Fractional chaotic maps based short signature scheme under human-centered IoT environments

Chandrashekhar Meshram a,⇑, Rabha W. Ibrahim b,c, Ahmed J. Obaid d, Sarita Gajbhiye Meshram e,f, Akshaykumar Meshram g, Alaa Mohamed Abd El-Latif h,i

a Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College, College of Barkatullah Vishwavidyalaya, Betul, M.P. 460001, India
b Informetrics Research Group, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
c Faculty of Mathematics & Statistics, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
d Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Iraq
e Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
f Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
g Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering, Nagpur, M.S., India
h Department of Mathematics, Faculty of Education, Ain Shams University, Roxy, Cairo, Egypt
i Department of Mathematics, Faculty of Arts and Science, Northern Border University, Rafha, Saudi Arabia

Abstract

Introduction: The Internet of Things (IoT) comprises of various smart devices for the sharing of sensed data through online services. People will be directly contacted to check their health parameters and the reports will be collected centrally through smart devices. The requirement is protection of messages during the exchange of data between sender and receiver in order to tackle human malicious attacks. Various signature-based schemes are discussed in the literature to provide secure communication.
Introduction

In this era of the Internet of Things (IoTs), in which various device types are connected to the Internet. Such devices can be household appliances, agricultural equipments, manufacturing, energy meter, industrial machinery, healthcare monitoring machinery, mining sensors, surveillance system, environmental equipment, smart grids and smart city, etc. which includes Machine-to–Machine model. With the advent of IoT enable devices, monitoring or control of various types of systems on the tips of the fingers has become very easy. IoT devices are smart enough to share and exchange data for cloud storage over a public internet. IoT is an effective method for applying to domain variables and proves the vital function by providing substantial advantages.

Some acknowledged literature are [1–8], the application of IoT witness in various domains ranging from manufacturing automation to healthcare. Moreover, every attempt is made to improve hardware interfaces, software, improved communication, and less focus is on user interaction and experience, and protection and privacy policies. This means, less significance is given to human related Internet of Things. Subsequently, we investigate human-centered IoT enabled device to offer more preference to human viewpoint in technology. Human-centered IoT is an upcoming filed of research connects to various aspects of life includes smart cards, e-commerce, business, healthcare, and sensitive private data. That means, the human-related Internet of Things is given less significance. Subsequently, we have investigated devices enabled by human-centered IoT to offer more preference in technology to the human viewpoint. Human-centered IoT is an upcoming field of research connected to various aspects of life that includes smart cards, e-commerce, business, healthcare, and sensitive private data. Nonetheless, the design of human-centered IoT [9] offers many opportunities and challenges. Thus, it not only is focuses on IoT system performance, integration, communication and interoperability, but more emphasis is placed on user application features, user need, and human-centered IoT motivation (see Fig. 1).

Smart factories have emerged as a result of the Industry 4.0 revolution and are capable of intelligently managing data produced from the overall production system [10]. Tracking or labeling of items or objects in this scenario is often achieved by RFID tags, QR codes, and barcodes named as labels or tags. The challenges are the incorporated of too many practices in an IoT-centric human world. So we have to address all these challenges to build productive 4.0 industry with human-centric applications using smart labels. We are witnessing that human participation in human-centered IoT-based applications in which the design approach adopted focuses less on devices and more on the human-centered [11,12]. In human-centered IoT, information is exchanged over the public communication channel through various devices. Thus, fraudulent practices occur to steal or change the information. Because of this, the major challenge is preserving confidentiality and privacy during transmission time. Hence, for information exchange, we need more effective and reliable security mechanism. IoT systems are resource-constrained and heavy computing resources lose out. Radwan et al. [13] presented the concept of the synchronization with active control technique of different fractional order chaotic systems. Based on the switching parameters, four different cases of synchronization are also introduced. Ibrahim et al. [14] discussed some symmetric conformable fractional derivatives of complex variables for fractional chaotic maps generalizations. The standard DSA such as RSA [15], ElGamal [16], ECDSA [17], and bilinear pairing [18] are therefore not necessary to apply. We need a quick and lightweight short-size signature security scheme for IoT. It does, however, take time to check the bilinear maps used by the short–signature schemes based on pairing. Moreover, such short signature schemes are not as computationally efficient as the signature schemes of the DSA-type. Hence the storage capacity of pairing-based signatures comes at the expense of losing computational performance. Vaidyanathan et al. [19] introduced a novel 3D jerk chaotic system with one-quadratic nonlinearity and two-cubic nonlinearities designed to produce complex chaotic signals, and addressed voice encryption applications. Vaidyanathan et al. [20] proposed a new model of hyperchaotic temperature fluctuations and described its modeling, and also discussed the characteristics of the new model of hyperchaotic temperature fluctuations, such as its phase portraits, rest points, symmetry, invariance, characteristic exponents of Lyapunov, bifurcation analysis etc. Explain it for image encryption application just briefly. Mobayen et al. [21] introduced 3-D chaotic system with a closed equilibrium point curve, which has the form of a boomerang and modeled the theoretical system’s electronic circuit implementation to test its feasibility. Also addressed the sound encryption applications.

A short signature scheme using a chaotic map is more efficient and costs less in terms of computation. Consequently, we have adopted chaotic maps for human-centered IoT’s proposal for a short signature security scheme. Chaotic maps are used in [22] to introduce the authentication scheme for ID-based digital signature. Schemes security promise based on the assumptions of chaotic
maps hardness (Diffie-Hellman) and difficulties (DL). In 2016, Gao et al. \[23\] presented an authentication scheme based on chaotic maps for wireless body area network in which health data was recorded and monitored. The cost of multiplication and exponential computation was achieved with reduced communication cost. User confidentiality was the key element in sharing of information during authentication. An anonymity which preserves authentication scheme is shown in \[24\]. AVISPA was used for analyzing and verifying security. Compared to other approaches the enhanced performance was recorded. Meshram et al. \[25–27\] proposed more efficient authentication schemes using extended chaotic maps. The results obtained in these schemes are testimony to the suitability of chaotic maps as the good choice for proposing a new security scheme.

Motivation

While some researchers have proposed security mechanisms, they are not lightweight enough to meet the IoT based system’s needs. In this paper, we have proposed an efficient secure and lightweight short signature scheme using fractional chaotic maps which provides security under adaptive chosen-message attack (CMA) in random oracle model.

Recently, Mughal et al. \[43\] presented a digital signature scheme using complex numbers for providing secure communication among smart devices in human-centered IoT based systems but have not discussed its security in any standard security model as discussed in the previous literature. A variety of signature-based schemes are discussed in literature to provide secure communication, but smart devices need more lightweight operations by ensuring the required security strengths. Due to the large real numbers required for signature and verification processes, the main problem during signature-based approaches is the computational overhead. This paper presents a lightweight short signature scheme using fractional chaotic maps for providing secure communication between smart devices in human centered IoT. We have used less extensive operations to achieve processes of signing and verification, as human beings do signatures on legal documents and then verify as per witness. The presented scheme is secure under adaptive chosen-message attack (CMA) in random oracle model.

Contribution

This paper presents an efficient provably secure short signature scheme using fractional chaotic map for smart devices in human centric IoT. During verification and signing operations, it uses the less detailed operations based on fractional chaotic maps to generate security credentials. The main advantage of this strategy over the DSA signature scheme is a one-fourth reduction in the verification process as well as signature frequency. The methodology is illustrated with simple step-by-step, outstanding principles to prove proof of notion. In DSA-based systems, this eliminates overhead computation and communication, and coordination along with improved flexibility compared to existing detailed operations based on real number. However, we show the reliability of the proposed SSS is closely linked, if not strongly, to the difficulty of solving fractional chaotic maps. Under adaptive chosen attacks in ROM, an efficient security proof exists for unforgeability, i.e. the presented scheme provides superior security guarantees than the

Fig. 1. 3D-fractal Chebyshev polynomials for $\alpha = 0, 0.5$ and 0.75 respectively.

C. Meshram, R.W. Ibrahim, A.J. Obaid et al. Journal of Advanced Research 32 (2021) 139–148
existing other signature schemes. The scheme presented does not use pairings resulting in effortless implementation and higher performance, nor is it relying on the relatively untested and recent assumptions of hardness associated with pairing-based cryptography. Results show that our methodology presented is less time consuming than equivalents for the verification and signature process. It requires less time to check the variations in the length of the message, less communication costs needed for signature messages, fewer bytes exposed by undermining devices and less ability to compromise midway devices.

Road map of article: Section ‘Related materials’ describes the definition and terminology associated with the presented scheme. The proposed new scheme based on fractal calculus to generalize the Chebyshev polynomial are listed in Section ‘PROPOSED SHORT SIGNATURE SCHEME (SSS)’. Section ‘Security analysis and discussion’ explains the security target of signature schemes, security models and provably security in ROM, and we are also presenting a reductionist proof of security against forgery that occurs under the adaptive chosen message attacks (EUF-CMA) in ROM. Section ‘Performance comparison’ describes the study by which other similar recent schemes are contrasted with the scheme proposed. Finally, Section ‘Conclusion’ stretches the conclusions.

Related materials

In this segment, we have highlighted Chebyshev polynomial and fractional chaotic maps subsequently we would use in the proposed technique. We will then define some necessary notations used in the article (see Table 1).

Chebyshev chaotic transforms

We reviewed Chebyshev sequential polynomials (CSP) (see [28]) and assessed their operational. CSP $T_s (\tau)$ is a polynomial of $n$-degree in the variant. Let $\tau \in [-1, 1]$ be the version, and let $n$ be an integer. In general, CSP stated as follows:

$$T_n (\tau) = \cos(n \times \cos^{-1} (\tau)),$$

$$T_0 (\tau) = 1$$

$$T_1 (\tau) = \tau$$

$$T_n (\tau) = 2\tau T_{n-1} (\tau) - T_{n-2} (\tau); n \geq 2$$

In this case, the functional $\cos^{-1} (\tau)$ and $\cos (\tau)$ represented as $\cos^{-1} : [-1, 1] \rightarrow [0, \pi]$ and $\cos : \mathbb{R} \rightarrow [-1, 1]$.

There are two main properties of CSP [25–26,29–32]: chaotic properties and semi-group properties.

(1) The chaotic possessions: The CSP transform demarcated as $T_s : [-1, 1] \rightarrow [-1, 1]$ with degree $n > 1$, is a chaotic transform connected to the functional (invariant density) $f^*(\tau) = \frac{1}{\pi \sqrt{1-\tau^2}}$.

| $\tau^*$ | Fractal Chebyshev chaotic maps |
|----------|-------------------------------|
| $r$      | Random number per message     |
| $h_1$, $h_2$ | One Way Hash Functions |
| $M$      | Message                       |
| $s$      | 1st parameter of signature    |
| $g$      | 2nd parameter of signature    |
| $l$      | Digital Signature             |
| $\pi$    | Large prime number of bit length |
| $\sqrt{h}$ | Large prime factors of $h-1$ |

(2) The properties of what is called semi-group satisfies the following equalities:

$$T_n (T_s (\tau)) = \cos(\cos^{-1} (\cos(\cos^{-1} (\tau)))) = \cos(\cos^{-1} (\tau)) = T_{n-s} (\tau),$$

where $\omega$ and $\ell$ are positive integers and $\tau \in [-1, 1]$.

Chebyshev polynomials have two tests that in polynomial time considered handling:

(1) The discrete log’s (DL) assignment is to find the integer $\omega$ with the end goal $T_{\omega} (\tau) = \gamma$ given two components rand $\gamma$.

(2) Because of three components, $T_s (\tau)$, and $T_r (\tau)$, the Diffie-Hellman problem (DHP) assignment is to measure the $T_{\omega} (\tau)$ element.

Fractional Chebyshev polynomials (FCP)

Fractional discrete systems have a most important benefit over their conservative complements due to the infinite minimal feature, which agrees for more flexibility in demonstrating and indicates a higher degree of chaotic performance. We have confidence in the fractional calculus approaches and fractional discrete formulation that will give us a recovering explanation of discrete fractional maps. From our research, we discovered that the fictionalized standard map could also be employed in the information security field. In this section, we aim to formulate the Fractional Chebyshev Polynomials.

Assume the fractional (arbitrary) number $\alpha \in [0, 1]$. An operator $\delta^\alpha$ is fractional derivative if and only if \cite{30}

$$\delta^\alpha \varphi (x) = \lim_{x \to 0} \frac{\Delta^\alpha (\varphi (x) - \varphi (x_0))}{(x - x_0)^\alpha} = \Gamma (x + 1) (\varphi (x) - \varphi (x_0)).$$

The fractal integral corresponds to $\delta^\alpha$ is defined by

$$\delta^\alpha \varphi (x) = \frac{\Gamma (x + 1)}{\Gamma (x + 1)} \int_a^b \varphi (x) = x^\alpha.$$

Note that

$$\delta^\alpha \varphi (x) = \frac{(b - a)^\alpha}{\Gamma (x + 1)} \varphi (x), \quad a \leq x \leq b. \quad (1)$$

By employing the concept of Fractal Calculus to simplify the polynomial $T_n (\tau)$, we can attain the subsequent structure:

$$\delta^\alpha T_n (\tau) := T_n^\alpha (\tau) = \frac{(2)^\alpha}{\Gamma (x + 1)} T_n (\tau), \quad (2)$$

Eq. (2) is named the Fractal Chebyshev polynomials (FCP). Formula that is more frequent can be seen in the following result:

**Proposition 2.1.** The FCP fulfills the frequent associations

$$T_n^\alpha (\tau) = \frac{(2)^\alpha}{\Gamma (x + 1)} (2\tau T_{n-1} (\tau) - T_{n-2} (\tau)). \quad (3)$$

Proof. Connection (2) with the frequent formula implies that

$$T_n (\tau) = 2\tau T_{n-1} (\tau) - T_{n-2} (\tau); n \geq 2$$

we have

$$T_n^\alpha (\tau) = \frac{(2)^\alpha}{\Gamma (x + 1)} T_n (\tau)$$

$$= \frac{(2)^\alpha}{\Gamma (x + 1)} (2\tau T_{n-1} (\tau) - T_{n-2} (\tau)).$$

Note that when $\alpha \to 0$, we have the main ordinary result, which can be seen in [33].
**Proposition 2.2.** The semi-group possesses clamps for FCP positioned on interval $(-\infty, \infty)$. By Proposition 2.1, we obtain

$$T_n^2(\tau) = \frac{(2^n)^3}{1^3 + 1}(2xT_n(\tau) - T_n(\tau)).$$

The above preparation proposes an adjustment equation (disconnected equation) which has a typical principle

$$\omega^2 - 2h\omega + \mu_1 = 0$$

Satisfying the relations

$$\omega_1 + \omega_2 = 2h, \quad \omega_1\omega_2 = \mu_1, \quad \omega_1 + \omega_2 = h \pm \sqrt{h^2 - \mu_1}.$$ 

A computation yields that

$$T_n^2(\tau) = (\omega_1^n + \omega_2^n)/2$$

$$= \frac{(h + \sqrt{h^2 - \mu_1})^n + (h - \sqrt{h^2 - \mu_1})^n}{2}$$

$$= \frac{n}{m} \left( h^{n-2m}(h^2 - \mu_1)^m \right)$$

A computation yields that

$$T_n^2(\tau) = T_n^2(T_n^2(\tau)) = T_n^{4}(\tau).$$

Hence, we have the important relation

$$T_n^2(\tau) = T_n^2(T_n^2(\tau)) = T_n^{4}(\tau).$$

The closed form expression for Chebyshev polynomials of any order is

$$T_i(x) = \sum_{j=0}^{i/2} (-1)^j \binom{i}{j} x^{i-2j}(1-x^2)^j$$

where \([i/2]\) is the integer part of \((i/2)\). Then the FCP becomes

$$T_n^2(x) = \frac{(2^n)^3}{1^3 + 1}(2xT_{n,1}(\tau) - T_{n,1}(\tau)).$$

$$= \frac{(2^n)^3}{1^3 + 1} \left( 2x \left( \sum_{j=0}^{i/2} (-1)^j \binom{i}{j} x^{i-2j}(1-x^2)^j \right) \right)$$

**Proposed short signature scheme (SSS)**

In this section, we presented a secure FCM based SSS under the environment of IoT. The presented scheme as follows (see Fig. 2):

- **Setup**: Let $\varphi$ and $\theta$ be huge prime numbers with $\varphi|\theta - 1$. Similarly let $G_{\varphi}\varphi = \{E_1, E_2, \ldots, E_{\varphi}^{-1}\}$ be a subgroup with prime order $\varphi$ of the multiplicative group $Z_\varphi^*$, where $E_1$ is a generator with prime order $\varphi$. Let $h_1$ and $h_2$ be one way hash functions where

$$h_1 : \{0,1\}^* \times Z_\varphi^* \to \{0,1\}^{m_p/2} \text{ and } h_2 : \{0,1\}^* \to Z_\theta^*$$

We will omit the “mod $p$” and “mod $\varphi$” markers for notational convenience. We denote the bit length by $|\varphi| = m_p$ and $|\theta| = m_\theta$. The notation $r \in S$ implies that an is selected randomly from a set $S$ at random. We are now explaining the SSS in full detail.

- **Key generation algorithm**

  1. Picks an arbitrary $r \in Z_\varphi^*$ as the private key.
  2. The corresponding public key is $p \leftarrow T_n^2(g)$. 

- **Signing algorithm**: The inputs are the private key, the public key $p$ and a message $M \in \{0,1\}^*$. 

  1. First choose an arbitrary $r \in Z_\varphi^*$.
  2. Computes $B \leftarrow h_2(M), \kappa \leftarrow B, T_n^2(g), D \leftarrow h_1(M, \kappa)$ and $s \leftarrow r - D_k$.

![Fig. 2. Digital Signature and Verification Process.](image-url)
The signature of the message \( m \) is \( \varepsilon \leftarrow (D, s) \).

- **Verification algorithm:** The inputs are the message \( M \), the public key \( p \), and the signature \( \varepsilon \leftarrow (D, s) \).
1. Computes \( B \leftarrow h_\varepsilon(M), \kappa' \leftarrow \mathcal{H}_{\varepsilon}(p)T_\varepsilon^b(g) \) and \( D' \leftarrow h_\varepsilon(M, \kappa') \).
2. If \( D = D' \), verification outputs valid, otherwise it outputs in valid.

**Consistency of the proposed scheme:** Because \( s = r - D_2 \) and \( \kappa = B \mathcal{H}^b(g), r = s + D_2 \) imply \( T_\varepsilon^b(p)T_\varepsilon^b(g) = T_\varepsilon^b(g) \) and \( \kappa' = \mathcal{H}_{\varepsilon}(p)T_\varepsilon^b(g) = \mathcal{H}_{\varepsilon}(g) = \kappa \). So \( D' = h_\varepsilon(M, \kappa') = h_\varepsilon(M, \kappa) = D \). Hence, the signature \( \varepsilon \leftarrow (D, s) \) produced by the signing algorithm is always valid.

### Security analysis and discussion

At the very outset, the prototype of the security inspection for presented short signature schemes is observed. Secondly, the concept of the random oracle and the “probable security” are investigated. Finally, a near-reductivist method is brought forth to prove that SSS is safe to prevent existential forgery in the setup of chosen attacks in ROM assuming FCM are difficult under human-centered Internet of Things environments.

### Security frameworks and provably security analysis

The primary safety principles of the short signature schemes, the first of its kind technique to use, were described by Goldwasser et al. [35]. Universal forgery, existential forgery (EUF), and absolute break are the three types of attacks chosen by the enemy. However, to destabilize the signature’s security the strategies used by enemy may be different. Attacker has the basic knowledge of the signer’s public key in the First instance. Secondly attacker has access to a set of accurate pairs such as message and signature. On the basis of earlier obtained feedback of the questions, the adaptive chosen-message attack (CMA) authorizes the attacker to use the signer’s sign for some of his/her chosen message. In order to avoid many other formerly signatures to correspond to single given message the algorithm for signature generation has to be definite in nature. The attacker is allowed to ask for each message at most one signature due to compromised defensive system in Single-chance CMA group unless \( T \) depends only on \( s_e \). We can derive subsequent standard outcome with the help of direct use of techniques in [40].

**Theorem 4.1.** (Forking lemma): Let \( \Gamma \) be a Turing machine with probabilistic polynomial time, the input of which contains public information only. By \( A \) and \( \varrho \), we denote count of relevant queries \( \Gamma \) may request from the random oracle, and count of relevant queries \( A \) may request from the signer, respectively. Suppose in time limit \( T, \Gamma \) produces a valid signature \((M, E_\Gamma, C_\Gamma, D_\Gamma)\) with a probability of \( \varepsilon \) for a signature scheme. When an input message \( M \) is provided, it generates \((s_\Gamma, \Delta_\Gamma, E_\Gamma) \) in which \( s_\Gamma \) arbitrarily chose its value in a set consist of larger values, \( D \) is hash value \((h_\varepsilon(M, s_\Gamma)), h_\varepsilon(M)) \) and \( s_\Gamma \) depends only on \( s_e \), \( M \), and \( D \).

We can get the definite private value with the help of this method

\[
\begin{align*}
\varepsilon & = (s - s')/h_\varepsilon(M, s) - h_\varepsilon(M, s) \right)
\end{align*}
\]

When \((t, q_{\text{auth}}, T)\) is hard to be ruined by any counterfeiter, the short signature scheme is \((t, q_{\text{auth}}, T)\) secure.

**Definition 4.2.** (FCM Assumption): If \( \varrho \) runs in a maximum of \( t \) steps and computes the fractional chaotic maps \( F_M \left( \mathcal{T}_\varrho(\mathcal{E}_1) \right) \equiv \mathcal{E}_\varrho \) input \((\mathcal{E}_1, q, \varrho)\) and \( \mathcal{T}_\varrho(\mathcal{E}_1) \) with a probability where probability is based on uniformly selected coins of \( \varrho \) and \( q \) from \( Z \), \( \varrho \) probabilistic algorithm is said to \((t, q, \varrho)\)-split FCM in a group \( G_{\mathcal{E}_{\varrho}} \).

Here it can be said that group \( G_{\mathcal{E}_{\varrho}} \) is a \((t, q, \varrho)\)-FCM group unless algorithm in group \( G_{\mathcal{E}_{\varrho}} \) can split FCM.

**Security proof of the introduced SSS utilizing FCM**

The recommended SSS is based on [39,40] which is a prevalent signature scheme. When an input message \( M \) is provided, it generates \((s_\Gamma, D_\Gamma, C_\Gamma) \) in which \( s_\Gamma \) arbitrarily chose its value in a set consist of larger values, \( D \) is hash value \((h_\varepsilon(M, s_\Gamma)), h_\varepsilon(M)) \) and \( s_\Gamma \) depends only on \( s_e \), \( M \), and \( D \).

We can derive subsequent standard outcome with the help of direct use of techniques in [40].
Theorem 4.2. Let $G_{E_i}$ be a $(\langle t', E' \rangle)$-FCM group, then the SSS in the ROM is $(\langle t, q_{b_0}, q_{b_0}, q_{a_0}, \sigma \rangle)$ secure against EUF-CMA, where
\[
t' = \frac{2^{2(4t_2 + 2 t_2)}}{16} \cdot \left( 1 + \frac{1}{2^{2(t_2 + t_2)}} + \frac{1}{2^{2(t_2 + t_2)}} \right)
\]
\[
n' = \frac{2^{2(t_2 + t_2)}}{16} \cdot \left( 1 + \frac{1}{2^{2(t_2 + t_2)}} + \frac{1}{2^{2(t_2 + t_2)}} \right)^2
\]
Here $C.$ refers to the expense of computing a long exponentiation in $G_{E_i}$.

Proof. For proving security of SSS, ROM is used. We assume that a EUF-CMA counterfeiter $g$ that $(\langle t, q_{b_0}, q_{b_0}, q_{a_0}, \sigma \rangle)$ separates the SSS is found. The random oracles $h_1, h_2, S$ can be queried with a polynomial number of queries by which it is a probabilistic polynomial time program arranged with extended open sequence of arbitrary bits.

An algorithm $\mathcal{A}$, which receives $(\langle q, p, g, p \rangle)$ as input is needed to be generated for us being a "simulator." For calculating the FCM i.e. $T_p(g)$ as a computer program, $\mathcal{A}$ tries to utilize $g$.

Algorithm $\mathcal{A}$ simulates one or two SSS runs to counterfeiter $A$. Hash inquiries $h_1$ and $h_2$ are reacted by A, S signature inquiries by Algorithm $\mathcal{A}$, and tries to twist A’s potential forgeries $(M, \sigma)$ into an FCM i.e. $T_p(g)$ solution. By providing $(\langle q, p, g, p \rangle)$ Algorithm $\mathcal{A}$ commences the first imitation and an extensive series of arbitrary bits for A. Then, A’s inquiries are responded by as follows:

**Responding $h_1$-oracle inquiries:** To get the compliant answer, $\mathcal{A}$ search for the $h_1$-list (query-response list in which entries contain of tuples $(\langle M, \sigma \rangle, B_i, t)$ which A subjects a random oracle inquiry $(M, \sigma)$ in which $1 \leq i \leq q_{b_0}$) $\mathcal{A}$ replies with $D_i$ when tuple $(\langle M, \sigma \rangle, B_i, t)$ is in the $h_1$-list. Then $\mathcal{A}$ homogeneously at random generates $D_i$ from $Z$, responds with it, and improves tuple $(\langle M, \sigma \rangle, B_i, t)$.

**Responding $h_2$-oracle inquiries:** In the attempt of achieving the compliant answer, $\mathcal{A}$ search for the $h_2$-list (list of inquiry-response) where entries contain of tuples $(\langle M, \sigma \rangle, B_i, t)$ which $g$ subjects a random oracle inquiry $(M, \sigma)$ where $1 \leq i \leq q_{b_0}$. If the $q_{b_0}$-list contains a tuple $(\langle M, \sigma \rangle, B_i, t)$, then $\mathcal{A}$ reacts with $\psi_i$.

$\mathcal{A}$ will search for the $h_2$-list in the condition of $(M, \sigma)$ is a new inquiry. If the $h_2$-list contains some tuples $(\langle M, \sigma \rangle, B_i, t)$, $\mathcal{A}$ elects to choose one $\psi_{i\prime}$, creates $t_{i\prime}$ from $Z$, homogeneously at random, evaluates $\psi_{i\prime} = (M, \sigma, 0)$ in the absence of tuple $(\langle M, \sigma \rangle, B_i, t)$ in the $h_2$-list.

**Responding $S$-oracle inquiries:** For the purpose of obtaining the accurate reply, $\mathcal{A}$ search for the $S$-list (list of query-response) in which entries contain $(\langle M, \sigma \rangle, D_i, s_i)$ proviso $g$ subjects an inquiry for signature $(M, \sigma)$ in which $1 \leq i \leq q_{a_0}$. When a tuple $(\langle M, \sigma \rangle, D_i, s_i)$ occurs in $S$-list then $\mathcal{A}$ retorts with $(D_i, s_i)$.

$\mathcal{A}$ search for the $h_2$-list for the first time in the event of $(M, \sigma)$ is a new query for signature. $\mathcal{A}$ chooses $\psi_i$ if the $h_2$-list contains a tuple $(\langle M, \sigma \rangle, B_i, t)$ or else $\mathcal{A}$ homogeneously generates $t_{i\prime}$ at random from $Z$, calculates $\psi_{i\prime} = (M, \sigma, 0)$ in the absence of tuple $(\langle M, \sigma \rangle, B_i, t)$ in the $h_2$-list.

Then $\mathcal{A}$ homogeneously opts for $s_i$ from $Z$, at random and evaluates $\psi_{i\prime} = (M, \sigma, D_i, s_i)$; $\mathcal{A}$ replies with $(\langle M, \sigma \rangle, D_i, s_i)$, improves the tuple $(\langle M, \sigma \rangle, D_i, s_i)$, to S-list, and improves the tuple $(M, \sigma, D_i, k_i)$ to $h_2$-list. If tuple $(M, \sigma, D_i, k_i)$ is in the $h_2$-list with $D_i \neq D_i$, the simulation will be aborted and restarted (this unfortunate occurrence is at most probability $q_{b_0} + q_{a_0} + q_{b_0} + q_{a_0}$).

We can say that in order to bring entirely distinct outcomes contrary to the real attacks oracle based simulations are helpful.

We can presume that a novel authorized message and signature tuple $\psi$ with probability $g$ are ensued by counterfeiter $\mathcal{A}$. When $h_2$ $(M)$ or $h_1$ $(M, \sigma)$ is not inquired by $\mathcal{A}$, the probability is $p_r h_2(M, h_2(M, \sigma)^{2q_{b_0}^2} g^{2q_{b_0}^2}) = 0$. Let both $h_2$ $(M)$ or $h_1$ $(M, \sigma)$ are elected arbitrarily. Thus, the counterfeiter $\mathcal{A}$ carries on with the probability $h_2(M, h_2(M, \sigma)^{2q_{b_0}^2} g^{2q_{b_0}^2}) = 1$ a new signature $(\langle M, D, s \rangle)$ such that $h_2(M, h_2(M, \sigma)^{2q_{b_0}^2} g^{2q_{b_0}^2}) = D$ and $h_2(M) \in h_2 - list, h_1(M, \sigma) \in h_1 - list$.

The $h_2$-list consists of two kinds of entries. If $h_2(M) = k_{T_p(g)}$, then $h_2(M)^{2q_{b_0}^2} g^{2q_{b_0}^2} = 1$ implies $T_p(g)^{2q_{b_0}^2} g^{2q_{b_0}^2} = 1$, and $\sigma = \langle \sigma \rangle / D$. Considering that the number of $h_1$-query $(M, \sigma)$ with $h_2(M) = k_{T_p(g)}$ is $q_{b_0}$. Therefore, in the first replication the probability of solving the FCM is $\varepsilon$.

We assume $\mathcal{A}$ acquires the signature and message pair $(\langle M, D_i, s_i \rangle)$ in the first simulation, with $D_i = h_1(M, \sigma)$. Thus, the probability of solving the FCM is $\varepsilon$.

Thus various series of random bits, signatures, and diverse values for random functions tend to be given by $\mathcal{A}$. The point to be noted here is that $\mathcal{A}$ acts in response with the same value which is at the time of first simulation when the $h_2$-query $(M)$ is asked after this argument. Here, "Forking lemma" in [40] is applied. We expect that yields signature $(\langle M, D_i, s_i \rangle)$ this time around such that $h_2(M) \neq k_{T_p(g)}$ and $h_2(M, \sigma)^{2q_{b_0}^2} g^{2q_{b_0}^2}$ or the signature $(\langle M, D_i', s_i' \rangle)$ with $D_i' \neq D_i$.

Here, the "Splitting lemma" [34] is employed to calculate the probability in order to work $\mathcal{A}$ as anticipated. Let $U$ be the set of probable random bits series and random function estimates that carry forger $g$ up to the argument where $g$ requests for $h_2(M, \sigma)$, let $V$ be the set of probable random bits series and random function estimates after that. By inference, the probability at which $g$, supplying the series of random bits and random estimates $(\langle e, p \rangle)$ produces a forgery is $\langle g, p, g, p \rangle$ for any ubiquity $x \in U, p \in V$. Using "Splitting lemma", a "agreeable" subset occurs $\Omega \in U$ such that

\[
(\langle e, p \rangle) \geq \varepsilon / 2.
\]

(ii) The probability that $A$, delivered the arbitrary bits and arbitrary values sequences $(\langle e, p \rangle)$ in which $\theta \in \Omega \ ; p \in V$, produces a copy is at least $\varepsilon / 2$.

Expect the sequences of random bit and random function values given up to the argument in first simulation are $\varepsilon$. Consequently, the probability that $A$, delivered $(\langle e, p \rangle)$ in second simulation in the condition of any $p \in V$ is $(\varepsilon / 2)^2$.

Forged signature probability $(M, D_i, s_i)$ with $h_2(M, \sigma) = k_{T_p(g)}$ and $h_2(M, \sigma)^{2q_{b_0}^2} g^{2q_{b_0}^2} \neq k_{T_p(g)}$. Forged signature probability $(M, D_i', s_i')$ with $D_i' \neq D_i$ is $(1 - \varepsilon) / (1 - \varepsilon) q_{b_0} = 1 / q_{b_0}$.

The probability of $\mathcal{A}$ resolving the FCM in the second simulation is thus
The probabilities can be concluded such that Algorithm $\mathcal{G}$ at least solves the FCM with probability \((nearly)$$

\begin{align*}
E - \left( \frac{1}{2^{\lceil m/2 \rceil}} + \frac{q_a(q_a + q_b)}{2^{\lceil m/2 \rceil}} \right) & \geq \left( E - \frac{1}{2^{\lceil m/2 \rceil}} + \frac{q_a(q_a + q_b)}{2^{\lceil m/2 \rceil}} \right)^2 \left( \frac{1}{q_a} + \frac{1}{q_b} \right) \\
\approx \left( E - \frac{1}{2^{\lceil m/2 \rceil}} + \frac{q_a(q_a + q_b)}{2^{\lceil m/2 \rceil}} \right)^{\frac{3}{4}} \left( \frac{1}{q_a} + \frac{1}{q_b} \right) & \geq \left( E - \frac{1}{2^{\lceil m/2 \rceil}} + \frac{q_a(q_a + q_b)}{2^{\lceil m/2 \rceil}} + (1 - \varepsilon) (E - \frac{1}{2^{\lceil m/2 \rceil}} + \frac{q_a(q_a + q_b)}{2^{\lceil m/2 \rceil}}) \right) \rightarrow (2 - \delta) \left( 2q_a + q_b \right)^2 + t).
\end{align*}

The single $h_1$-query and one $D'$ query are allowed for each $M$ request in the approximation of the probability $\varepsilon$: akin to the slightly feeble SO-CMA security structure, that is to say, the counterfeiter $y$ demands $(M, k)$ for both $h_1$-query and one $D'$ query. At the same time Algorithm $\mathcal{G}$ reacts with $h_1(M, k) = D$, and $h_1(M) = k \mathcal{G}(g)$. In this case, $\varepsilon = 1$. Here a robust reductionist evidence of safety is obtained.

Each $h_1$-query $(M, k)$ is consequently the $D'$ query acting against this affirmative approximation. It leads to find a movable reductionist security evidence as it is observed when $\varepsilon = 0$ similar to the Schnorr signature scheme. We are eclectically letting $\varepsilon = 1/2$ because the set of series of arbitrary bits and arbitrary function values that $\mathcal{G}$ supplies to counterfeiter $y$ is arbitrary. Therefore

\begin{align*}
t' & = 3 \left( \frac{q_a + q_b}{2} + \frac{1}{2^{\lceil m/2 \rceil}} \right) \text{ and} \\
E' & = \left( E - \frac{1}{2^{\lceil m/2 \rceil}} + \frac{q_a(q_a + q_b)}{2^{\lceil m/2 \rceil}} \right) + \frac{1}{16} \left( E - \frac{1}{2^{\lceil m/2 \rceil}} + \frac{q_a(q_a + q_b)}{2^{\lceil m/2 \rceil}} \right) \rightarrow (2 - \delta) \left( 2q_a + q_b \right)^2 + t).
\end{align*}

Essentially, this reductionist technique effectively works on the utilization of $h_1$-query command and $h_2$-query for the duplicate message insisted by counterfeiter $A$. Hence, we are led to believe that lying among tight and loose, this reductionist evidence is complete (Goh and Tarecki [36]).

The security of the hash functions: For acquiring a short signature we allow $p$ to be 160 bits. Recovering $M$ and $M'$ messages is unproblematic such that $h_1(M, k) = h_1(M', k)$ by birthday attacks consequently the hash value of $h_2$ is 80 bits. The signature returned by the signer is based on a random number $k$ instead of $k$ whenever the attacker insists on a signature on $M$. Despite the uncertainty of viability in finding other $M'$ message with $h_2(M, k) = h_1(M', k)$, it is for certain that finding $M$ with $h_2(M') = h_2(M)$ is impracticable, as the hash value of $h_2$ is at least 1024 bits. In the meantime no process will recover $s_d$ from the multivariate congruence $h_1(M, h_2(M))^{2^m}(g)^{2^m}(p)$ or find $k, s$ from $h_2(M)^{2^m}(g)^{2^m}(p) = k$. Since the ROM adopts that hash functions are perfect, the probability is

\begin{align*}
\Pr_{ex_{h_1}} \left[ h_1(M, k) = D \mid VM \in \{0, 1 \}^*, \forall D \in \mathbb{Z}_{2^m/2} \right] = \frac{1}{2^{m/2}}.
\end{align*}

Performance comparison

In this section, we discussed the performance comparison between the proposed technique and the recent presented technique such as Cui et al. [41], Shen et al. [18], Esposito et al. [42], Mughal et al. [43], Meshram and Obaid [44] and Zhang et al. [45]. The performance of the proposed work has been discussed based on the storage cost, communication cost, and the computational cost. The performance has been compared based on the cost for signing stage, and the verification stage. Table 2 give information about the notations used for comparative estimations.

It has been noted that the signing stage and the verification stage require more computational costs compared to the stage of installation and extraction. Therefore, the comparative study has been done based on the computational cost for signing stage and the verification stage. The state-of-the-art studies discussed in Cui et al. [41], Shen et al. [18], Esposito et al. [42], and Mughal et al. [43], Meshram and Obaid [44] and Zhang et al. [45] have been compared with the proposed work on performance metrics. The relations between $\mathcal{T}_{\text{exp}}, \mathcal{T}_{\text{chaotic}}, \mathcal{T}_{\text{mul}}, \mathcal{T}_{\text{exp}}, \mathcal{T}_{\text{exp}}$, and $\mathcal{T}_{\text{pair}}$ with respect to $\mathcal{T}_{\text{hash}}$ = 0.32 ms have been established in [25-27,46,47]. The proposed work has used the above mentioned notations and their relations are shown in Table 3.

Using Table 2, the computational complexity order among the metrics is shown as:

\begin{align*}
\mathcal{T}_{\text{hash}} \approx \mathcal{T}_{\text{chaotic}} < \mathcal{T}_{\text{mul}} < \mathcal{T}_{\text{exp}} < \mathcal{T}_{\text{exp}} < \mathcal{T}_{\text{pair}}
\end{align*}

Fig. 3 shows the comparative analysis between the existing schemes and the proposed scheme based on the computational cost for signing stage. The proposed scheme is seen effective as compared to the existing schemes. The proposed scheme requires 2.56 ms for signing stage, shows the effectiveness over the existing schemes. Fig. 4 shows the comparison on the computational cost for verification stage. It shows that the proposed technique is also efficient in verification stage.

Table 4 present the quantitative analysis of the proposed technique and show the comparison based on the total cost including signing stage and the verification stage. It from Table 4 that the total cost has been reduced to 4.97 ms. Thus, the proposed technique is found to be efficient as compared to the other techniques in the literature.

| Sr. No. | Notation | Meaning |
|---------|----------|---------|
| 1       | $\mathcal{T}_{\text{exp}}$ | Execution time for a modular exponentiation in group |
| 2       | $\mathcal{T}_{\text{chaotic}}$ | Execution time for chaotic map operation |
| 3       | $\mathcal{T}_{\text{mul}}$ | Execution time for one modular multiplication |
| 4       | $\mathcal{T}_{\text{hash}}$ | Execution time for one way hash function |
| 5       | $\mathcal{T}_{\text{pair}}$ | Execution time for one bilinear pairing operation |
| 6       | $\mathcal{T}_{\text{inv}}$ | Execution time for one modular inverse operation |

Table 3 Relationship among notations.

| Sr. No. | Relationships among notations |
|---------|------------------------------|
| 1       | $\mathcal{T}_{\text{chaotic}} \approx \mathcal{T}_{\text{hash}}$ |
| 2       | $\mathcal{T}_{\text{mul}} \approx 2.5 \mathcal{T}_{\text{hash}}$ |
| 3       | $\mathcal{T}_{\text{inv}} \approx 7.5 \mathcal{T}_{\text{hash}}$ |
| 4       | $\mathcal{T}_{\text{exp}} \approx 600 \mathcal{T}_{\text{hash}}$ |
| 5       | $\mathcal{T}_{\text{pair}} \approx 1550 \mathcal{T}_{\text{hash}}$ |
In human-centered IoT, the protection of sensitive data is essential to provide a protection from forgery attacks. Digital signature is the safest option in asymmetric cryptography for ensuring the ownership and validity of the contact parties. This paper uses fractional chaotic maps for secure communication in human-centered IoT to present an effective provably secure short signature technique. This is existentially unforgeable under EUF-CMA at ROM. Results demonstrate the superiority of our strategy, in comparison with competitors, to take fewer overhead based on computing and communication costs alongside resilience studies. The proposed SSS achieves less processing time and less overhead communication in verification and signature operations, in addition to improved resistance to capture attacks. It is therefore very difficult to crack FCM-based SSS compared to DSA which is based on discrete logarithm. In future work, we will develop a new efficient fuzzy signature scheme using fractional chaotic maps for Block-
chain using Biometrics under human-centered IoT environments. The limitation of fractional chaotic maps based scheme is only sample selection.

Compliance with Ethics Requirements

This article does not contain any studies with human or animal data subjects.

Declaration of Competing Interest

The authors have declared no conflict of interest.

Acknowledgments

The authors are grateful to the learned reviewers and their critical comments. Their comments have guided the authors to improve the manuscript.

References

[1] Bera S, Misra S, Roy SK, Obaidat MS. Soft-WSN: software-defined WSN management system for IoT applications. IEEE Syst J 2018;12(3):2074–81.
[2] Misra S, Roy SK, Roy, Obaidat MS. MEGAN: multipurpose energy-efficient, adaptable, and low-cost wireless sensor node for the internet of things. IEEE Syst J 2020;14(1):144–51.
[3] Nazir S, Ali Y, Ullah N, Garcia-Magariño I. Internet of things for healthcare using effects of mobile computing: A systematic literature review. Special Issue: Internet of Things for Healthcare Using Wireless Communications or Mobile Computing. 2019, Article ID 5931315, 20 pages, https://doi.org/10.1155/2019/5931315.
[4] Ayaz M, Sharif MAUZ, Mansour A. Internet-of-Things (IoT)-based smart agriculture: toward making the fields talk. IEEE Access 2019;7:129551–83.
[5] Samih H. Smart cities and internet of things. J Infranet Technol Case Appl Res 2019;21(1):3–12.
[6] Yang C, Shen W, Wang X. Applications of internet of things in manufacturing. In: IEEE 20th Int. Conf. on computer supported cooperative work in design (CSCWD), Nanchang, 2016, p. 670–675.
[7] Yinghua Z, Guanghua F, Zhigang Z, Zhan H. Discussion on application of IoT technology in coal mine safety supervision. Procedia Eng 2012;34:233–7.
[8] Yang H, Lee W, Lee H. IoT Smart home adoption: the importance of proper level automation. Special Issue: Advanced Internet of Things and Big Data Technology for Smart Human-Care Services, 2018, Article ID 6646036, 11 pages, https://doi.org/10.1155/2018/6646036.
[9] Wafa A, Zayanuy CA, Amousy I, Sedy F. User-centric IoT: challenges and perspectives. In: UBICOMM 2018: The Twelfth Int. Conf. on Mobile Ubiquitous Computing, Systems, Services and Technologies, 2019, p. 27–34.
[10] Fernández-Carrión TM, Fraga-Lamas P. A review on human-centered IoT-connected smart labels for the industry 4.0. IEEE Access 2018;6:29399–57.
[11] Coulton P, Lindley JG. More-than human centred design: considering other things. Des J 2019;22(4):463–81.
[12] Kotrotsis C, Routis I, Politi E, Nikolaidou M, Dimitrakopoulos G, Anagnostopoulos D, et al. Evaluating Internet of Medical Things (IoMT)-based systems from a human-centric perspective. Internet Things (2019):8:100–25.
[13] Radovan AG, Moaddy K, Salama KN, Momani S, Hashim I. Control and switching synchronization of fractional order chaotic systems using active control technique. J Adv Res 2014;5:125–32.
[14] Ibrahim RW, Elbaid RM, Obayis SJ. Symmetric configurable fractional derivative of complex variables. Mathematics 2020;8:363. doi: https://doi.org/10.3390/maths8030369.
[15] Rivest R, Shamir A, Adleman LA. Method for obtaining digital signatures and public-key cryptosystems. Commun ACM 1978;21(2):120–6.
[16] ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 1985;31(4):469–72.
[17] Johnson D, Menezes A, Vanstone S. The elliptic curve digital signature algorithm (ECDSA). Int J Inf Secur 2001;1(1):36–63.
[18] Shen L, Ma J, Liu X, Wei F, Miao M. A secure and efficient ID-based aggregate signature scheme for wireless sensor networks. IEEE Internet Things J 2017;4(2):546–54.
[19] Vaidyanathan S, Sambas A, Mamat M, Sanjaya WSM. Analysis, synchronisation and circuit implementation of a novel jerk chaotic system and its application for voice encryption. Int J Model Identif Control 2017;28(2):153–66.
[20] Vaidyanathan A, Azari AT, Rajagopal K, Sambas A, Kacar S, Cavusoglu U. A new hyperchaotic temperature fluctuations model, its circuit simulation, FPGA implementation and an application to image encryption. Int J Simulat Process Model 2018;13(3):281–96.
[21] Mobayed S, Vaidyanathan S, Sambas A, Kacar S, Cavusoglu U. A novel chaotic system with boomerang-shaped equilibrium, its circuit implementation and application to sound encryption. Iranian J Sci Technol Trans Electrical Eng 2019;43:1–12.
[22] Hazifzl Islam SK. Identity-based encryption and digital signature schemes using extended chaotic maps. IACR Cryptology, ePrint Archive (275), 2014.
[23] Gao G, Peng X, Tian Y, Qin Z. A Chaotic maps-based authentication scheme for wireless body area networks. Int J Distrib Sensor Netw 2016;12(7):2174720.
[24] Lu Y, Li, Zhang H, Yang Y. An extended chaotic maps-based three-party password-authenticated key agreement with user anonymity. PLoS One 2016;11(4):e0153870. doi: http://dx.doi.org/10.1371/journal.pone.0153870.
[25] Meshram C, Lee CT, Meshram SG, Li CT. An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem. Soft Comput 2019;23(16):6937–46.
[26] Meshram C, Li CT, Meshram SG. An efficient online/offline ID-based short signature procedure using extended chaotic maps. Soft Comput 2019;23(3):747–53.
[27] Meshram C, Obaidat MS, Meshram SG. Chebyshev chaotic map-based ID-based cryptographic model using subtree and fuzzy-entity data sharing for public key cryptography. Sec Privacy 2018;1(1):e12.
[28] Mason JC, Handscomb DC. Chebychev polynomials. Boca Raton: Chapman & Hall/CRC; 2003.
[29] Bergamo F, D’Arco P, Santis A, Kokarev L. Security of public key cryptosystems based on Chebychev polynomials. IEEE Trans Circuits Syst I 2005;52(7):1382–93.
[30] Han S, Chang E. Chaotic map-based key agreement with out clock synchronization. Chaos Soliton Fractals 2009;39(3):1283–9.
[31] Zhang L. Cryptanalyses of the public key encryption based on multiple chaotic systems. ChaosSoliton Fractals 2008;37(3):669–74.
[32] Chen F, Liao X, Wong KW, Han Q, Li Y. Period distribution analysis of some linear maps. Commun Nonlinear Sci Numer Simul 2012;17:3848–56.
[33] Yang XJ, Baleanu D, Srivastava HM. Local fractional integral transforms and their applications. Academic Press; 2015.
[34] Canetti R, Goldreich O, Halevi S. The random oracle methodology. In: Proc. of the 30st Annual ACM symposium on Theory of Computing, ACM Press, New York, 1998, p. 209–218.
[35] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attacks. SIAM J Comput 1988;17(2):281–308.
[36] Goh EJ, Jarecki S. A signature scheme as secure as the Diffie–Hellman problem. In: Proc. of Eurocrypt’03, LNCS, vol. 2656, Springer-Verlag, Berlin, 2003, p. 401–415.
[37] Maurer U, Wolf S. The relationship between breaking the Diffie–Hellman protocol and computing discrete logarithms. SIAM J Comput 1999;28(5):1689–721.
[38] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. J Cryptolo 2000;13(3):361–96.
[39] Shao Z. A provably secure short signature scheme based on discrete logarithms. Inf Sci 2007;177(23):5432–40.
[40] Pointcheval D, Stern J. Security proofs for signature schemes. In: Proc. of Eurocrypt’96, LNCS, vol. 1070, Springer-Verlag, Berlin, 1996, p. 387–398.
[41] Cui H, Deng RH, Liu Y, Li Y, Liu N. Server-aided attribute-based signature with revocation for resource-constrained industrial-internet-of-things devices. IEEE Trans Inf Sec 2018;14(8):3724–32.
[42] Esposito C, Castiglione A, Palmieri F, Santis AD. Integrity for an event notification within the industrial internet of things by using group signature. IEEE Trans Inf Sec 2018;14(8):3699–708.
[43] Mughal MA, Luo A, Ullah A, Ullah S, Mahmood Z. A Lightweight digital signature based security scheme for human-centered internet of things. IEEE Access 2018;6:31630–43.
[44] Meshram C, Obaidat MS. An efficient provably secure IBS protocol using integer factorization problem. In: Lecture Notes in Networks and Systems, vol. 121, Springer (ICAS1 2019), 2020, p. 427–439.
[45] Zhang C, Luo Y, Fan Y, Liang Y. Security analysis of an identity-based signature from factorization problem. IEEE Access 2020;8:23277–83.
[46] Benasser AM, Samsudin A. A new identity-based encryption (IBE) scheme using extended chebyshev polynomial over finite fields Zp. Phys Lett A 2014;370:7468–73.
[47] Ibrahim MH, Kumari S, Das AK, Wazid M, Odeul V. Secure anonymous mutual authentication for star two-tier wireless body area networks. Comput Methods Programs Biomed 2016;135:37–50.