Hindawi
Complexity
Volume 2022, Article ID 6302328, 11 pages
https://doi.org/10.1155/2022/6302328

WILEY | Hindawi

Research Article

An Efficient Conformable Fractional Chaotic Map-Based Online/Offline IBSS Scheme for Provable Security in ROM

Chandrashekhar Meshram,[1] **Rabha W. Ibrahim**,[2] **and Rafida M. Elobaid**[3]

[1]*Department of Post Graduate Studies and Research, Mathematics, Jaywanti Haksar Government Post Graduation College, College of Chhindwara University, Betul 480001, India*
[2]*The Institute of Electrical and Electronics Engineers (IEEE) 94086547, Portland, USA*
[3]*Deanship of Educational Service, Price Sultan University, Riyadh, Saudi Arabia*

Correspondence should be addressed to Rafida M. Elobaid; robaid@psu.edu.sa

Received 11 February 2020; Revised 19 November 2021; Accepted 25 January 2022; Published 31 March 2022

Academic Editor: Honglei Xu

Chaos distributes with a covert method to condense the dynamic of complexity and satisfies the security requirements of a cryptographic system. This study gives an ability online/offline (O/O) ID-based short signature (IBSS) scheme using conformable fractional chaotic maps. Furthermore, we establish its security under IBSS existential unforgeability of identity-based short signature (IBSS) under chosen message attack (EUF-IBSS-CMA) in the random oracle model (ROM). Some of the stimulating preparations of obtainable processes are that they give a multiperiod application of the offline storage, which licenses the agent to recycle the offline pre-registered data in time series (especially the polynomial time), rather than one-period usage in all past IBSS processes.

1. Introduction

Newly, the time-fractional difference [1] provides a robust concept for discrete (not continuous) fractional display. It has a limited fractional alteration formula, which rests on the change consequences of all the past figurines. This attribute can show the disconnected arrangements long historical properties or long interactions. In the meantime, chaos definitions, formulas, ideas, and chaos synchronization have wide uses [2–5]. Discrete maps can produce chaotic signatures. Therefore, they rewarded much care in all areas of mathematical sciences. The logistic map idea (is a well-known repeated record founded on the first-order nonlinear alteration equation) and other types of maps have converted straightforward representations. Nevertheless, fewer works utilized the fractional discrete arrangements, which clamp compound chaotic dynamics. This action presents the disconnected memory, which occurs in the chaotic records. Then, chaos and harmonization of the fractional logistic record are specified. The diverse fractional powers yield different chaotic ranges so that the chaotic activities will take extra problematical [6, 7]. Discrete maps are used regularly in disconnected natural phenomena. The standing fractional disconnected arrangements (equations, inequalities, and inclusions) are typically joined with two techniques: mathematical discretization (the process of changing continuous functions, simulations, variables, and equations into discrete complements) of time-fractional differential equations and fractional time-difference equations. The former one is a numerical formulation of fractional continuous simulations and the Grünwald–Letnikov difference usually accepted in the numerical action. In this study, we shall use the fractional Caputo difference operator. Our aim is to use a new fractional calculus, called fractional conformable calculus, to generalize the Chebyshev polynomials [8].

The inquiry into chaotic constructions and their possible cryptographic structures has been the subject of considerable interest in research over the past few years. Chaotic systems are clearly characterized by their delicate reliance on the initial conditions and random surrounding operations, both

of which are fundamentally similar to the behavior of some cryptographic primitives [9]. Even et al. [10] introduced the concept of the O/O sign in 1989. In an O/O system, a message signing is broken into two phases with (i) more computational and time-consuming phase being executed offline in advance and (ii) much faster phase being conducted online at the point of signing the message. Even et al. created a general construction that could turn any digital signature scheme into an O/O sign structure [10]; nevertheless, the system is not very practical as it lengthens a quadratic variable in each signature. Instead, in 2001, as a response to the impracticality of Even et al.'s 1989 scheme, Shamir and Tauman [11] introduced a new theoretical idea called "hash-sign-switch" to more effectively transform any signature scheme into an O/O sign structure. This hash-sign-switch process converts signature schemes into O/O sign operations irrespective of the types as a generalized tool. In order to address certain types of signature schemes specialized in specific applications, some researchers have proposed their own designs [12–16], among which [15] is the most efficient [16], while the work of Kurosawa and Schmidt-Samoa included the possibility of creating O/O sign operations without random oracles [12]. Nonetheless, all the above schemes concentrated on the public-key-based standard setting without participating in identity-based settings. Several identities-based sign structures using pairing have been published in [17–20] since about a decade ago. On the other hand, for a discrete log setting that does not require pairing, Galindo and Garcia [21] adapted Schnorr's sign to construct an identity-based sign structure. Xu et al. [22] imposed an idea of O/O-IBSs and multisign in 2006. Xu et al. proposed the *O*=*O* IBS sign structure and then transformed it to O/O-ID-based multisign structure. Xu et al.'s [22] sign structure can be extended to different routing protocols using the pairing technique. Later on, however, Li et al. [23] showed that the sign structure of Xu et al. [22] was in fact weak against the attack on the forgery and thus deficient in security. In addition, a truly secure O/O–IBSS scheme has yet to be found in the relevant literature. On the other hand, since the 1990s [9, 24, 25], chaotic cryptography has been used in the development of secure communication techniques. Chaotic records are now essential for different methods of symmetric encryption [26–30], hash functions [31, 32], and S-boxes [33]. Recently, numerous chaotic methods were released on key convention models [34–38], authentication protocols [39, 40], and telecommute medicine information systems [41–43].

As given above, we suggest the well-organized conformable chaotic map (CCM)-based O/O–IBSS arrangement. The existing scheme allows the reusability of the offline data. Consequently, the agent is not dynamic to device the offline technique-assigning stopping when he/she requests to indicate other communication. In addition, in view of circumstances, such as an extensive section of the present O/O signs (non-ID-based), an obtainable offline passing scheme does not require any private signer information [44–58]. Thus, some favorite associates covering the private key group (PKG) can build it. A new ID-based setting requires no approval of confirmation attached to the sign, which is displayed in ROM. The suggested O/O–IBSS structure is locked when the selected communication occurs in the logic of the ability of IBSS, assuming that the CCM theory grips in the ROM with less ranked cost [56–58].

Recently, Meshram et al. [59] developed a subtree-centric paradigm for cryptosystems in cloud-based environments using chaotic maps. Meshram et al. [58] also used chaos theory to develop a level online/offline subtree-based short signature framework that is both efficient and secure. A new chaotic system with the hyperbolic sinusoidal function was presented by Mobayen et al. [60]. This chaotic system introduces a novel type of chaotic flow that allows for a better understanding of chaotic attractors. In the presence of external disturbances and Lipchitz nonlinearities, Karami et al. [61] developed the observer-based state feedback stabiliser design for a class of chaotic systems. For the robust synchronization of uncertain delayed chaotic systems, Mofid et al. [62] developed the disturbance observer-based Sliding mode control (SMC) scheme. More studies can be located in [63–66].

We present a detailed literature review of the existing identity-based online/offline short signature schemes. Unfortunately, most schemes are built on difficult problems like the elliptic curve and pairing and pose huge computational and communication costs. It is also worth noting that most of the schemes have not been thoroughly tested with Scyther, AVISPA, and other high-end security validation tools. As a result, small devices with limited processing resources find it difficult to manage such schemes.

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

(i) Under the security of the random oracle model, we propose a secure and efficient conformable fractional chaotic map-based online/offline identity-based short signature scheme.

(ii) The proposed scheme is secure with unforgeability under chosen message attack (UF-IBSS-CMA) in the random oracle model.

(iii) Unlike past identity-based online/offline signature schemes, the proposed scheme's design allows the signer to enter the offline storage numerous times to reuse the offline preinformation in polynomial time.

(iv) The presented scheme has the lowest computational cost amid six competing schemes.

(v) The proposed scheme is a separated signing method that does not call all types of secluded key data. It can be recorded by an insulated key group with offline data equally being employed. It consistently assumes the very slightest process in every practice.

(vi) The proposed scheme is an astonishing promising model in wireless sensor network circumstances as the detached data may be complex-inserted into the sensor hub in the collecting or procedure position.

The article is organized as follows: Materials and Methods involve essential mathematical initiations offered in Section 2. Section 3 deals with the results, including the

O/O–IBSS by using CCM. Security examination and other discussion can be seen in Section 4. Finally, Section 5 concludes the suggested algorithm.

2. Materials and Methods

In the analysis of arbitrary calculus, a part of the major experiments is to discover appropriate algorithms, which are correctly given by difference derivatives with the history of this measure. The Chebyshev polynomials are one of the greatest valuable polynomials, which are appropriate in numerical analysis comprising polynomial approximation. We briefly explain the fractional Chebyshev polynomial-2 (second type), generalize chaotic records, and develop it as a sector of the suggested technique, correspondingly.

2.1. Chebyshev Polynomials-2. Chebyshev polynomials-2 of degree n on the interval $[-1, 1]$ is formulated in terms of $\sin\vartheta$, $\vartheta = arccos(t)$.

$$\Upsilon_n(t) = \frac{\sin(n+1)\vartheta}{\sin(\vartheta)}, \ \vartheta \in [0, \pi]. \tag{1}$$

This satisfies (see Figure 1)

$$\begin{aligned} &\Upsilon_0(t) = 1 \\ &\Upsilon_1(t) = 2t \\ &\quad \vdots \\ &\Upsilon_n(t) = 2t\Upsilon_{n-1}(t) - \Upsilon_{n-2}(t), \ n = 2, 3, \ldots \end{aligned} \tag{2}$$

The polynomials of the second type fulfill

$$\Upsilon_{n-1}(\cos\vartheta) \cdot \sin\theta = \sin n\vartheta, \tag{3}$$

or

$$\Upsilon_n(\cos\vartheta) = \frac{\sin((n+1)\vartheta)}{\sin\vartheta}. \tag{4}$$

This is systemically likewise to the Dirichlet kernel:

$$\sigma_n(t) = \frac{\sin((2n+1)t/2)}{\sin t/2} = \Upsilon_{2n}\left(\cos\frac{t}{2}\right). \tag{5}$$

The polynomials Υ_n are orthogonal on $[-1,1]$ connecting with the inner products:

$$\left(\Upsilon_n(t), \Upsilon_q(t)\right) = \int_{-1}^{1} \Upsilon_n(t)\Upsilon_q(t)\left(\sqrt{1-t^2}\right)\mathrm{d}t = \frac{\pi}{2}\delta_{nq}, \tag{6}$$

where $\sqrt{1-t^2}$ is the weight function and δ_{nq} is the well-known Kronecker function. The analytic representation takes the following summation:

$$\Upsilon_n(t) = \sum_{m=0}^{[n/2]} (-1)^m \frac{\Gamma(n-m+1)2^{n-2m}}{\Gamma(n-2m+1)\Gamma(m+1)} t^{n-2m}, \tag{7}$$

where $[n/2]$ is the integer part of $n/2$. And the first derivative is

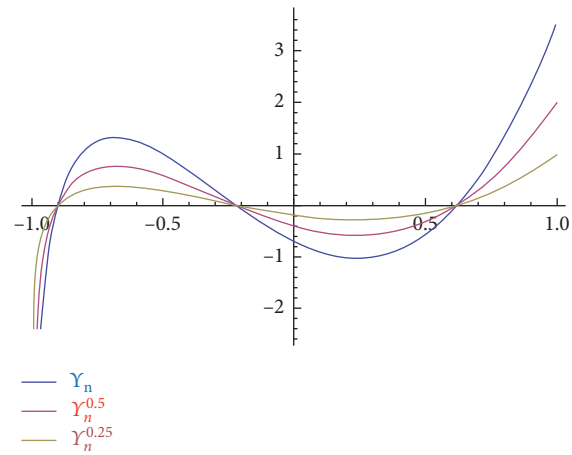

FIGURE 1: CCP for different values of ν and $\kappa_1(\nu,t) = (1-\nu)/\Gamma(\nu+1), \kappa_0(\nu,t) = \nu/\Gamma(\nu+1)$. It pretenses to the historical illustrations for $\Upsilon_n(t)$ (see [67]).

$$D\Upsilon_n(t) \coloneqq \Upsilon_n'(t) = 2\sum_{m=0}^{n-1}(m+1)\Upsilon_m(t). \tag{8}$$

As a special case (shifted second-type Chebyshev polynomial), when the variable is $2t-1$, we have the following formula:

$$\begin{aligned} \Upsilon_n(2t-1) &\coloneqq \Upsilon_n^*(t) \\ &= 2(2t-1)\Upsilon_{n-1}^*(t) - \Upsilon_{n-2}^*(t), \\ n &= 2, 3, \ldots. \end{aligned} \tag{9}$$

with $\Upsilon_0^*(t) = 1$ and $\Upsilon_1^*(t) = 2(2t-1)$. Moreover, it achieves the analytic representation formula:

$$\Upsilon_n^*(t) = \sum_{m=0}^{n} (-1)^m \frac{\Gamma(2n-m+2)2^{2n-2m}}{\Gamma(m+1)\Gamma(2n-m+2)} t^{n-m}. \tag{10}$$

Clearly, $\Upsilon_n^*(0) = (-1)^n$ and $\Upsilon_n^*(1) = 2$. In addition, the orthogonal representation is of the following form:

$$\left(\Upsilon_n^*(t), \Upsilon_q^*(t)\right) = \int_0^1 \Upsilon_n^*(t)\Upsilon_q^*(t)\left(\sqrt{t-t^2}\right)\mathrm{d}t = \frac{\pi}{8}\delta_{nq}. \tag{11}$$

The first derivative of the shifted second-type Chebyshev polynomial is given by [8]

$$D\Upsilon_n^*(t) \coloneqq \Upsilon_n^{*\prime} = 4\sum_{m=0}^{n-1}(m+1)\Upsilon_m^*(t). \tag{12}$$

2.2. Conformable Calculus. Recently, connected to the arbitrary calculus field, Khalil et al. [44] formulated a "conformable fractional derivative" definition of a given real-valued function ϕ: $[0,\infty) \longrightarrow \mathbb{R}$ as follows:

$$\mathscr{D}^{\nu}[\phi(t)] = \lim_{\epsilon \longrightarrow 0} \frac{\phi\left(t + \epsilon t^{1-\nu}\right) - \phi(t)}{\epsilon}, \tag{13}$$

for all $t > 0$ and a fractional power $\nu \in (0, 1)$. If ϕ is ν-differentiated in the interval $(0, \varrho), \varrho > 0$ and $lim_{t \longrightarrow 0^+} \phi^{\nu}(t)$ occurs and then $\phi^{\nu}(0) = lim_{x \longrightarrow 0^+} \phi^{\nu}(t)$ is introduced.

More generalization criteria for differential operators to be a real-valued conformable fractional derivative was recently proposed by Anderson and Ulness (see [45]).

Definition 1. Conformable differential operator.

Let ν be a fractional power, such that $\nu \in [0, 1]$. A differential functional $\mathscr{D}^{\nu}$ is called conformable $\Leftrightarrow \mathscr{D}^0$ is the identity function and $\mathscr{D}^1$ is the ordinary derivative function. Particularly, $\mathscr{D}^{\nu}$ is conformable $\Leftrightarrow$ for differentiable function $\phi(t)$.

$$\begin{aligned} \mathscr{D}^0 \phi(t) &= \phi(t) \text{ and} \\ \mathscr{D}^1 \phi(t) &= \frac{\mathrm{d}}{\mathrm{d}t} \phi(t) \\ &= \phi\prime(t). \end{aligned} \tag{14}$$

In general, for two continuous functions $\kappa_0, \kappa_1 \colon [0, 1] \times \mathbb{R} \longrightarrow (0, \infty)$, we obtain

$$\mathscr{D}^{\nu} \phi(t) = \kappa_1(\nu, t) \phi(t) + \kappa_0(\nu, t) \phi\prime(t), \tag{15}$$

such that $\kappa_1(\nu, t) \neq -(\kappa_0(\nu, t))$,

$$\begin{aligned} \lim_{\nu \longrightarrow 0} \kappa_1(\nu, t) &= 1, \\ \lim_{\nu \longrightarrow 1} \kappa_1(\nu, t) &= 0, \\ \kappa_1(\nu, t) &\neq 0, \ \forall t, \ \nu \in (0, 1). \end{aligned} \tag{16}$$

$$\begin{aligned} \lim_{\nu \longrightarrow 0} \kappa_0(\nu, t) &= 0, \\ \lim_{\nu \longrightarrow 1} \kappa_0(\nu, t) &= 1, \\ \kappa_0(\nu, t) &\neq 0, \ \forall t, \ \nu \in (0, 1). \end{aligned} \tag{17}$$

In [46], the authors noted that in the theory of control systems, a comparative controller for supervisory result μ at the variable t with two correction factors has the following process:

$$\mu(t) = \kappa_p \Xi(t) + \kappa_d \frac{\mathrm{d}}{\mathrm{d}t} \Xi(t), \tag{18}$$

where κ_p is the comparative gain, κ_d is the changing gain, and Ξ is the slip between the formal variable and the practice variable.

2.3. Conformable Chebyshev Polynomials-2 (CCP). In this section, we employ the concept of conformable derivative to obtain the CCP (of the second type). By using equations (1) and (3) in (8), we have the following CCP:

$$\mathscr{D}^{\nu} \Upsilon_n(t) = \kappa_1(\nu, t) \Upsilon_n(t) + \kappa_0(\nu, t) \Upsilon_n\prime(t). \tag{19}$$

Moreover, the shifted CCP can be formulated by applying (5) and (6) in (8) to obtain

$$\mathscr{D}^{\nu} \Upsilon_n^*(t) = \kappa_1(\nu, t) \Upsilon_n^*(t) + \kappa_0(\nu, t) \Upsilon_n^{*\prime}(t), \tag{20}$$

where κ_1 and κ_0 are given in Definition 1. In our discussion, we shall select one of the following formulas of κ_1 and κ_0:

$$\begin{aligned} \kappa_1(\nu, t) &= (1 - \nu) t^{\nu}, \\ \kappa_0(\nu, t) &= \nu t^{1-\nu}, \ t \in (0, \infty), \\ \kappa_1(\nu, t) &= (1 - \nu) |t|^{\nu}, \\ \kappa_0(\nu, t) &= \nu |t|^{1-\nu}, \\ \kappa_1(\nu, t) &= \cos\left(\frac{\nu\pi}{2}\right) t^{\nu}, \\ \kappa_0(\nu, t) &= \sin\frac{\nu\pi}{2} t^{1-\nu}, \ t \in (0, \infty). \end{aligned} \tag{21}$$

Or,

$$\begin{aligned} \kappa_1(\nu, t) &= \cos\left(\frac{\nu\pi}{2}\right) |t|^{\nu}, \\ \kappa_0(\nu, t) &= \sin\frac{\nu\pi}{2} |t|^{1-\nu} t \in \mathbb{R}\{0\}. \end{aligned} \tag{22}$$

Furthermore, constant functions can be realized by using the gamma function as follows:

$$\begin{aligned} \kappa_1(\nu, t) &= \frac{(1 - \nu)}{\Gamma(\nu + 1)}, \\ \kappa_0(\nu, t) &= \frac{\nu}{\Gamma(\nu + 1)}. \end{aligned} \tag{23}$$

Obviously, for finite case $m = n - 1$ in relations (3) and (6), respectively, we have the qualities

$$\begin{aligned} \Upsilon_n\prime(t) &= 2n \Upsilon_{n-1}(t), \\ \Upsilon_n^{*\prime} &= 4n \Upsilon_{n-1}^*(t). \end{aligned} \tag{24}$$

Consequently, by utilizing the definition of $\mathscr{D}^{\nu} \Upsilon_n(t)$ and $\mathscr{D}^{\nu} \Upsilon_n^*(t)$, we have the CCP-2 and its shifted polynomial:

$$\mathscr{D}^{\nu} \Upsilon_n(t) = \kappa_1(\nu, t) \Upsilon_n(t) + 2n\gamma(t) \kappa_0(\nu, t) \Upsilon_{n-1}(t), \tag{25}$$

where

$$\underbrace{\gamma(t) = 1 + 2t + \left(4t^2 - 1\right) + 4t\left(2t^2 - 1\right) + \ldots +}_{(n-1)-\text{times}} \tag{26}$$

$$\mathscr{D}^{\nu} \Upsilon_n^*(t) = \kappa_1(\nu, t) \Upsilon_n^*(t) + 4n\gamma^*(t) \kappa_0(\nu, t) \Upsilon_{n-1}^*(t), \tag{27}$$

where

$$\underbrace{\gamma^*(t) = 1 + 2(2t - 1) + \ldots +}_{(n-1)-\text{times}}. \tag{28}$$

In the sequel, we put $\Upsilon^{(\nu)}(t) \coloneqq \mathscr{D}^{\nu} \Upsilon_n(t)$ and $\Upsilon^{*(\nu)}(t) \coloneqq \mathscr{D}^{\nu} \Upsilon_n^*(t)$. Then, we have the following constructions.

Proposition 1. *The CCP satisfies the following recurrent relations:*

$$\Upsilon_n^{(\nu)}(t) = \left[2t\kappa_1(\nu,t) + 2n\gamma(t)\kappa_0(\nu,t)\right]\Upsilon_{n-1}(t) - \kappa_1(\nu,t)\Upsilon_{n-2}(t). \tag{29}$$

$$\begin{aligned}\Upsilon_n^{*\,(\nu)}(t) &= \left[2\kappa_1(\nu,t)(2t-1) + 4n\gamma^*(t)\kappa_0(\nu,t)\right]\Upsilon_{n-1}^*(t)\\ &\quad - \kappa_1(\nu,t)\Upsilon_{n-2}^*(t).\end{aligned} \tag{30}$$

From (1) and (25), we conclude that

$$\begin{aligned}\Upsilon_n^{(\nu)}(t) &= \Upsilon_n(t)\kappa_1(\nu,t) + 2n\gamma(t)\kappa_0(\nu,t)\Upsilon_{n-1}(t)\\ &= \left[2t\Upsilon_{n-1}(t) - \Upsilon_{n-2}(t)\right]\kappa_1(\nu,t) + 2n\gamma(t)\kappa_0(\nu,t)\Upsilon_{n-1}(t)\\ &= 2\left[t\kappa_1(\nu,t) + n\gamma(t)\kappa_0(\nu,t)\right]\Upsilon_{n-1}(t) - \kappa_1(\nu,t)\Upsilon_{n-2}(t).\end{aligned} \tag{31}$$

Now, in view of (9) and (27), we obtain

$$\begin{aligned}\Upsilon_n^{*\,(\nu)}(t) &= \Upsilon_n^*(t)\kappa_1(\nu,t) + 4n\gamma^*(t)\kappa_0(\nu,t)\Upsilon_{n-1}^{\∗}(t)\\ &= \left[2(2t-1)\Upsilon_{n-1}^*(t) - \Upsilon_{n-2}^*(t)\right]\kappa_1(\nu,t) + 2n\gamma^*(t)\kappa_0(\nu,t)\Upsilon_{n-1}(t)\\ &= 2\left[\kappa_1(\nu,t)(2t-1) + 2n\gamma^*(t)\kappa_0(\nu,t)\right]\Upsilon_{n-1}^*(t) - \kappa_1(\nu,t)\Upsilon_{n-2}^*(t).\end{aligned} \tag{32}$$

Remark 1. It is clear that when $\nu \longrightarrow 0$, we have the original case that was proved in [47].

Proposition 2. *The semigroup possessions clamps for CCP positioned on interval* $(-\infty, \infty)$.

We take $T \coloneqq [t\kappa_1(\nu,t) + n\gamma(t)\kappa_0(\nu,t)]$, where $\nu \longrightarrow 0$ implies $T = t$ (the original case). From Proposition 1, we have

$$\Upsilon_{n+2}^{(\nu)}(t) = 2T\Upsilon_{n+1}(t) - \kappa_1\Upsilon_n(t). \tag{33}$$

The previous formula implies an alteration equation (disconnected equation) which has a typical formula

$$\lambda^2 - 2T\lambda + \kappa_1 = 0, \tag{34}$$

with the two roots $\lambda_{1,2} = T \pm \sqrt{T^2 - \kappa_1}$ satisfying $\lambda_1 + \lambda_2 = 2T$ and $\lambda_1\lambda_2 = \kappa_1$. Then, for a positive integer n, we obtain the conclusion

$$\begin{aligned}\Upsilon_n^{(\nu)}(t) &= \left(\lambda_1^n + \lambda_2^n\right)/2\\ &= \frac{\left(T - \sqrt{T^2 - \kappa_1}\right)^n + \left(T + \sqrt{T^2 - \kappa_1}\right)^n}{2}\\ &= \sum_{m=0}^{[n/2]} \binom{n}{m} T^{n-2m}\left(T^2 - \kappa_1\right)^m.\end{aligned} \tag{35}$$

Following the proof in [47] on the above summation, we obtain

$$\begin{aligned}\Upsilon_\ell^{(\nu)}\left(\Upsilon_\flat^{(\nu)}\right)(t) &= \frac{\left(\rho_1^\ell + \rho_2^\ell\right)}{2},\\ \rho_1 + \rho_2 &= 2\Upsilon_\flat^{(\nu)},\\ \rho_1\rho_2 &= \kappa_1.\end{aligned} \tag{36}$$

Then, in general, we obtain the following relation for positive integers ℓ and $\flat$:

$$\begin{aligned}\Upsilon_{\ell\flat}^{(\nu)}(t) &= \Upsilon_\ell^{(\nu)}\left(\Upsilon_\flat^{(\nu)}\right)(t)\\ &= \Upsilon_\flat^{(\nu)}\left(\Upsilon_\ell^{(\nu)}\right)(t)\,(\mathrm{mod}\,N),\end{aligned} \tag{37}$$

where N is large, as much as data set size.

Remark 2. It is clear that when $\nu \longrightarrow 0$, we have the main theorem (see Figure 1).

3. Proposed CCM-Based IBSS

In this section, we demonstrate an efficient conformable chaotic map (CCM) found by the online/offline IBSS method. It covers the supplementary five parts. Figure 2 depicts the proposed online/offline IBSS scheme's configuration.

3.1. Setup

(i) Pick out a large enough prime q_1 and general parameter $t \in Z_{q_1}^*$

(ii) Adopt a random parameter $a \leftarrow Z_{q_1}^*$ and infer $u \leftarrow \Upsilon_a^{(\nu)}(t)\,(\mathrm{mod}\,q_1)$

(iii) Opt a function $\hbar$ (chaotic hash function) such that $\hbar$ achieves $\hbar$: $\{0,1\}^\infty \longrightarrow Z_{q_1}^*$

(iv) The appearance of keys can be seen by the formal $(mpk = q_1, t, \hbar, u)$ (master public key) and $(msk = a)$ (master secret key)

3.2. Extract. Assumed customer an individuality $i\,d$, the PKG performs the following:

(i) Opts inordinate $k \leftarrow^R Z_{q_1}^*$

(ii) Assesses $A \leftarrow \Upsilon_k^{(\nu)}(t)\,(mo\ dq_1)$ and $v \leftarrow \hbar(A, i\,d)$

(iii) Considers $x \leftarrow (av * k)\,(mo\ dq_1)$

(iv) The specific key of mediators is obtainable by the ordered pair (A, x)

3.3. Offline Signing. Any agent that performs the uniting is shown in the following steps:

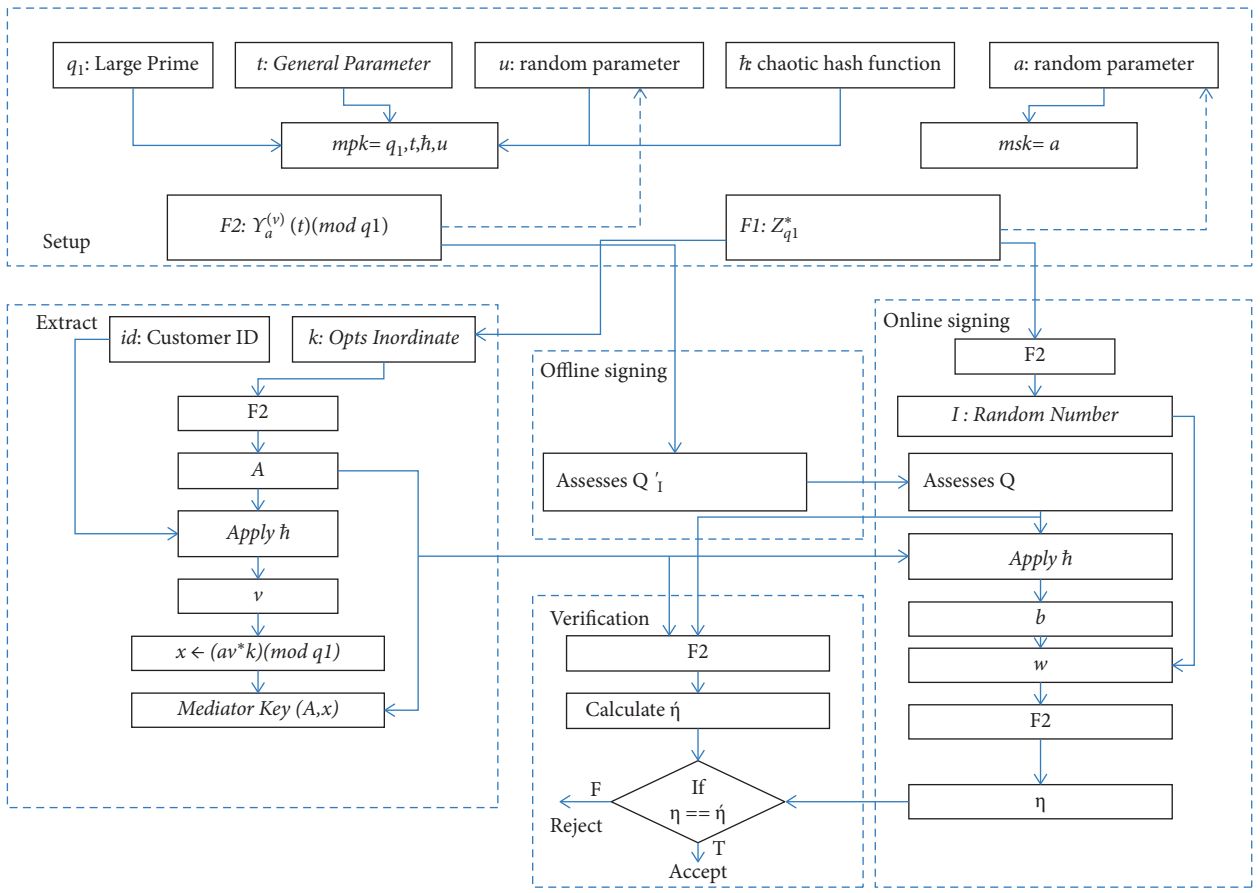

Figure 2: Block diagram of the proposed scheme.

Assesses $Q_i' \leftarrow \Upsilon_{2^i}^{(v)}(t)(mo\ dq_1),\ \forall i \in [0, q_1 - 1]$

3.4. Online Signing. In the recent step, to symbol a missive $M \in (-\infty, +\infty)$, tiring (A, x) the agent stays as occurs subsequently:

(i) Select $l \leftarrow Z(q_1)^*$ randomly such that l_i is the i-th bit of l

(ii) Assess $Q \leftarrow \Pi_{i=1}^{p_1} Q_{i-1}^{'}$

(iii) Assess $b \leftarrow \hbar(A, M, Q)$

(iv) Assess $w \leftarrow l * bx(mo\ dq_1)$; consequently, deliver $\eta \leftarrow \Upsilon_w^{(v)}(t)(mo\ dq_1)$

(v) The sign σ of any missive M assumed by: $\sigma \leftarrow (A, Q, w)$

3.5. Verification. A confirmation of any sign σ on the set of M with the identity of the agent $i\ d$ remains as receipts subsequently:

(i) Calculate $\eta' \leftarrow Q\Upsilon_b^{(v)}(A)\Upsilon_{bv}^{(v)}(u)(mo\ dq_1)$

(ii) If we arrive at the state $\eta = \eta'$, then in this situation, the sign is agreeable; otherwise, it is ostracized

3.6. Reliability of the Process. The private key needs to attain the effectiveness with fairness:

$$\Upsilon_x^{(v)}(t)(mo\ dq_1) = A\Upsilon_v^{(v)}(u)(mo\ dq_1). \tag{38}$$

To prove the reliability of the procedure, we utilize $Q = \Upsilon_l^{(v)}(t)(mo\ dq_1)$ to compute the following:

$$\begin{aligned} Q\Upsilon_b^{(t)v}(A)(mo\ dq_1)\Upsilon_{bv}^{(v)}(u)(mo\ dq_1) &= \Upsilon_l^{(v)}(t)\Upsilon_{kb}^{(v)}(t)\Upsilon_{abv}^{(v)}(t)(mo\ dq_1) \\ &= \Upsilon_w^{(v)}(t)(mo\ dq_1). \end{aligned} \tag{39}$$

4. Security Investigation and Discussion

To demonstrate the security of our new O/O–IBSS utilizing CCM, we apply the security proofs contributed in [54].

Theorem 1. *The suggested IBSS is* $(\epsilon, t, Q_\hbar, Q_s, Q_E)$ *secure in the knowledge of unforgeability of IBSS based on the chosen message attack (UF-IBSS-CMA) in the ROM, implementing the* $(\epsilon', t\imath)$*–CCM hypothesis in* $Z_{q_1}^*$*, where*

$$\epsilon' = \left((q_1 - 1)/q_1\right)\left((q_1 - Q_\hbar(Q_E + Q_s))/(q_1 Q_\hbar)\right)\epsilon,$$
$$t' = t + \tau O(Q_s + Q_E). \tag{40}$$

And, $Q_\hbar$-hashing queries, Q_s-signing queries, and Q_E-extraction queries are the quantity of chaos. Here, τ is the period of a function of exponentiation.

Suppose that $\exists$ is a foe F. We develop an algorithm A depending on the utilization of F to solve CCM. The algorithm A is provided with a z_{q1}^* that comes with a variable $D \in z_{q1}^*$ and a general parameter t. Algorithm A is tested to check $\beta \in Z_{q_1}^*$ in such a method that $\Upsilon_\beta^{(\nu)}(t)(mo\ dw) = D$. We apply the same approach in [54].

Setting Algorithm A takes $\hbar$ (chaotic hash function), which is similar to a ROM behavior. A is liable for the model of this reformation method. A assigns a variable $u \leftarrow D$ that yields the general argument $(p_1, t, \hbar, u)$ to F.

Removal advice investigation: F is allowed to inquire for $i\ d$ in the extraction device. A recreates the oracle. It requires random $c, d \in Z_{q_1}^*$ and sets

$$A_\nu \leftarrow \Upsilon_d^{(\nu)}(t)/\Upsilon_c^{(\nu)}(u)(mo\ dq_1),\ x \leftarrow d,\ \hbar(A_\nu, i\ d) \leftarrow c. \tag{41}$$

A yields (A_ν, t) as a private key for $i\ d$ and stores the consistency evaluation $(A_\nu, x, \hbar(A_\nu, i\ d), i\ d)$ in the list. Note that, when $\nu \longrightarrow 0$, we have the case in [56].

Indication oracle requests F make an inquiry for and sign a message. The algorithm A discovers whether $i\ d$ has been requested for the device $\hbar$ or the extraction device in the past. If yes, it will only improve the list $(A_\nu, x, \hbar(A_\nu, i\ d), i\ d)$. Then, algorithm A utilizes these estimates to indicate the missive by performing the passing procedures. It generates the signature (A_ν, Q, w) on the message and maintains the list of (A_ν, Q, w) for reliability in the chaotic hash construction. If $i\ d$ is not requested to extract the oracle, then A starts the removal advice simulation procedure by shattering the secretive key to symbolize the missive.

Productivity calculation: eventually, F produces a fake sign $\sigma_1^* = (Q^*, A^*, w_1^*)$ on id^* and M^*. The algorithm A_ν changes F to the view that it makes an inquiry $\hbar(A^*, M^*, Q^*)$ and provides another value to the justified. Foe F produces a few other signatures $\sigma_2^* = (Q^*, A^*, w_2^*)$. Algorithm A rehashes again and obtains $\sigma_3^* = (Q^*, A^*, w_3^*)$. It is well known that Q^* and A^* must inevitably be likewise. We put n_1, n_2, n_3 in order to be created three times in a row from the arbitrary advice investigations $\hbar(Q^*, A^*, M^*)$.

For each $k, a, l \in Z_{q_1}^*$, we now project CCM of A_ν, u, and Q separately, i.e.,

$$A_\nu = \Upsilon_k^{(\nu)}(t)(mo\ dq_1),$$
$$u = \Upsilon_a^{(\nu)}(t)(mo\ dq_1), \tag{42}$$

and $Q = \Upsilon_l^{(\nu)}(t)(mo\ dq_1)$. From equation (18), we obtain the following facts:

$$w_j^* = a(n_j) \times \hbar(A^*, i\ d) \times l \times k(n_j),$$
$$(mo\ dq_1)\ j = 1, 2, 3. \tag{43}$$

Only k, a, and l are unfamiliar with A in these mathematical examinations. For the estimates of the overhead linear autonomous mathematical proclamations, the algorithm A_ν estimates for $j = 1, 2, 3$ and generates a as the solution of the CCM.

Ranked cost test: the simulation practicability with removal oracle failures presupposes that the consignment $\hbar(A_\nu, i\ d)$ of the random oracle is irregular, suggesting a combined probability of no less than $Q_\hbar/q_1$. Accordingly, the simulation procedure is effective $(Q_s + Q_E)$ times (ensued from the consideration that $\hbar(A, i\ d)$ also can furthermore be requested in the sign advice, if $i\ d$ is not requested in the removal advice) with the probability as follows:

$$\left(1 - \frac{Q_\hbar}{q_1}\right)^{Q_s + Q_E} \geq \left(1 - \frac{((Q_s + Q_E)Q_\hbar)}{q_1}\right). \tag{44}$$

Because of the arbitrary advice's ideal mediation, an inquiry $\hbar(A^*, M^*, Q^*)$ occurs with a probability of no less than $(1 - (1/q_1))$ Algorithm Aν guesses that it is exactly because of the rewind, at least as a possibility of $(1/Q_\hbar)$. The overall possibility of success is as follows:

$$\left(\frac{(q_1 - 1)}{q_1}\right)\left(\frac{(q_1 - Q_\hbar(Q_E + Q_s))}{(q_1 Q_\hbar)}\right)\epsilon. \tag{45}$$

The period density of procedure A_ν is determined by the exponentiation achieved in sign and removal procedures which is equivalent to $t + \tau O(Q_s + Q_E)$.

4.1. Discussion. In this position, we discuss the analysis and the performance of the CCM-based IBSS model by comparing it with some competing O/O identity-based sign (IBS) models and non-O/O models.

4.1.1. Contrast with Other O/O-IBS Models. Here, we contrast the performance of six well-designed O/O identity-based signature (IBS) schemes including Shamir and Tauman's scheme [11], Xu et al.'s model [22], Kar's scheme [55], Gao et al.'s model [16], Meshram et al.'s 2016 model [53], Meshram et al.'s 2019 model [57], Meshram et al.'s 2020 model [58], and our new CCM based IBSS model in view of the ranked cost. We note that, among the models, Xu et al.'s work[22] has no multiperiod adaptation to it, so the multiperiod evaluation for it was carried out by linking the same type of technique together. However, it is not possible to apply Shamir and Tauman's technique [11] for a multiperiod performance test.

The ranked cost $C(\zeta)$ of operation ζ is estimated by the bits of $|\xi|$. Besides that, ρ, μ, m, and η, which stands for the pairing operation, the multiplication function (similar to point addition in ECC) in the group, the modular multiplication operation in $Z_{q_1}^*$, and exponentiation function (similar to scalar multiplication in ECC) in a group, respectively, are all included in the evaluations. Other operations such as addition in $Z_{q_1}^*$ and representative hashing are negligible and are therefore ignored.

Table 1 indicates the outcomes of performance evaluations in the form of rank cost. The recent method depends on $\Upsilon^{(\nu)}, \nu = 0.998$. Therefore, when $\nu \longrightarrow 0$ yields $\kappa_0 = 0$ (the

Table 1: Contrast in terms of the ranked cost.

C1	C2	C3	C4	C5
—	—	$C(h) + C(\sigma_G)$	m	$C(\sigma_V) + C(h) + C(C_V)$
$\eta(\lvert q\rvert - 1)$	$3m + \mu O(\lvert q\rvert - 1)$	$\eta(\lvert q\rvert - 1)$	2m	$\mu + \rho$
$2\eta\lvert q\rvert$	$m + 2\mu O(\lvert q\rvert)$	$2\eta + m$	m	$\mu + 2(\eta + \rho)$
0	$m + \mu O(\lvert N^2\rvert)$	0	m	$2\eta + \mu$
0	$m + \mu O(\lvert q_1\rvert)$	0	m	2μ
$\mu(\lvert q\rvert - 1)$	$3m + \mu O(\lvert q\rvert - 1)$	$\eta(\lvert q\rvert - 1)$	3m	$3\mu + 2\rho + \eta$
0	$m + \mu$O(|.|)	0	m	μO(| · |)
$\kappa_0(\nu)$	$m + \kappa_0(\nu) + \mu O(\lvert q_1\rvert)$	$\kappa_0(\nu)$	$m + \kappa_0(\nu)$	$2\mu + \kappa_0(\nu)$

case in [55]). C_1: the ranked cost of offline (multistep); C_2: the ranked cost of online (multistep); C_3: the ranked cost of offline (single-step); C_4: the ranked cost of online (single-step); C_5: the ranked cost in confirmation step. The rows are the outcomes of [11, 16, 22, 55, 56] and the proposed method, respectively. For example, h is a Chameleon-hash function, which needs the minimum of one η computation; $\hbar$ 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, C_V is the operation of one record confirmation, which requires no less than one η computation.

4.1.2. Estimation with Other Methods. As with IBS models (O/O), we also contrast the planned model with some well-established IBS schemes (non-O/O) recognized by ISO/IEC including Cha and Cheon's design [56], Guillou and Quisquater's scheme [57], Hess's formula [17], Meshram et al.'s system [55], and Meshram et al.'s system [58]. The full outcomes can be located in Table 2 with the same notations used as in Table 1. Notably, non-O/O models may not run very smoothly in wireless sensor networks since the lightweight wireless sensors probably will be overwhelmed by the operation demand. For example, both Hess's design [17] and Cha and Cheon's model [56] inevitably require operation ρ (pairing) in the verification phase and operation η in the signing phase, which amounts to too much of a burden for lightweight gadgets.

Table 2: Contrast in virtue of the ranked cost and sign measure for $\nu \longrightarrow 1$.

Cost techniques	Cost in verification stage	Cost in signing stage	Size of signature (bits)
[17]	$\eta + 2\rho$	$\mu + 3\eta$	320
[55]	$\mu + 2\eta$	m	480
[56]	2μ	m	480
[56]	$\mu + 2(\eta + \rho)$	2η	320
[57]	$2(\mu + 2\eta)$	$2(m + \eta)$	2048
[58]	μ	m	480
Proposed method	$2\mu + \kappa_0(\nu)$	$m + \kappa_0(\nu)$	480

4.2. Vision on the Recent Method. This section deals with the following visions on the suggested method.

In the present study, we have discussed the new generalization of Chebyshev polynomials using the fractional calculus that is called fractional conformable calculus. Also, we have discussed the necessary properties such as semigroup property and chaotic property of conformable fractional chaotic maps, which are very useful for designing of a new cryptography scheme. This paper introduces an online/offline ID-based short signature (IBSS) scheme that uses conformable fractional chaotic maps for secure communication. The presented scheme is secure under an existential enforce-ability of identity-based short signature (IBSS) under chosen message attack (EUF-IBSS-CMA) in the random oracle model (ROM). We have used less rigorous operations to carry out signing and verification procedures, similar to human signing on valid documents and then verifying them as per witness. The proposed online/offline ID-based short signature (IBSS) offers a better security assurance than currently established signature schemes.

The use of conformable fractional chaotic maps increased the security of ID-based short signature under the probabilistic polynomial time and decreased the computational cost. The key advantage of the presented online/offline ID-based short signature (IBSS) scheme that uses conformable fractional chaotic maps is that at the verification stage and signing period, it takes less computation; it retains the degree of protection. Therefore, the presented scheme indicates less bandwidth for storage, communication, and computing resources, particularly applicable to wireless devices and smart cards.

As a real-world application, wireless sensor networks (WSNs) have made rapid progress in recent years and have been widely applied by various works, such as healthcare centers, institutes of ecological and environmental research, and government and military organizations. 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 most sensitive, confidential, or personal, secure information transmission is a critical challenge and one of the most significant security requirements is authentication. The online/offline ID-based short signature (IBSS) plays a key role in ensuring data integrity, authentication, and nonrepudiation.

5. Conclusion

Here, we established an effective CCM based on the IBSS method. Our new design does not involve a record devoted

to the sign for confirmation, and there is no pairing operation involved either in the signature obstetrics phase or in the verification phase. It is secure in the ROM with unfeasibility based on EUF-IBSS-CMA-secure. Our new scheme provides multistep use of offline storage, enabling the agent to reuse the data set in a polynomial format contrasting to the single-attempt inconvenience in most other processes. In our new method, a preregistration procedure can be carried out with a private key and then no private key is needed in the offline phase. In such a design, we only need the least operations in each procedure. This structure does not request any type of record, registration, or verification related to the sign for assertion and does not demand any combination in both stage's confirmation and signature group. Our presented disconnected signing method does not request all kinds of secluded key data. It can -record by an isolated key group with offline data equally be utilized. It correspondingly consumes the very slightest operation in every procedure. This is an astonishing promising model in wireless sensor network circumstances as the disengaged data may be complex-inserted into the sensor hub in the accumulating or arrangement position. 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 complex-inserted into the device hub. Our performance analysis reveals that the proposed method has the lowest ranked cost among competing methods. In future work, we will develop a new efficient online/offline ID-based aggregation short signature scheme using conformable fractional chaotic maps under fuzzy user data sharing for wireless sensor networks by using the presented scheme.

Data Availability

The data are not applicable. We use algorithm and difference derivatives, and all equations and formulas used are included in the manuscript.

Conflicts of Interest

The authors declare that there are no conflicts of interest.

Authors' Contributions

All authors contributed equally and significantly to writing this article. All authors read and approved the final manuscript.

References

[1] T. Abdeljawad, "On Riemann and Caputo fractional differences," *Computers & Mathematics with Applications*, vol. 62, no. 3, pp. 1602–1611, 2011.

[2] H. Liu and A. Kadir, "Asymmetric color image encryption scheme using 2D discrete-time map," *Signal Processing*, vol. 113, pp. 104–112, 2015.

[3] S. H. Islam, "Design and analysis of a three party password-based authenticated key exchange protocol using extended chaotic maps," *Information Sciences*, vol. 312, pp. 104–130, 2015.

[4] G.-C. Wu, D. Baleanu, H.-P. Xie, and F.-L. Chen, "Chaos synchronization of fractional chaotic maps based on the stability condition," *Physica A: Statistical Mechanics and Its Applications*, vol. 460, pp. 374–383, 2016.

[5] A. Ouannas, Z. Odibat, A. Alsaedi, A. Hobiny, and T. Hayat, "Investigation of Q-S synchronization in coupled chaotic incommensurate fractional order systems," *Chinese Journal of Physics*, vol. 56, no. 5, pp. 1940–1948, 2018.

[6] G.-C. Wu and D. Baleanu, "Discrete fractional logistic map and its chaos," *Nonlinear Dynamics*, vol. 75, no. 1-2, pp. 283–287, 2014.

[7] W. Wang and J. Meng, "Xiao han liao, yong deng, zhi jun Li, yi ceng zeng, and ming lin ma. "Bursting, dynamics, and circuit implementation of a new fractional-order chaotic system with coexisting hidden attractors," *Journal of Computational and Nonlinear Dynamics*, vol. 14, Article ID 071002, 2019.

[8] J. C. Mason and D. C. Handscomb, *Chebyshev Polynomials*, Chapman & Hall/CRC, Boca Raton, USA, 2003.

[9] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[10] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures," in *Proc. CRYPTO '89, Lecture Notes in Computer Science*, vol. 2442, pp. 263–277, Springer, NY, USA, 1989.

[11] A. Shamir and Y. Tauman, "Improved online/offline signature schemes," in *Advances in Cryptology - CRYPTO 2001*, vol. 2139, pp. 355–367, Springer, Berlin, 2001.

[12] K. Kurosawa and K. Schmidt-Samoa, "New online/offline signature schemes without random oracles," in *Public Key Cryptography - PKC 2006*, vol. 3958, pp. 330–346, Springer, Berlin, 2006.

[13] 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, 2007.

[14] M. Joye, "An efficient on-line/off-line signature scheme without random oracles," in *Cryptology and Network Security*, vol. 5339, pp. 98–107, Springer, Berlin, 2008.

[15] D. Boneh and X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups," *Journal of Cryptology*, vol. 21, no. 2, pp. 149–177, 2008.

[16] Y. Gao, P. Zeng, K. K. Raymond Choo, and F. Song, "An improved online/offline identity-based signature scheme for WSNs," *International Journal on Network Security*, vol. 18, no. 6, pp. 1143–1151, 2016.

[17] F. Hess, "Efficient identity based signature schemes based on pairings," in *Selected Areas in Cryptography*, vol. 2595, pp. 310–324, Springer, Berlin, Germany, 2003.

[18] J. Herranz, "Deterministic identity-based signatures for partial aggregation," *The Computer Journal*, vol. 49, no. 3, pp. 322–330, 2005.

[19] D. Galindo and F. D. Garcia, "A Schnorr-like lightweight identity-based signature scheme," *Progress in Cryptology - AFRICACRYPT 2009*, Springer, vol. 5580, pp. 135–148, Berlin, Germany, 2009.

[20] S. Xu, Y. Mu, and W. Susilo, "Online/offline signatures and multisignatures for AODV and DSR routing security," in *Information Security and Privacy*, vol. 4058, pp. 99–110, Springer, Berlin, Germany, 2006.

[21] F. Li, M. Shirase, and T. Takagi, "On the security of online/offline signatures and multisignatures from ACISP' 06," in *Cryptology and Network Security*, vol. 5339, pp. 108–119, Springer, Berlin, Germany, 2008.

[22] F. Dachselt and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 48, no. 12, pp. 1498–1509, 2001.

[23] K. W. Wong, "A fast chaotic cryptographic scheme with dynamic look-up table," *Physics Letters A*, vol. 298, no. 4, pp. 238–242, 2002.

[24] G. Chen, Y. Mao, and C. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[25] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dynamics*, vol. 62, no. 3, pp. 615–621, 2010.

[26] S. Jye, "A speech encryption using fractional chaotic systems," *Nonlinear Dynamics*, vol. 65, pp. 103–108, 2011.

[27] X. Wang, X. Wang, J. Zhao, and Z. Zhang, "Chaotic encryption algorithm based on alternant of stream cipher and block cipher," *Nonlinear Dynamics*, vol. 63, no. 4, pp. 587–597, 2011.

[28] S. Deng, Y. Li, and D. Xiao, "Analysis and improvement of a chaos-based Hash function construction," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 5, pp. 1338–1347, 2010.

[29] D. Xiao, F. Y. Shih, and X. Liao, "A chaos-based hash function with both modification detection and localization capabilities," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 9, pp. 2254–2261, 2010.

[30] Y. Wang, K.-W. Wong, X. Liao, and T. Xiang, "A block cipher with dynamic S-boxes based on tent map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3089–3099, 2009.

[31] 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 Dynamics*, vol. 69, no. 1-2, pp. 79–87, 2012.

[32] C.-C. Lee and C.-W. Hsu, "A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps," *Nonlinear Dynamics*, vol. 71, no. 1-2, pp. 201–211, 2013.

[33] 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 Dynamics*, vol. 79, no. 4, pp. 2485–2495, 2014.

[34] 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 Dynamics*, vol. 76, no. 1, pp. 853–866, 2014.

[35] 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, Article ID e0155064, 2016.

[36] 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 Dynamics*, vol. 73, no. 1-2, pp. 125–132, 2013.

[37] C.-C. Lee, C.-W. Hsu, Y.-M. Lai, and A. Vasilakos, "An enhanced mobile-healthcare emergency system based on extended chaotic maps," *Journal of Medical Systems*, vol. 37, no. 5, p. 9973, 2013.

[38] 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," *Journal of Medical Systems*, vol. 38, no. 9, p. 77, 2014.

[39] 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," *Journal of Medical Systems*, vol. 40, no. 11, p. 233, 2016.

[40] K. Chain and W.-C. Kuo, "A new digital signature scheme based on chaotic maps," *Nonlinear Dynamics*, vol. 74, no. 4, pp. 1003–1012, 2013.

[41] C. Meshram, C.-C. Lee, C.-T. Li, and C.-L. Chen, "A secure key authentication scheme for cryptosystems based on GDLP and IFP," *Soft Computing*, pp. 1–7, 2016.

[42] R. Khalil, M. Al Horani, A. Yousef, and M. Sababheh, "A new definition of fractional derivative," *Journal of Computational and Applied Mathematics*, vol. 264, pp. 65–70, 2014.

[43] D. R. Anderson and D. J. Ulness, "Newly defined conformable derivatives," *Advances in Dynamical Systems and Applications*, vol. 10, no. 2, pp. 109–137, 2015.

[44] D. R. Anderson, "On the nature of the conformable derivative and its applications to physics," *J. Frac. Calc. Appl.*vol. 10, no. 2, pp. 92–135, 2019.

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

[46] C. Meshram, S. A. Meshram, and M. Zhang, "An ID-based cryptographic mechanisms based on GDLP and IFP," *Information Processing Letters*, vol. 112, no. 19, pp. 753–758, 2012.

[47] C. Meshram and S. Meshram, "An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem," *Information Processing Letters*, vol. 113, no. 10-11, pp. 375–380, 2013.

[48] C. Meshram, "An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem," *Information Processing Letters*, vol. 115, no. 2, pp. 351–358, 2015.

[49] C. Meshram, "An efficient ID-based beta cryptosystem," *International Journal of Security and Its Applications*, vol. 9, no. 2, pp. 189–202, 2015.

[50] C. Meshram and M. S. Obaidat, "An ID-based Quadratic-Exponentiation Randomized Cryptographic Scheme," in *Proceedings of the International Conference on Computer, Information and Telecommunication Systems*, pp. 1–5, Gijon, Spain, July 2015.

[51] C. Y. Meshram, P. L. Powar, M. S. Obaidat, and C.-C. Lee, "An IBE technique using partial discrete logarithm," *Procedia Computer Science*, vol. 93, pp. 735–741, 2016.

[52] C. Meshram and P. L. Powar, "An efficient identity-based QER cryptographic scheme," *Complex & Intelligent Systems*, vol. 2, no. 4, pp. 285–291, 2016.

[53] 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 Computing*, vol. 23, no. 16, pp. 6937–6946, 2019.

[54] C. Meshram, P. L. Powar, M. S. Obaidat, C. C. Lee, and S. G. Meshram, "Efficient online/offline IBSS protocol using partial discrete logarithm for WSNs," *IET Networks*, vol. 7, no. 6, pp. 363–367, 2018.

[55] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," *Journal of Cryptology*, vol. 22, no. 1, pp. 1–61, 2009.

[56] J. Kar, "Provably secure online/off-line identity-based signature scheme for wireless sensor network," *International Journal on Network Security*, vol. 16, no. 1, pp. 29–39, 2014.

[57] J. Cha and J. Cheon, "An identity-based signature from gap Diffie Hellman groups," in *Proc. PKC'2003, Lecture Notes in Computer Science*, vol. 2567, pp. 18–30, Springer, Berlin, Germany, 2003.

[58] L. C. Guillou and J. J. Quisquater, "A "Paradoxical" Identity-based signature scheme resulting from zero-knowledge," in *Proc. Crypto 88 Lecture Notes in Computer Science*, vol. 403, pp. 216–231, Springer, Berlin, Germany, 1989.

[59] C. Meshram, C.-C. Lee, S. G. Meshram, and A. Meshram, "An efficient online/offline subtree-based short signature scheme using Chebyshev chaotic maps for wireless sensor network," *IEEE Access*, vol. 8, no. 1, pp. 80063–80073, 2020.

[60] 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," *International Journal of Communication Systems*, vol. 33, no. 7, Article ID e4307, 2020.

[61] S. Mobayen, C. Volos, Ü. Çavuşoğlu, and S. Kaçar, "A simple chaotic flow with hyperbolic sinusoidal function and its application to voice encryption," *Symmetry*, vol. 12, no. 12, p. 2047, 2020.

[62] H. Karami, S. Mobayen, M. Lashkari, F. Bayat, and A. Chang, "LMI-Observer-Based stabilizer for chaotic systems in the existence of a nonlinear function and perturbation," *Mathematics*, vol. 9, no. 10, p. 1128, 2021.

[63] O. Mofid, M. Momeni, S. Mobayen, and A. Fekih, "A disturbance-observer-based sliding Mode control for the robust synchronization of uncertain delayed chaotic systems: application to data security," *IEEE Access*, vol. 9, pp. 16546–16555, 2021.

[64] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, "Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption," *IEEE Access*, vol. 9, pp. 25911–25925, 2021.

[65] B. Vaseghi, S. S. Hashemi, S. Mobayen, and A. Fekih, "Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems," *IEEE Access*, vol. 9, pp. 21332–21344, 2021.

[66] J. Mostafaee, S. Mobayen, B. Vaseghi, M. Vahedi, and A. Fekih, "Complex dynamical behaviors of a novel exponential hyper–chaotic system and its application in fast synchronization and color image encryption," *Science Progress*, vol. 104, no. 1, Article ID 00368504211003388, 2021.

[67] S. Mobayen, C. K. Volos, S. Kaçar, Ü. Çavuşoğlu, and B. Vaseghi, "A chaotic system with infinite number of equilibria located on an exponential curve and its chaos-based engineering application," *International Journal of Bifurcation and Chaos*, vol. 28, no. 9, Article ID 1850112, 2018.

[68] C. Meshram, S. G. Meshram, R. W. Ibrahim, H. A. Jalab, and S. S. Jamal, S. K. Barve, Conformal Chebyshev chaotic map-based remote user password authentication protocol using smart card," *Complex & Intelligent Systems*, pp. 1–15, 2021.