However, recent studies have shown that Li et al.'s scheme is not entirely free from security flaws. Several security schemes reported in the literature have demonstrated various limitations requiring massive improvements. In order to address this problem, chaotic maps assisted schemes are currently being

deployed to secure 5G wireless communication channels [27]. These schemes have been widely applied to hash functions [28], symmetric encryption [29], S-boxes [30], and provably secure online/offline identity-based signature techniques [31].

Chain et al. [32], proposed a chaotic map-based digital signature scheme. Similarly, chaotic map-assisted cryptographic schemes have been highlighted in [33], and identity-based encryption schemes have been presented [34]. Lately, Meshram et al. [33] presented an online/offline IBSS scheme based on a partial discrete logarithm. The scheme accepts pre-stored information for offline signature in a polynomial time. Furthermore, Meshram et al. [35] suggested an aggregation scheme for deployment in WSNs. The scheme requires lower computational resources and presents a faster processing time compared to the preliminaries. In recent times, a chaotic maps-assisted subtree-centric model for cryptosystems in cloud-based environments was proposed [36]. In [37], fractional chaotic maps based on short signature schemes under human-centered IoT situations have been reported. Also, the authors [38] created an efficient and highly secured level subtree-based online/offline short signature procedure using chaotic theory.

There is no doubt that a few works related to the current paper have been reported. For instance, Maxwell's source issue with random input data has been expanded leveraging conformally mapped polynomials [39]. Also, conformal-based mapped polynomial chaos expansions have been carried out for uncertain dynamical systems [39]. Additionally, conformal Chebyshev chaotic maps have been deployed for the robust construction of authentication protocol for healthcare telemedicine services [40]. It is worth mentioning that Conformable Chaotic Maps (CCM)-based lightweight schemes are highly coveted to support the security of critical user information transmitted over 5G WSNs channels. However, the works [39–41] did not consider the application of conformable chaotic maps in the design of secure lightweight subtree-based online/offline signature procedure for massive devices in 5G WSNs as in the current paper.

3 Background and Material

The notations we utilize in our new procedure, SBOOSP using conformable chaotic maps under the fuzzy user data allotment for 5G WSNs, will be laid out in this section. Then we will go over some mathematical definitions and some fundamental notions of conformable chaotic maps.

3.1 Notations

Our SBOOSP for 5G WSNs uses conformable chaotic maps with fuzzy user data sharing. The following are the notations we used in our presented SBOOSP. When there is no doubt, we use $[y, \mathfrak{z}]$ as a shorthand for $\{y, y+1, \ldots, \mathfrak{z}\}$, and $[y]$ for $[1, y]$. Allow $\mathrm{S}_{\mathrm{id}_\iota} = \{\mathrm{id}_{\iota_1}, \ldots, \mathrm{id}_{\iota_k}\}$ to be a set of (id_ι) identities that comprise all identities execution in id_ι for every $\mathrm{id}_\iota = (\mathrm{id}_{\iota_1}, \mathrm{id}_{\iota_2}, \ldots, \mathrm{id}_{\iota_k})$, where id_ι is an identity vector. The position histories of id_ι in the model's tree structure are defined as $\mathrm{I}_{\mathrm{id}_\iota} = \left\{\mathrm{i}: \mathrm{id}_i \in \mathrm{S}_{\mathrm{id}_\iota}\right\}$. The expected recipients form a subtree in a tree-organized identity-based signature/encryption procedure [38,42]. In the tree structure, the identity vectors and the positions of their receivers are unified into $\mathbb{T}$. Any genuine $\mathbb{T}$ must be able to cover the root node. This indicates that the PKG is in control of the structure. Also, $\mathbb{T}$'s identity set and $\mathbb{T}$'s position indices are denoted by $\mathrm{S}_{\mathbb{T}} = \cup_{\mathrm{id}_\iota \in \mathbb{T}} \mathrm{S}_{\mathrm{id}_\iota}$ and $\mathrm{I}_{\mathrm{id}_\iota} = \{\mathrm{i}: \mathrm{id}_i \in \mathrm{S}_{\mathbb{T}}\}$. Similarly, the phrase $\mathrm{Sup}\,(\mathrm{id}_\iota) = \{(\mathrm{id}_{\iota_1}, \mathrm{id}_{\iota_2}, \ldots, \mathrm{id}_{\iota_{k'}}): k' \leq k\}$ can be used to show that $\mathrm{id}_\iota = (\mathrm{id}_{\iota_1}, \mathrm{id}_{\iota_2}, \ldots, \mathrm{id}_{\iota_k})$ is superior. Subtree $\mathbb{T}$'s anticipated receivers are considered as $Sup\,(\mathbb{T}) = \cup_{\mathrm{id}_\iota \in \mathbb{T}} \mathrm{Sup}\,(\mathrm{id}_\iota)$.

Let us explore how the symbolizations work with the subtree-based architecture SBOOSP for massive devices in 5G WSNs. The proposed procedure is good for ensuring fuzzy entity data

distribution while meeting security standards and specifications. Nevertheless, it has problems with multi-receiver efficiency. Assume the users are arranged in the tree structure, as indicated in Fig. 1. To specify a prearranged user with $id = (\mathcal{B}, \mathcal{F},)$, the position indices of id and identity set are $I_{id} = \{2, 6\}$ and $S_{id} = \{\mathcal{B}, \mathcal{F}\}$ respectively. The user builds a collection of Sup $(id) = \{(\mathcal{B}, \mathcal{F}), (\mathcal{B})\}$ that includes both herself/himself and her/his superiors. When a data owner delivers a message to a subtree like $\mathbb{T} = \{(\mathcal{B}, \mathcal{G}), (\mathcal{B}, \mathcal{F}), (\mathcal{A})\}$, the message is sent to a set of receivers in that subtree. $S_{\mathbb{T}} = \{\mathcal{A}, \mathcal{B}, \mathcal{F}, \mathcal{G}\}$ and $I_{\mathbb{T}} = \{1, 2, 6, 7\}$ are the identity set and location indices of $\mathbb{T}$, respectively. $\mathbb{T}$'s superiors are demarcated as $\text{Sup}(\mathbb{T}) = \{(\mathcal{A}), (\mathcal{B}), (\mathcal{B}, \mathcal{F}), (\mathcal{B}, \mathcal{G})\}$, which is the user contract that the proprietor of the data wants to express.

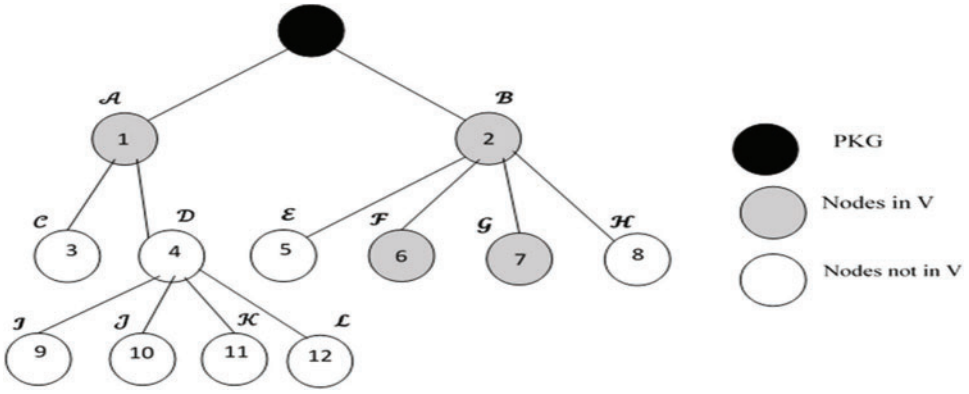

Figure 1: An illustration of a signature structure based on subtrees

3.2 Chebyshev Chaotic Polynomials

We examine the operatory of Chebyshev sequential polynomials (CSP) (see [43]). CSP $\mathcal{T}_{\eta}(y)$ is a η-degree polynomial in the y variant. Let $y \in [-1, 1]$ be the arrangement, and η be an integer. CSP reported the following in general:

$$\mathcal{T}_{\eta}(y) = cos(\eta \times cos^{-1}(y)), \mathcal{T}_0(y) = 1, \quad \mathcal{T}_1(y) = y, \quad \mathcal{T}_{\eta}(y) = 2y\mathcal{T}_{\eta-1}(y) - \mathcal{T}_{\eta-2}(y); \eta \geq 2$$

Under this circumstance, the functional $cos^{-1}(y)$ and $\cos(y)$ represented as $cos^{-1}: [-1, 1] \to [0, \pi]$ and $\cos: R \to [-1, 1]$.

CSP [33,36–38,44] has two primary properties: chaotic and semi-group properties.

1. The chaotic properties: The CSP map is demarcated as $\mathcal{T}_{\eta}: [-1, 1] \to [-1, 1]$ with degree $\eta > 1$, is a chaotic map associated with the (invariant density) functional $f^*(y) = \frac{1}{\left(\pi\sqrt{1-y^2}\right)}$ for the positive Lyapunov exponent $\lambda = \ln \eta > 0$.
2. The possessions of what is referred to as a semi-group satisfy the following conditions:

$$\mathcal{T}_a(\mathcal{T}_c(y)) = \cos(a \cos^{-1}(\cos(c \cos^{-1}(y)))) = \cos(ac \cos^{-1}(y)) = \mathcal{T}_{ca}(y) = \mathcal{T}_c(\mathcal{T}_a(y)),$$

where $y \in [-1, 1]$ and a and c are positive integers.

Zhang [44] demonstrated that the semi-group property retains the interval $(-\infty, +\infty)$, which may be used to improve the property as tracks:

$$\mathcal{T}_{\eta}(y) = 2y\mathcal{T}_{\eta-1}(y) - \mathcal{T}_{\eta-2}(y); \quad \eta \geq 2$$

where $\mathrm{y} \in (-\infty, +\infty)$ and q_1 is a large and safe prime. Thus, the property follows:

$$\mathcal{T}_a\left(\mathcal{T}_c\left(\mathrm{y}\right)\right)\left(mod q_1\right) = \mathcal{T}_{ca}\left(\mathrm{y}\right)\left(mod q_1\right) = \mathcal{T}_c\left(\mathcal{T}_a\left(\mathrm{y}\right)\right)\left(mod q_1\right)$$

and the semi-group property is also preserved. It is noteworthy that the extended Chebyshev polynomials also commute under conformation.

Chebyshev polynomials (CP) have two assessments that consider handling in polynomial time:

1. Given two elements y and v, the discrete log's (DL) task is to invent an integer a with the end goal $\mathcal{T}_a\left(\mathrm{y}\right) = v$.
2. Because of three elements y, $\mathcal{T}_a\left(\mathrm{y}\right)$, and $\mathcal{T}_c\left(\mathrm{y}\right)$, the Diffie-Hellman problem (DHP) task is to measure the $\mathcal{T}_{ac}\left(\mathrm{y}\right)$ element.

3.3 Conformable Chebyshev Chaotic Maps (CCCM)

The conformable calculus (CC) was previously specified as conformable fractional calculus (CFC) [45]. Nonetheless, it is straining the recognized properties for fractional calculus (derivatives of non-integer power). Fundamentally, CC takes the subsequent preparation:

Assume $\mathrm{w} \in [0, 1]$ is a fractional (arbitrary) number. If and only if δ^0 is the self-operator and δ^1 is the typical difference operational, an operator δ^{w} is conformable differential. Clearly, δ^{v} is conformable if and only if $\vartheta = \vartheta(\mathrm{z})$, for differentiable utility.

$$\delta^0\vartheta\left(\mathrm{z}\right) = \vartheta\left(\mathrm{z}\right), \quad \delta^1\vartheta\left(\mathrm{z}\right) = \vartheta'\left(\mathrm{z}\right).$$

Recently, Anderson et al. [45] offered a novel formulation of CC created by the control theory to designate the performance of proportional-differentiation controller conforming to the error function. The instruction has the following organization.

Definition 3.1 Suppose that $\mathrm{w} \in [0, 1]$, then CC has in the subsequent documentation:

$$\delta^{\mathrm{w}}\vartheta\left(\mathrm{z}\right) = \mu_1\left(\mathrm{w}, \mathrm{z}\right)\vartheta\left(\mathrm{z}\right) + \mu_0\left(\mathrm{w}, \mathrm{z}\right)\vartheta'\left(\mathrm{z}\right),$$

where the functions μ_1 and μ_0 attain the boundaries

$$\lim_{\mathrm{w}\to 0}\mu_1\left(\mathrm{w}, \mathrm{z}\right) = 1, \lim_{\mathrm{w}\to 1}\mu_1\left(\mathrm{w}, \mathrm{z}\right) = 0,$$

$$\lim_{\mathrm{w}\to 0}\mu_0\left(\mathrm{w}, \mathrm{z}\right) = 0, \lim_{\mathrm{w}\to 1}\mu_0\left(\mathrm{w}, \mathrm{z}\right) = 1.$$

In order to get the overhead description, we shall deliberate $\mu_1\left(\mathrm{w}, \mathrm{z}\right) = (1-\mathrm{w})\mathrm{z}^{\mathrm{w}}$ and $\mu_0\left(\mathrm{w}, \mathrm{z}\right) = \mathrm{w}\mathrm{z}^{1-\mathrm{w}}$, or $\mu_1\left(\mathrm{w}, \mathrm{z}\right) = \frac{(1-\mathrm{w})}{\Gamma(1+\mathrm{w})}$ and $\mu_0\left(\mathrm{w}, \mathrm{z}\right) = \frac{\mathrm{w}}{\Gamma(1+\mathrm{w})}$ where $\delta^{\mathrm{w}}\vartheta\left(\mathrm{z}\right)$ is the name of the $\vartheta\left(\mathrm{z}\right)$ function's conformable differential operator. As a result, μ_1, μ_0 are dependably the fractional tuning connections of the function and its derivative.

By relating the notion of CC to specify the polynomial $\mathcal{T}_{\mathfrak{y}}(\mathrm{z})$, we attain the resulting structure:

Since $\mathcal{T}_{\mathfrak{y}}\left(\mathrm{z}\right) = 2\mathfrak{y}\mathcal{T}_{\mathfrak{y}-1}(\mathrm{z})$, then $\delta^{\mathrm{w}}\mathcal{T}_{\mathfrak{y}}(\mathrm{z})$ has the following formal relationship (1)

$$\mathcal{T}_{\mathfrak{y}}^{\mathrm{w}}\left(\mathrm{z}\right) := \delta^{\mathrm{w}}\mathcal{T}_{\mathfrak{y}}\left(\mathrm{z}\right) = \mu_1\left(\mathrm{w}, \mathrm{z}\right)\mathcal{T}_{\mathfrak{y}}(\mathrm{z}) + \mu_0\left(\mathrm{w}, \mathrm{z}\right)\mathcal{T}_{\mathfrak{y}}'(\mathrm{z}) \tag{1}$$

The frequent formula (1) can replace by (2)

$$\mathcal{T}_{\mathfrak{y}}^{\mathrm{w}}\left(\mathrm{z}\right) = \mu_1\left(\mathrm{w}, \mathrm{z}\right)\mathcal{T}_{\mathfrak{y}}\left(\mathrm{z}\right) + 2\mathfrak{y}\ \mu_0\left(\mathrm{w}, \mathrm{z}\right)\ *\ \omega(\mathrm{x})\mathcal{T}_{\mathfrak{y}-1}\left(\mathrm{z}\right), \tag{2}$$

where $\omega(\mathrm{z}) = 1 + 2\mathrm{z} + (4\mathrm{z}^2 - 1) + \ldots + (\mathfrak{y} - 1)$-times. Eq. (2) is titled the Conformable Chebyshev Polynomials (CCP) (see Fig. 2). The following result demonstrates formulary recurrence:

3.3.1 Properties of CCCM: TheCCCM has the Following Two Stimulating Possessions

Definition 3.2 *(Chaotic properties of CCCM)*. The Conformable Chebyshev Chaotic Maps fulfills the recurrent relations under chaotic property [46] i.e.,

$$\mathcal{T}_{\eta}^{w}(z) = [2z\mu_1(\alpha, z) + 2\eta\mu_0(w, z) * \omega(z)]\,\mathcal{T}_{\eta-1}(z) - \mu_1(w, z)\,\mathcal{T}_{\eta-2}(z).$$

Definition 3.3 *(Semi-group properties of CCCM)*. The semi-group properties look for CCCMs located on interval $(-\infty, \infty)$ [46], i.e., $\mathcal{T}_{k}^{w}\left(\mathcal{T}_{\eta}^{w}(z)\right) = \mathcal{T}_{\eta}^{w}\left(\mathcal{T}_{k}^{w}(z)\right) = \mathcal{T}_{k\eta}^{w}(z)$

Note that, when $w \to 0$ is used, we get the original case from [44].

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

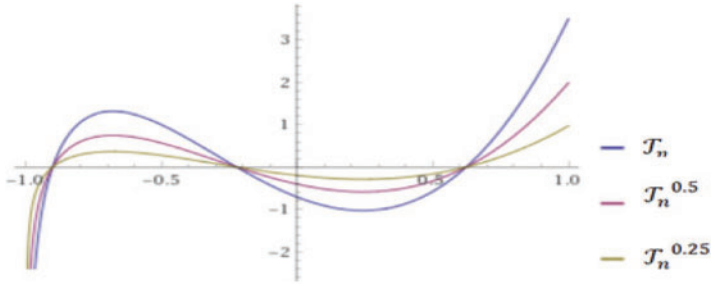

Figure 2: CCP for different values of $w = 0.25, 0.5, 1$ with $\mu_1(w, z) = \frac{(1-w)}{\Gamma(1+w)}$ and $\mu_0(w, z) = \frac{w}{\Gamma(1+w)}$

4 The Proposed SBOOSP Using Conformable Chaotic Maps

We will describe the novel efficient SBOOSP for massive devices in 5G WSNs that we have devised in this section. The plan is made up of five steps described as follows.

4.1 Setup

Let $\mathbb{G}$ be a prime q_1 order multiplicative group. The PKG chooses an integer in $\wr \in_R \mathcal{Z}_{q_1}^{*}$ and a rational number $w \in [0, 1]$ at random and also picks a random generator $\alpha \in \mathbb{G}$. It sets $\gamma = \mathcal{T}_{\wr}^{w}(\alpha)\,(mod\, q_1)$. Let $\mathfrak{h}$: $Sup(\mathbb{T}) \to \mathcal{Z}_{q_1}^{*}$ be a hash function. The master public key (mpk) and master secret key (msk) is specified by

$$mpk = \{\mathbb{G}, \alpha, q_1, \mathfrak{h}, \gamma\}, \quad msk = (\wr, w)$$

4.2 Extraction

To create a secret key for $id_{\wr} \in Sup(\mathbb{T})$, the PKG picks $u \in_R \mathcal{Z}_{q_1}^{*}$ at random, calculates

$\xi = \mathcal{T}_{u}^{w}(\alpha)\,(mod\, q_1)$, $c = \mathfrak{h}(id_{\wr}, \xi)$ and $\chi = u * \wr c (mod\, q_1)$.

The client's private key is the pair (ξ, χ). It is worth noting that a properly created secret key must satisfy the following equality:

$$\mathcal{T}_{\chi}^{w}(\alpha)\,(mod\, q_1) = \xi\mathcal{T}_{c}^{w}(\gamma)\,(mod\, q_1) \tag{3}$$

4.3 Offline-Signing

In the offline stage, the signer does the following calculation:

$$\mathcal{V}_i = \mathcal{T}_2^{w}(\alpha)\,(mod\, q_1), \quad \text{for } i \in [0, |q_1| - 1].$$

At the offline phase, we do not need the private key or knowledge of the message. It can also be considered a public parameter prepared by the (trusted) PKG rather than the offline-signing step.

4.4 Online-Signing

At the online phase, to register a message $\mathcal{M} \in (-\infty, \infty)$ using (ξ, χ), the signer selects $x \in_R \mathcal{Z}_{q_1}^*$ at random. Let $x[i]$ be the i^{th} bit of x. Describe $\mathcal{Y} \subset \{1, \ldots, |q_1|\}$ to be the set of indices such that $x[i] = 1$.

Calculate $\mathcal{V} = \prod_{i=1}^{q_1} \mathcal{V}_{i-1}(mod\, q_1)$, $\zeta = \mathfrak{h}(\mathcal{V}, \xi, \mathcal{M})$, and $\hbar = x * \chi\eta(mod\, q_1)$.

The signature ς is $(\mathcal{V}, \xi, \hbar)$.

4.5 Verification

To verify the signature $\varsigma = (\mathcal{V}, \xi, \hbar)$ for id and $\mathcal{M}$, the verifier initially calculates $\zeta = \mathfrak{h}(\mathcal{V}, \xi, \mathcal{M})$ and determines whether

$$\mathcal{T}_{\hbar}^{w}(\alpha)(mod\, q_1)? = \mathcal{V}\mathcal{T}_{\zeta}^{w}(\xi)\,\mathcal{T}_{\zeta c}^{w}(\gamma)\,(mod\, q_1) \tag{4}$$

If it is equal, accept it. Reject otherwise.

For exactness, note that $\mathcal{V} = \mathcal{T}_x^{w}(\gamma)\,(mod\, q_1)$. We have

$$\mathcal{V}\mathcal{T}_{\zeta}^{w}(\xi)\,\mathcal{T}_{\zeta c}^{w}(\gamma)\,(mod\, q_1) = \mathcal{T}_x^{w}(\alpha)\,\mathcal{T}_{\zeta u}^{w}(\alpha)\,\mathcal{T}_{\backslash\zeta c}^{w}(\alpha)\,(mod\, q_1) = \mathcal{T}_{\hbar}^{w}(\alpha)\,(mod\, q_1)$$

Remark 1. Following earlier discussions in this paper, any trusted third party can execute the offline signing algorithm as no secret data is required. Additionally, offline data can be reused gainfully. In practice, If the offline signing stage, which the PKG handles, is included in the setup process (and the offline data is placed as part of the public parameter). The suggested technique is a usual identity-based signature procedure with a fast-signing process that does not need exponentiation.

5 Security Investigations and Discussions

To demonstrate that our novel SBOOSP based on conformable chaotic maps is secure, we employ the Bellare et al. [47] acquiesced security proofs.

Theorem 5.1: The proposed SBOOSP is $(\epsilon, t, \mathrm{q}_{\mathfrak{h}}, \mathrm{q}_{\mathfrak{s}}, \mathrm{q}_E)$ secure in the facts of unforgeability of subtree-based signature procedure (STBP) under chosen message attack (UF-STBP-CMA) in the ROM, executing the (ϵ', t')—conformable chaotic maps supposition in $\mathbb{G}$, where:

$$\epsilon' \approx \left(\frac{q_1 - 1}{q_1}\right)\left(\frac{1}{\mathrm{q}_{\mathfrak{h}}} - \frac{(\mathrm{q}_{\mathfrak{s}} + \mathrm{q}_E)}{q_1}\right)\epsilon \tag{5}$$

$$t' \approx t + \mathcal{O}(\mathrm{q}_E + \mathrm{q}_{\mathfrak{s}})\tau \tag{6}$$

and $\mathrm{q}_{\mathfrak{s}}$—Signing Oracle (SO) signing inquiries, $\mathrm{q}_{\mathfrak{h}}$—hashing inquiries, q_E—Extraction Oracle (EO) inquiries measure chaos, and τ is the time to do an exponentiation operation.

Proof: Assume there is an adversary named $\mathfrak{F}$. We create the process $\mathfrak{B}$, which is based on the use of $\mathfrak{F}$, to solve conformable chaotic maps. The process $\mathfrak{B}$ includes a $\mathbb{G}$ (multiplicative group) with

generator α and prime order q_1, as well as a group element $\mathcal{K} \in \mathbb{G}$ that is verified to locate $\mathbb{v} \in \mathbb{Z}_{q_1}^*$ in such a way that $\mathcal{K} = \mathcal{T}_{\mathbb{v}}^{\mathbb{w}}(\alpha)\,(mod\, q_1)$. The approach [47] is utilized.

Setup: $\mathfrak{B}$ is responsible for replicating the reformation process using a hash function $\mathfrak{fj}$ that performs similarly to a random oracle. $\gamma \leftarrow \mathcal{K}$ is a variable assigned by $\mathfrak{B}$, and it outputs the public parameter $(\mathbb{G}, y, q_1, \gamma, \mathfrak{fj})$ to $\mathfrak{F}$.

EO inquiries: $\mathfrak{F}$ can search for $\mathrm{id} \in \mathrm{Sup}(\mathbb{T})$ using the extraction oracle, and $\mathfrak{B}$ can re-create the oracle. It necessitates the use of random $s, t \in \mathbb{Z}_{q_1}^*$, and the following sets:

$$\xi = \mathcal{T}_t^{\mathbb{w}}(\alpha)/\mathcal{T}_s^{\mathbb{w}}(\gamma)\,(mod\, q_1), \quad \chi \leftarrow t, \quad \mathfrak{fj}(\xi, \mathrm{id}) \leftarrow s \tag{7}$$

(ξ, χ) is generated as a secret key for $\mathrm{id} \in \mathrm{Sup}(\mathbb{T})$ by $\mathfrak{B}$, and the uniformity assessment $(\xi, \mathfrak{fj}(\xi, \mathrm{id}), \chi, \mathrm{id})$ is saved in a list by $\mathfrak{B}$.

SO inquiries: The adversary $\mathfrak{F}$ sends a message to $\mathrm{id} \in \mathrm{Sup}(\mathbb{T})$ inquiring about him/her. The process $\mathfrak{B}$ looks to see if oracle $\mathfrak{fj}$ or the extraction oracle has ever been asked for $\mathrm{id} \in \mathrm{Sup}(\mathbb{T})$. If this is the case, the list $(\xi, \chi, \mathfrak{fj}(\xi, \mathrm{id}))$ will be improved as indicated in the table. The signature processes on the message are then performed employing these estimates using process $\mathfrak{B}$. It constructs the message's signature $(\mathcal{V}, \xi, \mathbb{k})$ and keeps a list of $\mathfrak{fj}(\mathcal{V}, \xi, \mathcal{M})$ in the hash table for dependability. If $\mathrm{id} \in \mathrm{Sup}(\mathbb{T})$ is not called to extract the oracle, $\mathfrak{B}$ starts the simulation by signing the message with the secret key.

Output Computation: Finally, adversary $\mathfrak{F}$ creates a bogus signature $\mathfrak{c}_1^* = (\mathcal{V}^*, \xi^*, \mathbb{k}_1^*)$ on $\mathrm{id}^* \in \mathbb{T}^*$ and $\mathcal{M}^*$, where $\mathbb{T}^*$ is the challenge subtree. In the sense that it performs a $\mathfrak{fj}(\mathcal{V}^*, \xi^*, \mathcal{M}^*)$ and returns a different result to the justified, the process $\mathfrak{B}$ reverses the adversary $\mathfrak{F}$. Other signatures produced by adversary $\mathfrak{F}$ are $\mathfrak{c}_2^* = (\mathcal{V}^*, \xi^*, \mathbb{k}_2^*)$. The $\mathfrak{B}$ process rehashes the data and returns $\mathfrak{c}_3^* = (\mathcal{V}^*, \xi^*, \mathbb{k}_3^*)$. It is worth mentioning that $\mathcal{V}^*$ and ξ^* are always the same. We constructed $\mathfrak{y}_1, \mathfrak{y}_2, \mathfrak{y}_3$ three times in a row using the random oracle query $\mathfrak{fj}(\mathcal{V}^*, \xi^*, \mathcal{M}^*)$.

For individually $\mathfrak{l}, x, u \in Z_{q_1}^*$, we now project conformable chaotic maps of γ, ξ, and $\mathcal{V}$, respectively. Specifically, $\xi = \mathcal{T}_u^{\mathbb{w}}(\alpha)\,(mod\, q_1)$, $\gamma = \mathcal{T}_{\mathfrak{l}}^{\mathbb{w}}(\alpha)\,(mod\, q_1)$ and $\mathcal{V} = \mathcal{T}_x^{\mathbb{w}}(\alpha)\,(mod\, q_1)$. We can deduce the following from Eq. (4):

$$\mathbb{k}_i^* = x * u\mathfrak{y}_i * \mathfrak{l}\mathfrak{y}_i\mathfrak{fj}(\xi^*, \mathrm{id})\,(mod\, q_1) \quad \text{for } i = 1, \ldots, 3 \tag{8}$$

Only, $\mathfrak{l}$, ℓ, and u are unfamiliar to $\mathfrak{B}$ in these mathematical inspections. For autonomous overhead linear mathematical proclamations, the process $\mathfrak{B}$ evaluations for $i = 1, ., 3$ and generates $\mathfrak{l}$ as the solution of conformable chaotic maps.

Cost Reduction Investigation: The random oracle's consignment $\mathfrak{fj}(\xi, \mathrm{id})$ is irregular, requiring a mutual probability of at least $\frac{\mathfrak{q}_{\mathfrak{fj}}}{q_1}$. This is assumed in the simulation procedure with extraction oracle failures. The simulation technique is effective $(\mathfrak{q}_E + \mathfrak{q}_{\mathfrak{z}})$ times (as a result of the fact that $\mathfrak{fj}(\xi, \mathrm{id})$ can also be asked in the signing oracle if $\mathrm{id} \in \mathrm{Sup}(\mathbb{T})$ is not demanded in the extraction oracle), with the probability being:

$$\left(1 - \frac{(\mathfrak{q}_{\mathfrak{z}} + \mathfrak{q}_E)\,\mathfrak{q}_{\mathfrak{fj}}}{q_1}\right) \leq \left(1 - \frac{\mathfrak{q}_{\mathfrak{fj}}}{q_1}\right)^{(\mathfrak{q}_{\mathfrak{z}} + \mathfrak{q}_E)}$$

There exists an inquiry $\mathfrak{fj}(\mathcal{V}^*, \xi^*, \mathcal{M}^*)$ with a probability of at least $\left(1 - \frac{1}{q_1}\right)$ due to the random oracle's perfect unpredictability. At least with a $\left(\frac{1}{q_{\mathfrak{fj}}}\right)$ probability, $\mathfrak{B}$ estimates it correctly as the rewind point. Overall, the chances of success are:

$$\left(\frac{q_1 - 1}{q_1}\right)\left(\frac{1}{\mathfrak{q}_{\mathfrak{fj}}} - \frac{(\mathfrak{q}_s + \mathfrak{q}_E)}{q_1}\right)\epsilon$$

The exponentiations used in the signature and extraction operations determine the process $\mathfrak{B}$'s temporal complexity, which is the same as:

$$t + \mathcal{O}(\mathfrak{q}_E + \mathfrak{q}_s)\tau$$

6 Aggregation Procedure (Agg-SBOOSP) of the SBOOSP for 5G WSNs

It would be highly advantageous if a sensor node (SN) could sign not just one but i separate messages simultaneously, with the aggregate signature having the same length as a single message's signature or substantially shorter than the length of a single signature multiplied by i. Such an aggregate signature is essential in massive devices in 5G WSNs since it can drastically reduce sensor node communication overheads. This paper presents the new online/offline identity-based aggregation strategy for the proposed SBOOSP using conformable chaotic maps. It is made up of the five segments listed as follows.

6.1 Setup

Let $\mathbb{G}$ be a prime q_1 order multiplicative group. The PKG chooses an integer in $\mathfrak{l} \in_R \mathcal{Z}_{q_1}^*$ and a rational number $\mathrm{w} \in [0, 1]$ at random and also picks a random generator $\alpha \in \mathbb{G}$. It sets $\gamma = \mathcal{T}_{\mathfrak{l}}^{\mathrm{w}}(\alpha)\,(mod\, q_1)$. Let $\mathfrak{fj}\colon Sup(\mathbb{T}) \rightarrow \mathcal{Z}_{q_1}^*$ be a hash function. The master public key (mpk) and master secret key (msk) is specified by

$$mpk = \{\mathbb{G}, q_1, \alpha, \mathfrak{fj}, \gamma\}, \quad msk = (\mathfrak{l}, \mathrm{w})$$

6.2 Extraction

To create a secret key for $\mathrm{id}_{\mathfrak{l}} \in \mathrm{Sup}(\mathbb{T})$, the PKG picks $u \in_R \mathcal{Z}_{q_1}^*$ at random, calculates

$\xi = \mathcal{T}_u^{\mathrm{w}}(\alpha)\,(mod\, q_1)$, $c = \mathfrak{fj}(\mathrm{id}_{\mathfrak{l}}, \xi)$ and $\chi = u * \mathfrak{l}\, c (mod\, q_1)$.

The client's private key is the pair (ξ, χ). It's worth noting that a properly created secret key must satisfy the following equality:

$$\mathcal{T}_{\chi}^{\mathrm{w}}(\alpha)\,(mod\, q_1) = \xi \mathcal{T}_c^{\mathrm{w}}(\gamma)\,(mod\, q_1)$$

6.3 Offline-Signing

In the offline phase, the signer does the following calculation:

$$\mathcal{V}_i = \mathcal{T}_{2i}^{\mathrm{w}}(\alpha)\,(mod\, q_1), \quad \text{for } i \in [0, |q_1| - 1].$$

As mentioned earlier in this work, a trustworthy third party or the PKG can perform this offline phase computation. For $i = 1, \ldots, |q_1| - 1$, the subsequenting value$^{\wedge}\mathcal{V}_i$ can also be provided as a portion of the public parameter.

6.4 Online-Signing

At the online stage, to register a message $\mathcal{M} \in (-\infty, \infty)$ using (ξ, χ), the signer selects $x_j \in_R \mathcal{Z}_{q_1}^*$ at random. Let $x_j[i]$ be the i^{th} bit of x_j. Describe $\mathcal{Y} \subset \{1, \ldots, |q_1|\}$ to be the set of indices such that $x_j[i] = 1$.

Calculate

$\mathcal{V}_j = \prod_{i=1}^{q_1} \mathcal{V}_{i-1} (mod\, q_1)$, $\zeta_j = \text{ʃ}\text{ʃ}(\mathcal{V}, \xi, \mathcal{M})$, and $k_j = x_j * \chi \zeta_j (mod\, q_1)$, for $j = 1, \ldots, n$

Also, compute

$$k = \sum_{i=1}^{n} k_i$$

The aggregate signature is $\varsigma = (\mathcal{V}_j, \xi, k)$ for $j = 1, \ldots, n$.

6.5 Verification

To verify the aggregate signature $\varsigma = (\mathcal{V}_j, \xi, k)$ for id and $\mathcal{M}_j$ for $j = 1, \ldots, n$, the verifier initially calculates $\eta_j = \text{ʃ}\text{ʃ}\left(\mathcal{V}, \xi, \mathcal{M}_j\right)$ and determines whether

$$\mathcal{T}_k^w(\alpha)(mod\, q_1)? = \left(\prod_{j=1}^{n} \mathcal{V}_j\right) \mathcal{T}_\varrho^w(\xi)\, \mathcal{T}_{\varrho d}^w(\gamma)\, (mod\, q_1) \tag{9}$$

If it is equal, accept it. Reject otherwise.

Note that the verification is correct: Since $\mathcal{V}_j = \mathcal{T}_{x_j}^w(\alpha)\, (mod\, q_1)$ for $j = 1, \ldots, n$

$$\left(\prod_{i=1}^{n} \mathcal{V}_i\right) \mathcal{T}_\varrho^w(\xi)\, \mathcal{T}_{\varrho d}^w(\gamma)\, (mod\, q_1) = \left(\prod_{i=1}^{n} \mathcal{V}_i\right) \mathcal{T}_{u\varrho}^w(\alpha)\, \mathcal{T}_{\varrho \wr d}^w(\alpha)\, (mod\, q_1)$$

$$= \mathcal{T}_x^w(\alpha)\, \mathcal{T}_{\varrho u}^w(\alpha)\, \mathcal{T}_{\wr \varrho d}^w(\alpha)\, (mod\, q_1) = \mathcal{T}_k^w(\alpha)\, (mod\, q_1)$$

7 Performance Investigation

We compare our new SBOOSP to six previous strategies proposed by [33,38,48–51], in this section. We also compare our presented Agg-SBOOSP (extended SBOOSP) procedure to five other related strategies proposed by [33,38,48,50,51], respectively, to demonstrate the efficacy of our innovative design. The notations $\dagger_{exp}, \dagger_{pair}, \dagger_{chaos}, \dagger_{mul}$ and $\dagger_{hash}$ are utilized to present our evaluation results. In the signature (online and offline) stage and verification stage, we represent the execution time for a group modular exponentiation ($\dagger_{exp}$), a bilinear pairing operation ($\dagger_{pair}$), a chaotic map operation ($\dagger_{chaos}$), a modular multiplication ($\dagger_{mul}$), and a one-way hash function ($\dagger_{hash}$). It is worth noting that the signature and verification steps are the only ones that require more computing power than the setup and extraction stages. By comparing the computational costs of our present SBOOSP to the works of [33,38,48–51], we look at the steps of signature and verification. In a similar vein, we compare our new presented Agg-SBOOSP with the works of [35,38,48,50,51].

Tab. 1 shows the proposed SBOOSP's functionalities, and Fig. 3 compares the computational costs of existing relevant protocols [33,38,48–51]. Tab. 2 also includes a functional study of the proposed Agg-SBOOSP, as well as a comparison of computational costs in Fig. 4 with other relevant protocols [35,38,48,50,51]. We arrive at the following computation time statistics with unit hashing

time based on the results of the experiments in [46,52,53]: $\dagger_{exp} = 600\dagger_{hash}$, $\dagger_{mul} = 2.5\dagger_{hash}$, $\dagger_{pair} = 1550\dagger_{hash}$ and $\dagger_{hash} \approx \dagger_{chaos}$. The following is the order of computational complexity in this method: $\dagger_{hash} \approx \dagger_{chaos} < \dagger_{mul} < \dagger_{exp} < \dagger_{pair}$. Recall the running time of hash is 0.06 ms [46,52] and that [w = 0.5]. References [33,38,48–51], and the SBOOSP, respectively, have total communication costs of 108.57, 144.9, 466.08, 315.48, 1.35, 1.05, and 0.85 ms. References [35,38,48,50,51], and the Agg-SBOOSP have total communication costs of 108.57, 279.87, 351.72, 108.57, 1.26 and 1.06 ms, respectively.

Based on the classical results in [46,52,53], we arrive at the following computation time values with unit hashing time:

Table 1: Computational cost assessment of SBOOSP with other procedures

Procedures	Signing stage (online and offline)	Verification stage	Total (ms)
[48]	$\dagger_{exp} + \dagger_{hash} + \dagger_{mul}$	$2\dagger_{exp} + \dagger_{hash} + 2\dagger_{mul}$	108.57
[49]	$2\dagger_{exp} + 4\dagger_{mul}$	$2\dagger_{exp} + 2\dagger_{mul}$	144.9
[50]	$\dagger_{pair} + 6\dagger_{mul} + \dagger_{hash}$	$4\dagger_{pair} + 2\dagger_{hash}$	466.08
[51]	$\dagger_{pair} + 2\dagger_{mul} + 2\dagger_{hash} + \dagger_{exp}$	$2\dagger_{pair} + \dagger_{hash}$	315.48
[33]	$2\dagger_{chaos} + \dagger_{hash} + 4\dagger_{mul}$	$2\dagger_{chaos} + 3\dagger_{mul}$	1.35
[38]	$2\dagger_{chaos} + \dagger_{hash} + 4\dagger_{mul}$	$2\dagger_{chaos} + 2\dagger_{mul}$	1.05
SBOOSP	$2\dagger_{chaos} + \dagger_{hash} + 2\dagger_{mul}$	$2\dagger_{chaos} + \dagger_{mul}$	0.85

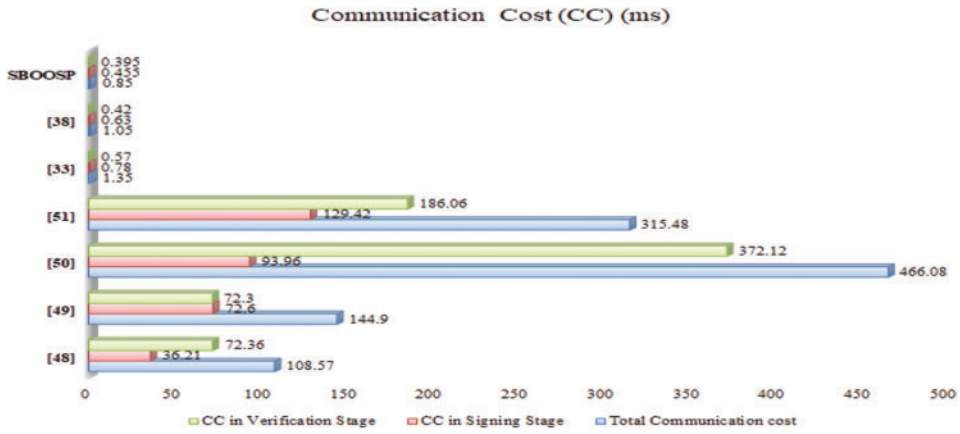

Figure 3: Communication cost (ms) analysis of SBOOSP with other procedures

As indicated in Fig. 3, the interaction value of the suggested SBOOSP is the lowest attained. The tests frequently transform into runtime excels the rest of the linked procedures when using the proposed SBOOSP. Similarly, as the study results in Fig. 4 reveal, the interaction value of the suggested Agg-SBOOSP is the lowest. The proposed Agg-SBOOSP frequently transforms tests into runtime and outperforms the other related procedures similar to the SBOOSP. It is interesting to note that the results presented in this paper show related characteristics to the results reported in [54]. Next, we shall examine the basic setting for implementing the proposed SBOOSP in massive devices in 5G WSNs.

Table 2: Computational cost assessment of Agg-SBOOSP with other procedures

Procedures	Signing stage (online and offline)	Verification stage	Total (ms)
[48]	$\dagger_{exp} + \dagger_{hash} + 2\dagger_{mul}$	$2\dagger_{exp} + \dagger_{hash} + \dagger_{mul}$	108.57
[50]	$\dagger_{pair} + 5\dagger_{mul} + \dagger_{hash}$	$2\dagger_{pair} + \dagger_{hash}$	279.87
[51]	$2\dagger_{pair} + 3\dagger_{mul} + \dagger_{hash} + \dagger_{exp}$	$\dagger_{pair} + \dagger_{mul} + \dagger_{hash} + \dagger_{exp}$	351.72
[35]	$\dagger_{exp} + \dagger_{hash} + 2\dagger_{mul}$	$2\dagger_{exp} + \dagger_{hash} + \dagger_{mul}$	108.57
[38]	$2\dagger_{chaos} + \dagger_{hash} + 3\dagger_{mul}$	$2\dagger_{chaos} + \dagger_{hash} + 2\dagger_{mul}$	1.26
Agg-SBOOSP	$2\dagger_{chaos} + \dagger_{hash} + 2\dagger_{mul}$	$2\dagger_{chaos} + \dagger_{hash} + \dagger_{mul}$	1.06

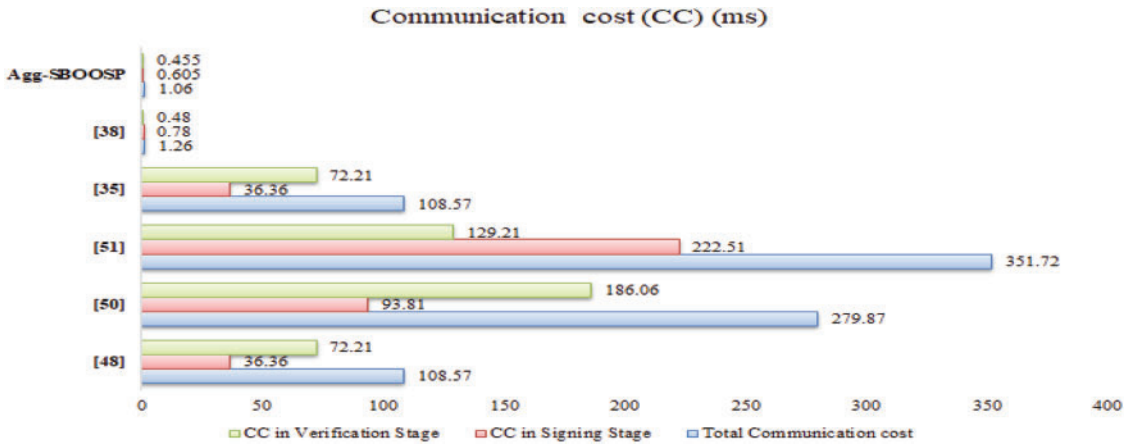

Figure 4: Communication cost (ms) analysis of Agg-SBOOSP with other procedures

8 Implementation for Massive Devices in 5G WSNs

8.1 Basic Setting

In a single-hop context (see Fig. 5), each SN can sign messages with its private signing key accompanying its id identifier information. According to our assumptions, the system parameter is created by the base station (BS). It is integrated with each SN when installed—assuming that either the sensor nodes or the base station can verify the signatures created by the SNs. As with 5G WSNs, we suppose that the BS is robust to computationally complex cryptographic processes, whereas the SNs have limited computing, memory, and battery power resources. Also, we assume that the BS's private key is safely stored in a trusted server.

The main components of the 5G wireless access network are the 5G access and core networks, as depicted in Fig. 6. In the 5G access network, two nodes called Next Generation evolved NodeB (ng-eNB) and Next Generation NodeB (gNB) are described briefly. In this configuration, the new radio (NR) user plane and control plane procedures and functions for 5G network users are provided by the gNB. Similarly, the NR user plane and control plane procedures and functions are provided by the ng-eNB for the 4G network users. As illustrated in Fig. 6, the interface among ng-eNB and gNB is called the Xn interface. The 5G core network part of the configuration in Fig. 6 comprises several nodes such as the 5G core Access and Mobility Management Function (AMF) and User Plane Function

(UPF) [55]. The function of the AMF involves accessing mobility management functions for access control and mobility management. The management of sessions associated with network policies is conducted by the session management function (SMF). Additionally, the UPF performs the user plane functions and can be deployed to different configurations and locations in the 5G wireless network. The proposed system model comprises the registration center (RC), the 5G Massive Devices (MDs), and the 5G core network (5GC). The RC is the entity designed to conduct honest and trust-based functions. The primary function of the RC is to register and or generate system parameters for the massive devices and the AMF based on their identities. The MDs transfer user information to the core network via the ng-eNB. Additionally, the AMF aggregates authentication on the user information received from the MDs and ensures the decryption of the authenticated data holistically. The proposed SBOOSP scheme can be deployed in this setting to provide efficient and robust security for MDs in 5G wireless sensor networks.

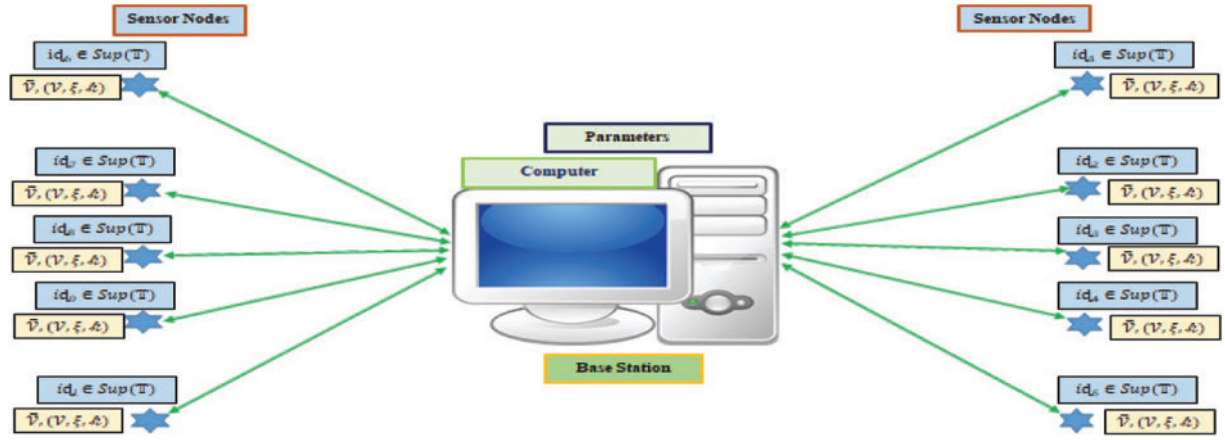

Figure 5: Overview of system implementation

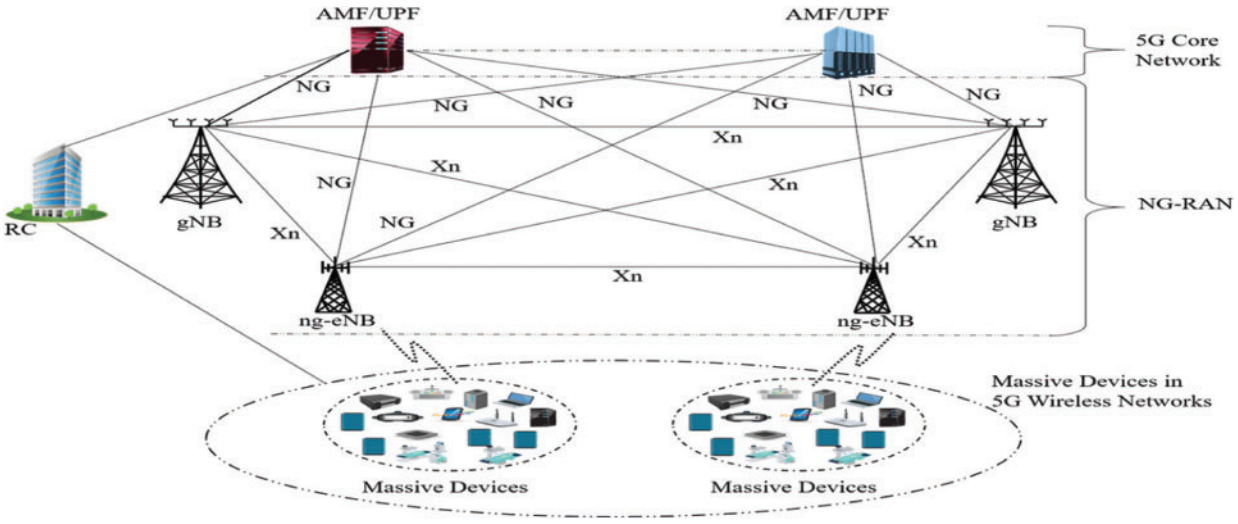

Figure 6: Basic setting of massive devices in 5G wireless networks for the proposed SBOOSP scheme

9 Conclusion

For massive devices in 5G wireless sensor networks with fuzzy user data sharing, this paper presented a new provably secure, lightweight SBOOSP and its aggregation (Agg-SBOOSP) leveraging conformable chaotic maps. In our proposition, each procedure is carried out with the fewest possible operations, thereby reducing the computational processing time of the scheme. Results indicate that the SBOOSP technique performs efficiently and independently of a certificate to verify and validate the signature without requiring pairing operations. As a result, the SBOOSP provides strong security in the random oracle paradigm with high unforgeability when a message is chosen. Additionally, the SBOOSP achieves multi-time offline storage at minimal complexity. Consequently, the signer can utilize the offline pre-stored information in polynomial time, demonstrating a significant advantage over most existing online/offline signature procedures that only allow for a single signature attempt. Furthermore, the new procedure allows for a secret key during the pre-registration process, but no secret key is necessary during the offline stage. The results of the performance investigation of SBOOSP and Agg-SBOOSP approaches are excellent. In comparison to various contenders, the proposed procedures have the lowest computing costs. Finally, both informal and formal security investigations of the proposed procedures demonstrate that the schemes can withstand all well-known attacks with exceptional security features at the lowest communication costs. Future work would focus on an efficient, lightweight, provably secure identity-based online/offline short signature procedure for massive devices in 5G WSNs using the concept of SBOOSP.

Acknowledgement: The authors would like to thank anonymous reviewers of Computers, Materials & Continua Journal for their careful and helpful comments. We extend our gratitude to 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.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. L. Massey, "An introduction to contemporary cryptology," *Proceedings of the IEEE*, vol. 76, no. 5, pp. 533–549, 1988.

[2] A. Gupta and R. K. Jha, "A survey of 5G network: Architecture and emerging technologies," *IEEE Access*, vol. 3, pp. 1206–1232, 2015.

[3] R. Fotohi, S. F. Bari and M. Yusefi, "Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol," *International Journal of Communication Systems*, vol. 33, no. 4, pp. 1–25, 2020.

[4] W. R. Heinzelman, J. Kulik and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *Proc. of the 5th Annual ACM/IEEE Int. Conf. on Mobile Computing and Networking*, Seattle Washington, USA, pp. 174–185, 1999.

[5] M. Agiwal, A. Roy and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016.

[6] J. Cao, M. Maode, L. Hui, Y. Zhang and Z. Luo, "A survey on security aspects for 3GPP 5G networks," *IEEE Communications Surveys Tutorials*, vol. 22, no. 1, pp. 170–195, 2020.

[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, pp. 1–58, 2021, 1709.
[8] M. Lavanya and V. Natarajan, "LWDSA: Light-weight digital signature algorithm for wireless sensor networks," *Sadhana Academy Proceedings in Engineering Sciences*, vol. 42, no. 10, pp. 1629–1643, 2017.
[9] Q. Qi, X. Chen, C. Zhong and Z. Zhang, "Physical layer security for massive access in cellular Internet of Things," *Science China Information Sciences*, vol. 63, no. 2, pp. 121301, 2020.
[10] F. Shu, X. Wu, J. Hu, J. Li, R. Chen *et al.,* "Secure and precise wireless transmission for random-subcarrier-selection-based directional modulation transmit antenna array," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 890–904, 2018.
[11] Y. Cai, Z. Wei, R. Li, D. W. K. Ng and J. Yuan, "Joint trajectory and resource allocation design for energy-efficient secure UAV communication systems," *IEEE Transactions on Communications*, vol. 68, no. 7, pp. 4536–4553, 2020.
[12] X. Chen, D. W. K. Ng, W. H. Gerstacker and H. H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Communications Surveys Tutorials*, vol. 19, no. 2, pp. 1027–1053, 2017.
[13] W. Wang, K. C. Teh and K. H. Li, "Secrecy throughput maximization for MISO multi-eavesdropper wiretap channels," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 3, pp. 505–515, 2017.
[14] X. Zhang, M. R. McKay, X. Zhou and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Transactions on Wireless Communications*, vol. 14, no. 5, pp. 2742–2754, 2015.
[15] X. Chen, C. Yuen and Z. Zhang, "Exploiting large-scale MIMO techniques for physical layer security with imperfect channel state information," in *2014 IEEE Global Communications Conf.*, Austin, TX, USA, pp. 1635–1648, 2014.
[16] X. Chen, Z. Zhang, C. Zhong, D. W. K. Ng and R. Jia, "Exploiting inter-user interference for secure massive non-orthogonal multiple access," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 788–801, 2018.
[17] S. Even, O. Goldreich and S. Micali, "Online/off-line digital signatures," in *Proc. of Advances in Cryptology. CRYPTO 1989, in Lecture Notes in Computer Science*, New York, NY, USA: Springer, vol. 2442, pp. 263–277, 1989.
[18] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," in *Proc. of Advances in Cryptology—CRYPTO 2001*, Santa Barbara, California, USA, pp. 355–367, 2001.
[19] Y. Gao, P. Zeng, K. K. R. Choo and F. Song, "An improved online/offline identity-based signature scheme for WSNs," *International Journal of Network Security*, vol. 18, no. 6, pp. 1143–1151, 2016.
[20] K. Kurosawa and K. S. Samoa, "New online/offline signature schemeswithout random oracles," in *Public Key Cryptography-PKC 2006*, New York, NY, USA, pp. 330–346, 2006.
[21] D. Boneh and X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups," *Journal of Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.
[22] M. Joye, "An efficient on-line/off-line signature scheme without randomoracles," in *Cryptology and Network Security*, CANS 2008, Hong-Kong, China, Springer, pp. 98–107, 2008.
[23] A. C. Yao and Y. Zhao, "Online/offline signatures for low-power devices," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 2, pp. 283–294, 2013.
[24] M. Zheng, S. J. Yang, W. Wu, J. Shao and X. Huang, "A new designof online/offline signatures based on lattice," in *Information Security Practice and Experience*, ISPEC 2018, Tokyo, Japan, Springer, pp. 198–212, 2018.
[25] S. Xu, Y. Mu and W. Susilo, "Online/offline signatures and multisignatures for AODV and DSR routing security," in *Information Security and Privacy*, ACISP 2006, Melbourne, Australia, Springer, pp. 99–110, 2006.
[26] F. Li, M. Shirase and T. Takagi, "On the security of online/offline signatures and multisignatures from ACISP'06," in *Cryptology and Network Security*, CANS 2008, Hong-Kong, China, Springer, pp. 108–119, 2008.

[27] N. Tahat and M. S. Hijazi, "A new digital signature scheme based on chaotic maps and quadratic residue problems," *Applied Mathematics and Information Sciences*, vol. 13, no. 1, pp. 115–120, 2019.
[28] S. Deng, Y. Li and D. Xiao, "Analysis and improvement of a chaos-based Hash function construction," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 5, pp. 1338–1347, 2010.
[29] G. Chen, Y. Mao and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, 2004.
[30] Y. Wang, K. W. Wong, X. Liao and T. Xiang, "A block cipher with dynamic S-boxes based on tent map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3089–3099, 2009.
[31] J. Kar, K. Naik and T. Abdelkader, "A secure and lightweight protocol for message authentication in wireless sensor networks," *IEEE Systems Journal*, vol. 15, no. 3, pp. 1–12, 2020.
[32] K. Chain and W. C. Kuo, "A new digital signature scheme based on chaotic maps," *Nonlinear Dynamics*, vol. 74, no. 4, pp. 1003–1012, 2013.
[33] C. Meshram, C. T. Li and S. G. Meshram, "An efficient online/offline ID-based short signature procedure using extended chaotic maps," *Soft Computing*, vol. 23, no. 3, pp. 747–753, 2019.
[34] C. Y. Meshram, P. L. Powar and M. S. Obaidat, "An UF-IBSS-CMA protected online/offline identity-based short signature technique using PDL," *Procedia Computer Science*, vol. 93, no. 6, pp. 847–853, 2016.
[35] C. Meshram, P. L. Powar, M. S. Obaidat, C. C. Lee and S. G. Meshram, "Efficient online/offline IBSS protocol using partial discrete logarithm for WSNs," *IET Networks*, vol. 7, no. 6, pp. 363–367, 2018.
[36] C. Meshram, C. C. Lee, A. S. Ranadive, C. T. Li, S. G. Meshram *et al.,* "A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing," *International Journal of Communication Systems*, vol. 33, no. 7, pp. 1–15, 2020.
[37] C. Meshram, R. W. Ibrahim, A. J. Obaid, S. G. Meshram, A. Meshram *et al.,* "Fractional chaotic maps based short signature scheme under human-centered IoT environments," *Journal of Advanced Research*, vol. 32, no. 3, pp. 139–148, 2020.
[38] 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.
[39] N. Georg and U. Romer, "Conformally mapped polynomial chaos expansions for uncertain dynamical systems," in *21st IFAC World Congress (Virtual)*, Berlin, Germany, pp. 7279–7282, 2020.
[40] D. Dharminder, U. Kumar and P. Gupta, "A construction of a conformal Chebyshev chaotic map-based authentication protocol for healthcare telemedicine services," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2531–2542, 2021.
[41] N. Georg and U. Römer, "Conformally mapped polynomial chaos expansions for Maxwell's source problem with random input data," *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*, vol. 33, no. 6, pp. 1–15, 2020.
[42] W. Liu, J. Liu, Q. Wu, B. Qin, D. Naccache *et al.,* "Efficient subtree-based encryption for fuzzy-entity data sharing," *Soft Computing*, vol. 22, no. 23, pp. 7961–7976, 2018.
[43] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*. Boca Raton: Chapman & Hall/CRC, 2003.
[44] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons Fractals*, vol. 37, no. 3, pp. 669–674, 2008.
[45] D. Anderson, E. Camrud and D. J. Ulness, "On the nature of the conformable derivative and its applications to physics," *Journal of Fractional Calculus and Applications*, vol. 10, no. 2, pp. 92–135, 2019.
[46] C. Meshram, R. W. Ibrahim, M. S. Obaidat, B. Sadoun and S. G. Meshram, "An effective mobile-healthcare emerging emergency medical system using conformable chaotic maps," *Soft Computing*, vol. 25, no. 14, pp. 8905–8920, 2021.
[47] M. Bellare, C. Namprempre and G. Neven, "Security proofs for identity-based identification and signature schemes," *Journal of Cryptology*, vol. 22, no. 1, pp. 1–61, 2009.
[48] J. K. Liu, J. Baek, J. Zhou, Y. Yang and J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network," *International Journal of Information Security*, vol. 9, no. 4, pp. 287–296, 2010.

[49] Z. Wang and W. Chen, "An ID-based online/offline signature scheme without random oracles for wireless sensor networks," *Personal and Ubiquitous Computing*, vol. 17, no. 5, pp. 837–841, 2013.
[50] J. Kar, "Provably secure online/off-line identity-based signature scheme for wireless sensor network," *International Journal of Network Security*, vol. 16, no. 1, pp. 29–39, 2014.
[51] Y. Gao, P. Zeng, K. K. R. Choo and F. Song, "An improved online/offline identity-based signature scheme for WSNs," *International Journal of Network Security*, vol. 18, no. 6, pp. 1143–1151, 2016.
[52] T. Guelzim, M. S. Obaidat and B. Sadoun, "Introduction and overview ofkey enabling technologies for smart cities and homes," in *Smart Cities and Homes: Key Enabling Technologies*, Cambridge, MA 02139, USA, Elsevier, pp. 1–16, 2016.
[53] M. H. Ibrahim, S. Kumari, A. K. Das, M. Wazid and V. Odelu, "Secure anonymous mutual authentication for star two-tier wireless body area networks," *Computer Methods and Programs in Biomedicine*, vol. 135, no. 1, pp. 37–50, 2016.
[54] G. K. Verma, B. B. Singh, N. Kumar, M. S. Obaidat, D. He *et al.,* "An Efficient and provable certificate-based proxy signature scheme for IIoT environment," *Information Science*, vol. 518, no. 5, pp. 142–156, 2020.
[55] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao *et al.,* "Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks," *IEEE Access*, vol. 7, pp. 114721–114730, 2019.