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

CHANDRASHEKHAR MESHRAM1, AGBOTINAME LUCKY IMOIZE2,3, (Member, IEEE), AZEDDINE ELHASSOUNY4, AMER ALJAEDI5, ADEL R. ALHARBI4,5, AND SAJJAD SHAUKAT JAMAL6

1Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, Chhindwara University, Betul, Madhya Pradesh 460001, India
2Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria
3Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University Bochum, 44801 Bochum, Germany
4ENSIAS, Mohammed V University in Rabat, Rabat 10000, Morocco
5College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
6Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia

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

This work was supported by the Deanship of Scientific Research at King Khalid University through the Research Groups Program under Grant R. G. P. 1/72/42. The work of Agbotiname Lucky Imoize was 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.

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 $10^8$ 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 a 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 Kurosawa 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 have 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] used 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.

A. 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 Seyerth, 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.

B. 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 $T_n (\nu)$ is an $n$-degree polynomial in the variant $\nu$. Allow $\nu \in [-1, 1]$ to be the edition and $n$ to be a large integer. CSP stated the following in general [49]:

$$T_n (\nu) = \cos (n \arccos (\nu)) , \quad T_0 (\nu) = 1 , \quad T_1 (\nu) = \nu$$
The Chebyshev polynomial’s recurrence relation is defined as
\[ T_n(v) = 2T_{n-1}(v) - T_{n-2}(v); \quad n \geq 2 \]

The functional \( \arccos(v) \) and \( \cos(v) \) represented as \( \arccos : [-1, 1] \rightarrow [0, \pi] \) and \( \cos : R \rightarrow [-1, 1] \) in this case.

**B. PROPERTIES OF CHAOTIC MAPS**

The following are two interesting properties of Chebyshev polynomials [49]–[52]:

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

**Definition 3 (Semi-Group Properties):** The semi-group property of the Chebyshev polynomial (CP) \( T_n(v) \) is demarcated as follows:
\[ T_r(T_l(v)) = \cos(\tau \cos^{-1}(\cos(l \cos^{-1}(v)))) = \cos(\tau \cos^{-1}(v)) = T_r(T_l(v)), \]
where \( l \) and \( \tau \) are (+) integers and \( v \in [-1, 1] \).

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:
\[ T_n(v) = 2T_{n-1}(v) - T_{n-2}(v) \mod q_1; \quad n \geq 2 \]
where \( v \in (-\infty, +\infty) \) and \( q_1 \) is a large and safe prime. Thus, the property follows:
\[ T_r(T_l(v)) \mod q_1 = T_r(T_l(v)) \mod q_1 \equiv T_r(T_l(v)) \mod q_1 \]

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

**C. COMPUTATIONAL PROBLEMS**

In this segment, some computational issues based on the CPs are described leveraging the propositions [16], [38], [51]–[55]:

**Definition 4 (Chaotic Map-Based Discrete Logarithm (CMDL) Problem):** Given a random tuple \(< y, v >\), any polynomial time-bounded algorithm that finds the integer \( \tau \) where \( y = T_{\tau}(v) \mod q_1 \) is infeasible.

**Definition 5 (Chaotic Map-Based Diffie-Hellman (CMDH) Problem):** For a given random tuple \(< v, T_{\tau}(v), T_{\tau}(y) >\), any polynomial time-bounded algorithm that tries to find the value \( T_{\tau}(v) \mod q_1 \) 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 \( \xi^\delta \) is defined by the formal expression for an arbitrary fractional-order \( \delta \in [0, 1] \):
\[ \xi^\delta \psi(y) = \Delta^\delta(\psi(y) - \psi(y_0)) = \Gamma(\delta + 1) (\psi(y) - \psi(y_0)) \]
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)
\[ I^\delta \psi(y) = \frac{1}{\Gamma(\delta + 1)} \int_a^b \psi(y) dy, \quad a \leq y \leq b. \]

Thus, we get the following construction by using the FC definition to generalize the polynomial \( T_n(v) \):
\[ I^\delta T_n(v) := T_{\delta n}(v) = \frac{(2)^\delta}{\Gamma(\delta + 1)} T_n(v), \]

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

**FIGURE 1. 3D-FCP when \( \delta = 0, 1/2 \) and 3/4 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.,
\[ T_{\delta n}(v) = \frac{(2)^\delta}{\Gamma(\delta + 1)} (2nT_{n-1}(v) - T_{n-2}(v)) \mod q_1. \]

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 \((-\infty, \infty)\) [16], the semi-group properties locks, i.e.,
\[ T_{\delta \tau} (T_{\delta n}(v) \mod q_1) = T_{\delta n}(T_{\delta \tau}(v) \mod q_1) \equiv T_{\delta \tau}(v) \mod q_1. \]

VOLUME 9, 2021
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 \( \rho_1 \) and a global parameter \( \vartheta \in \mathcal{G} \), where \( \mathcal{G} \) is a multiplicative group.

ii. Select an arbitrary \( \ell \in \mathbb{Z}_{\rho_1}^* \).

iii. Select an arbitrary rational number \( \delta \in [0, 1] \).

iv. Calculate \( \beta = \mathcal{T}_\delta^\vartheta (\vartheta) \pmod{\rho_1} \).

v. Choose \( \mathcal{H} \) hash functions: \( \mathcal{H} : \{0, 1\}^\infty \rightarrow \mathbb{Z}_{\rho_1}^* \).

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

B. EXTRACTION

The secret key is produced using a client’s identity \( \mathcal{id} \) by performing the following stages:

i. Select at random \( \varpi \in \mathbb{Z}_{\rho_1}^* \).

ii. Compute \( \mathcal{\mu} = \mathcal{T}_\vartheta^\varpi (\varpi) \pmod{\rho_1} \) and \( \mathcal{b} = \mathcal{H}(\mathcal{id}, \mathcal{\mu}) \).

iii. Compute \( \mathcal{\pi} = \varpi \cdot \mathcal{b} \pmod{\rho_1} \).

The pair \( \{\mathcal{\mu}, \mathcal{\pi}\} \) is the client’s secret key.

C. OFFLINE SIGNING

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

i. Compute \( \mathcal{W}' = \mathcal{T}_{\ell_1}^\vartheta (\vartheta) \pmod{\rho_1} \), for \( \ell_1 \in [0, |\rho_1| - 1] \).

D. ONLINE SIGNING

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

i. Pick an arbitrarily \( \ell \in \mathbb{Z}_{\rho_1}^* \), so that \( \ell_1 \) is the \( \ell \)th bit of \( \ell \).

ii. Compute \( \mathcal{W} = \prod_{j=1}^{\rho_1} \mathcal{W}'_{\ell_1} \pmod{\rho_1} \) and \( \eta = \mathcal{H}(\mathcal{W}, \mathcal{\mu}, M) \).

iii. Compute \( \mathcal{Y} = \mathcal{\pi} \cdot \mathcal{\pi} \pmod{\rho_1} \) as well as \( \gamma = \mathcal{T}_\vartheta^\mathcal{\pi} (\vartheta) \pmod{\rho_1} \).

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

E. VERIFICATION

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

i. Compute \( \mathcal{Y}' = \mathcal{W}_1 \mathcal{T}_\vartheta^\mathcal{\pi} (\mathcal{\mu}) \mathcal{T}_\vartheta^\mathcal{\pi} (\mathcal{\beta}) \pmod{\rho_1} \).

ii. If \( \mathcal{Y} = \mathcal{Y}' \), the signature is accepted, or else this is not.

1) CORRECTNESS

The correctly generated private key must meet the following criteria:

\[ \mathcal{T}_\vartheta^\mathcal{\pi} (\mathcal{\mu}) \mathcal{T}_\vartheta^\mathcal{\pi} (\mathcal{\beta}) \pmod{\rho_1} = \mathcal{\mu} \mathcal{T}_\vartheta^\mathcal{\pi} (\mathcal{\beta}) \pmod{\rho_1} \]  \hspace{1cm} (3)

For the reliability of an algorithm, note that \( \mathcal{W} = \mathcal{T}_\ell^\vartheta (\vartheta) \pmod{\rho_1} \). We have:

\[ \mathcal{W} \mathcal{T}_\vartheta^\mathcal{\pi} (\mathcal{\mu}) \mathcal{T}_\vartheta^\mathcal{\pi} (\mathcal{\beta}) \pmod{\rho_1} \]

IV. SECURITY EXAMINATIONS AND DISCUSSIONS

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

Theorem 1: The projected IBOOST is \((\mathcal{E}, t, \mathcal{Q}_\mathcal{E}, \mathcal{Q}_s, \mathcal{H}_E)\) secure in the knowledge of unforgeability of IBS technique under the chosen message attack (UF-IBS-CMA) in the ROM, implementing the \((\mathcal{E}', t')-\) FCM hypothesis in \( \mathcal{G} \), where:

\[ \mathcal{E}' \approx \left(1 - \left(\mathcal{Q}_\mathcal{E} + \mathcal{Q}_s\right)\right) \left(\frac{\rho_1 - \rho_1 \mathcal{Q}_\mathcal{E}}{\rho_1} \right) \]  \hspace{1cm} (5)

\[ \mathcal{E}' \approx t + \mathcal{O}(\mathcal{Q}_s + \mathcal{H}_E) \]  \hspace{1cm} (6)

and \( \mathcal{Q}_s \) — signing queries, \( \mathcal{Q}_E \) — extraction queries are the amount of chaos and \( \mathcal{Q}_\mathcal{E} \) — hashing queries. Here \( \tau \) is the time for an operation of exponentiation. Now \( \tau \) 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 \( \mathcal{B} \), which is dependent on the use of \( \mathcal{F} \). The algorithm \( \mathcal{B} \) comes with a multiplicative group \( \mathcal{G} \) that has a comprehensive \( \vartheta \) parameter and an exponent \( \kappa \in \mathcal{G} \) that is checked to find \( \nu \in \mathbb{Z}_{\rho_1}^* \) in a method that \( \kappa = \mathcal{T}_\vartheta^\nu (\vartheta) \pmod{\rho_1} \). The method of [57] is used.

A. SETUP

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

B. EXTRACTION ORACLE QUERIES

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

\[ \mathcal{\mu} = \mathcal{T}_s^\vartheta (\vartheta) \mathcal{T}_\delta^\vartheta (\beta) \pmod{\rho_1} \], \hspace{1cm} \( \kappa \leftarrow 1 \), \hspace{1cm} \mathcal{H}(\mathcal{\mu}, \mathcal{id}) \leftarrow s \]  \hspace{1cm} (7)

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

C. SIGNING ORACLE QUERIES

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

**D. OUTPUT CALCULATION**

Finally, \( T \) generates a bogus signature \( \psi_i^* = (\mathcal{W}^*, \mu^*, \psi_i^s) \) on \( M^* \) and \( \mathcal{I}^d \). The algorithm \( B \) converges \( T \) in the sense that it does a \( \mathcal{H}(\mathcal{W}^*, \mu^*, \mathcal{M}^*) \) and returns a different value to the acceptable. For \( T \) generates a few other signatures \( \psi_i^* = (\mathcal{W}^*, \mu^*, \psi_i^s) \). Algorithm \( B \) re-hashes the data and returns \( \psi_i^* = (\mathcal{W}^*, \mu^*, \psi_i^s) \). It is worth 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 \( \eta_1, \eta_2, \eta_3 \).

We now project FCM of \( \mu, \beta, \) and \( \mathcal{W} \) for each \( l, \ell, \omega \in \mathbb{Z}_{p_1} \), respectively. i.e., \( \mu = \mathcal{T}_\mathcal{W}^{\omega^*}(\theta)(\text{mod } p_1) \), \( \beta = \mathcal{T}_{\mathcal{W}^*}^{\omega^*}(\theta)(\text{mod } p_1) \) and \( \mathcal{W} = \mathcal{T}_\mathcal{W}^{\omega^*}(\theta)(\text{mod } p_1) \). From Eq. (4), we have:

\[
\psi_i^s = \ell \ast \omega \eta_i \ast \mathcal{W}_{j}(\mu^*, \mathcal{I}^d)(\text{mod } p_1) \quad \text{for } j = 1, 2, 3
\]

(8)

In these mathematical examinations, only \( l, \ell, \) and \( \omega \) are foreign to \( B \). The algorithm \( B \) computes for \( j = 1, 2, 3 \) and produces \( l \) as the solution of the FCM for overhead linear autonomous mathematical proclamations.

**E. REDUCTION COST INSPECTION**

The random oracle’s consignment \( \mathcal{H}(\mathcal{W}^*, \mu^*, \mathcal{M}^*) \) is irregular in the simulation process with extraction oracle failures, implying a combined probability of at least \( \frac{d \rho}{\rho_1} \). As a result, the simulation technique is effective \( (d^*+d^E) \) times (as a result of the fact that if \( \mathcal{I}^d \) is not demanded in the extraction oracle, \( \mathcal{H}(\mathcal{W}^*, \mu^*, \mathcal{M}^*) \) can also be asked in the signature oracle), with the probability being:

\[
\left(1 - \frac{d^* + d^E}{\rho_1}\right) \leq \left(1 - \frac{d^E}{\rho_1}\right)
\]

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. \( B \) suppositions it appropriately as the point of rewind, at least with a \( \left(\frac{1}{\rho_1}\right) \) probability. Overall, the probability of success is:

\[
\left(1 - \frac{d^E + d^*}{\rho_1}\right) \left(\frac{\rho_1}{\rho_1 d^E}\right) \epsilon
\]

The exponentiations done in the signing and extraction procedures determine the temporal complexity of algorithm \( B \), which is identical to:

\[
e + O(d^* + d^E)\tau
\]

\( \ell \) 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 \( l \) separate messages simultaneously. In this case, the aggregate signature can have the same length as a single message’s signature or \( l \) 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 \( \rho_1 \) and a global parameter \( \theta \in \mathcal{G} \), where \( \mathcal{G} \) is a multiplicative group.

ii. Select an arbitrary \( l \in \mathbb{Z}_{p_1} \).

iii. Select an arbitrary rational number \( \delta \in [0, 1] \).

iv. Calculate \( \beta = \mathcal{T}_\mathcal{W}^{\omega^*}(\theta)(\text{mod } p_1) \).

v. Choose \( \mathcal{H} \) chaotic hash functions: \( \mathcal{H} : [0, 1]^\infty \rightarrow \mathbb{Z}_{p_1} \).

The master public and private keys are given by \( \{\rho_1, \theta, \mathcal{H}, \beta\} \) and \( (l, \delta) \), respectively.

**B. EXTRACT**

The private key is produced using a client’s identity \( \mathcal{I}^d \) by implementing the subsequent steps:

i. Pick at random \( \omega \in \mathbb{Z}_{p_1} \).

ii. Computes \( \mu = \mathcal{T}_\mathcal{W}^{\omega^*}(\theta)(\text{mod } p_1) \) and \( \mathcal{W} = \mathcal{T}_\mathcal{W}^{\omega^*}(\theta)(\text{mod } p_1) \).

iii. Compute \( \pi = \omega \ast \mathcal{H}(\text{mod } p_1) \).

The client’s secret key is the pair \( (\mu, \pi) \).

**C. OFFLINE SIGNING**

The signer executes the subsequent estimation:

1) Compute \( \mathcal{W}^*_j = \mathcal{T}_\mathcal{W}^{\omega^*}(\theta)(\text{mod } p_1), \) for \( j \in [0, |\rho_1| - 1] \).

**D. ONLINE SIGNING**

To register a message \( M \in (-\infty, \infty) \) using \( (\mu, \pi) \), the signer follows the procedures below:

i. Select \( \ell^1 \in \mathbb{Z}_{p_1} \) at random where \( \ell^i \) is the \( i \)th bit of \( \ell^1 \).

ii. Define \( \ell^i \subseteq \{1, \ldots, |\rho_1|\} \) as the set of indices that makes \( \ell^i \) [1] = 1.

iii. Computes \( \mathcal{W}^*_1 = \prod_{i=1}^{\ell^1} \mathcal{W}^*_{i-1} \) and \( \eta_j = \mathcal{H}(\mathcal{W}^*, \mu^*, \mathcal{M}^*) \).

iv. Computes \( \eta_j = \ell^{\gamma} \ast \eta_j \ast (\text{mod } p_1) \) and \( \mathcal{Y} = \mathcal{T}^{\gamma^*}(\theta)(\text{mod } p_1) \).

The aggregate signature is given by \( \mathcal{E} = (\mathcal{W}^*_1, \mu^*, \mathcal{Y}) \).

**E. VERIFICATION**

The verifier executes these steps to validate a signature \( \mathcal{E} = (\mathcal{W}^*_1, \mu^*, \mathcal{Y}) \) on the \( \mathcal{M}^*_1 \) and \( \mathcal{I}^d \) for \( j = 1, \ldots, n \):

i. Computes \( \eta_j = \mathcal{H}(\mathcal{W}^*_1, \mu^*, \mathcal{M}^*_1) \) and \( \mathcal{Y}' = \left(\prod_{i=1}^{n} \mathcal{W}^*_i\right) \mathcal{T}^{\gamma^*}(\mu^*)(\text{mod } p_1), \) where \( \mathcal{Q} = \sum_{i=1}^{n} \eta_j \).
ii. The signature is allowed if $\gamma = \gamma'$; else, the signature is denied.

**F. CORRECTNESS**

The correctly generated private key must meet the following criteria:

$$\mathcal{W}_i = \mathcal{T}_i^{\delta} (\theta) \pmod{\varphi_1} \text{ for } i \in [1, \ldots, n].$$

We have

$$\gamma' = \left( \prod_{i=1}^{n} \mathcal{W}_i \right) \mathcal{T}_i^{\delta} (\mu) \mathcal{T}_i^{\delta} (\beta) \pmod{\varphi_1}$$

$$= \left( \prod_{i=1}^{n} \mathcal{W}_i \right) \mathcal{T}_i^{\delta} (\theta) \mathcal{T}_i^{\delta} (\varphi_1) \pmod{\varphi_1}$$

$$= \mathcal{T}_i^{\delta} (\theta) \mathcal{T}_i^{\delta} (\varphi_1) \pmod{\varphi_1}$$

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

**TABLE 1.** Computational cost assessment of IBOOST with other techniques.

| Techniques | Signing Stage (online and offline) | Verification Stage | Total (ms) |
|------------|-----------------------------------|-------------------|------------|
| [58]       | $t_c + t_h + t_m$                 | $2t_c + t_h$      | 579.04     |
| [59]       | $2t_c + 4t_m$                     | $2t_c + 2t_m$     | 772.80     |
| [60]       | $t_p + 6t_m + t_h$                | $4t_p + 2t_h$     | 2485.44    |
| [22]       | $t_p + 2t_m + 2t_h$               | $2t_p + t_h$      | 1682.56    |
| [40]       | $2t_c + t_h + 2t_m$               | $2t_c + 2t_m$     | 4.8        |
| [48]       | $2t_c + t_h + 3t_m$               | $2t_c + 2t_m$     | 5.6        |
| [61]       | $t_c + t_h + 2t_m$                | $2t_c + t_h + t_p$| 886.56     |
| IBOOST     | $2t_c + t_h + 2t_m$               | $2t_c + t_m$      | 4.424      |

The functionality analysis of the proposed IBOOST is shown in Table 1 and compares computational costs in Fig. 2 with other related protocols [22], [58]–[60], [40], [48], and [61]. 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], [22], [48], and [42], respectively. Based on the results of the experiments in [51]–[53], we reach the subsequent computation time figures with unit hashing time: $t_c = 600\mu h$, $t_m = 2.5t_h$, $t_i = 7.5t_h$, $t_p = 1550t_h$ and $t_h \approx t_c$. In this method, we have the following order of computing complexity: $t_h \approx t_c \approx t_m \approx t_i < t_p$. In addition, in this area, we give the results of our evaluation. The findings averaged 300 randomized simulation runs on a four-core 3.2 GHz computer with 8 GB memory [63]. Our simulator, which was created in MATLAB, was used to conduct the experiments. A one-way hash function takes 0.32 milliseconds (ms) [63], [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 [22], [58]–[60], [40], [48], [61] 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 4.424 ms, respectively. The total communication costs of the works of [58], [60], [22], [48], [42] and the A-IBOOST are 578.44 ms, 1492.64, 1875.84 ms, 5.92 ms, 579.04 ms, and 4.424 ms, respectively.

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

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

**VI. PERFORMANCE ANALYSIS**

In this section, we compare our new IBOOST with seven other techniques proposed by [22], [58]–[60], [40], [48], and [61]. Additionally, we compare our extended IBOOST technique referred to as A-IBOOST with five other related techniques proposed by [58], [60], [22], [48], and [42], respectively, to demonstrate the efficiency of our new design. The notations used to present our evaluation results include $t_m$, $t_i$, $t_c$, $t_p$, and $t_h$. We denote the execution time required for modular multiplication, modular inverse operation, group modular exponentiation, chaotic map operation, bilinear pairing 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], [22], [40], [48], and [61], respectively. Also, we contrast our new A-IBOOST with the works of [58], [60], [22], [48], and [42], respectively, in a similar fashion. The length of the signature in the proposed IBOOST and A-IBOOST is 480 (bit) each.

**FIGURE 2.** Comparison among A-IBOOST and non-A-IBOOST variants.
TABLE 2. Computational cost assessment of A-IBOOST with other techniques.

| Techniques  | Signing Stage (online and offline) | Verification Stage | Total (ms) |
|-------------|-----------------------------------|--------------------|------------|
| [58]        | $t_c + t_h + 2t_m$                | $2t_c + t_h$       | 578.44     |
| [60]        | $t_p + 5t_m + t_h$                | $2t_p + t_h$       | 1492.64    |
| [22]        | $2t_p + 3t_m + t_h$               | $t_p + t_m + t_h$  | 1875.84    |
| [42]        | $t_c + t_h + 2t_m$                | $2t_c + t_h$       | 579.04     |
| [48]        | $2t_c + t_h + 3t_m$               | $2t_c + t_h + t_m$ | 5.92       |
| A-IBOOST    | $2t_c + t_h + 2t_m$               | $2t_c + t_h + t_m$ | 4.744      |

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

FIGURE 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. Each sensor hub is equipped with the resources to sign messages using its private key in this technique. 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.

FIGURE 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.

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], [62]. 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 random oracle model with high unforgeability under chosen message attacks. Additionally, the IBOOST scheme achieves cost-effective and robust security in the random oracle model with high unforgeability under chosen message attacks. 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 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.

**REFERENCES**

[1] A. Gupta and E. R. K. Jha, “A survey of 5G network: Architecture and emerging technologies,” IEEE Access, vol. 3, pp. 1206–1232, Jul. 2015, doi: 10.1109/ACCESS.2015.2461602.
[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, Dec. 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, Feb. 2019, doi: 10.1007/s00500-018-3112-2.

[41] C. Y. Meshram, P. L. Power, and M. S. Obaidat, “An UF-ISSS-CMA protected online/offline identity-based short signature technique using PDL,” *Proc. Comput. Sci.*, vol. 93, pp. 847–853, 2016, doi: 10.1016/j.procs.2016.07.253.

[42] C. Meshram, P. L. Power, M. S. Obaidat, C. Lee, and S. G. Meshram, “Efficient online/offline IBSS protocol using partial discrete logarithm for WSNs,” *IET Netw.*, vol. 7, no. 6, pp. 363–367, Nov. 2018, doi: 10.1049/iet-net.2018.0019.

[43] Y. Gao, P. Zeng, and K.-K.-R. Choo, “Multi-sender broadcast authentication in wireless sensor networks,” in *Proc. 10th Int. Conf. Comput. Intell. Secur.*, Nov. 2014, pp. 633–637, doi: 10.1109/CISIS.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: 10.6663/INJS.201703.19(2).02.

[45] P. Kumar, S. Kumari, V. Sharma, X. Li, A. K. Sangaiah, and S. H. Islam, “Secure CSL and CL-AS schemes designed for VANETs,” *J. Supercomput.*, vol. 75, no. 6, pp. 3076–3089, Jun. 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., Inform. Syst.*, vol. 18, pp. 80–89, Jun. 2018, doi: 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, 2020, Art. no. e4307, 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] P. Bergamo, P. D’Arco, A. De Santis, and L. Kocarev, “Security of public-key cryptosystems based on Chebyshev polynomials,” *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 52, no. 7, pp. 1382–1393, Jul. 2005.

[50] L. Zhang, “Cryptanalysis of the public key encryption based on multiple chaotic systems,” *Chaos, Solitons Fractals*, vol. 37, no. 3, pp. 669–674, Aug. 2008.

[51] C. Meshram, C.-C. Lee, S. G. Meshram, and C.-T. Li, “An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem,” *Soft Comput.*, vol. 23, no. 16, pp. 6937–6946, Aug. 2019.

[52] C. Meshram, R. W. Ibrahim, L. Deng, S. W. Shende, S. G. Meshram, and S. K. Barve, “A robust smart card and remote user password authentication protocol using extended chaotic maps under smart city environments,” *Soft Comput.*, vol. 25, pp. 10037–10051, Jun. 2021, doi: 10.1007/s00500-021-09529-5.

[53] C. Meshram, M. S. Obaidat, J. V. Tembhurne, S. W. Shende, K. W. Kalare, and S. G. Meshram, “A lightweight provably secure digital short-signature technique using extended chaotic maps for human-centered IoT systems,” *IEEE Syst. J.*, early access, Dec. 29, 2021, doi: 10.1109/JSYST.2020.3043358.

[54] C. Meshram, R. W. Ibrahim, M. S. Obaidat, B. Sadoun, S. G. Meshram, and J. V. Tembhurne, “An effective mobile-healthcare emerging emergency medical system using conformable chaotic maps,” *Soft Comput.*, vol. 25, no. 14, pp. 8905–8920, Jul. 2021.

[55] S. Han and E. Chang, “Chaotic map based key agreement with/ou clock synchronization,” *Chaos, Solitons Fractals*, vol. 39, no. 3, pp. 1283–1289, Feb. 2009.

[56] X. J. Yang, D. Baleanu, and H. M. Srivastava, *Local Fractional Integral Transforms and Their Applications*. New York, NY, USA: Academic, 2015.

[57] M. Bellare, C. Namprempre, and G. Neven, “Security proofs for identity-based identification and signature schemes,” *J. Cryptol.*, vol. 22, pp. 1–61, Aug. 2009.

[58] J. K. Liu, J. Baek, J. Zhou, Y. Yang, and J. W. Wong, “Efficient online/offline identity-based signature for wireless sensor network,” *Int. J. Inf. Secur.*, vol. 9, pp. 287–296, Jun. 2010.

[59] Z. Wang and W. Chen, “An ID-based online/offline signature scheme without random oracles for wireless sensor networks,” *Pers. Ubiquitous Comput.*, vol. 17, pp. 837–841, Apr. 2013.

[60] J. Kar, “Provably secure online/off-line identity-based signature scheme for wireless sensor network,” *Int. J. Netw. Secur.*, vol. 16, no. 1, pp. 29–34, 2014.

[61] J. Lai, X. Huang, D. He, and W. Wu, “Provably secure online/offline identity-based signature scheme based on SM9,” *Comput., J.*, 2021, doi: 10.1093/comjnl/bxa009.

[62] S. H. Islam, “Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps,” *Inf. Sci.*, vol. 312, pp. 104–130, Aug. 2015, doi: 10.1016/j.ins.2015.03.050.

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

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

AGBOTINAME LUCKY IMOIZE (Member, IEEE) received the B.Eng. (Hons.) in electrical and electronics engineering from Ambrose Alli University, Nigeria, in 2008, and the M.Sc. degree in electrical and electronics engineering from the University of Lagos, Nigeria, in 2012. Before joining the University of Lagos, he was a Lecturer at Bells University of Technology, Nigeria. He worked as the Core Network Products Manager at ZTE, Nigeria, from 2011 to 2012, and a Network Switching Subsystem Engineer at Globacon, Nigeria, from 2012 to 2017. He was awarded Fulbright Fellowship as a Visiting Research Scholar at the Wireless@VT Laboratory, Bradley Department of Electrical and Computer Engineering, Virginia Tech, USA, where he worked under the supervision of Prof. R. Michael Buehrer, from 2017 to 2018. He is currently a Lecturer with the Department of Electrical and Electronics Engineering, University of Lagos. He is also a Research Scholar with Ruhr University Bochum, Germany, under the Nigerian Petroleum Technology Development Fund (PTDF) and the German Academic Exchange Service (DAAD) through the Nigerian-German Postgraduate Program. He has co-edited one book and coauthored over 40 papers in peer review journals and conferences. His research interests include beyond 5G and 6G wireless communications, chaotic communications, and wireless security systems. He is a Registered Engineer of the Council for the Regulation of Engineering in Nigeria (COREN) and a Nigerian Society of Engineers (NSE) Member.
AZEDDINE ELHASSOUNY received the M.S. and Ph.D. degrees in mathematics, computer science, and applications from UNM. He is currently an Assistant Professor with ENSIAS, IT College, Mohammed V University in Rabat, Morocco. He also holds a postdoctoral position with UNM. He has published two books, one chapter, and several research papers about artificial intelligence, cognitive computing, and multiple criteria decision making (MCDM). He supervised many projects (for more, see annex). His current research interests include artificial intelligence, deep learning in computer vision, machine learning, data science, multimedia signal processing, and pattern recognition. His research also explores the connections between these areas and mathematical fields, such as neutrosophic field theory, fusion theory, and MCDM.

AMER ALJAEDI received the B.Sc. degree from King Saud University, Saudi Arabia, in 2007, the M.Sc. degree in information systems security from Concordia University of Edmonton, Canada, in 2011, and the Ph.D. degree in security engineering from the Department of Computer Science, Colorado University, Colorado Springs, USA, in 2018. He was a Senior Research Member of the Cybersecurity Laboratory, Colorado University. He is currently an Assistant Professor with the College of Computing and Information Technology, University of Tabuk. His research interests include software-defined networking, network traffic control and monitoring, cloud computing, and cybersecurity. He received multiple research awards from UCCS and SACM for his outstanding research papers.

ADEL R. ALHARBI received the B.Sc. degree in computer science from Qassim University, Saudi Arabia, in 2008, and the M.Sc. degree in security engineering and the M.Sc. and Ph.D. degrees in computer engineering from Southern Methodist University, Dallas, TX, USA, in 2013, 2015, and 2017, respectively. He has been a Faculty Staff Member with the College of Computing and Information Technology, University of Tabuk, Saudi Arabia, since 2009. He acquired several academic certificates and published several scientific papers. His research interests include mobile and smart devices applications, biometric, security, networking, and machine learning.

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

* * *