

Received April 3, 2020, accepted April 26, 2020, date of publication April 29, 2020, date of current version May 13, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2991348

OOS-SSS: An Efficient Online/Offline Subtree-Based Short Signature Scheme Using Chebyshev Chaotic Maps for Wireless Sensor Network

CHANDRASHEKHAR MESHAM¹, CHENG-CHI LEE^{2,3}, (Member, IEEE), SARITA GAJBHIYE MESHAM^{4,5}, AND AKSHAYKUMAR MESHAM⁶

¹Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul 480001, India

²Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei 242, Taiwan

³Department of Photonics and Communication Engineering, Asia University, Taichung 41354, Taiwan

⁴Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam

⁵Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam

⁶Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering, Nagpur 441110, India

Corresponding author: Cheng-Chi Lee (cclee@mail.fju.edu.tw)


This work was supported in part by the Ministry of Science and Technology (MOST), Taiwan, under Contract MOST 108-2410-H-030-074.

ABSTRACT Wireless sensor network (WSN) is a network system that involves spatially distributed devices such as wireless sensor nodes. As the data collected by the sensor nodes and transmitted through WSNs are mostly sensitive, confidential, or personal data, secure information transmission is a critical challenge, and one of the most significant security requirements is authentication. The digital signature plays a key role in ensuring data integrity, authentication and non-repudiation. In this article, we shall present an efficient, high security level online/offline subtree-based short signature scheme (OOS-SSS) using Chebyshev chaotic maps for WSN fuzzy user data sharing over a Galois field. The proposed scheme is secure in an environment of random oracle unforgeability under chosen message attack (UF-SBSS-CMA). Notably, our new design has made multiple-time usage of offline storage possible, enabling the signer to reuse offline pre-info in polynomial time instead of having only one single attempt as in the currently available online/offline signing schemes. In addition, based on our OOS-SSS design, we can build up an aggregation scheme for wireless sensor network settings. Also, the proposed scheme can be extended with some applications attached to it to allow users to register messages and implement them on WSN. Lastly, our performance comparison reveals that the proposed scheme has the lowest computational cost among six competing schemes.

INDEX TERMS Chebyshev chaotic maps, wireless sensor networks systems, subtree, short signature scheme, Random oracle.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have made rapid progress in recent years and have been widely applied by various kinds of businesses, healthcare centers, institutes of ecological and environmental research, as well as government and military organizations. [1]–[5]. A WSN is a network system of spatially distributed devices such as wireless sensor nodes that can be used to monitor and record physical or environmental

The associate editor coordinating the review of this manuscript and approving it for publication was Kai Li .

conditions such as temperature, sound, and motion. In WSNs, the sensor nodes can collect their own raw data, process the data locally, and jointly send information to one or more collection points (base stations). As the data collected by the sensor nodes and transmitted through WSNs are mostly sensitive, confidential, or personal data, secure information transmission is a critical challenge, and one of the most significant security requirements is authentication. The digital signature plays a key role in ensuring data integrity, authentication and non-repudiation. A WSN domain generally includes a large number of sensor nodes and base stations [6]. Compared with

mobile ad hoc networks [7], [8], WSNs are fragile against a comprehensive range of attacks due to the open manner of wireless communication. In WSN apps, therefore, confirming sensor data is essential [9]–[12].

In recent years, the inquiry into chaotic constructions and their conceivable cryptographic systems has been the focus of tremendous research interest. Chaotic systems are truly defined by their sensitive dependence on the initial conditions and their random operations in the vicinity, both of which are fundamentally similar to the behavior of some cryptographic primitives [13].

In 1989, Even *et al.* [14] introduced the concept of online/offline signatures. In an online/offline signature scheme, the signing of a message is broken into two phases with the first, more computation-demanding and time-consuming phase executed offline beforehand and the second, much faster phase carried out online at the point of signing the message. Even *et al.* created a general construction that was able to transform any digital signature scheme into an online/offline signature scheme ([14]); however, the method is not very practical as it lengthens each signature by a quadratic factor. Then, in 2001, as a response to the impracticality of Even *et al.*'s 1989 scheme, Shamir and Tauman [15] introduced a new conceptual idea called “hash-sign-switch” to more efficiently convert any signature scheme into an online/offline signature scheme. As a generalized method, this hash-sign-switch mechanism does transform signature schemes to online/offline signature schemes regardless of the types. To address certain types of signature schemes specialized for some particular applications, some researchers have proposed their own designs [16]–[20], among which [19] is the most efficient [18], while Kurosawa and Schmidt-Samoa's work featured the possibility of constructing online/offline signature schemes without random oracles [16]. All the above schemes focused, however, on the standard public-key-based setting without engaging in identity-based settings. Since about a decade ago, some identity-based signature techniques based on pairing have been released in [21]–[24]. On the other hand, Galindo and Garcia [25] adapted Schnorr's signature to create an identity-based signature scheme for a discrete log environment that does not require pairing.

In 2006, Xu *et al.* [26] first raised the concept of identity-based online/offline signatures and multisignatures. Xu *et al.* offered an identity-based online/offline signature scheme and then converted it to an identity-based online/offline multisignature scheme. Using the pairing technique, Xu *et al.*'s scheme can be applied to different routing protocols. However, later on Li *et al.* [27] demonstrated that Xu *et al.*'s 2006 scheme was actually weak against the forgery attack and so was flawed in security. In fact, to date a truly secure online/offline identity-based short signature (IBSS) technique is yet to be found in the literature concerned. On the other hand, chaotic cryptography has been applied in the creation of secure communication techniques since 1990s [13], [28], [29]. Chaotic maps are now essential to

various symmetric encryption methods [30]–[33], hash functions [34], [35], and S-boxes [36]. Lately, many chaotic schemes have been released concerning key agreement methods [37]–[40], authentication techniques [41], [42] and telecare medicine information systems [43]–[45].

In 2013, Chain and Kuo [46] offered a digital signature scheme based on chaotic maps. Since then, quite some new methods based on chaotic cryptography such as authentication schemes [47], identity-based encryption schemes [48]–[55] and signature schemes [56]–[58] have been proposed. Recently, Meshram *et al.* proposed an online/offline IBSS technique using partial discrete logarithm in [56] that allows the signer to reapply the offline information that has already been processed in polynomial time as opposed to the single-time implementations in all the online/offline signature schemes prior to it. In addition, Meshram *et al.* also proposed an aggregation scheme for WSNs in [58].

The online/offline signature scheme is the best choice for WSNs when it comes to computational economy in the process of signature generation. According to Even *et al.* [14], the major advantage of an online/offline signature scheme is that the process of generating a signature is broken into two phases. The offline phase, which happens before the real action and therefore can be performed leisurely, deals with all the resource-demanding computations, while the online phase, which takes place right when the signature is being generated, is actually the most lightweight part of the scheme as far as computation is concerned. In a WSN, the offline stage can be implemented at the base station, and the online stage is to be implemented in the sensor nodes. The online phase is usually fast and can be performed by low power devices such as the sensor nodes in a WSN. This will result in increased overheads for communication. By using bilinear pairing, Gao *et al.* [12] introduced a modified online/offline identity-based signature operation for WSNs. Ling *et al.* [59] also presented a one-time password authentication scheme for WSN applications. WSNs have been widely accepted and put in use for a vast variety of purposes such as military sensing, wild animal tracking, environmental surveillance, as well as health monitoring etc. [60]–[64]. In WSNs [65], data security is vital. Recently Kumar *et al.* [66] proposed an efficient certificateless signature scheme and certificateless aggregate signature scheme for Vehicular Ad hoc Network and demonstrate that the presented certificateless aggregate signature scheme preserves the conditional privacy, in which message generated by a vehicle is mapped to a distinct pseudo-identity. Kumar *et al.* [67] introduced an efficient certificateless public key cryptography and, it removed the complexity of certificate management from public key cryptography as well as the key escrow problem inherited from identity-based cryptography. The aggregate signature scheme also featured is a map of many to one that maps multiple signatures to a single signature on various messages. Meshram *et al.* [68] proposed a subtree-based transformation model for cryptosystem based on chaotic maps

for fuzzy user data sharing under cloud computing environment.

Our contribution: The main contribution of this study can be stated in the following aspects:

- We propose a secure and efficient online/offline subtree-based short signature scheme (OOS-SSS) using Chebyshev chaotic maps for WSN under fuzzy user data sharing over a Galois field.
- The proposed scheme is secure in an environment of the random oracle model with unforgeability under chosen message attack (UF-SBSS-CMA).
- The design of the proposed scheme allows the signer to enter the offline storage multiple times to reuse the offline pre-info in polynomial time as opposed to the one time only limit in the prior online/offline signature schemes.
- We developed an efficient subtree-based aggregation scheme which is an extension of OOS-SSS for wireless sensor network settings.
- We show how to extend the system to allow an individual user to register various messages and implement them on WSN.
- The proposed scheme has the lowest computational cost among six competing schemes.

Article structure: The rest of this paper is organized as follows. The basic pre-requisites are given in Section II. Then, our new secure, efficient online/offline subtree-based short signature scheme (OOS-SSS) using Chebyshev chaotic maps under fuzzy user data sharing for WSN over Galois field will be detailed in Section III, followed by the security examinations and discussions in Section IV and the performance analysis in Section V. Then, in Section VI, our aggregation scheme extended from OOS-SSS for WSN will be presented. After that, Section VII will deal with the fundamental setting of the proposed scheme for WSNs. Finally, the conclusion will be given in Section VIII.

II. BACKGROUND AND RELATED INFORMATION

In this section, we shall first lay out the notations we use in our new scheme, namely OOS-SSS using Chebyshev chaotic maps under fuzzy user data sharing for WSN over Galois field. Then, we shall briefly introduce the mathematical definitions and theorems the design of our new scheme is based on, including some basic concepts of trigonometry in Galois fields as well as Chebyshev polynomials over Galois fields.

A. NOTATIONS

Our OOS-SSS using Chebyshev chaotic maps under fuzzy user data sharing for WSN is a novel attempt. The notations we will utilize in our scheme are as follows.

If there is no uncertainty, we use $[y, z]$ for the shorthand of $\{y, y + 1, \dots, z\}$, and $[y]$ for $[1, y]$. For every $id = (id_1, id_2, \dots, id_k)$, where id is an identity vector, let $S_{id} = \{id_1, \dots, id_k\}$ be a set of identities (id) that includes all identities performing in id . We define

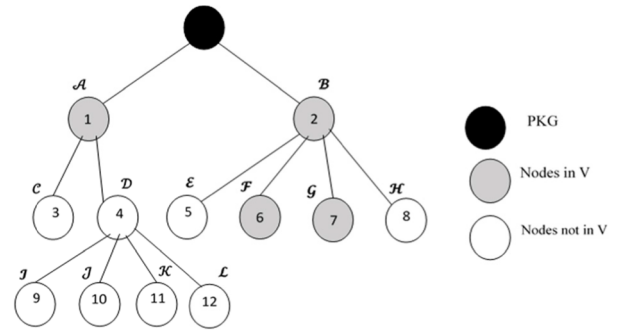


FIGURE 1. example of subtree-based short signature structure.

$I_{id} = \{i : id_i \in S_{id}\}$ as the location records of id in the tree structure of the model. The predicted receivers form a subtree in a tree-structured identity-based encryption technique [69]. The identity vectors and the locations of their receivers are integrated into \mathbb{T} in the tree structure. The root node must be covered by any legitimate \mathbb{T} . This represents the fact that the PKG is managing the structure. Similarly, \mathbb{T} 's identity set and \mathbb{T} 's location indices are represented by $S_{\mathbb{T}} = \cup_{id \in \mathbb{T}} S_{id}$ and $I_{id} = \{i : id_i \in S_{\mathbb{T}}\}$, respectively. By the same token, the expression $Sup(id) = \{(id_1, id_2, \dots, id_{k'}) : k' \leq k\}$ can be used to indicate the superiority of $id = (id_1, id_2, \dots, id_k)$. Subtree \mathbb{T} 's projected receivers are characterized as $Sup(\mathbb{T}) = \cup_{id \in \mathbb{T}} Sup(id)$.

Now let's see how the notations fit in with our new subtree-based design OOS-SSS using Chebyshev chaotic maps for WSN. The proposed scheme is promising candidate to ensure fuzzy entity data sharing while fulfilling the protection criteria, but experiences multi-receiver efficiency difficulty. Suppose that the users are positioned in a tree structure as shown in Fig.1. The identity set and position indices of id are $S_{id} = \{\mathcal{B}, \mathcal{F}\}$ and $I_{id} = \{2, 6\}$, respectively, to specify a predetermined user with $id = (\mathcal{B}, \mathcal{F})$. The user creates a set of $Sup(id) = \{(\mathcal{B}), (\mathcal{B}, \mathcal{F})\}$ which involves himself/herself and his/her superiors. When a data owner sends a message to a set of receivers in a subtree such as $\mathbb{T} = \{(\mathcal{A}), (\mathcal{B}, \mathcal{F}), (\mathcal{B}, \mathcal{G})\}$, we can denote \mathbb{T} 's identity set and position indices as $S_{\mathbb{T}} = \{\mathcal{A}, \mathcal{B}, \mathcal{F}, \mathcal{G}\}$ and $I_{\mathbb{T}} = \{1, 2, 6, 7\}$, respectively. \mathbb{T} 's superiors are described as $Sup(\mathbb{T}) = \{(\mathcal{A}), (\mathcal{B}), (\mathcal{B}, \mathcal{F}), (\mathcal{B}, \mathcal{G})\}$, which is clearly the user agreement that the owner of the data wants to convey.

B. TRIGONOMETRY IN GALOIS FIELDS (GF)

All through this article, we expect that calculations over $GF(\mathcal{Q})$, where $\mathcal{Q} = p^\ell$, ℓ being a positive integer and p being an odd prime, are completed modulo an irreducible polynomial $f(z)$ with degree ℓ whose coefficients are in $GF(\mathcal{P})$.

Definition 1: The arrangement of Gaussian integers over $GF(\mathcal{Q})$ is the set $GJ_{\mathcal{Q}} = \{c + d\mathcal{I}, \forall c, d \in GF(\mathcal{Q})\}$,

TABLE 1. All values for $\cos_{\xi_1}(\psi)$, where $\xi_1 = (u^2 + 2u) + (u^2 + u + 1)j$ is a unimodular component of order 28 in $GJ(27)$.

ψ	$\cos_{\xi_1}(\psi)$	ψ	$\cos_{\xi_1}(\psi)$	ψ	$\cos_{\xi_1}(\psi)$	ψ	$\cos_{\xi_1}(\psi)$
0	1	7	0	14	2	21	0
1	$u^2 + 2u$	8	$2u^2 + 2u + 2$	15	$2u^2 + u$	22	$u^2 + u + 1$
2	u^2	9	$u^2 + u$	16	$2u^2$	23	$u^2 + 2u$
3	$u^2 + 2$	10	$u^2 + 2u + 1$	17	$2u^2 + 1$	24	$2u^2 + u + 2$
4	$2u^2 + u + 2$	11	$2u^2 + 1$	18	$u^2 + 2u + 1$	25	$u^2 + 2$
5	$2u^2 + 2u$	12	$2u^2$	19	$u^2 + u$	26	u^2
6	$u^2 + u + 1$	13	$2u^2 + u$	20	$2u^2 + 2u + 2$	27	$u^2 + 2u$

TABLE 2. All possible estimates of $\cos_{\xi_2}(\psi)$, where $\xi_2 = \psi$ is a component of order 26 in $GF(27)$.

ψ	$\cos_{\xi_2}(\psi)$	ψ	$\cos_{\xi_2}(\psi)$	ψ	$\cos_{\xi_2}(\psi)$	ψ	$\cos_{\xi_2}(\psi)$
0	1	7	$2u + 2$	14	$2u^2 + u + 1$	20	$u + 1$
1	$u^2 + 2u + 2$	8	u	15	$2u + 1$	21	$2u$
2	$u + 2$	9	$u^2 + u + 2$	16	$u^2 + 2u + 2$	22	$2u^2 + 2u + 1$
3	$u^2 + 1$	10	$u^2 + 2u + 2$	17	$u^2 + u + 2$	23	$u^2 + 1$
4	$2u^2 + 2u + 1$	11	$2u + 1$	18	u	24	$u + 2$
5	$2u$	12	$2u^2 + u + 1$	19	$2u + 2$	25	$u^2 + 2u + 2$
6	$u + 1$	13	2				

such that $j^2 = -1$ is a quadratic nonresidue over $GF(\mathcal{Q})$, i.e., $\mathcal{Q} \equiv 3(mod 4)$.

Definition 2 (\mathcal{t} -trigonometric functions): [72], [73]. Let ξ be a nonzero element of $GF(\mathcal{Q})$, where $\mathcal{Q} \equiv 3(mod 4)$ and ξ has multiplicative order indicated by $ord(\xi)$. The \mathcal{t} -trigonometric functions \mathcal{t} -cosine and \mathcal{t} -sine identified with ξ are calculated modulo $f(\mathcal{z})$ as

$$\cos_{\xi}(\psi) := \frac{\xi^{\psi} + \xi^{-\psi}}{2} \quad \text{and} \quad \sin_{\xi}(\psi) := \frac{\xi^{\psi} - \xi^{-\psi}}{2j} \quad (1)$$

From Eq. (1), we notice that the \mathcal{t} -cosine function has period $ord(\xi)$ and even symmetry, i.e.

$$\cos_{\xi}(\psi) = \cos_{\xi}(-\psi(mod ord(\xi))) \quad (2)$$

The accompanying lemma 1 of [73] is likewise critical to the description of the \mathcal{t} -cosine function. The proofs of lemmas, propositions and theorems are discussed in [73].

Definition 3 (Unimodular Set): The unimodular set of $GJ(\mathcal{Q})$, signified by G_1 , is the arrangement of components $\xi = (c + d\mathcal{t}, j) \in GJ(\mathcal{Q})$, such that $c^2 + d^2 \equiv 1(mod w)$.

The accompanying propositions 1 and 2 of [73] and lemma 2 of [73] are likewise critical to the description the unimodular set.

Example 1: Let's take $GF(27)$ for example, namely the Galois fields created from the primitive polynomial $w = f(u) = u^3 + 2u + 1$. Let $\xi_1 = (u^2 + 2u) + (u^2 + u + 1)j$ be a unimodular element of order $ord(\xi_1) = 28$ in $GJ(27)$. Table 1 is a list of all likely estimates of $\cos_{\xi_1}(\psi)$. Take note of $\#\mathcal{J}_{\xi_1} = 15$ and, subsequently, the function $\arccos_{\xi_1}(\psi)$ is not characterized for each $\psi \in GF(27)$.

As outlined in Example 1, despite the fact that $\xi_1 \in GJ(\mathcal{Q})$ is a unimodular component by extreme multiplicative order ($\mathcal{Q} + 1$), the function $\arccos_{\xi_1}(\psi)$ is not characterized for each $\psi \in GF(\mathcal{Q})$.

To calculate the inverse \mathcal{t} -cosine function of the components included in $GF(\mathcal{Q})$ but not in \mathcal{J}_{ξ_1} , we need to choose a component $\xi_2 (\neq \xi_1)$ that satisfies $\mathcal{J}_{\xi_1} \cup \mathcal{J}_{\xi_2} = GF(\mathcal{Q})$. Such a component is indicated by the following theorem.

Theorem 1: [73] Let $\xi_1 \in GJ(\mathcal{Q})$ be a unimodular component of $ord \xi_1 = \mathcal{Q} + 1$ and likewise let $\xi_2 \in GJ(\mathcal{Q})$ be a unimodular component of $ord(\xi_2) = \mathcal{Q} - 1$. Then, we have $\mathcal{J}_{\xi_1} \cup \mathcal{J}_{\xi_2} = GF(\mathcal{Q})$.

Example 2: Let $\xi_2 = u$ be a component of order 26 in $GF(27)$, namely the Galois fields created from the primitive polynomial $w = f(u) = u^3 + 2u + 1$. Table 2 is a list of all the possible values for $\cos_{\xi_2}(\psi)$. Take note that, since ξ_2 was picked by Theorem 1, considering the set \mathcal{J}_{ξ_1} (Example 1), we have $\mathcal{J}_{\xi_1} \cup \mathcal{J}_{\xi_2} = GF(\mathcal{Q})$.

C. CHEBYSHEV POLYNOMIALS OVER GALOIS FIELDS

In the same way the discussions go in [74], the definition of Chebyshev polynomials over Galois fields can be given using the \mathcal{t} -cosine function [73] that is in immaculate relationship with the well-established common definition of Chebyshev polynomials over the field of real numbers [75].

Definition 4: The Chebyshev polynomials related to those that are already established over $GF(\mathcal{Q})$ are characterized in the following way:

$$\mathcal{T}_n(\psi) := \cos_{\xi}(n \times \arccos_{\xi}(\psi))(mod w) \quad (3)$$

Eq. (3) compares to the \mathcal{t} -cosines of the products of an arc. It produces the polynomials of degree n to as far as \mathcal{t} -cosines of the respective arc [75]. When we consider the example of a Galois field, it can be achieved by combining Definition 4 with the arcs formula in [72] as follows:

$$\mathcal{T}_n(\mathcal{Y}) = 2\mathcal{Y}\mathcal{T}_{n-1}(\mathcal{Y}) - \mathcal{T}_{n-2}(\mathcal{Y}) \pmod{\omega}, \quad (4)$$

where $\mathcal{Y} \in GF(\mathcal{Q})$, $n \in \mathbb{N}$, $\mathcal{T}_0(\mathcal{Y}) = 1$ and $\mathcal{T}_1(\mathcal{Y}) = \mathcal{Y}$. Chebyshev polynomials modulo $\omega = f(u)$ have the following periodicity:

Proposition 1: Let ξ be a nonzero component of $GJ(\mathcal{Q})$ such that $ord(\xi) = N$. If $\mathcal{Y} \in \mathcal{J}_\xi$, then $\mathcal{T}_{tN \pm n}(\mathcal{Y}) = \mathcal{T}_n(\mathcal{Q})$, $t \in \mathbb{Z}$.

Proof: From Definition 4, we have:

$$\mathcal{T}_{tN \pm n}(\mathcal{Y}) = \cos_\xi((tN \pm n) \times \arccos_\xi(\mathcal{Y})) \pmod{\omega}$$

Using the expansion of arcs formula, we can rephrase the statement as:

$$\begin{aligned} \mathcal{T}_{tN \pm n}(\mathcal{Y}) &= \cos_\xi(tN \times \arccos_\xi(\mathcal{Y})) \cos_\xi(n \\ &\quad \times \arccos_\xi(\mathcal{Y})) \mp \sin_\xi(tN \\ &\quad \times \arccos_\xi(\mathcal{Y})) \sin_\xi(n \times \arccos_\xi(\mathcal{Y})) \end{aligned}$$

As $ord(\xi) = N$, using Definition 2 of [46], we come to $\cos_\xi(tN \times \arccos_\xi(\mathcal{Y})) = 1$ and $\sin_\xi(tN \times \arccos_\xi(\mathcal{Y})) = 0$. Subsequently, the last condition is reduced to:

$$\mathcal{T}_{tN \pm n}(\mathcal{Y}) = \cos_\xi(n \times \arccos_\xi(\mathcal{Y})) = \mathcal{T}_n(\mathcal{Y})$$

The limitation that Definition 4 requires $\mathcal{Y} \in \mathcal{J}_\xi$ can be lifted if we want to estimate $\mathcal{T}_n(\mathcal{Y})$ for individual values of n, \mathcal{Y} with a prime power \mathcal{Q} . In this sense, Eq. (4) can be utilized not depending upon the estimation of \mathcal{t} -trigonometric functions.

Chebyshev polynomials have two significant properties [76]: the chaotic property and the semi-group property.

(1) The chaotic property: A Chebyshev polynomial map, defined as $\mathcal{T}_r : [-1, 1] \rightarrow [-1, 1]$ comprised of degree $n > 1$ is a chaotic map with an invariant density function $f^*(\mathcal{Y}) = 1/(\pi\sqrt{1-\mathcal{Y}^2})$ for some positive Lyapunov exponent $\lambda > \ln n$.

(2) The semi-group property:

$$\begin{aligned} \mathcal{T}_\omega(\mathcal{T}_\ell(\mathcal{Y})) &= \cos(\omega \cos^{-1}(\cos(\ell \cos^{-1}(\mathcal{Y})))) = \\ &= \cos(\omega \ell \cos^{-1}(\mathcal{Y})) = \mathcal{T}_{\ell\omega}(\mathcal{Y}) = \mathcal{T}_\ell(\mathcal{T}_\omega(\mathcal{Y})), \end{aligned}$$

where ω and ℓ are positive integers and $\mathcal{Y} \in [-1, 1]$.

The above two properties of Chebyshev polynomials are considered difficult problems in polynomial time:

- (1) The Discrete Logarithm (DL) problem is to find an integer ω such that $\mathcal{T}_\omega(x) = \mathcal{Y}$ for two given components x and \mathcal{Y} .
- (2) The Diffie-Hellman problem (DHP) is to estimate the element $\mathcal{T}_{\omega\ell}(x)$ for three given parts $x, \mathcal{T}_\omega(x)$, and $\mathcal{T}_\ell(x)$.

III. THE PROPOSED ONLINE/OFFLINE SUBTREE-BASED SHORT SIGNATURE SCHEME

In this section, we shall detail the new efficient OOS-SSS using Chebyshev chaotic maps under fuzzy user data sharing over Galois field that we have designed. The scheme is composed of five procedures.

A. SETUP

- a. Let $z \in GF(\mathcal{Q})$ be a global parameter such that $z \neq 0, 1$ and Galois fields generated from the primitive polynomial ω .
- b. Select an arbitrary $\mathcal{b} \leftarrow GJ(\mathcal{Q})$ such that $\mathcal{b} \neq 0, 1$.
- c. Calculate $\nu \leftarrow \mathcal{T}_\mathcal{b}(z) \pmod{\omega}$.
- d. Choose chaotic hash functions \mathfrak{h} such that $\mathfrak{h} : Sup(\mathcal{T}) \rightarrow GF(\mathcal{Q})$.

The master public key (mpk) and master private key (msk) are given by $\{\omega, z, \mathfrak{h}, \nu\}$ and \mathcal{b} .

B. EXTRACTION

Given a client's identity $id \in Sup(\mathbb{T})$, the private key is generated by executing the following steps:

- a. Select at random $r \xleftarrow{\mathbb{R}} GJ(\mathcal{Q})$ such that $r \neq 0, 1$.
- b. Calculate $\Omega \leftarrow \mathcal{T}_r(z) \pmod{\omega}$.
- c. Calculate $d \leftarrow \mathfrak{h}(id, \Omega)$.
- d. Calculate $\mathcal{b} \leftarrow r * \mathcal{b}d \pmod{\omega}$.

The pair (Ω, \mathcal{b}) is the client's private key.

C. OFFLINE SIGNING

The signer performs the following calculation in the offline phase:

- a. Calculate $\mathcal{D}'_i \leftarrow \mathcal{T}_{z^i}(z) \pmod{\omega}$, for $i \in [0, \mathcal{Q} - 1]$

D. ONLINE SIGNING

In the online phase, the signer performs the following steps to register a message $m \in [-1, 1]$ using (Ω, \mathcal{b}) :

- a. Select $\mathcal{k} \leftarrow GJ(\mathcal{Q})$ arbitrarily so that \mathcal{k}_i is the i^{th} bit of \mathcal{k} .
- b. Calculate $\mathcal{D} \leftarrow \prod_{i=1}^{\mathcal{Q}} \mathcal{D}'_{i-1}$.
- c. Calculate $c \leftarrow \mathfrak{h}(\mathcal{D}, \Omega, m)$.
- d. Calculate $x \leftarrow \mathcal{k} * \mathcal{b}c \pmod{\omega}$ as well as $\gamma \leftarrow \mathcal{T}_x(z) \pmod{\omega}$.

The signature of m is $\chi \leftarrow (\mathcal{D}, \Omega, x)$.

E. VERIFICATION

To verify a signature $\chi \leftarrow (\mathcal{D}, \Omega, x)$ on m and id , the verifier performs the two steps below:

- a. Calculate $\gamma' \leftarrow \mathcal{D}\mathcal{T}_c(\Omega)\mathcal{T}_{cd}(\nu) \pmod{\omega}$.
- b. If $\gamma = \gamma'$ then signature is accepted, or else this is not.

F. CONSTANCY OF THE ALGORITHM

The accurately produced private key should fulfil the equality below:

$$\mathcal{T}_\mathcal{b}(z) \pmod{\omega} = \Omega \mathcal{T}_d(\nu) \pmod{\omega} \quad (5)$$

For constancy of algorithm, note that $\mathcal{D} = \mathcal{T}_{\mathcal{h}}(\mathcal{v}) \pmod{\mathcal{w}}$. We have:

$$\begin{aligned} \mathcal{DT}_c(\Omega) \mathcal{T}_{cd}(\mathcal{v}) \pmod{\mathcal{w}} & \\ &= \mathcal{T}_{\mathcal{h}}(\mathcal{z}) \mathcal{T}_{cr}(\mathcal{z}) \mathcal{T}_{\mathcal{b}cd}(\mathcal{z}) \pmod{\mathcal{w}} \\ &= \mathcal{T}_x(\mathcal{z}) \pmod{\mathcal{w}} \end{aligned} \quad (6)$$

IV. SECURITY EXAMINATIONS AND DISCUSSIONS

To demonstrate the security of our new OOS-SSS using Chebyshev chaotic maps over Galois field under fuzzy user data sharing, we apply the security proofs contributed by Bellare et al. [77].

Theorem 1: The proposed OOS-SSS is $(\epsilon, t, \mathcal{Q}_h, \mathcal{Q}_s, \mathcal{Q}_E)$ secure in the knowledge of unforgeability of subtree-based short signature (SBSS) under the chosen message attack (UF-SBSS-CMA) in the random oracle model, implementing the (ϵ', t') -Chebyshev chaotic maps hypothesis in $GF(\mathcal{Q})$, where:

$$\epsilon' = \left(\frac{1}{\mathcal{Q}_h} - \frac{\mathcal{Q}_E + \mathcal{Q}_s}{\mathcal{w}} \right) \left(1 - \frac{1}{\mathcal{w}} \right) \epsilon \quad (7)$$

$$t' = t + \mathcal{O}(\mathcal{Q}_s + \mathcal{Q}_E)\tau \quad (8)$$

And \mathcal{Q}_h – hashing queries, \mathcal{Q}_s – signing queries and \mathcal{Q}_E – extraction queries are the quantity of chaos. Here τ is the time for an operation of exponentiation.

Proof: Assume that \exists a foe F . We develop an algorithm \mathfrak{A} that depends on the utilization of F to solve Chebyshev chaotic maps over Galois field. The algorithm \mathfrak{A} is provided with a $GF(\mathcal{Q})$ that comes with a global parameter \mathcal{z} and a variable $\lambda \in GF(\mathcal{Q})$. Algorithm \mathfrak{A} is tested to find $\vartheta \in GJ(\mathcal{Q})$ in such a way that $\mathcal{T}_{\vartheta}(\mathcal{z}) \pmod{\mathcal{w}} = \lambda$. We apply [77]’s approach.

Setup: \mathfrak{A} takes a chaotic hash function \mathfrak{h} , which is similar to a random oracle behavior. \mathfrak{A} is liable for the simulation of this reformation process. \mathfrak{A} assigns a variable $\mathcal{v} \leftarrow \lambda$ and yields the public parameter $(x, \mathcal{w}, \mathcal{v}, \mathfrak{h})$ to F .

Extraction Oracle inquiries: F is allowed to inquire for $id \in Sup(\mathbb{T})$ in the extraction oracle. \mathfrak{A} re-creates the oracle. It requires random $s, t \in GJ(\mathcal{Q})$ and sets:

$$\Omega \leftarrow \mathcal{T}_t(\mathcal{z}) / \mathcal{T}_s(\mathcal{v}) \pmod{\mathcal{w}}, \mathcal{b} \leftarrow t, \mathfrak{h}(\Omega, id) \leftarrow s \quad (9)$$

\mathfrak{A} yields (Ω, \mathcal{b}) as a private key for $id \in Sup(\mathbb{T})$ and stores the consistency evaluation $(\Omega, \mathfrak{A}(\Omega, id), \mathcal{b}, id)$ in list.

Signing Oracle inquiries: The foe F makes an inquiry for $id \in Sup(\mathbb{T})$ and signs a message. Algorithm \mathfrak{A} checks whether $id \in Sup(\mathbb{T})$ has been inquired for in oracle \mathfrak{h} or the extraction oracle in the past. If yes, it will only improve the list $(\Omega, \mathcal{b}, \mathfrak{h}(\Omega, id))$ as indicated in the table. Then algorithm \mathfrak{A} uses these estimates to sign the message by performing the signing procedures. It generates the signature (\mathcal{D}, Ω, x) on the message and maintains the list of $\mathfrak{h}(\mathcal{D}, \Omega, m)$ for reliability in the chaotic hash table. If $id \in Sup(\mathbb{T})$ is not requested to extract the oracle, then \mathfrak{A} starts the extraction oracle simulation procedure by exhausting the private key to sign the message.

Output Computation: Eventually, foe F produces a fake signature $\chi_1^* = (\mathcal{D}^*, \Omega^*, x_1^*)$ on $id^* \in \mathbb{T}^*$ and m^* , where \mathbb{T}^* is the challenge subtree. The algorithm \mathfrak{A} reverses F to the view that it makes an inquiry $\mathfrak{h}(\mathcal{D}^*, \Omega^*, m^*)$ and provides another value to the justified. Foe F produces a few other signatures $\chi_2^* = (\mathcal{D}^*, \Omega^*, x_2^*)$. Algorithm \mathfrak{A} rehashes again and obtains $\chi_3^* = (\mathcal{D}^*, \Omega^*, x_3^*)$. Note that \mathcal{D}^* and Ω^* must inevitably be the same. We let n_1, n_2, n_3 be created three times in a row from the random oracle inquiries $\mathfrak{h}(\mathcal{D}^*, \Omega^*, m^*)$.

For each $\mathcal{b}, \mathcal{h}, \mathcal{r} \in GJ(\mathcal{Q})$, we now project Chebyshev chaotic maps of Ω, \mathcal{v} and \mathcal{D} over the Galois field respectively, i.e., $\Omega = \mathcal{T}_{\mathcal{r}}(\mathcal{z}) \pmod{\mathcal{w}}, \mathcal{v} = \mathcal{T}_{\mathcal{b}}(\mathcal{z}) \pmod{\mathcal{w}}$ and $\mathcal{D} = \mathcal{T}_{\mathcal{h}}(\mathcal{z}) \pmod{\mathcal{w}}$. From Eq. (2), we have:

$$x_i^* = \mathcal{h} * \mathcal{r} n_i * \mathcal{b} n_i \mathfrak{h}(\Omega^*, id) \pmod{\mathcal{w}} \text{ for } i = 1, 2, 3 \quad (10)$$

Only \mathcal{b}, \mathcal{h} and \mathcal{r} are unfamiliar to \mathfrak{A} in these mathematical examinations. For the estimates of the overhead linear autonomous mathematical proclamations, the algorithm \mathfrak{A} estimates for $i = 1, 2, 3$ and generates \mathcal{b} as resolution over Galois field concerning Chebyshev chaotic maps.

Reduction Cost Examination: The simulation process with extraction oracle failures presupposes that the consignment $\mathfrak{h}(\Omega, id)$ of the random oracle is irregular, suggesting a combined probability of no less than $\frac{\mathcal{Q}_h}{\mathcal{w}}$. Accordingly, the simulation procedure is effective $(\mathcal{Q}_s + \mathcal{Q}_E)$ times (ensued from the consideration that $\mathfrak{h}(\Omega, id)$ also can furthermore be requested in the signing oracle, if id is not requested in the extraction oracle) with the probability being:

$$\left(1 - \frac{(\mathcal{Q}_s + \mathcal{Q}_E)\mathcal{Q}_h}{\mathcal{w}} \right) \leq \left(1 - \frac{\mathcal{Q}_h}{\mathcal{w}} \right)^{\mathcal{Q}_s + \mathcal{Q}_E}$$

Because of the rewind, at least at a probability of $\left(\frac{1}{\mathcal{Q}_h} \right)$. The overall probability of success is:

$$\left(\frac{1}{\mathcal{Q}_h} - \frac{\mathcal{Q}_E + \mathcal{Q}_s}{\mathcal{w}} \right) \left(1 - \frac{1}{\mathcal{w}} \right) \epsilon$$

The time complexity of algorithm \mathfrak{A} determined by the exponentiations performed in signing and extracting procedures is equivalent to:

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

V. PERFORMANCE ANALYSIS

In this section, we analyze the performance of our new scheme OOS-SSS by comparing it with some competing online/offline techniques and non-online/offline techniques.

A. AUTHENTICATION PROOF BASED ON BAN LOGIC PERFORMANCE COMPARISON AMONG ONLINE/OFFLINE SCHEMES

Here we compare the performance of six well-designed online/offline identity-based signature schemes including Shamir and Tauman’s scheme [15], Xu et al.’s scheme [26], Kar’s scheme [78], Gao et al.’s scheme [20], Meshram et al.’s

TABLE 3. Comparison in terms of computational cost.

Techniques ↓ / Computational Cost (C) →	C_1	C_2	C_3	C_4	C_5
Shamir and Tauman's [15] technique	-	-	$C(\mathcal{H}) + C(\sigma_G)$	m	$C(\sigma_V) + C(\mathcal{H}) + C(\mathcal{C}_V)$
Gao et al.'s [20] technique	$\eta(\mathcal{P} - 1)$	$3m + \mu\mathcal{O}(\mathcal{P} - 1)$	$\eta(\mathcal{P} - 1)$	2m	$\mu + \rho$
Xu et al.'s [26] technique	$2\eta \mathcal{P} $	$m + 2\mu\mathcal{O}(\mathcal{P})$	$2\eta + m$	m	$\mu + 2(\eta + \rho)$
Meshram et al.'s 2016 [55] technique	0	$m + \mu\mathcal{O}(N^2)$	0	m	$2\eta + \mu$
Meshram et al.'s 2019 [56] technique	0	$m + \mu\mathcal{O}(\mathcal{P}_1)$	0	m	2μ
Kar's [78] technique	$\eta(\mathcal{P} - 1)$	$3m + \mu\mathcal{O}(\mathcal{P} - 1)$	$\eta(\mathcal{P} - 1)$	3m	$3\mu + 2\rho + \eta$
The proposed technique	0	$m + \mu\mathcal{O}(\mathcal{W})$	0	m	2μ

C_1 : Computational cost in offline (multi-time) stage; C_2 : Computational cost in online (multi-time) stage; C_3 : Computational cost in offline (one-time) stage; C_4 : Computational cost in online (one-time) stage; C_5 : computational cost in verification stage.

TABLE 4. Comparison in terms of computational cost and signature size.

Techniques ↓ / Computational Cost →	Computational cost in Verification stage	Computational cost in Signing stage	Size of signature (bits)
Hess's [21] technique	$\eta + 2\rho$	$\mu + 3\eta$	320
Meshram et al.'s 2016 [55] technique	$\mu + 2\eta$	m	480
Meshram et al.'s 2019 [56] technique	2μ	m	480
Cha and Cheon's [79] technique	$\mu + 2(\eta + \rho)$	2η	320
Guillou and Quisquater's [80] technique	$2(\mu + 2\eta)$	$2(m + \eta)$	2048
The proposed technique	μ	m	480

2016 scheme [55], Meshram et al.'s 2019 scheme [56], and our new scheme OOS-SSS in terms of computational cost. Please note that, among the schemes, Xu et al.'s work [26] has no multi-time adaptation to it, so the multi-time evaluation for it was done by linking the same type of technique together.

However, it is not possible to apply Shamir and Tauman's technique [15] for a multi-time performance test.

The execution cost $C(\zeta)$ of operation ζ is estimated by the bits of $|\xi|$. Besides that, ρ , μ , m and η , which stand for the pairing operation, the multiplication operation (similar to point addition in ECC) in group, the modular multiplication operation in $GI(q)$ (i.e. Gaussian integers over $GF(\mathcal{Q})$) and exponentiation operation (similar to scalar multiplication in ECC) in group, respectively, are all included in the evaluations. Other operations such as addition in $GI(q)$ and representative hashing are negligible and are therefore ignored.

Table 3 shows the results of performance evaluations in the form of execution cost. For example, H is a Chameleon hash operation, which requires the minimum of one η computation; \mathcal{A} stands for a chaotic hash operation σ_V and σ_G represent usual verification and signature creation,

respectively, and each requires no less than one η computation. Similarly, \mathcal{C}_V is the operation of one certificate verification, which requires no less than one η computation.

B. PERFORMANCE COMPARISON AMONG NON-ONLINE/OFFLINE SCHEMES

As with online/offline identity-based signature schemes, we also compare the proposed scheme with some well-established non-online/offline identity-based signature schemes recognized by ISO/IEC including Cha and Cheon's scheme [79], Guillou and Quisquater's scheme [80], Hess's scheme [21] and Meshram et al.'s scheme [55]. The full results are shown in Table 4 with the same notations used as in Table 3.

Notably, non-online/offline schemes may not run very smoothly in WSNs since the lightweight wireless sensors probably will be overwhelmed by the operation demand. For example, both Hess's scheme [21] and Cha and Cheon's scheme [79] inevitably require operation ρ (pairing) in the verification phase and operation η in the signing phase, which amounts to too much a burden for lightweight gadgets.

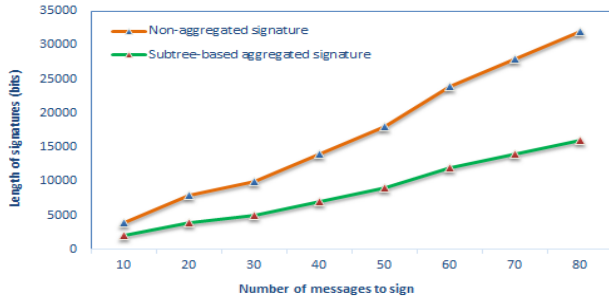


FIGURE 2. Comparison between subtree-based aggregation and non-aggregation variants.

VI. SUBTREE-BASED AGGREGATION (EXTENSION) FOR THE PROPOSED SCHEME

It would be very useful if at a time a sensor node can sign not just one message but i different messages with the length of the aggregate signature being the same as the length of a signature on a single message, in other words significantly shorter than i times the length of a single signature. Such an aggregate signature is of incredible significance in WSNs, as it can sharply decrease the communication overheads on the side of the sensor nodes. In this section, we present the new subtree-based aggregation scheme for the proposed OOS-SSS. It is composed of the following five segments.

A. SETUP

- Let $z \in GF(\mathcal{Q})$ be the global parameter such that $z \neq 0, 1$ and Galois fields generated from the primitive polynomial w .
- Select an arbitrary $\mathcal{B} \leftarrow GJ(\mathcal{Q})$ such that $\mathcal{B} \neq 0, 1$.
- Calculate $v \leftarrow \mathcal{T}_{\mathcal{B}}(z) \pmod{w}$.
- Choose chaotic hash functions \mathfrak{h} such that $\mathfrak{h} : Sup(\mathbb{T}) \rightarrow GF(\mathcal{Q})$.

The master public key (mpk) and master private key (msk) are given by $\{w, z, \mathfrak{h}, v\}$ and \mathcal{B} .

B. EXTRACT

Given clients with identities $id \in Sup(\mathbb{T})$, the private key generation procedure is as follows:

- Select at random $r \xleftarrow{R} GJ(\mathcal{Q})$ such that $r \neq 0, 1$.
- Calculate $\Omega \leftarrow \mathcal{T}_r(z) \pmod{w}$.
- Calculate $d \leftarrow \mathfrak{h}(id, \Omega)$.
- Calculate $\mathcal{B} \leftarrow r * \mathcal{B}d \pmod{w}$.

The pair (Ω, \mathcal{B}) is the client's private key.

C. OFFLINE SIGNING

The signer performs the following calculation:

- Calculate $\mathcal{D}'_i \leftarrow \mathcal{T}_{2^i}(z) \pmod{w}$, for $i \in [0, \mathcal{Q} - 1]$.

D. ONLINE SIGNING

The signer performs the following steps to register a message $m \in [-1, 1]$ using (Ω, \mathcal{B}) :

- Select $\mathcal{K}_i \xleftarrow{R} GJ(\mathcal{Q})$ at random where $\mathcal{K}_j[i]$ is the j^{th} bit of \mathcal{K}_i .
- Define $\mathcal{K}_i \subset \{1, \dots, \mathcal{Q}\}$ to be the set of indices such that $r_j[i] = 1$.
- Compute $\mathcal{D}_i \leftarrow \prod_{i \in \mathcal{K}_i} \mathcal{D}'_{j-1}$.
- Compute $c_i \leftarrow \mathfrak{h}(\mathcal{D}, \Omega, m_i)$
- Compute $x_i \leftarrow \mathcal{K}_i * c_i \mathcal{B} \pmod{w}$, $x = \sum_{i=1}^n x_i$ and $\gamma \leftarrow \mathcal{T}_x(z) \pmod{w}$.

The aggregate signature is given by $\chi \leftarrow (\mathcal{D}_i, \Omega, x)$.

E. VERIFICATION

To verify a signature $\chi \leftarrow (\mathcal{D}_i, \Omega, x)$ on m_i and id for $i = 1, \dots, n$, the verifier proceeds as follows:

- Compute $c_i \leftarrow \mathfrak{h}(\mathcal{D}, \Omega, m_i)$
- Compute $\delta' = (\prod_{i=1}^n \mathcal{D}_i) \mathcal{T}_{\Omega}(\mathcal{D}) \mathcal{T}_{\Omega}(\mathcal{D}) \mathcal{T}_{\Omega}(\mathcal{D}) \pmod{w}$, where $\zeta = \sum_{i=1}^n c_i$
- If $\delta = \delta'$ then signature is accepted; otherwise it is rejected.

F. CONSISTENCY OF THE ALGORITHM

The accurately produced private key should fulfil the equality below:

$$\mathcal{D}_i = \mathcal{T}_{\mathcal{K}_i}(z) \pmod{w} \text{ for } i \in [1, \dots, n].$$

We have

$$\begin{aligned} \delta' &= \left(\prod_{i=1}^n \mathcal{D}_i \right) \mathcal{T}_{\Omega}(\mathcal{D}) \mathcal{T}_{\Omega}(\mathcal{D}) \pmod{w} \\ &= \left(\prod_{i=1}^n \mathcal{D}_i \right) \mathcal{T}_{r\zeta}(z) \mathcal{T}_{\zeta} \mathcal{B}d(z) \pmod{w} \\ &= \mathcal{T}_{\mathcal{K}}(z) \mathcal{T}_{\zeta} r(z) \mathcal{T}_{\mathcal{B}\zeta} d(z) \pmod{w} \\ &= \mathcal{T}_x(z) \pmod{w} \end{aligned}$$

As shown in Fig.2, when the recommended subtree-based aggregation method is used, the signature size is decreased almost by half compared to the subtree-based non-aggregate variant.

VII. BASIC SETTING ON WIRELESS SENSOR NETWORKS

In this section, we show the fundamental setting of our suggested aggregation scheme so the system is UF-S-SS-CMA secure in ROM on WSN. This is an extension of our new online/offline subtree-based short signature scheme using Chebyshev chaotic maps under fuzzy user data sharing over Galois field presented in Section 3. In the single-hop scenario, we know the objective of the online/offline subtree-based short signature scheme (see the execution system in Fig.3) is for each sensor hub to be able to sign messages using its private key so the messages are under proper security protection.

We expect the base station to produce the parameters for the scheme to be embedded in each sensor node. Also, we assume that either the base station or the sensor nodes themselves can check the signatures generated by the sensor nodes. As in the general WSN scenario, it is assumed that

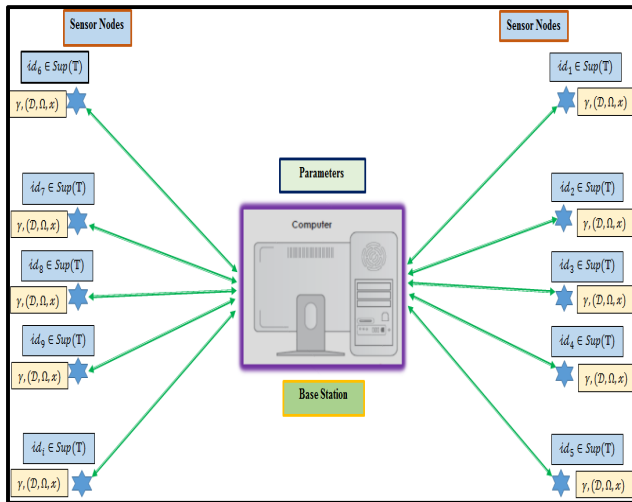


FIGURE 3. Overview of system implementation.

the base station is efficient enough to perform computationally exhaustive cryptographic operations. The sensor nodes, on the other hand, will have restricted computational power, memory, and electricity backup. We also expect the base station's secret key to be securely installed.

VIII. CONCLUSION

In this article, we have proposed an efficient, secure online/offline subtree-based short signature scheme using Chebyshev chaotic maps for WSN under fuzzy user data sharing over Galois field. Our new design does not require a certificate attached to the signature for confirmation, and there is no pairing operation involved either in the signature generation phase or in the verification phase. It is secure in the random oracle model with unforgeability under chosen message attack (UF-SSS-CMA-secure). Our new scheme provides multi-time use of offline storage, enabling the signer to reuse the offline pre-info in polynomial time as opposed to the single attempt inconvenience in most other online/offline signature schemes. In our new scheme, a pre-registration procedure can be done with a private key, and then no private key is required in the offline phase. In such a design, we only need the least operations in each procedure. This is a notably desirable feature for wireless sensor network applications, for this way the offline information in the setup or configuration stage can be hard-coded to the sensor hub. Our performance analysis reveals that the proposed scheme has the lowest computational cost among competing schemes. Also, we have developed an aggregation system based on the proposed OOS-SSS for wireless sensor network settings. Similarly, in the offline phase the signer does not need to provide any private data. It can be implemented by PKG. Also we have shown how to extend the proposed system to allow a single user to register various messages and implement them on WSN. This is especially suitable for applications over large-scale networks. Clustering is an efficient, feasible way of improving WSN device efficiency. For future research, we

may propose secure and efficient data transmission protocols for clustered wireless sensor networks using proposed online/offline subtree-based short signature scheme using Chebyshev chaotic maps.

ACKNOWLEDGMENT

The authors would like to thank anonymous reviewers of the IEEE ACCESS JOURNAL for their careful and helpful comments.

REFERENCES

- [1] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO*, in Lecture Notes in Computer Science, vol. 196, 1984, pp. 47–53.
- [2] D. Liu and P. Ning, *Security for Wireless Sensor Networks*. Berlin, Germany: Springer, 2007.
- [3] K. Ren and W. Lou, *Communication Security in Wireless Sensor Networks*. Worcester, MA, USA: Worcester Polytechnic Institute, 2007.
- [4] M. Ge, K.-K.-R. Choo, H. Wu, and Y. Yu, "Survey on key revocation mechanisms in wireless sensor networks," *J. Netw. Comput. Appl.*, vol. 63, pp. 24–38, Mar. 2016.
- [5] M. Luk, A. Perrig, and B. Whillock, "Seven cardinal properties of sensor network broadcast authentication," in *Proc. 4th ACM Workshop Secur. Ad Hoc Sensor Netw. (SASN)*, 2006, pp. 147–156.
- [6] K. Grover and A. Lim, "A survey of broadcast authentication schemes for wireless networks," *Ad Hoc Netw.*, vol. 24, pp. 288–316, Jan. 2015.
- [7] A. Aburumman and K.-K.-R. Choo, "A domain-based multi-cluster SIP solution for mobile ad hoc network," in *Proc. Int. Conf. Secur. Privacy Commun. Netw.*, 2014, pp. 267–281.
- [8] A. Aburumman, W. J. Seo, R. Islam, M. K. Khan, and K.-K.-R. Choo, "A secure cross-domain SIP solution for mobile ad hoc network using dynamic clustering," in *Proc. Int. Conf. Secur. Privacy Commun. Netw.*, 2015, pp. 649–664.
- [9] J. Nam, K.-K.-R. Choo, S. Han, M. Kim, J. Paik, and D. Won, "Efficient and anonymous two-factor user authentication in wireless sensor networks: Achieving user anonymity with lightweight sensor computation," *PLoS ONE*, vol. 10, no. 4, 2015, Art. no. e0116709.
- [10] P. Zeng, Z. Cao, K.-K.-R. Choo, and S. Wang, "Security weakness in a dynamic program update protocol for wireless sensor networks," *IEEE Commun. Lett.*, vol. 13, no. 6, pp. 426–428, Jun. 2009.
- [11] P. Zeng, K.-K. Choo, and D.-Z. Sun, "On the security of an enhanced novel access control protocol for wireless sensor networks," *IEEE Trans. Consum. Electron.*, vol. 56, no. 2, pp. 566–569, May 2010.
- [12] 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.
- [13] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, 3rd Quart., 2001.
- [14] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," in *Proc. CRYPTO*, in Lecture Notes in Computer Science, vol. 2442. New York, NY, USA: Springer, 1989, pp. 263–277.
- [15] A. Shamir and Y. Tauman, "Improved Online/Offline signature schemes," in *Proc. CRYPTO*, in Lecture Notes in Computer Science, vol. 2139. Berlin, Germany: Springer, 2001, pp. 355–367.
- [16] K. Kurosawa and K. Schmidt-Samoa, "New Online/Offline signature schemes without random oracles," in *Proc. PKC*, in Lecture Notes in Computer Science, vol. 3958. Berlin, Germany: Springer, 2006, pp. 330–346.
- [17] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic baker maps," *Chaos, Solitons Fractals*, vol. 31, no. 3, pp. 571–579, Feb. 2007.
- [18] M. Joye, "An efficient On-Line/Off-Line signature scheme without random oracles," in *Proc. CANS*, in Lecture Notes in Computer Science, vol. 5339. Berlin, Germany: Springer, 2008, pp. 98–107.
- [19] 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, Apr. 2008.
- [20] 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.
- [21] F. Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in Cryptography* (Lecture Notes in Computer Science), vol. 2595. Berlin, Germany: Springer, 2003, pp. 310–324.

- [22] J. Herranz, "Deterministic identity-based signatures for partial aggregation," *Comput. J.*, vol. 49, no. 3, pp. 322–330, 2005.
- [23] B. Kang, C. Boyd, and E. Dawson, "A novel identity-based strong designated verifier signature scheme," *J. Syst. Softw.*, vol. 82, no. 2, pp. 270–273, Feb. 2009.
- [24] S. D. Selvi, V. Sree, and C. P. Rangan, "Identity-based deterministic signature scheme without forking-lemma," in *Advances in Information and Computer Security (Lecture Notes in Computer Science)*, vol. 7038. Berlin, Germany: Springer, 2011, pp. 79–95.
- [25] D. Galindo and F. D. Garcia, "A Schnorr-like lightweight identity-based signature scheme," in *Progress in Cryptology—AFRICACRYPT (Lecture Notes in Computer Science)*, vol. 5580. Berlin, Germany: Springer, 2009, pp. 135–148.
- [26] S. Xu, Y. Mu, and W. Susilo, "Online/Offline signatures and multisignatures for AODV and DSR routing security," in *Proc. ACISP*, in Lecture Notes in Computer Science, vol. 4058. Berlin, Germany: Springer, 2006, pp. 99–110.
- [27] F. Li, M. Shirase, and T. Takagi, "On the security of online/offline signatures and multisignatures from ACISP'06," in *Proc. CANS*, in Lecture Notes in Computer Science, vol. 5339. Berlin, Germany: Springer, 2008, pp. 108–119.
- [28] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 48, no. 12, pp. 1498–1509, Dec. 2001.
- [29] K. W. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," *Phys. Lett. A*, vol. 298, no. 4, pp. 238–242, Jun. 2002.
- [30] 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, Jul. 2004.
- [31] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, Nov. 2010.
- [32] L. J. Sheu, "A speech encryption using fractional chaotic systems," *Nonlinear Dyn.*, vol. 65, nos. 1–2, pp. 103–108, Jul. 2011.
- [33] X. Wang, X. Wang, J. Zhao, and Z. Zhang, "Chaotic encryption algorithm based on alternant of stream cipher and block cipher," *Nonlinear Dyn.*, vol. 63, no. 4, pp. 587–597, Mar. 2011.
- [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, May 2010.
- [35] D. Xiao, F. Y. Shih, and X. Liao, "A chaos-based hash function with both modification detection and localization capabilities," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 9, pp. 2254–2261, Sep. 2010.
- [36] 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, Jul. 2009.
- [37] C. C. Lee, C. L. Chen, C. Y. Wu, and S. Y. Huang, "An extended chaotic maps-based key agreement scheme with user anonymity," *Nonlinear Dyn.*, vol. 69, nos. 1–2, pp. 79–87, 2012.
- [38] C.-C. Lee and C.-W. Hsu, "A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps," *Nonlinear Dyn.*, vol. 71, nos. 1–2, pp. 201–211, Jan. 2013.
- [39] C.-C. Lee, C.-T. Li, S.-T. Chiu, and Y.-M. Lai, "A new three-party-authenticated key agreement scheme based on chaotic maps without password table," *Nonlinear Dyn.*, vol. 79, no. 4, pp. 2485–2495, Mar. 2015.
- [40] C.-C. Lee, D.-C. Lou, C.-T. Li, and C.-W. Hsu, "An extended chaotic-maps-based protocol with key agreement for multiserver environments," *Nonlinear Dyn.*, vol. 76, no. 1, pp. 853–866, Apr. 2014.
- [41] Y.-M. Lai, P.-J. Cheng, C.-C. Lee, and C.-Y. Ku, "A new ticket-based authentication mechanism for fast handover in mesh network," *PLoS ONE*, vol. 11, no. 5, 2016, Art. no. e0155064.
- [42] C. C. Lee, C. T. Li, and C. W. Hsu, "A three-party password-based authenticated key exchange scheme with user anonymity using extended chaotic maps," *Nonlinear Dyn.*, vol. 73, nos. 1–2, pp. 125–132, 2013.
- [43] C.-C. Lee, C.-W. Hsu, Y.-M. Lai, and A. Vasilakos, "An enhanced mobile-healthcare emergency system based on extended chaotic maps," *J. Med. Syst.*, vol. 37, no. 5, p. 9973, Oct. 2013.
- [44] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems," *J. Med. Syst.*, vol. 38, no. 9, p. 77, Sep. 2014.
- [45] 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, Nov. 2016.
- [46] K. Chain and W. C. Kuo, "A new digital signature scheme based on chaotic maps," *Nonlinear Dyn.*, vol. 74, pp. 1003–1012, Dec. 2013.
- [47] C. Meshram, C.-C. Lee, C.-T. Li, and C.-L. Chen, "A secure key authentication scheme for cryptosystems based on GDLF and IFP," *Soft Comput.*, vol. 21, no. 24, pp. 7285–7291, Dec. 2017.
- [48] C. Meshram, S. A. Meshram, and M. Zhang, "An ID-based cryptographic mechanisms based on GDLF and IFP," *Inf. Process. Lett.*, vol. 112, no. 19, pp. 753–758, Oct. 2012.
- [49] C. Meshram and S. A. Meshram, "An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem," *Inf. Process. Lett.*, vol. 113, nos. 10–11, pp. 375–380, May 2013.
- [50] C. Meshram, "An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem," *Inf. Process. Lett.*, vol. 115, no. 2, pp. 351–358, Feb. 2015.
- [51] C. Meshram, "An efficient ID-based beta cryptosystem," *Int. J. Secur. Appl.*, vol. 9, no. 2, pp. 189–202, 2015.
- [52] C. Meshram and M. S. Obaidat, "An ID-based quadratic-exponentiation randomized cryptographic scheme," in *Proc. Int. Conf. Comput., Inf. Telecommun. Syst. (CITS)*, Jul. 2015, pp. 1–5.
- [53] C. Y. Meshram, P. L. Powar, M. S. Obaidat, and C.-C. Lee, "An IBE technique using partial discrete logarithm," *Procedia Comput. Sci.*, vol. 93, pp. 735–741, Jan. 2016.
- [54] C. Meshram and P. L. Powar, "An efficient identity-based QER cryptographic scheme," *Complex Intell. Syst.*, vol. 2, no. 4, pp. 285–291, Dec. 2016.
- [55] 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, Jan. 2016.
- [56] 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.
- [57] 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, 2019.
- [58] 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 Netw.*, vol. 7, no. 6, pp. 363–367, Nov. 2018.
- [59] 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.
- [60] M. Asadi, C. Zimmerman, and A. Agah, "A gametheoretic approach to security and power conservation in wireless sensor networks," *Int. J. Netw. Secur.*, vol. 15, no. 1, pp. 50–58, 2013.
- [61] T. H. Feng, W. T. Li, and M. S. Hwang, "A false data report filtering scheme in wireless sensor networks: As Survey," *Int. J. Netw. Secur.*, vol. 17, no. 3, pp. 229–236, 2015.
- [62] T. H. Feng, N. Y. Shih, and M. S. Hwang, "A safety review on fuzzy-based relay selection in wireless sensor networks," *Int. J. Netw. Secur.*, vol. 17, no. 6, pp. 712–721, 2015.
- [63] W. T. Li, T. H. Feng, and M. S. Hwang, "Distributed detecting node replication attacks in wireless sensor networks: A survey," *Int. J. Netw. Secur.*, vol. 16, no. 5, pp. 323–330, 2014.
- [64] Y. B. Saied and A. Olivereau, "A lightweight threat detection system for industrial wireless sensor networks," *Int. J. Netw. Secur.*, vol. 18, no. 5, pp. 842–854, 2016.
- [65] H. Saini, "1-2 skip list approach for efficient security checks in wireless mesh networks," *Int. J. Electron. Inf. Eng.*, vol. 1, no. 1, pp. 9–15, 2014.
- [66] P. Kumar, S. Kumari, V. Sharma, X. Li, A. K. Sangaiah, and S. H. Islam, "Secure CLS and CL-AS schemes designed for VANETs," *J. Supercomput.*, vol. 75, no. 6, pp. 3076–3098, Jun. 2019.
- [67] 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.
- [68] C. Meshram, C.-C. Lee, A. S. Ranadive, C.-T. Li, S. G. Meshram, and J. V. Temburne, "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, May 2020, Art. no. e4307, doi: 10.1002/dac.4307.

- [69] W. Liu, J. Liu, Q. Wu, B. Qin, D. Naccache, and H. Ferradi, "Efficient subtree-based encryption for fuzzy-entropy data sharing," *Soft Comput.*, vol. 22, no. 23, pp. 7961–7976, Dec. 2018.
- [70] C. Meshram, C.-C. Lee, S. G. Meshram, and M. K. Khan, "An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment," *Soft Comput.*, vol. 23, no. 24, pp. 13127–13138, Dec. 2019, doi: [10.1007/s00500-019-03855-1](https://doi.org/10.1007/s00500-019-03855-1).
- [71] C. Meshram, M. S. Obaidat, and S. G. Meshram, "Chebyshev chaotic map-based ID-based cryptographic model using subtree and fuzzy-entropy data sharing for public key cryptography," *Secur. Privacy*, vol. 1, no. 1, p. e12, Jan. 2018.
- [72] R. M. Campello De Souza, H. M. de Oliveira, A. N. Kauffman, and A. J. A. Paschoal, "Trigonometry in finite fields and a new Hartley transform," in *Proc. IEEE Int. Symp. Inf. Theory*, vol. 293, Aug. 1998, p. 293.
- [73] J. B. Lima, D. Panariob, and R. M. Campello de Souza, "Public-key encryption based on Chebyshev polynomials over GF(q)," *Inf. Process. Lett.*, vol. 111, pp. 51–56, Dec. 2010.
- [74] J. B. Lima, R. M. Campello de Souza, and D. Panario, "Security of public-key cryptosystems based on chebyshev polynomials over prime finite fields," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2008, pp. 1843–1847.
- [75] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*. Boca Raton, FL, USA: CRC Press, 2003.
- [76] S. Han and E. Chang, "Chaotic map based key agreement with/out clock synchronization," *Chaos, Solitons Fractals*, vol. 39, no. 3, pp. 1283–1289, Feb. 2009.
- [77] M. Bellare, C. Namprempe, and G. Neven, "Security proofs for identity-based identification and signature schemes," *J. Cryptol.*, vol. 22, no. 1, pp. 1–61, Jan. 2009.
- [78] J. Kar, "Provably secure online/off-line identity-based signature scheme for wireless sensor network," *Int. J. Netw. Secur.*, vol. 16, no. 1, pp. 29–39, 2014.
- [79] J. C. Choon and J. Hee Cheon, "An identity-based signature from gap Diffie-Hellman groups," in *Proc. PKC*, in Lecture Notes in Computer Science, vol. 2567. Berlin, Germany: Springer, 2003, pp. 18–30.
- [80] L. C. Guillou and J.-J. Quisquater, "A 'paradoxical identity-based signature scheme resulting from zero-knowledge,'" in *Proc. CRYPTO*, in Lecture Notes in Computer Science, vol. 403. Berlin, Germany: Springer, 1990, pp. 216–231.



CHANDRASHEKHAR MESHARAM 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 a Research in mathematics, Jaywanti Haksar Government Post Graduation College, College of Chhindwara University, Betul, India. He has published more than 95 scientific

articles on the above research fields in international journals and conferences. His research interested in the field of cryptography and its application, neural networks, the IoT, medical information systems, ad hoc networks, number theory, time series analysis and climate change, mathematical modeling and chaos theory. He is a member of IAENG, Hong Kong, WASET, New Zealand, CSTA, USA, ACM, USA, IACSIT, Singapore, EATCS, Greece, IAROR, The Netherland, EAI, ILAS, Haifa, Israel, the Science and Engineering Institute (SCIEI), Machine Intelligence Research Labs (MIR Labs), USA, Society: Intelligent Systems, the KES International Association, U.K., the Universal Association of Computer and Electronics Engineers (UACEE), The Society of Digital Information and Wireless Communications (SDIWC), and a Life-time member of the Internet Society (ISOC), USA, the Indian Mathematical Society and Cryptology Research Society of India. He is a regular Reviewer of 60 international journals and international conferences.



CHENG-CHI LEE (Member, IEEE) received the Ph.D. degree in computer science from National Chung Hsing University (NCHU), Taiwan, in 2007. He is currently a Professor with the Department of Library and Information Science, Fu Jen Catholic University. His current research interests include data security, cryptography, network security, mobile communications and computing, and wireless communications. He has published more than 200 scientific articles on the

above research fields in international journals and conferences. He is a member of the Chinese Cryptology and Information Security Association (CCISA), the Library Association of The Republic of China, and the ROC Phi Tau Phi Scholastic Honor Society. He is also as an Editorial Board Member of the *International Journal of Network Security*, the *Journal of Computer Science, Cryptography*, the *International Journal of Internet Technology and Secured Transactions*, and *The Open Automation and Control Systems Journal*. He has also served as a Reviewer in many SCI-index journals, other journals, other conferences.



SARITA GAJBHIYE MESHARAM received the M.Tech. degree in soil and water engineering from the College of Agricultural Engineering, Jawaharlal Nehru Krishi Vishwa Vidhyalaya, Jabalpur, in 2009, and the Ph.D. degree in water resource development and management from IIT Roorkee, (U.K.) India, in 2015. She is currently a Dr. D. S. Kothari Postdoctoral Fellow with the Department of Mathematics and Computer Sciences, Rani Durgawati University, Jabalpur, India.

She is also associated as a Research Faculty with the Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam, where she is also with the Faculty of Environment and Labour Safety. Her current research interests include geographical information systems, rainfall-runoff sediment yield modeling, and SCS-CN. She is also carrying out her research work in the field of rainfall-runoff, sediment yield, water quality, application of RS and GIS water networks, and cryptographic protocol. She has published more than 80 research articles in refereed journals, conference and workshop proceedings, and books. She is a member of some international society and a Reviewer of the reputed journal. She received the Gold Medal, for her M.Tech. degree.



AKSHAYKUMAR MESHARAM is currently an Assistant Professor with the Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering, India. His current research interests include cryptography, network security, soft computing, and wireless communications. He has published more than ten scientific articles on the above research fields in international journals and conferences.

...