IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.Doi Number

IBOOST: A Lightweight Provably Secure Identity-based Online/Offline Signature Technique based on FCM for Massive Devices in 5G Wireless Sensor Networks

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

[1]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Govt. Post-Graduation College, College of Chhindwara University, Betul, 460001, Madhya Pradesh, India.
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, 100213 Akoka, Lagos, Nigeria.
[3]Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany.
[4]ENSIAS, Mohammed V University in Rabat, Avenue Mohammed Ben Abdallah Regragui, Madinat Al Irfane, BP 713, Agdal Rabat, Morocco
[5]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[6]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

*Corresponding author: C. Meshram (cs_meshram@rediffmail.com), S. S. Jamal (shussain@kku.edu.sa), and A. L. Imoize (aimoize@unilag.edu.ng)

ABSTRACT The fifth-generation (5G) wireless network is commercialized. The need to integrate massive devices in 5G and wireless sensor networks (WSN) to provide several convenient services for network users becomes imperative. However, there are growing concerns that 5G-WSNs pose new security threats to sensitive user information. User authentication and key agreement have been provided for secure end-to-end communication. However, stricter security techniques are required as billions of massive devices are being networked to collect and process complex user data in real-time. Therefore, anonymous authentication and authorization are highly coveted for privacy preservation and prevention of unlawful exploitation of user data. However, guaranteeing data integrity, authentication, and non-repudiation require special-purpose identity-based signature techniques that are quite difficult to design in practice. In order to address this problem, this paper proposes a lightweight, provably secure identity-based online/offline signature technique (IBOOST) and its extension for massive devices in 5G-WSNs using fractional chaotic maps. The IBOOST scheme achieves multi-time use of offline storage at a lower processing time. Therefore, the signer can reuse the offline pre-stored information in a polynomial time. This makes our IBOOST superior to the existing online/offline signature techniques that allow only a single signature. Additionally, the new technique enables the pre-registration process with a secret key, and no secret key is required in the offline stage. Also, the proposed IBOOST proves to be secure in the random oracle unforgeability under the chosen message attack (UF-IBS-CMA). Finally, the IBOOST and its enhanced version (A-IBOOST) give the lowest computational costs compared to several contending techniques. Therefore, the proposed IBOOST shows superior security and performance with better computational overhead than the preliminary techniques.

INDEX TERMS 5G wireless sensor network systems, Fractional chaotic maps, Identity-based signature scheme, Provably secure.

I. INTRODUCTION

The fifth-generation (5G) wireless networks that are rapidly deployed worldwide have ushered in great relief to the proliferating issues inherent in the ubiquitous 4G wireless networks [1]. 5G wireless networks support the application of blockchain technology [2], holographic communication [3], Industrial Internet of Things (IIoT) [4], wireless security networks [5], and more. Wireless sensor nodes are spatially distributed devices that make up a network system referred to as a wireless sensor network (WSN) [6]. Generally, WSNs find practical applications in environmental conditioning, surveillance systems, military equipment monitoring, healthcare delivery, systems modeling, smart agriculture, intelligent information gathering, smart metering, and more. Sensitive data obtained by the sensor nodes can be transmitted to the receiver seamlessly via WSN-supported channels. The integration of these sensor nodes and several massive machine type communication (MTC) devices (MD) in 5G wireless networks has facilitated the rapid design and growth of sophisticated wireless technologies to connect billions of data-hungry applications [7].

In the Third Generation Partnership Project (3GPP) 5G wireless networks, up to 10^6 devices per km^2 and over 100 billion devices are supported [8], [9]. The user equipment (UE) and massive MDs are defined in the 3GPP standards. Currently, the scope of 5G applications extends to critical areas such as human-centered MTC [10], ultradense Internet of Things (IoT) [11], vehicular networking [12], automation of industrial processes [13], cybersecurity [14], and more. Therefore, the security and confidentiality of data transmitted over 5G WSN-enabled communication channels should be treated seriously. Furthermore, the security of sensitive user data transmitted across 5G-enabled communication channels is critical. Therefore, the need to secure sensitive user information against malicious attackers becomes imperative. Thus, the transmission of personal data over these wireless channels needs to be supported by lightweight and provably secure online/offline identity-based signature techniques (IBS) [15].

Fractional chaotic maps-based lightweight digital signatures have been proposed to strengthen the security, confidentially, and integrity of sensitive information transmitted over insecure channels [16]. Interestingly, these signatures are designed to satisfy stringent security requirements. In current literature, chaotic maps [17], based on their cryptographic characteristics, have been used to develop provably secure online/offline IBS techniques to enhance the security of confidential and sensitive user information. Compared to the ubiquitous mobile ad hoc networks [18], WSNs are susceptible to several attacks due to their deployment and operation in open or unsecured communication channels. It is worth mentioning that a typical WSN domain could aggregate several sensor nodes and wireless base stations [19].

The concept of online/offline signature was proposed in 1989 by Even et al. [20]. Online/offline signature schemes require that part of the signing is done online and the other is carried out offline. The offline-based signing, which is the first phase, is time-consuming and more computationally expensive. In contrast, the online signing phase, which could be conducted when signing the message, is much faster. In terms of computational complexity, the second phase is the lightweight aspect of the scheme. Even et al. [20] demonstrated a generalized construction for transforming any digital signature scheme to their online/offline signature scheme equivalents [20]. However, Even et al.'s approach has several practical limitations. Several literature reports show that the generalized construction due to Even et al. extends each signature quadratically. In 2001, Shamir and Tauman [21] reported the hash-sign-switch scheme to address the fundamental limitations of Even et al.'s scheme.

The generalized hash-sign-switch scheme converts any signature scheme into its online/offline signature scheme more efficiently, irrespective of the signature type. To further enhance the capabilities of the Shamir and Tauman scheme, some special purpose schemes have been designed [22]. The scheme reported by Kuro- Sawa and Schmidt-Samoa [23] can create online/offline signature schemes without a random oracle. Online/offline signature schemes have been reported for low-power devices [24], and the use of lattice for the design of new online/offline signature schemes has been reported by [25]. The scheme in [26] appears to be efficient, as remarked by [27]. However, a closer look at these schemes shows that they capture the identity-based settings but focused mainly on the usual public-key-based situation. It is interesting to note that pairing-enabled IBS schemes have been reported [28]. Also, Galindo and Garcia [29] utilized Schnorr's signature to design a non-pairing IBS scheme for use in a discrete logarithm environment.

In 2006, the idea of online/offline identity-based signatures and multi-purpose signatures was raised by Xu et al. [30]. Xu et al. presented an online/offline IBS scheme modified to an online/offline identity-based multi-signature scheme. It is worth mentioning that an appropriate pairing technique can apply Xu et al.'s scheme to several routing procedures. However, several limitations have been identified in Xu et al.'s scheme. For instance, Li et al. [31] have shown that Xu et al.'s scheme failed some less complex forgery attacks. Thus, it is not unlikely that the supposed secure scheme offered by Li et al. [31] has several security flaws.

Currently, it is quite difficult to find a flawless online/offline IBS technique. It is worth noting that chaos-based cryptographic schemes have been used to design secure communication channels to address this problem [32]. In practice, chaotic maps find useful applications in symmetric encryption [33], hash functions [34], and S-boxes [35]. Chaos-based key agreement schemes [36], provably secure online/offline IBS techniques [37], and healthcare delivery systems [38], have been reported. Furthermore, Chain and Kuo [39] presented a chaotic map-based digital signature scheme. After the work of Chain and Kuo [39] in 2013, new chaotic map-empowered cryptographic schemes [40] and identity-based encryption schemes [41] have been reported.

In recent literature, Meshram et al. [40] used the concept of the partial discrete logarithm to create an online/offline IBSS scheme. It is noteworthy that this scheme supports pre-stored information to enable offline signature in a polynomial time. This feature demonstrates the superiority of Meshram et al.'s IBSS scheme over the preliminaries. Additionally, an aggregation scheme suitable for application in WSNs has been proposed by Meshram et al. [42]. The choice of this scheme for WSNs is premised on its low computational complexity and fast processing time. The online stage could be executed in the sensor nodes (SN), whereas the offline stage can be executed at the base station (BS) in a typical WSN configuration. Interestingly, the online phase is relatively fast and can be easily supported by lightweight devices- SN in a WSN, enabling seamless communications. In recent times, the concept of bilinear pairing has been adopted to develop online/offline several IBSSs [26]. Also, a modified online/offline IBS scheme suitable for WSNs has been presented by Gao et al. [43].

Additionally, Ling et al. [44] reported a one-time password security scheme for applications in WSNs. To enhance the security of the Vehicular Ad hoc Network (VANET), Kumar et al. [45] introduced a secure certificateless signature scheme (CSS) and certificateless aggregated signature scheme (CASS). The work shows that the CASS satisfies the conditional privacy requirement. It is pretty easy to map messages created by a vehicle to a distinguishable pseudo-identity in this case. Furthermore, Kumar et al. [46] presented a secure certificateless public key cryptography (CPKC) scheme with low complexity. The scheme is capable of removing the vast certificate management issues from public-key cryptography (PKC). The scheme is also able to resolve the key escrow problem inherent in identity-based cryptography.

Recently, Meshram et al. [47] use chaotic maps to develop a subtree-centric model for cryptosystems in cloud-based environments. Additionally, Meshram et al. [48] leveraged chaotic theory to create an efficient and highly secured level online/offline subtree-based short signature scheme (OOS-SSS). The proposed OOS-SSS scheme, which applies to a WSN environment, enables the fuzzification of user data over a Galois field. Additionally, the scheme was found to be unforgeable and secure under several sophisticated message attacks. Finally, the scheme is extendable and supports offline signatures leveraging pre-stored information and enabling an aggregation scheme for WSN-based applications.

Motivation and Contribution: We present a detailed literature review of the existing lightweight, provably secure identity-based online/offline signature techniques. Unfortunately, most schemes are based on hard problems like the elliptic curve and pairing and pose huge computational and communication costs. Furthermore, it is worth mentioning that most of the schemes are not subjected to a comprehensive test using Scyther, AVISPA, and other high-end security validation tools. Consequently, it becomes challenging for small devices with limited computational resources to handle such schemes. Therefore, a lightweight, provably secure identity-based online/offline signature technique (IBOOST) based on FCM for massive devices in 5G wireless sensor networks is required to achieve low computational costs. Additionally, efficient, lightweight, provably secure IBOOSTs need to be exploited for enhanced cryptographic solutions to support the battery lifetimes of resource-constrained lightweight devices in 5G-WSNs. This idea motivates the proposed scheme, referred to IBOOST for massive devices in 5G-WSNs. The main contributions of this paper are outlined as follows.

- We proposed a lightweight, provably secure IBOOST based on Fractional Chaotic Maps (FCM) for massive devices in 5G-WSNs. The IBOOST is protected in a situation of random oracle unforgeability of IBS under chosen message attack (UF-IBS-CMA). Thus, it helps address the limitations inherent in the existing techniques used for resource-limited and low-powered devices in 5G wireless sensor networks.
- We present an extension to the IBOOST to support the registration of various messages and implementing them in the 5G-WSN environment.
- We tested the IBOOST using standard metrics and compared it with the existing techniques, and we demonstrate that our IBOOST gives greater efficiency in terms of communication and computational costs.
- We provided a suitable setting for applying the IBOOST to massive devices in 5G wireless sensor networks.

Road map: The remainder of this work is organized in the following manner. Section II outlines the basic prerequisites. Then, our new provably secure, efficient IBOOST using FCM is detailed in Section III. Section IV contains the security examinations and explanations. Section V presents our aggregation (extended IBOOST) scheme of the IBOOST for massive devices in 5G wireless sensor networks. The performance analysis of IBOOST is discussed in Section VI. Following that, Section VII deals with the essential setting of the IBOOST for massive devices in 5G wireless sensor networks. Finally, Section VIII contains the conclusion to the paper.

II. BACKGROUND INFORMATION

This segment briefly introduces the mathematical definitions and related theorems used in designing our new and efficient IBOOST, including some basic concepts of the Chebyshev polynomial, fractal Chebyshev polynomial, and fractional chaotic maps.

A. CHEBYSHEV CHAOTIC MAPS

The concepts of ambiguity and diffusion are two basic conditions in the development of cryptographic systems. The sensitivity of the primary situations, ergodicity, and pseudo-randomness assets of chaotic frameworks make them acceptable for achieving uncertainty and diffusion assets in cryptography. Consequently, several asymmetric and symmetric key cryptosystems have been developed using chaotic maps [49].

Definition 1. (Chaotic map). The CSP $\mathrm{T}_n(\mathrm{v})$ is an n-degree polynomial in the variant v. Allow $\mathrm{v} \in [-1, 1]$ to be the edition and n to be a large integer. CSP stated the following in general [49]:

$$\mathrm{T}_n(\mathrm{v}) = cos\big(n \ arccos(\mathrm{v})\big), \mathrm{T}_0(\mathrm{v}) = 1, \mathrm{T}_1(\mathrm{v}) = \mathrm{v}$$

The Chebyshev polynomial's recurrence relation is defined as

$$\mathrm{T}_n(\mathrm{v}) = 2\mathrm{v}\mathrm{T}_{n-1}(\mathrm{v}) - \mathrm{T}_{n-2}(\mathrm{v});\ n \geq 2$$

The functional $arccos(\mathrm{v})$ and $cos(\mathrm{v})$ represented as $arccos\colon [-1, 1] \rightarrow [0,]$ and $cos\colon R \rightarrow [-1, 1]$ in this case.

B. PROPERTIES OF CHAOTIC MAPS

The following are two interesting properties of Chebyshev polynomials [49], [50], [51], [52]:

Definition 2. ***(****Chaotic properties).* The CSP transform is known as $Ʈ_n: [-1, 1] \rightarrow [-1, 1]$ with degree n 1, is a chaotic transform associated with the functional (invariant density) $f^*(\mathrm{v}) = 1/\left(\pi\sqrt{1-\mathrm{v}^2}\right)$ for positive Lyapunov exponent $\lambda = ln\, n > 0$.

Definition 3. ***(****Semi-group properties).* The semi-group property of the Chebyshev polynomial (CP) $Ʈ_n(\mathrm{v})$ is demarcated as follows:

$$Ʈ_\tau\,(Ʈ_l(\mathrm{v})) = cos(\tau\, cos^{-1}(cos(l\, cos^{-1}(\mathrm{v})))) = cos(\tau l\, cos^{-1}(\mathrm{v})) = Ʈ_{l\tau}(\mathrm{v}) = Ʈ_l(Ʈ_\tau\,(\mathrm{v})),$$

where l and τ are (+) integers and $\mathrm{v}[-1, 1]$.

According to Bergamo *et al.* [49], public-key cryptography using CP map semi-group property is not stable, and Zhang [50] proved that the semi-group property retains an interval $(-\infty, +\infty)$, which can boost the property as tracks:

$$Ʈ_n(\mathrm{v}) = 2\mathrm{v}Ʈ_{n-1}(\mathrm{v}) - Ʈ_{n-2}(\mathrm{v})(mod\ q_1);\ n \geq 2$$

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

$$Ʈ_\tau\big(Ʈ_l(\mathrm{v})\big)(modq_1) = Ʈ_{l\tau}(\mathrm{v})(modq_1)$$
$$= Ʈ_l\big(Ʈ_\tau(\mathrm{v})\big)(modq_1)$$

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

C. COMPUTATIONAL PROBLEMS

In this segment, some computational issues based on the CPs are described leveraging the propositions [16], [38], [51], [52], [53], [54], [55].

Definition 4. (Chaotic Map-based Discrete Logarithm (CMDL) problem). Given a random tuple $< y, \mathrm{v} >$, any polynomial time-bounded algorithm that finds the integer τ where $y = Ʈ_\tau(\mathrm{v})\ (mod\ q_1)$ is infeasible.

Definition 5. (Chaotic Map-based Diffie-Hellman (CMDH) problem). For a given random tuple $< \mathrm{v}, Ʈ_\tau(\mathrm{v}), Ʈ_l(\mathrm{v}) >$, any polynomial time-bounded algorithm that tries to find the value $Ʈ_{\tau l}(\mathrm{v})\ (mod\ q_1)$ fails.

D. FRACTAL CHAOTIC MAPS (FCM)

The Fractal Calculus (FC) was historically known as a local fractional calculus [16], [56]. However, it accepted possessions for fractional calculus (derivatives of non-integer power). Thus, FC, in essence, comes before the corresponding preparation:

Assume that the fractional difference operator ξ^δ is defined by the formal expression for an arbitrary fractional-order $\delta\epsilon[0, 1]$.

$$\xi^\delta\psi(y) = \frac{\Delta^\delta\,(\psi(y)-\psi(y_0))}{(y-y_0)^\delta} = \Gamma(\delta+1)\big(\psi(y)-\psi(y_0)\big)$$

and it is the same as the fractal integral operator.

$$I^\delta\psi(y) = \frac{1}{\Gamma(\delta+1)}\int_a^b \psi(y)\,(dy)^\delta.$$

The formula can be used to approximate it as in (1)

$$I^\delta\psi(y) = \frac{(b-a)^\delta}{\Gamma(\delta+1)}\,\psi(y), \qquad a \leq y \leq b. \tag{1}$$

Thus, we get the following construction by using the FC definition to generalize the polynomial $Ʈ_n(\mathrm{v})$:

$$I^\delta Ʈ_n(\mathrm{v}) \coloneqq {Ʈ_n}^\delta(\mathrm{v}) = \frac{(2)^\delta}{\Gamma(\delta+1)}Ʈ_n(\mathrm{v}), \tag{2}$$

which is the Fractal Chebyshev polynomial, and FCP represents it (see Fig.1).

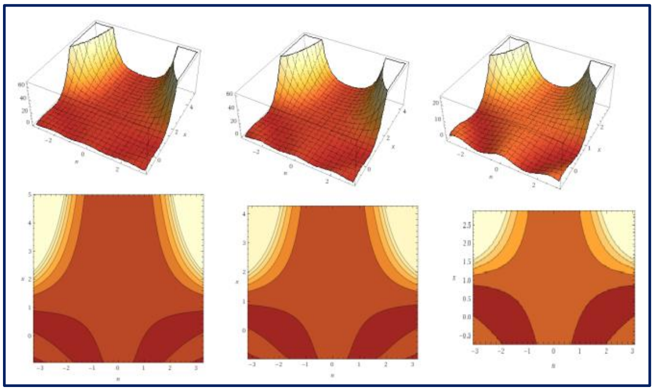

Fig. 1 3D-FCP when δ = 0, 1/2 and ¾ correspondingly

E. PROPERTIES OF FRACTAL CHAOTIC MAPS

The following are two relaxing features of the FCP:

Definition 6 ***(****Chaotic properties of FCM).* The recurrent relations under the chaotic property is fulfilled by the Fractal Chaotic Maps [16], i.e.,

$${Ʈ_n}^\delta(\mathrm{v}) = \frac{(2)^\delta}{\Gamma(\delta+1)}(\,2\mathrm{v}Ʈ_{n-1}(\mathrm{v}) - Ʈ_{n-2}(\mathrm{v}))\ (mod\ \rho_1).$$

The usual prominent effect, seen in Yang *et al.* [56], is well understood when $\delta \rightarrow 0$ is used.

Definition 7 (*Semi-group properties of FCM****).*** For FCMs on the interval (-∞, ∞) [16], the semi-group properties locks, i.e.,

$${Ʈ_k}^\delta\left({Ʈ_n}^\delta(\mathrm{v})\right)\ (mod\ \rho_1) = {Ʈ_n}^\delta\left({Ʈ_k}^\delta(\mathrm{v})\right)\ (mod\ \rho_1)$$
$$= {Ʈ_{kn}}^\delta(\mathrm{v}).\,(mod\ \rho_1)$$

III. THE PROPOSED IBOOST TECHNIQUE BASED ON FRACTIONAL CHAOTIC MAPS

This section describes the novel and efficient IBOOST technique for massive devices in 5G wireless sensor networks. The plan is made up of five steps as follows.

A. SETUP

i. Select a large prime ρ_1 and a global parameter $\vartheta \in Ɠ$, where $Ɠ$ is a multiplicative group.
ii. Select an arbitrary $♭ \in_R Z^*_{\rho_1}$.
iii. Select an arbitrary rational number $\delta \in [0,1]$.
iv. Calculate $\beta = Ʈ^{\delta}_{♭}(\vartheta)(mod\ \rho_1)$.
v. Choose $\mathcal{H}$ hash functions: $\mathcal{H}: \{0,1\}^{\infty} \rightarrow Z^*_{\rho_1}$.

The master public and secret keys are specified by $\{\rho_1, \vartheta, \mathcal{H}, \beta\}$ and $(♭, \delta)$, respectively.

B. EXTRACTION

The secret key is produced using a client's identity id by performing the following stages:

i. Select at random $𝓌 \in_R Z^*_{\rho_1}$.
ii. Computes $\mu = Ʈ^{\delta}_{𝓌}(\vartheta)(mod\ \rho_1)$ and $ƅ = \mathcal{H}(id, \mu)$.
iii. Compute $\pi = 𝓌 * ♭ƅ(mod\ \rho_1)$.

The pair (μ, π) is the client's secret key.

C. OFFLINE SIGNING

In the offline stage, the signer does the subsequent estimations:

i. Compute $\mathcal{W}'_{j} = Ʈ^{\delta}_{2^{j}}(\vartheta)(mod\ \rho_1)$, for $j \in [0, |\rho_1| - 1]$.

D. ONLINE SIGNING

To register a message $\mathcal{M} \in (-\infty, \infty)$ using (μ, π), the signer conducts the subsequent steps in the online phase:

i. Pick an arbitrarily $\ell \in_R Z^*_{\rho_1}$, so that ℓ_j is the j^th^ bit of ℓ.
ii. Compute $\mathcal{W} = \prod_{j=1}^{\rho_1} \mathcal{W}'_{j-1}\ (mod\ \rho_1)$ and $\eta = \mathcal{H}(\mathcal{W}, \mu, \mathcal{M})$
iii. Compute $𝓎 = \ell * \pi\eta(mod\ \rho_1)$ as well as $\Upsilon = Ʈ^{\delta}_{𝓎}(\vartheta)(mod\ \rho_1)$.

The signature $ɕ$ of $\mathcal{M}$ is given by $ɕ = (\mathcal{W}, \mu, 𝓎)$.

E. VERIFICATION

The verifier conducts the following two stages to verify a signature $ɕ = (\mathcal{W}, \mu, 𝓎)$ on the $\mathcal{M}$ and id:

i. Compute $\Upsilon' = \mathcal{W}Ʈ^{\delta}_{\eta}(\mu)Ʈ^{\delta}_{\etaƅ}(\beta)(mod\ \rho_1)$.
ii. If $\Upsilon = \Upsilon'$, the signature is accepted, or else this is not.

Correctness:

The correctly generated private key must meet the following criteria:

$$Ʈ^{\delta}_{\pi}(\vartheta)(mod\ \rho_1) = \mu Ʈ^{\delta}_{ƅ}(\beta)(mod\ \rho_1) \quad (3)$$

For the reliability of an algorithm, note that $\mathcal{W} = Ʈ^{\delta}_{\ell}(\beta)(mod\ \rho_1)$. We have:

$$\begin{aligned}\mathcal{W}\, Ʈ^{\delta}_{\eta}(\mu)Ʈ^{\delta}_{\etaƅ}(\beta)(mod\ \rho_1) &\\ &= Ʈ^{\delta}_{\ell}(\vartheta)Ʈ^{\delta}_{\eta𝓌}(\vartheta)Ʈ^{\delta}_{♭\etaƅ}(\vartheta)(mod\ \rho_1)\\ &= Ʈ^{\delta}_{𝓎}(\vartheta)(mod\ \rho_1) \quad (4)\end{aligned}$$

IV. SECURITY EXAMINATIONS AND DISCUSSIONS

To validate the security of IBOOST based on FCM, we employ the security confirmations due to Bellare et al. [57].

Theorem 1: The projected IBOOST is $(\epsilon, t, ʠ_{\mathcal{H}}, ʠ_{𝓈}, ʠ_{E})$ secure in the knowledge of unforgeability of IBS technique under the chosen message attack (UF-IBS-CMA) in the ROM, implementing the $(\epsilon', 𝓉')-$ FCM hypothesis in $Ɠ$, where:

$$\epsilon' \approx \left(1 - \frac{(ʠ_E + ʠ_{𝓈})ʠ_{\mathcal{H}}}{\rho_1}\right)\left(\frac{\rho_1 - 1}{\rho_1 ʠ_{\mathcal{H}}}\right)\epsilon \quad (5)$$

$$𝓉' \approx 𝓉 + \mathcal{O}(ʠ_{𝓈} + ʠ_E)\tau \quad (6)$$

and $ʠ_{𝓈} -$ signing queries, $ʠ_E -$ extraction queries are the amount of chaos and $ʠ_{\mathcal{H}} -$ hashing queries. Here τ is the time for an operation of exponentiation. Now τ is the time to do an exponentiation operation.

Proof: Suppose that there is a foe named $\mathcal{F}$. To solve the FCM-based problem, we develop the algorithm $\mathfrak{B}$, which is dependent on the use of $\mathcal{F}$. The algorithm $\mathfrak{B}$ comes with a multiplicative group $Ɠ$ that has a comprehensive ϑ parameter and an exponent $\kappa \in Ɠ$ that is checked to find $ⱴ \in Z^*_{\rho_1}$ in a method that $\kappa = Ʈ^{\delta}_{ⱴ}(\vartheta)(mod\ \rho_1)$. The method of [57] is used.

Setup: $\mathfrak{B}$ uses a $\mathcal{H}$ hash function that behaves similarly to a random oracle and is responsible for simulating the reformation procedure. $\mathfrak{B}$ allocates an exponent $\beta \leftarrow \kappa$ and outputs the public parameter $(𝓎, \rho_1, \beta, \mathcal{H})$ to $\mathcal{F}$.

Extraction Oracle queries: The extraction oracle allows $\mathcal{F}$ to search for id, and $\mathfrak{B}$ reproduces the oracle. It needs random $s, t \in Z^*_{\rho_1}$, and the following sets:

$$\mu = Ʈ^{\delta}_{𝓉}(\vartheta)/Ʈ^{\delta}_{𝓈}(\beta)(mod\ \rho_1),\ \pi \leftarrow t,\ \ \mathcal{H}(\mu, id) \leftarrow s \quad (9)$$

$\mathfrak{A}$ generates (μ, π) as a secret key for id and saves the consistency assessment $(\mu, \mathcal{H}(\mu, id), \pi, id)$ in a list.

Signing Oracle queries: The foe $\mathcal{F}$ inquires id and signs a message. The algorithm $\mathfrak{B}$ examines whether $\mathcal{H}$ oracle or the extraction oracle has been queried for id in the past. If this is the case, it will simply expand the list $(\mu, \pi, \mathcal{H}(\mu, id))$ as shown in the table. Then, using these estimates, algorithm $\mathfrak{B}$ performs the signature processes on the message. It creates the message's signature $(\mathcal{W}, \mu, 𝓎)$ and keeps a list of $\mathcal{H}(\mathcal{W}, \mu, \mathcal{M})$ for consistency in the hash table. If id is not demanded to extract the oracle, $\mathfrak{B}$ begins the extraction oracle simulation method by signing the message with the secret key.

Output Calculation: Finally, $\mathcal{F}$ generates a bogus signature $ɕ^*_1 = (\mathcal{W}^*, \mu^*, 𝓎^*_1)$ on $\mathcal{M}^*$ and id^*. The algorithm $\mathfrak{B}$ converses $\mathcal{F}$ in the sense that it does a $\mathcal{H}(\mathcal{W}^*, \mu^*, \mathcal{M}^*)$ and returns a different value to the acceptable. Foe $\mathcal{F}$ generates a few other signatures $ɕ^*_2 = (\mathcal{W}^*, \mu^*, 𝓎^*_2)$. Algorithm $\mathfrak{B}$ re-hashes the data and returns $ɕ^*_3 = (\mathcal{W}^*, \mu^*, 𝓎^*_3)$. It is worth

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2021.3114287, IEEE Access

noting that $\mathcal{W}^*$and $\mu^*$are invariably the same. We assume that the output of the random oracle queries $\mathcal{H}(\mathcal{W}^*, \mu^*, \mathcal{M}^*)$, for three times in a row, is $\text{ŋ}_1, \text{ŋ}_2, \text{ŋ}_3$.

We now project FCM of μ, β, and $\mathcal{W}$ for each $\text{ƅ}, \ell, \mathcal{w} \in Z_{\rho_1}^*$, respectively. i.e., $\mu = \text{Ʈ}_{\mathcal{w}}^{\delta}(\vartheta)(mod\ \rho_1)$, $\beta = \text{Ʈ}_{\text{ƅ}}^{\delta}(\vartheta)(mod\ \rho_1)$ and $\mathcal{W} = \text{Ʈ}_{\ell}^{\delta}(\vartheta)(mod\ \rho_1)$. From Eq. (4), we have:

$\mathcal{y}_{\text{ȷ}}^* = \ell * \mathcal{w}\text{n}_{\text{ȷ}} * \text{ƅ}\text{ŋ}_{\text{ȷ}}\mathcal{H}(\mu^*, \mathcal{id})(mod\ \rho_1)$for $\text{ȷ} = 1,2,3$ (10)

In these mathematical examinations, only $\text{ƅ}, \ell$, and $\mathcal{w}$ are foreign to $\mathfrak{B}$. The algorithm $\mathfrak{B}$ computes for $\text{ȷ} = 1,2,3$ and produces ƅ as the solution of the FCM for overhead linear autonomous mathematical proclamations.

Reduction Cost Inspection: The random oracle's consignment $\mathcal{H}(\mu, \mathcal{id})$ is irregular in the simulation process with extraction oracle failures, implying a combined probability of at least $\frac{\text{ɋ}_{\mathcal{H}}}{\rho_1}$. As a result, the simulation technique is effective $(\text{ɋ}_{\mathcal{s}} + \text{ɋ}_E)$ times (as a result of the fact that if $\mathcal{id}$ is not demanded in the extraction oracle, $\mathcal{H}(\mu, \mathcal{id})$ can also be asked in the signature oracle), with the probability being:

$$\left(1 - \frac{(\text{ɋ}_{\mathcal{s}} + \text{ɋ}_E)\text{ɋ}_{\mathcal{H}}}{\rho_1}\right) \leq \left(1 - \frac{\text{ɋ}_{\mathcal{H}}}{\rho_1}\right)^{(\text{ɋ}_{\mathcal{s}}+\text{ɋ}_E)}$$

There exists an inquiry $\mathcal{H}(\mathcal{W}^*, \mu^*, \mathcal{M}^*)$ with a probability of at least $\left(1 - \frac{1}{\rho_1}\right)$ due to the random oracle's perfect unpredictability. $\mathfrak{B}$ suppositions it appropriately as the point of rewind, at least with a $\left(\frac{1}{\text{ɋ}_{\mathcal{H}}}\right)$ probability. Overall, the probability of success is:

$$\left(1 - \frac{(\text{ɋ}_E + \text{ɋ}_{\mathcal{s}})\text{ɋ}_{\mathcal{H}}}{\rho_1}\right)\left(\frac{\rho_1 - 1}{\rho_1 \text{ɋ}_{\mathcal{H}}}\right)\epsilon$$

The exponentiations done in the signing and extraction procedures determine the temporal complexity of algorithm $\mathfrak{B}$, which is identical to:

$$\mathcal{t} + \mathcal{O}(\text{ɋ}_{\mathcal{s}} + \text{ɋ}_E)\tau$$

ȷ times the length of a single signature is significantly shorter.

V. AGGREGATION (EXTENSION) TECHNIQUE OF THE IBOOST FOR 5G WIRELESS SENSOR NETWORKS

It would be highly advantageous if an SN could sign not just one but ȷ separate messages simultaneously. In this case, the aggregate signature can have the same length as a single message's signature or ȷ times the length of a single signature, which is significantly shorter. Such an aggregate signature is highly significant in massive devices in 5G wireless sensor networks since it can drastically reduce sensor node communication overheads. This section presents the new online/offline identity-based aggregation strategy for the proposed IBOOST technique using FCM. It comprises the five segments listed as follows.

A. SETUP

i. Select a large prime ρ_1 and a global parameter $\vartheta \in \text{Ɠ}$, where Ɠ is a multiplicative group.
ii. Select an arbitrary $\text{ƅ} \in_R Z_{\rho_1}^*$.
iii. Select an arbitrary rational number $\delta \in [0,1]$.
iv. Calculate $\beta = \text{Ʈ}_{\text{ƅ}}^{\delta}(\vartheta)(mod\ \rho_1)$.
v. Choose $\mathcal{H}$ chaotic hash functions: $\mathcal{H}: \{0,1\}^{\infty} \rightarrow Z_{\rho_1}^*$.

The master public and private keys are given by $\{\rho_1, \vartheta, \mathcal{H}, \beta\}$ and $(\text{ƅ}, \delta)$, respectively.

B. EXTRACT

The private key is produced using a client's identity $\mathcal{id}$ by implementing the subsequent steps:

i. Pick at random $\mathcal{w} \in_R Z_{\rho_1}^*$.
ii. Computes $\mu = \text{Ʈ}_{\mathcal{w}}^{\delta}(\vartheta)(mod\ \rho_1)$ and $\text{б} = \mathcal{H}(\mathcal{id}, \mu)$.
iii. Compute $\pi = \mathcal{w} * \text{ƅ}\text{б}(mod\ \rho_1)$.

The client's secret key is the pair (μ, π).

C. OFFLINE SIGNING

The signer executes the subsequent estimation:

i. Compute $\mathcal{W}_{\text{ȷ}}' = \text{Ʈ}_{2^{\text{ȷ}}}^{\delta}(\vartheta)(mod\ \rho_1)$, for $\text{ȷ} \in [0, |\rho_1| - 1]$.

D. ONLINE SIGNING

To register a message $\mathcal{M} \in (-\infty, \infty)$ using (μ, π), the signer follows the procedures below:

i. Select $\ell_{\text{ȷ}} \in_R Z_{\rho_1}^*$ at random where $\ell_i[\text{ȷ}]$ is the i^{th} bit of $\ell_{\text{ȷ}}$.
ii. Define $\ell_{\text{ȷ}} \subset \{1, \dots., |\rho_1|\}$ as the set of indices that makes $\ell_i[\text{ȷ}] = 1$.
iii. Computes $\mathcal{W}_{\text{ȷ}} = \prod_{\text{ȷ}\in\ell_{\text{ȷ}}} \mathcal{W}_{i-1}'$ and $\eta_{\text{ȷ}} = \mathcal{H}\left(\mathcal{W}, \mu, \mathcal{M}_{\text{ȷ}}\right)$.
iv. Computes $\mathcal{y}_{\text{ȷ}} = \ell_{\text{ȷ}} * \eta_{\text{ȷ}}\pi(mod\ \rho_1), \mathcal{y} = \sum_{\text{ȷ}=1}^{n} \mathcal{y}_{\text{ȷ}}$ and $\Upsilon = \text{Ʈ}_{\mathcal{y}}^{\delta}(\vartheta)(mod\ \rho_1)$.

The aggregate signature is given by $\text{ɕ} = (\mathcal{W}_{\text{ȷ}}, \mu, \mathcal{y})$.

E. VERIFICATION

The verifier executes these steps to validate a signature $\text{ɕ} = \left(\mathcal{W}_{\text{ȷ}}, \mu, \mathcal{y}\right)$on the $\mathcal{M}_{\text{ȷ}}$ and $\mathcal{id}$ for $\text{ȷ} = 1, \dots., n$:

i. Computes $\eta_{\text{ȷ}} = \mathcal{H}\left(\mathcal{W}, \mu, \mathcal{M}_{\text{ȷ}}\right)$ and $\Upsilon' = \left(\prod_{\text{ȷ}=1}^{n} \mathcal{W}_{\text{ȷ}}\right)\text{Ʈ}_{\varsigma}^{\delta}(\mu)\text{Ʈ}_{\varsigma d}^{\delta}(\beta)(mod\ \rho_1)$, where $\varrho = \sum_{\text{ȷ}=1}^{n} \eta_{\text{ȷ}}$
ii. The signature is allowed if $\Upsilon = \Upsilon'$; else, the signature is denied.

Correctness:

The correctly generated private key must meet the following criteria:

$\mathcal{W}_{\text{ȷ}} = \text{Ʈ}_{\ell_{\text{ȷ}}}^{\delta}(\vartheta)(mod\ \rho_1)$ for $\text{ȷ} \in [1, \dots., n]$.

We have

$$\Upsilon' = \left(\prod_{\text{ȷ}=1}^{n} \mathcal{W}_{\text{ȷ}}\right)\text{Ʈ}_{\varrho}^{\delta}(\mu)\text{Ʈ}_{\varrho d}^{\delta}(\beta)(mod\ \rho_1)$$

$$= \left(\prod_{\mathrm{j}=1}^{n} \mathcal{W}_{\mathrm{j}}\right)\mathrm{Ʈ}^{\delta}_{w\varrho}(\vartheta)\mathrm{Ʈ}^{\delta}_{\varrho\flat d}(\vartheta)(mod\ \rho_1)$$

$$= \mathrm{Ʈ}^{\delta}_{\ell}(\vartheta)\mathrm{Ʈ}^{\delta}_{\varrho w}(\vartheta)\mathrm{Ʈ}^{\delta}_{\flat\varrho d}(\vartheta)(mod\ \rho_1)$$

$$= \mathrm{Ʈ}^{\delta}_{y}(\vartheta)(mod\ \rho_1)$$

When the recommended A-IBOOST approach is utilized, the signature size is reduced by about half when compared to the non-A-IBOOST variation, as illustrated in Fig.2.

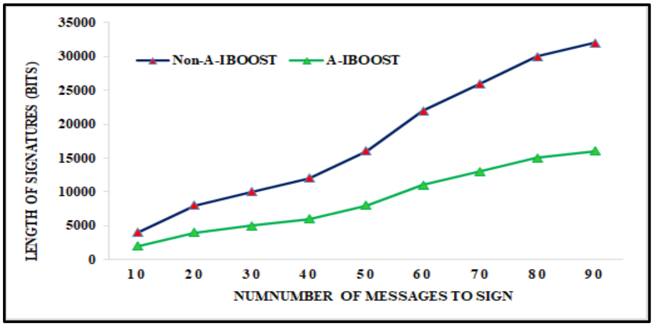

Fig.2. Comparison among A-IBOOST and non-A-IBOOST variants.

VI. PERFORMANCE ANALYSIS

In this section, we compare our new IBOOST with seven other techniques proposed by [58], [59], [60], [61], [40], [48], and [62]. Additionally, we compare our extended IBOOST technique referred to as A-IBOOST with five other related techniques proposed by [58], [60], [61], [48], and [42], respectively, to demonstrate the efficiency of our new design. The notations used to present our evaluation results include $\mathbb{t}_{m,}$ $\mathbb{t}_{i,}$, $\mathbb{t}_e$,$\mathbb{t}_c$, $\mathbb{t}_p$ and $\mathbb{t}_h$. We denote the execution time required for modular multiplication, modular inverse operation, group modular exponentiation, chaotic map operation, bilinear paring operation, and one-way hash function in the signing (online and offline) stage and verification phase. It is worth noting that only the signing and verification phases are the dominant processes that need more computing resources than the setup and extraction stages. Therefore, in our computational cost comparison, we concentrate only on the stages of signing and verification as we contrast our current IBOOST with the works of [58], [59], [60], [61], [40], [48], and [62], respectively. Also, we contrast our new A-IBOOST with the works of [58], [60], [61], [48], and [42], respectively, in a similar fashion. The length of the signature in the proposed IBOOST and A-IBOOST is 480 (bit) each.

The functionality analysis of the proposed IBOOST is shown in Table 1 and compares computational costs in Fig. 2 with other related protocols [58], [59], [60], [61], [40], [48], and [62]. Additionally, the functionality analysis of the proposed A-IBOOST is shown in Table 2 and compares computational costs in Fig. 3 with other related protocols [58], [60], [61], [48], and [42], respectively. Based on the results of the experiments in [51-53], we reach at the subsequent computation time figures with unit hashing time: $\mathbb{t}_e = 600\mathbb{t}_h$, $\mathbb{t}_m = 2.5\mathbb{t}_h$,$\mathbb{t}_i = 7.5\mathbb{t}_h$,$\mathbb{t}_p = 1550\mathbb{t}_h$ and $\mathbb{t}_h \approx \mathbb{t}_c$. In this method, we have the following order of computing complexity: $\mathbb{t}_h \approx \mathbb{t}_c \approx< \mathbb{t}_m < \mathbb{t}_i < \mathbb{t}_e < \mathbb{t}_p$. In addition, in this area, we give the results of our evaluation. The findings were averaged across 300 randomized simulation runs on a four-core 3.2 GHz computer with 8 GB memory [64]. Our simulator, which was created in MATLAB, was used to conduct the experiments. A one-way hash function takes 0.32 milliseconds (ms) [64] [16] and [$\delta = 0.75$]. The computational expenses of XOR, timestamp and random number generation are generally overlooked because they are significantly less expensive than one-way hash computations. The total communication costs of the works of [58], [59], [60], [61], [40], [48], [62] and the IBOOST are 579.04 ms, 772.80 ms, 2485.44 ms, 1682.56 ms, 4.8 ms, 5.6 ms, 886.56 ms, and 4.424ms, respectively. The total communication costs of the works of [58], [60], [61], [48], [42] and the A-IBOOST are 578.44 ms, 1492.64, 1875.84 ms, 5.92 ms, 579.04 ms, and 4.424ms, respectively.

We arrive at the following computation time numbers with unit hashing time based on the experimental results in [51-53]:

Table 1: Computational cost assessment of IBOOST with other techniques

Techniques	Signing Stage (online and offline)	Verification Stage	Total (ms)
[58]	$\mathbb{t}_e + \mathbb{t}_h + \mathbb{t}_m$	$2\mathbb{t}_e + \mathbb{t}_h + 2\mathbb{t}_m$	579.04
[59]	$2\mathbb{t}_e + 4\mathbb{t}_m$	$2\mathbb{t}_e + 2\mathbb{t}_m$	772.80
[60]	$\mathbb{t}_p + 6\mathbb{t}_m + \mathbb{t}_h$	$4\mathbb{t}_p + 2\mathbb{t}_h$	2485.44
[61]	$\mathbb{t}_p + 2\mathbb{t}_m + 2\mathbb{t}_h + \mathbb{t}_e$	$2\mathbb{t}_p + \mathbb{t}_h$	1682.56
[40]	$2\mathbb{t}_c + \mathbb{t}_h + 2\mathbb{t}_m$	$2\mathbb{t}_c + 2\mathbb{t}_m$	4.8
[48]	$2\mathbb{t}_c + \mathbb{t}_h + 3\mathbb{t}_m$	$2\mathbb{t}_c + 2\mathbb{t}_m$	5.6
[62]	$\mathbb{t}_e + \mathbb{t}_h + 2\mathbb{t}_m + \mathbb{t}_i$	$\mathbb{t}_e + 2\mathbb{t}_h + 2\mathbb{t}_m + \mathbb{t}_p$	886.56
IBOOST	$2\mathbb{t}_c + \mathbb{t}_h + 2\mathbb{t}_m$	$2\mathbb{t}_c + \mathbb{t}_m$	4.424

Table 2: Computational cost assessment of A-IBOOST with other techniques

Techniques	Signing Stage (online and offline)	Verification Stage	Total (ms)
[58]	$\mathbb{t}_e + \mathbb{t}_h + 2\mathbb{t}_m$	$2\mathbb{t}_e + \mathbb{t}_h + \mathbb{t}_m$	578.44
[60]	$\mathbb{t}_p + 5\mathbb{t}_m + \mathbb{t}_h$	$2\mathbb{t}_p + \mathbb{t}_h$	1492.64
[61]	$2\mathbb{t}_p + 3\mathbb{t}_m + \mathbb{t}_h + \mathbb{t}_e$	$\mathbb{t}_p + \mathbb{t}_m + \mathbb{t}_h + \mathbb{t}_e$	1875.84
[42]	$\mathbb{t}_e + \mathbb{t}_h + 2\mathbb{t}_m$	$2\mathbb{t}_e + \mathbb{t}_h + \mathbb{t}_m$	579.04
[48]	$2\mathbb{t}_c + \mathbb{t}_h + 3\mathbb{t}_m$	$2\mathbb{t}_c + \mathbb{t}_h + 2\mathbb{t}_m$	5.92
A-IBOOST	$2\mathbb{t}_c + \mathbb{t}_h + 2\mathbb{t}_m$	$2\mathbb{t}_c + \mathbb{t}_h + \mathbb{t}_m$	4.744

The interaction value of the suggested IBOOST is by far the lowest, as shown by the analysis results in Fig. 3. With the proposed IBOOST, the tests often turn into runtime excels the rest of the related techniques. In the same vein, the interaction value of the suggested A-IBOOST is by far the lowest, as shown by the analysis results in Fig. 4. With the proposed A-IBOOST, the tests often turn into runtime excels the rest of the related techniques similar to the IBOOST.

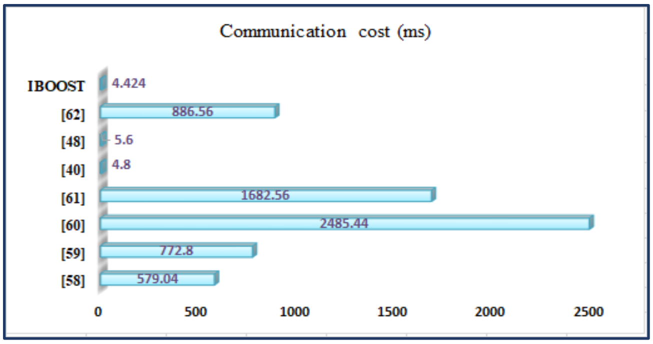

Fig. 3. Total communication cost (ms) analysis of IBOOST with other techniques

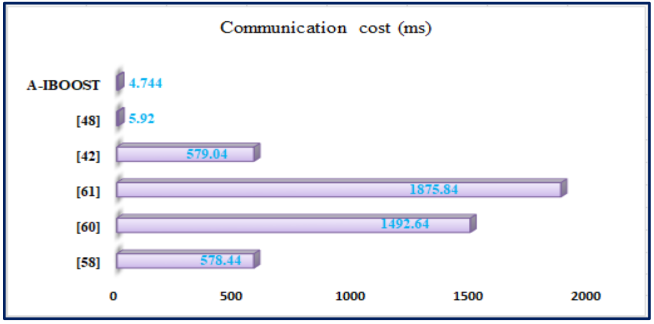

Fig. 4. Total communication cost (ms) analysis of A-IBOOST with other techniques.

VII. BASIC SETTING ON MASSIVE DEVICES IN 5G WIRELESS SENSOR NETWORKS

One prominent use case of 5G and beyond 5G wireless networks is massive access, called massive machine type communication (mMTC) or massive connectivity. Massive access finds practical applications in cellular WSNs and supports reliable and efficient communications for massive devices in 5G-WSNs. Also, wireless access is characterized by broad coverage and low power, requiring new concepts for designing emerging cellular networks. Furthermore, massive access enables reliable connection among distributed end devices and a centralized base station. Practically, massive wireless devices often share the same bandwidth resources using multiple access techniques owing to radio spectrum constraints. Generally, multiple access performance is evaluated by considering several factors comprising device requirements and channel conditions.

Generally, the 5G-WSNs have a simple architecture comprising of devices with limited energy storage capabilities. These devices cannot afford computationally intensive signal processing and need to be supported by lightweight applications for efficient operations. Therefore, the security architecture requires highly efficient lightweight techniques. For example, the proposed IBOOST uses fractional chaotic maps. In this technique, each sensor hub is equipped with the resources to sign messages using its private key. This procedure ensures that the messages get maximum security protection against adversarial attacks. As depicted in Fig. 5, the BS is configured to generate the parameters required for the scheme to be successfully embedded in the individual SN. In this scenario, the BS can inspect the signatures created by the SNs independently. In general, the 5G-WSN system assumes that the base station can perform computationally-intensive cryptographic operations efficiently, and its secret key is securely installed. However, the computational power, memory, and storage of the sensor nodes are vastly limited. Therefore, the proposed IBOOST deployed in 5G-WSN poses tough resistance to various security vulnerabilities.

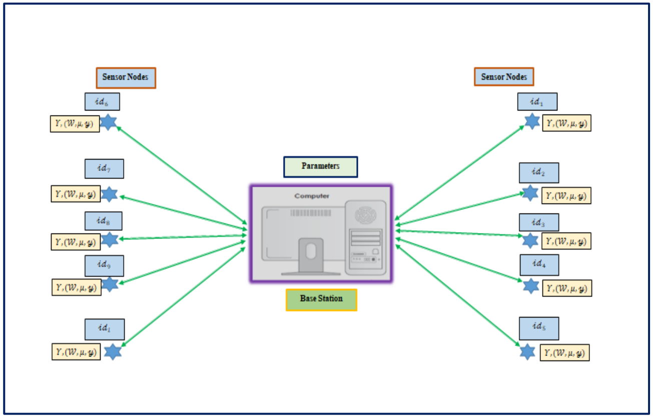

Fig.5. Overview of system implementation

Typically, Figure 6 shows a potential implementation of a 5G network architecture comprising three network domains; access network (AN), serving network (SN), and home network (HN). Mobile equipment such as user equipment (UEs) and massive devices (MDs), and several radio ANs are housed in the 5G AN domain. Whereas the radio ANs comprise 5G-NG radio ANs and non-3GPP ANs. These consist of gNBs referred to as the NR Node Bs and access points (APs). In our design, user equipment (UE), the newly defined radio access network for 5G referred to as NG-RAN, the non-3GPP access point and massive devices are interconnected in the 5G access network. The 5G serving network comprises the non-3GPP access interworking function (N3IWF), access and mobility management function (AMF)/security anchor function (SEAF)/session management function (SMF), and user plane function (UPF). Additionally, the 5G home network aggregates the AUSF and the unified data management (UDM). Thus, the key components of our design are the 5G access network, 5G serving network and 5G home network, all interconnected via various interfaces.

In order to establish mutual authentication between UEs or MDs and SNs, the legality of the access network must be ascertained. The confidentiality and integrity of the data transmitted over the air interface should be taken into consideration. Thus, the distinct session key needs to agree between each UE or MD in the network and the SN. The proposed setting helps to achieve identity privacy protection comprising identity anonymity and unlinkability. In this case, the identity of each UE/MD should not be made public in the ciphertext throughout the authentication process. This ensures that no attacker can associate a UE/MD with any public message harvested from the communication channel.

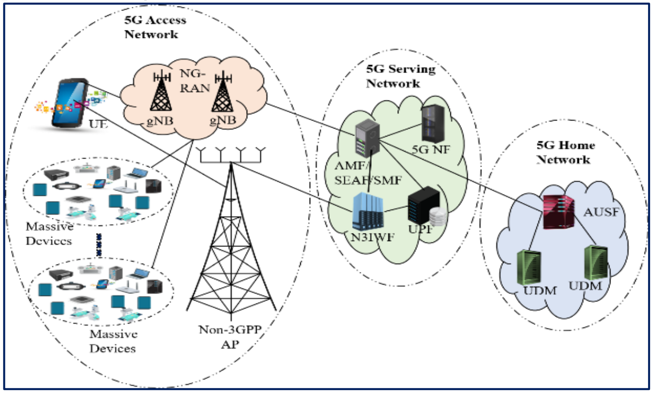

Figure 6. Practical 5G Network Architecture where the proposed IBOOST can be deployed.

The serving network domain facilitates access and communications for the participating UEs and massive devices to the data networks. The SN also empowers the AMF to provide desired functions required by the user and ease the control plane session management. In the SN, authentication functionalities are provided by the SEAF through the AMF. The AMF/SEAF can initiate communication with the AUSF when an MD or UE connects to the SN over the NG-RAN. This communication helps get the associated authentication vectors to aid mutual authentication with the MD or UE [17]. When the MD or UE connects to the SN via the non-3GPP AN, the MD or UE and the N3IWF housed in the SN use the Internet Key Exchange Protocol version 2 to establish the desirable security [17], [63]. In this case, the authentication server function (AUSF)/SEAF establishes connections with the AUSF and enables the EAP-5G protocol to achieve mutual authentication with the MD or UE. Other functional entities of the SN domain comprising SMF and UPF are well described in Figure 6. The UDM and the AUSF are configured to provide the required security for MDs or UEs. In our design, the AUSF handles authentication requests for the non-3GPP and 3GPP access. The resources used for security association setup are being protected from all forms of attacks in the UDM. Finally, the proposed architecture is robust, efficient, cost-effective, and suitable for deployment.

VIII. CONCLUSION

This article projected a lightweight, provably secure IBOOST based on fractional chaotic maps for massive devices in 5G wireless sensor networks. We introduced a system architecture tailored for 5G-WSNs. In our proposition, only the least possible operations are carried out in each procedure. It is worth noting that this security feature is highly desirable in WSN applications, enabling the hard-coding of offline data in the configuration stage to the sensor hub. Also, we present an aggregated system in line with the proposed IBOOST in a typical 5G-WSN setting. The IBOOST performs independently without attaching a certificate to the signature for verification and validation. Moreover, the technique does not require pairing operation in the signature generation and verification phases. Thus, the IBOOST demonstrates robust security in the random oracle model with high unforgeability under chosen message attacks. Additionally, the IBOOST scheme achieves multi-time use of offline storage at extremely low complexity. Therefore, the signer can reuse the offline pre-stored information in a polynomial time, depicting high superiority over most existing online/offline signature schemes that allow only a singular signature attempt. Besides, the new scheme enables the pre-registration process with a secret key, and no secret key is required in the offline stage. The performance analyses of the IBOOST and the enhanced IBOOST (A-IBOOST) techniques show impressive results. The proposed technique gives the lowest computational cost in comparison with several contending techniques. Finally, formal and informal security analyses of the projected scheme demonstrate that our technique can withstand all well-known attacks with remarkable security features at the lowest communication cost. Future work would focus on an efficient, provably secure, lightweight subtree-based online/offline signature procedure for massive devices in 5G WSNs using the concept of IBOOST in an experimental setting.

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers of IEEE Access 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. 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.

REFERENCES

[1] A. Gupta and R. K. Jha, “A Survey of 5G Network: Architecture and Emerging Technologies,” *IEEE Access*, vol. 3, pp. 1206–1232, 2015, doi: 10.1109/ACCESS.2015.2461602.

[2] M. B. H. Weiss, K. Werbach, D. C. Sicker, and C. E. C. Bastidas, “On the application of blockchains to spectrum management,” *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 2, pp. 193–205, 2019, doi: 10.1109/TCCN.2019.2914052.

[3] E. Calvanese Strinati *et al.*, “6G: The Next Frontier: From Holographic Messaging to Artificial Intelligence Using Subterahertz and Visible Light Communication,” *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 42–58, 2019, doi: 10.1109/MVT.2019.2921162.

[4] V. Souza, R. Cruz, W. Silva, S. Lins, and V. Lucena, “A Digital Twin Architecture Based on the Industrial Internet of Things Technologies,” in *2019 IEEE International Conference on Consumer Electronics, ICCE 2019*, 2019, pp. 1–2, doi: 10.1109/ICCE.2019.8662081.

[5] R. Fotohi, S. Firoozi Bari, and M. Yusefi, “Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol,” *Int. J. Commun. Syst.*, vol. 33, no. 4, pp. 1–25, 2020, doi: 10.1002/dac.4234.

[6] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, “Adaptive protocols for information dissemination in wireless sensor networks,” *Proc. 5th Annu. ACM/IEEE Int. Conf. Mob. Comput. Netw.*, pp. 174–185, 1999, doi: 10.1145/313451.313529.

[7] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 1617–1655, 2016, doi: 10.1109/COMST.2016.2532458.

[8] J. Cao *et al.*, "A Survey on Security Aspects for 3GPP 5G Networks," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 170–195, 2020, doi: 10.1109/COMST.2019.2951818.

[9] A. L. Imoize, O. Adedeji, N. Tandiya, and S. Shetty, "6G Enabled Smart Infrastructure for Sustainable Society: Opportunities, Challenges, and Research Roadmap," *Sensors*, vol. 21, no. 5, 1709, pp. 1–58, 2021, doi: 10.3390/s21051709.

[10] J. Cao, M. Ma, and H. Li, "GBAAM: group-based access authentication for MTC in LTE networks," *Secur. Commun. Networks*, vol. 8, no. April, pp. 3282–3299, 2015, doi: 10.1002/sec.1252.

[11] C. Meshram *et al.*, "A Provably Secure Lightweight Subtree-Based Short Signature Scheme with Fuzzy User Data Sharing for Human-Centered IoT," *IEEE Access*, vol. 9, pp. 3649–3659, 2021, doi: 10.1109/ACCESS.2020.3046367.

[12] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future Intelligent and Secure Vehicular Network Toward 6G: Machine-Learning Approaches," *Proc. IEEE*, vol. 108, no. 2, pp. 292–307, 2020, doi: 10.1109/JPROC.2019.2954595.

[13] R. Wdowik and R. M. C. Ratnayake, "Collaborative Technological Process Planning with 5G Mobile Networks and Digital Tools: Manufacturing Environments' Perspective," in *2019 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 2019, pp. 349–353, doi: 10.1109/IEEM44572.2019.8978721.

[14] M. A. Khan and J. Kim, "Toward developing efficient Conv-AE-based intrusion detection system using heterogeneous dataset," *Electron.*, vol. 9, no. 11, pp. 1–17, 2020, doi: 10.3390/electronics9111771.

[15] M. Lavanya and V. Natarajan, "LWDSA: lightweight digital signature algorithm for wireless sensor networks," *Sadhana - Acad. Proc. Eng. Sci.*, vol. 42, no. 10, pp. 1629–1643, 2017, doi: 10.1007/s12046-017-0718-5.

[16] C. Meshram, R. W. Ibrahim, A. J. Obaid, S. G. Meshram, A. Meshram, and A. M. A. El-Latif, "Fractional chaotic maps based short signature scheme under human-centered IoT environments," *J. Adv. Res.*, no. xxxx, 2020, doi: 10.1016/j.jare.2020.08.015.

[17] J. Cao, Z. Yan, R. Ma, Y. Zhang, Y. Fu, and H. Li, "LSAA: A lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5329–5344, 2020, doi: 10.1109/JIOT.2020.2976740.

[18] D. Djenouri, L. Khelladi, and N. Badache, "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks," *IEEE Commun. Surv. Tutorials*, vol. 7, no. 4, pp. 2–28, 2005.

[19] S. Ifzarne, I. Hafidi, and N. Idrissi, "Secure Data Collection for Wireless Sensor Network," in *Emerging Trends in ICT for Sustainable Development*, 2021, pp. 241–248.

[20] S. Even, O. Goldreich, and S. Micali, "On-line/offline digital signatures," *Proc. CRYPTO 1989, Lect. Notes Comput. Sci. New York, NY, USA Springer*, vol. 2442, pp. 263–277, 1989.

[21] A. Shamir and Y. Tauman, "Improved Online/Offline Signature Schemes," in *Advances in Cryptology --- CRYPTO 2001*, 2001, pp. 355–367.

[22] Y. Gao, P. Zeng, K. K. R. Choo, and F. Song, "An improved online/offline identity-based signature scheme for WSNs," *Int. J. Netw. Secur.*, vol. 18, no. 6, pp. 1143–1151, 2016.

[23] K. Kurosawa and K. Schmidt-Samoa, "New Online/Offline Signature Schemes Without Random Oracles," in *Public Key Cryptography - PKC 2006*, 2006, pp. 330–346.

[24] A. C. Yao and Y. Zhao, "Online/Offline Signatures for Low-Power Devices," *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 2, pp. 283–294, 2013, doi: 10.1109/TIFS.2012.2232653.

[25] M. Zheng, S.-J. Yang, W. Wu, J. Shao, and X. Huang, "A New Design of Online/Offline Signatures Based on Lattice," in *Information Security Practice and Experience*, 2018, pp. 198–212.

[26] D. Boneh and X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups," *J. Cryptol.*, vol. 21, no. 2, pp. 149–177, 2008, doi: 10.1007/s00145-007-9005-7.

[27] M. Joye, "An Efficient On-Line/Off-Line Signature Scheme without Random Oracles," in *Cryptology and Network Security*, 2008, pp. 98–107.

[28] F. Hess, "Efficient Identity Based Signature Schemes Based on Pairings," in *Selected Areas in Cryptography*, 2003, pp. 310–324.

[29] D. Galindo and F. D. Garcia, "A Schnorr-Like Lightweight Identity-Based Signature Scheme," in *Progress in Cryptology -- AFRICACRYPT 2009*, 2009, pp. 135–148.

[30] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," in *Information Security and Privacy*, 2006, pp. 99–110.

[31] F. Li, M. Shirase, and T. Takagi, "On the Security of Online/Offline Signatures and Multisignatures from ACISP'06," in *Cryptology and Network Security*, 2008, pp. 108–119.

[32] N. Tahat and M. S. Hijazi, "A new digital signature scheme based on chaotic maps and quadratic residue problems," *Appl. Math. Inf. Sci.*, vol. 13, no. 1, pp. 115–120, 2019, doi: 10.18576/amis/130115.

[33] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004, doi: https://doi.org/10.1016/j.chaos.2003.12.022.

[34] S. Deng, Y. Li, and D. Xiao, "Analysis and improvement of a chaos-based Hash function construction," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 5, pp. 1338–1347, 2010, doi: https://doi.org/10.1016/j.cnsns.2009.05.065.

[35] Y. Wang, K.-W. Wong, X. Liao, and T. Xiang, "A block cipher with dynamic S-boxes based on tent map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 7, pp. 3089–3099, 2009, doi: https://doi.org/10.1016/j.cnsns.2008.12.005.

[36] C.-C. Lee and C.-W. Hsu, "A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps," *Nonlinear Dyn.*, vol. 71, no. 1, pp. 201–211, 2013, doi: 10.1007/s11071-012-0652-3.

[37] J. Kar, K. Naik, and T. Abdelkader, "A Secure and Lightweight Protocol for Message Authentication in Wireless Sensor Networks," *IEEE Syst. J.*, pp. 1–12, 2020, doi: 10.1109/jsyst.2020.3015424.

[38] C.-T. Li, C.-C. Lee, C.-Y. Weng, and S.-J. Chen, "A Secure Dynamic Identity and Chaotic Maps Based User Authentication and Key Agreement Scheme for e-Healthcare Systems," *J. Med. Syst.*, vol. 40, no. 11, p. 233, 2016, doi: 10.1007/s10916-016-0586-2.

[39] K. Chain and W.-C. Kuo, "A new digital signature scheme based on chaotic maps," *Nonlinear Dyn.*, vol. 74, no. 4, pp. 1003–1012, 2013, doi: 10.1007/s11071-013-1018-1.

[40] C. Meshram, C.-T. Li, and S. G. Meshram, "An efficient online/offline ID-based short signature procedure using extended chaotic maps," *Soft Comput.*, vol. 23, no. 3, pp. 747–753, 2019, doi: 10.1007/s00500-018-3112-2.

[41] 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 Comput. Sci.*, vol. 93, pp. 847–853, 2016, doi: https://doi.org/10.1016/j.procs.2016.07.253.

[42] 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, doi: 10.1049/iet-net.2018.0019.

[43] Y. Gao, P. Zeng, and K.-K. R. Choo, "Multi-sender Broadcast Authentication in Wireless Sensor Networks," in *2014 Tenth International Conference on Computational Intelligence and Security*, 2014, pp. 633–637, doi: 10.1109/CIS.2014.147.

[44] C. H. Ling, C. C. Lee, C. C. Yang, and M. S. Hwang, "A secure and efficient one-time password authentication scheme for WSN," *Int. J. Netw. Secur.*, vol. 19, no. 2, pp. 177–181, 2017, doi: 10.6633/IJNS.201703.19(2).02.

[45] P. Kumar, S. Kumari, V. Sharma, X. Li, A. K. Sangaiah, and S. K. H. Islam, "Secure CLS and CL-AS schemes designed for VANETs," *J. Supercomput.*, vol. 75, no. 6, pp. 3076–3098, 2019, doi: 10.1007/s11227-018-2312-y.

[46] P. Kumar, S. Kumari, V. Sharma, A. K. Sangaiah, J. Wei, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," *Sustain. Comput. Informatics Syst.*, vol. 18, pp. 80–89, 2018, doi: https://doi.org/10.1016/j.suscom.2017.09.002.

[47] C. Meshram, C. C. Lee, A. S. Ranadive, C. T. Li, S. G. Meshram, and J. V. Tembhurne, "A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing," *Int. J. Commun. Syst.*, vol. 33, no. 7, pp. 1–15, 2020, doi: 10.1002/dac.4307.

[48] C. Meshram, C. C. Lee, S. G. Meshram, and A. Meshram, "OOS-SSS: An Efficient Online/Offline Subtree-Based Short Signature Scheme Using Chebyshev Chaotic Maps for Wireless Sensor Network," *IEEE Access*, vol. 8, pp. 80063–80073, 2020, doi: 10.1109/ACCESS.2020.2991348.

[49] Bergamo, P., Arco, P., Santis, A., Kocarev, L.: Security of public key cryptosystems based on Chebyshev polynomials, *IEEE Trans. Circ. Syst. –* I 52, 1382–1393 (2005).

[50] Zhang, L.: Cryptanalysis of the public key encryption based on multiple chaotic systems, *Chaos Solit. Fract.*, vol. 37 (3), pp. 669–674 (2008).

[51] Meshram, C., Lee, CC., Meshram, SG., Li, CT.: An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem. *Soft Computing*, vol. 23(16), pp. 6937-6946 (2019).

[52] Meshram, C., Ibrahim, RW., Deng, L., Shende, SW., Meshram, SG., Barve, SK.: A Robust Smart Card and Remote User Password-based Authentication Protocol using Extended Chaotic-Maps under Smart Cities Environment. *Soft Computing*, (2021) https://doi.org/10.1007/s00500-021-05929-5.

[53] Meshram, C., Obaidat, MS., Tembhurne, JV., Shende, SW., Kalare, KW., Meshram, S. G.: A Lightweight Provably Secure Digital Short Signature Technique using Extended Chaotic Maps for Human-Centered IoT Systems. *IEEE Systems Journal*, (2021) DOI 10.1109/JSYST.2020.3043358.

[54] C. Meshram, R. W. Ibrahim, M. S. Obaidat, B. Sadoun, S. G. Meshram, J.V. Tembhurne, *"*An Effective Mobile-Healthcare Emerging Emergency

Medical System using Conformable Chaotic Maps*" Soft Computing*, (2021), vol. 25, pp. 8905–8920

[55] Han, S., Chang, E.: Chaotic map based key agreement with/out clock synchronization. Choas Soliton and Fractals. 39(3),1283–1289 (2009).

[56] Yang, XJ., Baleanu, D., Srivastava, HM.: Local fractional integral transforms and their applications. Academic Press, (2015).

[57] M. Bellare, C. Namprempre, G. Neven, "Security proofs for identity based identification and signature schemes", *Journal of Cryptology*, vol. 22, pp. 1–61, 2009.

[58] Joseph K. Liu, Joonsang Baek· Jianying Zhou, Yanjiang Yang, Jun Wen Wong, Efficient online/offline identity-based signature for wireless sensor network, *Int. J. Inf. Secur*. (2010), vol. 9, pp. 287–296.

[59] Zhiwei Wang, Wei Chen, An ID-based online/offline signature scheme without random oracles for wireless sensor networks, *Pers Ubiquit Comput* (2013), vol. 17, pp. 837–841.

[60] J. Kar, "Provably Secure Online/Off-line Identity-based Signature Scheme for Wireless Sensor Network", *International Journal of Network Security*, vol. 16(1), pp. 29-39, 2014.

[61] Y. Gao, P. Zeng, K. K. R. Choo, F. Song, "An Improved Online/Offline Identity-based Signature Scheme for WSNs", *International Journal of Network Security*, vol. 18 (6), pp. 1143-1151, 2016.

[62] Jianchang Lai, Xinyi Huang, Debiao He, Wei Wu, Provably Secure Online/Offline Identity-Based Signature Scheme Based on SM9, *The Computer Journal*, 2021, doi: 10.1093/comjnl/bxab009

[63] S. H. Islam, "Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps." *Information Sciences*, 2015, *312*, pp.104-130, doi: 10.1016/j.ins.2015.03.050

[64] D. He, N. Kumar, J. H. Lee, R. S. Sherratt, "Enhanced three factor security protocol for consumer USB mass storage devices," *IEEE Trans. Consum. Electron.*, vol. 60, no. 1, pp. 30–37, 2014.