Soft Computing (2019) 23:6937–6946
https://doi.org/10.1007/s00500-018-3332-5

METHODOLOGIES AND APPLICATION

An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem

Chandrashekhar Meshram[1,2] · Cheng-Chi Lee[3,4] · Sarita Gajbhiye Meshram[1] · Chun-Ta Li[5]

Published online: 19 June 2018

Abstract

Recently, the chaos theory has been dealt with as a decent approach to reducing the computational complexity of a cryptographic technique while fulfilling the security necessities. In an ID-based cryptographic system where public keys are distributed to individual users, the application of chaotic maps allows users to set their network addresses or names as their individual public keys. This makes the public key cryptographic technique very user-friendly in that the public key confirmation process can be very informal and direct. In such a design, no huge public key database is required, and therefore, those security issues arising as a result of the existence of a public key database can be avoided. The aim of this article is to go deep into the possibility of transforming a chaotic-map-based cryptosystem into an ID-based technique without having to build a new framework from scratch or to do adjustment to the chaotic maps.

Keywords Chaotic maps · Public key cryptography · ID-based cryptography · IND-CCA · IND-sID-CCA · Random oracle model

1 Introduction

The research into the world of chaotic maps as well as their applications in the field of cryptography has gained extensive attention in recent years, taking up a mainstream course in the realm of cryptosystems. Chaotic frameworks are mostly characterized by delicate reliance on beginning conditions and closeness to arbitrary behavior, properties which appear to be essentially similar to some required by a few cryptographic primitives (Kocarev 2001; Wei et al. 2017).

In 1976, Diffie and Hellman proposed one of the world's first public key cryptographic systems in their well-known paper "*New Directions in Cryptography*" (Diffie and Hellman 1976). Shortly after, Rivest, Shamir and Adlemann proposed the notable RSA cryptosystem (Rivest et al. 1978) and confirmed the practicality of public key cryptosystems. Since then, numerous new cryptosystems have been developed and publicly presented (see Menezes et al. 1997; Stinson 2002 for some related examples). In general, public key cryptography has been recognized as a well-established domain of research and study in the field of information transmission/communication security.

In 1993, in his doctoral dissertation, Hwu (1993) introduced the chaos theory to public key cryptography and presented his chaotic public key cryptosystem design with a one-dimensional difference equation (1DDE) as well as a quadratic difference equation. In addition, Hwu's framework makes use of ElGamal's technique (ElGmal 1995) to accomplish the encryption process. Basically, a 1DDE (i.e.,

Communicated by V. Loia.

✉ Cheng-Chi Lee
cclee@mail.fju.edu.tw

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Chun-Ta Li
th0040@mail.tut.edu.tw

[1] Department of Mathematics and Computer Science, Rani Durgavati University, Jabalpur, India

[2] Department of Mathematics, RTM Nagpur University, Nagpur, India

[3] Department of Library and Information Science, Fu Jen Catholic University, New Taipei 24205, Taiwan, ROC

[4] Department of Photonics and Communication Engineering, Asia University, Wufeng Shiang, Taichung 413, Taiwan, ROC

[5] Department of Information Management, Tainan University of Technology, 529 Jhong Jheng Road, Tainan 710, Taiwan, ROC

reiteration map) is well qualified as a one-way function. The security of this framework relies upon the infeasibility of resolving discrete logarithm (DL) defined over finite fields. Here, a trapdoor, however, can be worked out by letting the real possessor know the reiteration times of the distinction condition.

Kocarev and Tasev (2003) developed a public key cryptographic technique using Chebyshev polynomials defined over real numbers by supplanting the multiplications in traditional procedures with the reiteration of Chebyshev polynomials characterized on real numbers. This work was distinguished both for giving new directions of research to the world of public key cryptography and for bringing in the fundamental mathematical problem of RSA. This solid mathematical problem here is that given an underlying point x and its rth iteration esteem $\mathcal{T}_r(x)$, to locate a huge integer is challenging and just as hard as integer factorization (IF), which is what RSA depends on. Kocarev and Tasev's work can be applied to do authentication (Mason and Handscomb 2003; Lee et al. 2013a, 2014a; Lee and Hsu 2013), as in Telecare Medicine Information System (Li et al. 2014) as well as Mobile Emergency Medical Care System (Lee et al. 2013b) in addition, Chebyshev polynomials can also be utilized in some key agreement techniques (Lee et al. 2012, 2014b).

ID-based cryptography, on the other hand, is an augmentation of the public key cryptography paradigm, which was first suggested by Shamir (1984) at CRYPTO'84. In order to better understand ID-based cryptography, we start by reviewing how traditional public key systems are usually put to use in real-life applications. First, for the system to run at a reasonable speed, public key cryptographic techniques are usually used in conjunction with a private key cryptographic technique. More precisely, the public key technique is utilized in order to produce a shared encryption key for the secret key scheme, where the encryption key is known to the receiver and the sender in communication. Once this is done, they simply use this common secret key for encrypting the rest of the messages exchanged. This initial stage is usually called a key exchange technique. It can be devised in several ways.

Cocks (2001) utilized a variation of IF to build an ID-based encryption technique. Unfortunately, the technique is ineffective in that a plaintext is encrypted bit-by-bit and thus the length of the ciphertext produced is way too long. After some time Boneh and Boyen (2004) provided an effective ID-based cryptographic technique without ROM that was safe in the selective identity model, and Waters (2005) also proposed a proficient and secure ID-based cryptographic technique without ROM. Meanwhile, Heng and Kurosawa (2006) utilized a polynomial-based model to build an ID-based cryptographic technique. Their technique does not require random oracles and is semantically secure under the DL supposition. Also, Lee and Liao (2004) offered a transformation procedure that can translate DL-based cryptosystems into ID-based cryptographic techniques without having to build up a new framework from scratch. Meshram et al. (2012a, b, c) presented some new efficient ID-based cryptographic techniques and ID-based mechanisms using DL, GDL and IF. The security of these techniques relies on the difficulty of solving DL, GDL and IF simultaneously. Meshram and Meshram (2011, 2013, 2017) proposed new variants of the ID-based beta cryptographic technique and offered a transformation method to transfer a public key cryptographic technique into an ID-based cryptographic technique without having to develop a new ID-based framework. In addition, Meshram (2015a, b, c) presented a new provably secure ID-based cryptographic protocol, a new variant of ID-based beta cryptographic technique and an efficient technique based on IF and DL. The efficiency of Meshram's works can be compared to that of ElGamal's cryptosystem (ElGmal 1995). Besides, Meshram and Obaidat (2015) also offered a new ID-based system that was a quadratic-exponentiation randomized cryptographic scheme. Most recently, Meshram et al. (2016) proposed a new ID-based cryptographic technique based on partial discrete logarithm. Liu et al. (2017) purposed efficient encryption using subtree for fuzzy-entity data sharing under cloud computing environment, and Meshram et al. (2017a, b) presented a new secure key authentication technique for public key cryptography and efficient ID-based cryptographic technique using GDL and IF.

Our contribution: This article offers an efficient transformation model that can translate a chaotic-map-based cryptosystem into a secure ID-based cryptographic scheme without having to build up a new framework from scratch. In particular, our new model comes with a key generation stage that operates at extremely low computation complexity. In addition, with our new model, no adjustment needs to be done to the original chaotic maps in the cryptosystem. By transforming a chaotic-map-based cryptosystem into an ID-based cryptographic scheme, our new model offers the secure ID-based scheme the same kind of convenience and user-friendliness the original chaotic-map-based cryptosystem provides, as now individual users get to pick their own names or network addresses as their public keys. This makes public key confirmation extremely natural and direct. In such a model, no huge public key database is needed. Besides, we also provide an efficient reductionist security proof against the selective identity adaptive chosen ciphertext attack (IND-sID-CCA) by Canetti et al. (2003) in the ROM.

Structure of the article: The rest of this article is organized as follows: Firstly, some background materials will be given in Sect. 2. Then, our efficient ID-based cryptographic transformation model will be presented in Sect. 3. Then, an example of how the proposed model works will be shown in Sect. 4 to help confirm the practicality of the model. After that, the security properties of the new model will be analyzed in Sect. 5. Then, in Sect. 6, we will see how the proposed

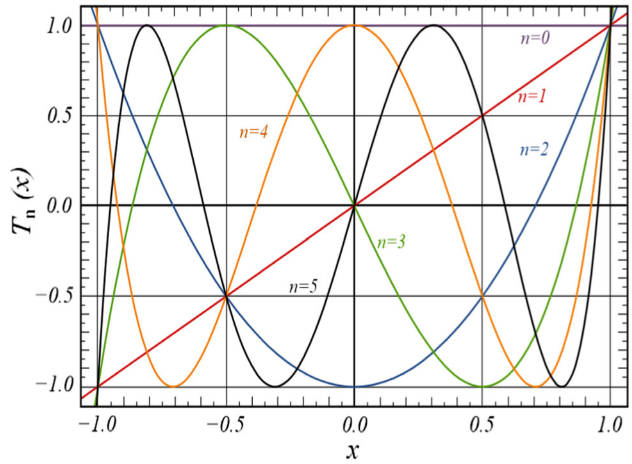

Fig. 1 Chebyshev polynomials

model compares with some other protocols in terms of efficiency performance. Finally, the conclusion will be given in Sect. 7.

2 Background materials

In this section, we review the Chebyshev polynomial and extended chaotic maps, both of which we will utilize as parts of the proposed scheme. After that, we shall specify some required security notions, respectively.

2.1 Chebyshev chaotic maps

In this subsection, we take a look at Chebyshev polynomials (Mason and Handscomb 2003) and see how they work as illustrated in Fig. 1. Chebyshev polynomial $\mathcal{T}_r(x)$ is a polynomial in the variant of x with degree n. Let $x \in [-1, 1]$ be the variant and n be an integer. The Chebyshev polynomial is specified by

$$\mathcal{T}_n(x) = \cos(n \times \arccos(x)),$$

$$\mathcal{T}_0(x) = 1$$

$$\mathcal{T}_1(x) = x$$

$$\mathcal{T}_n(x) = 2x\mathcal{T}_{n-1}(x) - \mathcal{T}_{n-2}(x); \quad n \geq 2$$

Here, $\arccos(x)$ and $\cos(x)$ are trigonometric functions (Bergamo et al. 2005) characterized as $\arccos : [-1, 1] \to [0, \pi]$ and $\cos : R \to [-1, 1]$. A few cases of Chebyshev polynomials for n=1, 2, 3, 4, 5 are illustrated in Fig. 1.

Chebyshev polynomials have two significant properties (Han and Chang 2009; Li et al. 2017): the chaotic property and the semigroup property.

(1) The chaotic property:

The Chebyshev polynomial map, defined as $\mathcal{T}_r$: $[-1, 1] \to [-1, 1]$ with degree $n > 1$, is a chaotic map with its invariant density function being $f^*(x) = \frac{1}{\left(\pi\sqrt{1-x^2}\right)}$ for some positive Lyapunov exponent $\lambda = \text{In}\, n > 0$.

(2) The semigroup property:

$\mathcal{T}_w(\mathcal{T}_l(x)) = \cos\big(w \cos^{-1}\big(\cos\big(l \cos^{-1}(x)\big)\big)\big) = \cos\big(wl \cos^{-1}(x)\big) = \mathcal{T}_{lw}(x) = \mathcal{T}_l(\mathcal{T}_w(x))$, where w and l are positive integers and $x \in [-1, 1]$.

Chebyshev polynomials come with two challenges, which are considered to be hard to handle within polynomial time:

(1) Given two components x and y, the assignment of the DL is to find the integer w with the end goal $\mathcal{T}_w(x) = y$.
(2) Given three components x, $\mathcal{T}_w(x)$, and $\mathcal{T}_l(x)$, the assignment of the Diffie–Hellman problem (DHP) is to calculate the component $\mathcal{T}_{wl}(x)$.

2.2 Extended chaotic maps

Zhang (2008) demonstrated that the above semigroup property holds for Chebyshev polynomials within the interval $(-\infty, +\infty)$, which can be enhanced by:

$$\mathcal{T}_n(x) = (2x\mathcal{T}_{n-1}(x) - \mathcal{T}_{n-2}(x))(\text{mod}\ q)$$

where $n \geq 2$, $x \in (-\infty, +\infty)$, and q is a prime number. Now we consider recurrence equation $\mathcal{T}_n(x) = 12\mathcal{T}_{n-1}(x) - \mathcal{T}_{n-2}(x))(\text{mod}\ 13)$ with $\mathcal{T}_0(x) = 1$ and $\mathcal{T}_1(x) = 6$, where $q = 13$. Then $\mathcal{T}_n(x)$ generated by this recurrence is 1, 6, 6, 1, 6, 6,… Its period is $\mathcal{T} = 3$ (Chen et al. 2012; Meshram et al. 2018). Obviously,

$$\mathcal{T}_w(\mathcal{T}_l(x)) \equiv \mathcal{T}_{lw}(x) \equiv \mathcal{T}_l(\mathcal{T}_w(x))(\text{mod}\ q),$$

so the semigroup property still holds, and the enhanced Chebyshev polynomials also commute under composition. Now we consider recurrence equation $\mathcal{T}_n(x) = \left(2^{131}\mathcal{T}_{n-1}(x) - \mathcal{T}_{n-2}(x)\right)\left(\text{mod}\ (2^{130} + 7)\right)$ with $\mathcal{T}_0(x) = 1$ and $\mathcal{T}_1(x) = 2^{130}$, where $q = 2^{130} + 7$. Then $\mathcal{T}_n(x)$ generated by this recurrence as below table (Chen et al. 2012; Meshram et al. 2018).

n	$\mathcal{T}_n(x)$
2	276350163825134130984024071869462216704
3	1039683198921322055717709420856678023168
4	1152244783873809830411690210056778809344
5	1164071919187354590884341147753577971712
6	1254725722161536169166953951337782444032
7	939844861111050535260748695617199407104
8	45559776274841150240913805300992049152
9	767388050443263617908949049536120094720
10	765975301349993996335937120326362595328
11	765975301349993996335937120326362595328
12	765975301349993996335937120326362595328
13	765975301349993996335937120326362595328

2.3 Security notions

The chosen ciphertext attack (IND-CCA) (Hwan et al. 2004; Kiltz and Vahlis 2008) is the standard security challenge a public key cryptographic technique has to be tried out against. Boneh and Franklin (2003) reinforced chosen ciphertext security for ID-based cryptographic technique by presenting IND-ID-CCA, where a foe $\mathfrak{F}$ gets to adaptively pick an objective public key to attack even if it is not the general identity pre-chosen by the challenger. Indeed, IND-ID-CCA is the most demanding security requirement imposed on an ID-based cryptographic technique, for it gives the foe the greatest possible convenience and power to attack. Canetti et al. (2003) then characterized another security notion for ID-based cryptographic techniques where the foe must submit an early signal to notify it will attack. We refer to this kind of attack as IND-sID-CCA. Now we specify IND-CCA and IND-sID-CCA as follows:

Definition 2.2.1 A public key cryptographic technique is said to be IND-CCA secure if $\exists$ no probabilistic polynomial time (PPT) foe $\mathfrak{F}$ has a non-negligible advantage (Hwan et al. 2004; Kiltz and Vahlis 2008), as illustrated in Fig. 2.

Definition 2.2.2 An ID-based cryptographic technique $\mathcal{I}$ is said to be IND-sID-CCA secure if $\exists$ no PPT foe $\mathfrak{F}$ has a non-negligible advantage (Canetti et al. 2003), as illustrated in Fig. 3.

3 Proposed transformation model

In this section, we shall present our new model that can transfer a chaotic-map-based cryptosystem into an ID-based cryptographic scheme. Please pay special attention to our key generation stage, as it is what really makes a difference. By effectively formulating private keys, chaotic-map-based cryptosystems can be transformed into ID-based cryptographic schemes in a straightforward way.

3.1 Setup phase

1. PKG picks any k users that will not collaborate together. The security limitation k then decides the minimum bit size of the user's identity.
2. Let q be a huge safe prime, s.t. $p|(q-1)$(Shao 2007) and $\log_2 p > k$ (Lee and Liao 2004), and also let

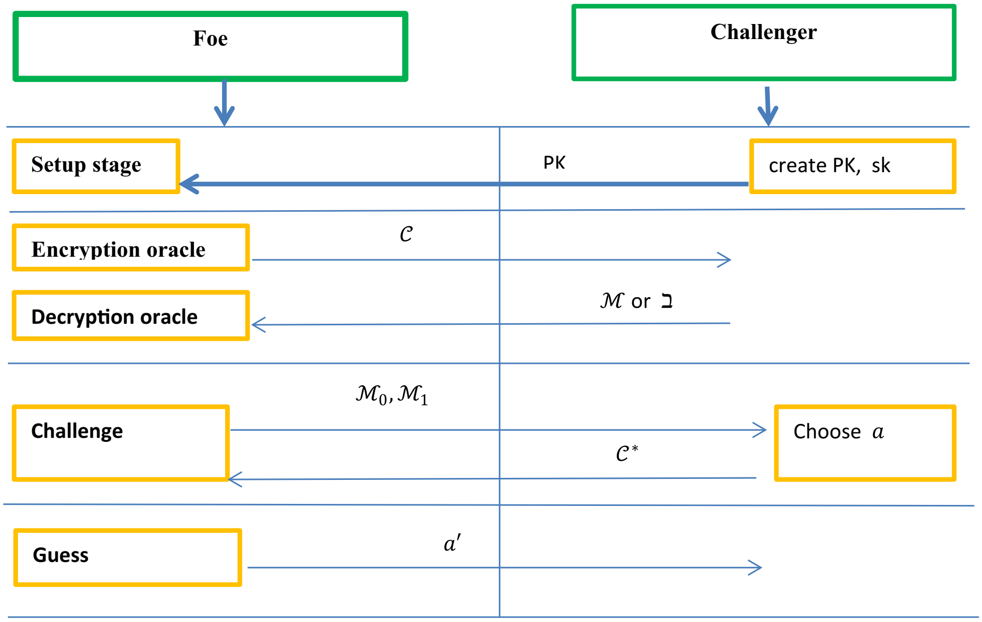

Fig. 2 Diagrammatic depiction of IND-CCA

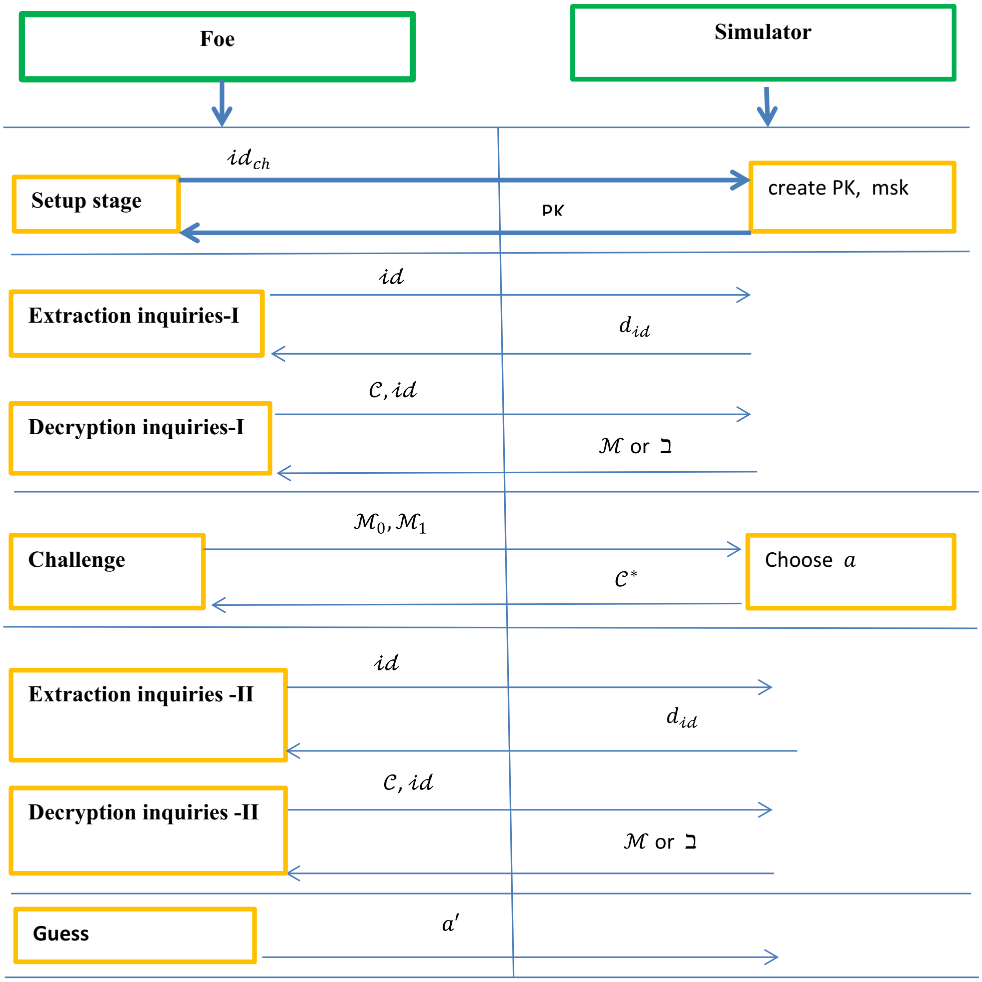

Fig. 3 Diagrammatic depiction of IND-sID-CCA

$G_{y,q} = \{y^0, y^1, \ldots, y^{p-1}\}$ be a subgroup of multiplicative group Z_q^* with prime order p, where y is a generator with prime order p (Shao 2007). Assume that v and $u = \mathcal{T}_v(y) (\text{mod } q)$ are the secret key and public key of PKG.

3. PKG randomly selects secret information $\{s_1, s_2, \ldots, s_k\}$, where $\sum_{i=1}^{k} s_i < p$, and the corresponding public information is given by $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_k\}$, where $\mathcal{P}_i = \mathcal{T}_{s_i}(y) (\text{mod } q), \forall i \in (1, k)$.
4. Each user U has a unique k-bit identity $id_U = (id_{U1}, id_{U2}, \ldots, id_{Uk})$, where $id_{Ui} \in \{0, 1\}$, $\forall i \in (1, k)$.
5. Define the hash function : $\{0, 1\} \rightarrow Z_q^*$.

Since $\log_2 p > k$; if p and q are 160 and 512 bits prime number, respectively, the maximal bit length of k is therefore 159 bits. Instead, the maximum threshold value we can characterize is 159. This obviously impacts the applications for the model. Hence, the choice of a suitable parameter depends not just on the quality of the chaotic maps but also on the number of members that will not plot together.

3.2 Key generation phase

Without loss of generality, suppose some user U wishes to start the procedure. Then, PKG and U go through the key generation phase to produce the private key. Figure 4 illustrates how the private key is generated.

1. An user U sends PKG his/her hashed identity $(id_U) = (\hbar_{U1}, \hbar_{U2}, \ldots, \hbar_{Uk})$, where $\hbar_{Ui} \in Z_q^*, \forall i \in (1, k)$.
2. PKG checks whether an identity (id_U) conforms to a specific arrangement. In the event that the identity checks out, then PKG utilizes its secret info to calculate $s_U = \sum_{i=1}^{k} s_i \hbar_{Ui} (\text{mod } p)$ and

$$\kappa_U = v * s_U \mathcal{P}_U (\text{mod } p), \tag{3.2.1}$$

where $\mathcal{P}_U = \prod_{i=1}^{k} \mathcal{T}_{\hbar_{Uk}}(\mathcal{P}_i) (\text{mod } q)$.

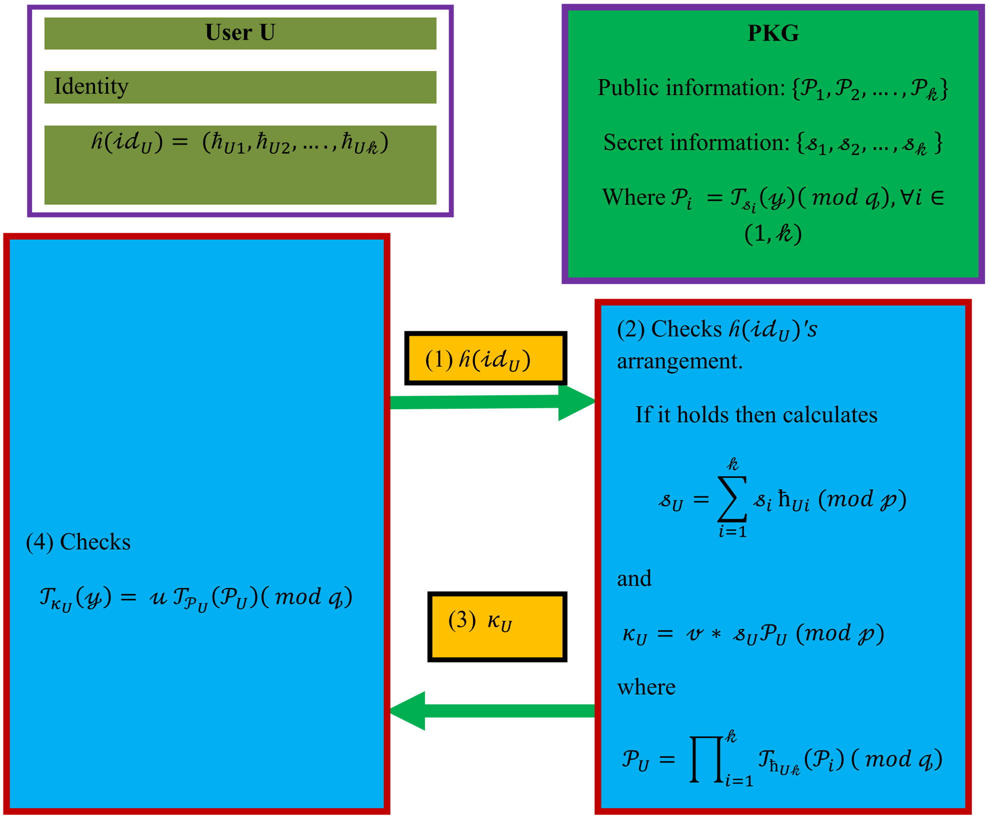
User U
Identity
$\hbar(id_U) = (\hbar_{U1}, \hbar_{U2}, \ldots, \hbar_{Uk})$
PKG
Public information: $\{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_k\}$
Secret information: $\{s_1, s_2, \ldots, s_k\}$
Where $\mathcal{P}_i = \mathcal{T}_{s_i}(y)(mod\ q), \forall i \in (1, k)$
(1) $\hbar(id_U)$
(2) Checks $\hbar(id_U)'s$ arrangement.
If it holds then calculates
$s_U = \sum_{i=1}^{k} s_i \hbar_{Ui}\ (mod\ p)$
and
$\kappa_U = v * s_U\mathcal{P}_U\ (mod\ p)$
where
$\mathcal{P}_U = \prod_{i=1}^{k} \mathcal{T}_{\hbar_{Uk}}(\mathcal{P}_i)\ (mod\ q)$
(3) κ_U
(4) Checks
$\mathcal{T}_{\kappa_U}(y) = u\,\mathcal{T}_{\mathcal{P}_U}(\mathcal{P}_U)(mod\ q)$

Fig. 4 Private key generation (PKG)

3. PKG secretly sends κ_U to U as U's private key.
4. U checks whether the condition $\mathcal{T}_{\kappa_U}(y) = u\mathcal{T}_{\mathcal{P}_U}(\mathcal{P}_U)(\mathrm{mod}\ q)$ holds, where $\mathcal{P}_U = \prod_{i=1}^{k}\mathcal{T}_{\hbar_{Uk}}(\mathcal{P}_i)(\mathrm{mod}\ q)$ can be derived from public info with no dispute.

The correctness of above equation can be proven as follows.

$$\mathcal{T}_{\kappa_U}(y)(\mathrm{mod}\ q) = \mathcal{T}_{(v*s_U\mathcal{P}_U)}(y)(\mathrm{mod}\ q)$$
$$= \mathcal{T}_v(y) * (\mathcal{T}_{\mathcal{P}_U}\left(\mathcal{T}_{s_U}(y)\right)(\mathrm{mod}\ q) = u\mathcal{T}_{\mathcal{P}_U}(\mathcal{P}_U)(\mathrm{mod}\ q)$$

Note: $\mathcal{P}_i = \mathcal{T}_{s_i}(y)(\mathrm{mod}\ q), \forall i \in (1, k)$. (Setup phase 3.1 point 3)

3.3 An ID-based transformation model

Through the key generation process, a chaotic-map-based cryptographic system can be straightforwardly transferred into an ID-based cryptographic system. Given a huge safe prime q such that $p|(q-1)$ accompanied by a global parameter $y \in Z_q^*$, the chaotic-map-based system (CMS) can be defined as CMS $= \{(q, y, v, u) : u = \mathcal{T}_v(y)\}$, where q, y, u and v are public and secrete keys, respectively. The proposed ID-based cryptographic transformation technique goes as follows:

a. Describe the configuration of the identity

As the biggest feature of an ID-based cryptographic technique, users simply utilize their identities as their public keys. Therefore, the first step is to check whether the identity matches a specific predetermined configuration.

b. Compute the private key as indicated by the key generation process

A user U, for instance, will obtain her/his κ_U as is produced through the key generation phase. As a result, both $\{s_1, s_2, \ldots, s_k\}$ and u will go public in the proposed scheme. In such a design, everybody can simply calculate the analogous public assessment of U by computing: $\mathcal{U}_U = \mathcal{T}_{\kappa_U}(y) = u\mathcal{T}_{\mathcal{P}_U}(\mathcal{P}_U)(\mathrm{mod}\ q)$, where

$$\mathcal{P}_U = \prod_{i=1}^{k}\mathcal{T}_{\hbar_{Uk}}(\mathcal{P}_i)(\mathrm{mod}\ q) \qquad (3.2.2)$$

In view of that, the proposed transformation procedure translates chaotic-map-based cryptosystems into ID-based cryptographic schemes using chaotic maps, where κ_U is kept as a private key and $\mathcal{U}_U$ is the corresponding public key.

As the user's identity is the only key included in the transformation procedure, our new model is indeed capable of transforming any chaotic-map-based cryptosystem into an ID-based cryptographic scheme.

4 Example

In this section, we give an example of how our new model actually works. Suppose we have a signature scheme based on chaotic maps. Let m be a text that U desires to sign, v_U is U's private key, and $u_U = \mathcal{T}_{v_U}(y)(\mathrm{mod} q)$ is the analogous public key. With the key pair (KP) $\{(q, y, v_U, u_U) : u_U = \mathcal{T}_{v_U}(y)(\mathrm{mod} q)\}$ along with a private arbitrary number $r \in Z_p^*$, the signature scheme based on chaotic maps can be formulated as:

$\mathrm{Sig}_{KP}(m, r) = (w, b)$, where $w = \mathcal{T}_r(y)(\mathrm{mod} q)$ and $b = \left(\frac{m}{r v_U w}\right)(\mathrm{mod}\, p)$

For $m, w \in Z_q^*$ and $b \in Z_p^*$, the verification is formulated as follows:

$$\mathrm{Ver}_{KP}(m, w, b) = \text{true} \Leftrightarrow \mathcal{T}_m(y) = \mathcal{T}_b(w)\mathcal{T}_w(u_U)(\mathrm{mod}\ q)$$

The correctness of the above equation can be confirmed as follows:

$$\begin{aligned}\mathcal{T}_b(w)\mathcal{T}_w(u_U)(\mathrm{mod}\ q) &= \mathcal{T}_b(\mathcal{T}_r(y))\mathcal{T}_w\big(\mathcal{T}_{v_U}(y)\big)(\mathrm{mod}\ q)\\ &= \mathcal{T}_{br}(y)\mathcal{T}_{wv_U}(y)(\mathrm{mod}\ q)\\ &= \mathcal{T}_{m*(v_U w)^{-1}}(y)\mathcal{T}_{wv_U}(y)(\mathrm{mod}\ q) = \mathcal{T}_m(y)\end{aligned}$$

To outline our concept, the novel ID-based signature scheme using chaotic maps will go as follows:

1. Describe the identity arrangement for U as (id_U).
2. Through the key generation phase, U, for instance, will obtain her/his secrete value κ_U. Now $KP = \{(q, y, v_U, u_U) : u_U = \mathcal{T}_{v_U}(y)(\mathrm{mod} q)\}$ is transformed into an ID-based cryptographic model as IDKP $= \{(q, y, \kappa_U, \mathcal{U}_U) : \mathcal{U}_U = \mathcal{T}_{\kappa_U}(y)(\mathrm{mod} q)\}$, where κ_U can be found as Eq. (3.2.1), and $\mathcal{U}_U$ can be figured out by Eq. (3.2.2). Along these lines, the original signature scheme using chaotic maps can be transformed as $\mathrm{Sig}_{KP}(m, r) = (w, b)$, where $w = \mathcal{T}_r(y)(\mathrm{mod} q)$ and $b = \left(\frac{m}{r v_U w}\right)(\mathrm{mod}\, p)$

For given $m, w \in Z_q^*$ and $b \in Z_p^*$, the verification is characterized as:

$$\mathrm{Ver}_{KP}(m, w, b) = \text{true} \Leftrightarrow \mathcal{T}_m(y) = \mathcal{T}_b(w)\mathcal{T}_w(\mathcal{U}_U)(\mathrm{mod} q)$$

By the same token, we can undoubtedly implant the idea of ID-based cryptography into new signature techniques, such as the ElGamal signature (ElGmal 1995) and DL-based signature techniques (Tsujii and Itoh 1989), by using chaotic maps.

5 Security investigation

In this section, we shall analyze the security of our new model. To confirm that our transformation model is capable of translating a well-designed, secure chaotic-map-based scheme into an equally strong and robust ID-based cryptosystem, we used a reductionist method to try the ID-based system out against IND-sID-CCA in the ROM. The results demonstrated that our proposed technique is IND-sID-CCA secure on the condition that the inputted cryptosystem using chaotic maps is IND-CCA secure.

Theorem 1 *Let be a random oracle. The proposed ID-based cryptosystem using chaotic maps is IND-sID-CCA secure if the original cryptosystem using chaotic maps is IND-CCA secure. To be more specific, assume that $\exists$ an IND-sID-CCA foe $\mathfrak{F}$ that has advantage $\epsilon(k)$ in contradiction to the ID-based cryptosystem using chaotic maps. Then $\exists$ an IND-CCA foe with an advantage of at least $\epsilon(k)$ in contradiction to the cryptosystem using chaotic map. Its running time is $O($ time $(\mathfrak{F}))$.*

Proof The primary concept of the confirmation here is to develop an IND-CCA foe to pick up the advantage in contradiction to the cryptosystem using chaotic maps in an IND-CCA game.

Toward the start of the game, the IND-CCA challenger creates $PK = \langle q, y, u\rangle$ and a SK v that fulfills $u = \mathcal{T}_v(y)(\mathrm{mod} q)$. The challenger offers PK to foe F, then F stands an IND-CCA attack utilizing the assistance of procedure $\mathfrak{F}$ as follows:

Initialization stage: The foe yields an identity id_{ch} which it wants to be challenged.

Setup stage: The challenger enters the setup procedure. The foe is now provided with the scheme parameters. It preserves the master key to itself.

h-Inquiries: To react to a h-inquiry, F keeps up a list of tuples $\langle id_{\mathfrak{F}i}, \mathcal{U}_{\mathfrak{F}i}, \kappa_{\mathfrak{F}i}\rangle$ which we allude to as list $\mathcal{L}$. The list is first unfilled. When $\mathfrak{F}$ requests for at a point $id_{\mathfrak{F}i}$, F reacts as follows:

1. On the off chance that the inquiry shows up on list $\mathcal{L}$ in a tuple $\langle id_{\mathfrak{F}i}, \mathcal{U}_{\mathfrak{F}i}, \kappa_{\mathfrak{F}i}\rangle$, then reacts with $\big(id_{\mathfrak{F}i}\big) = u_{\mathfrak{F}i}$.
2. Otherwise, if $\langle id_{\mathfrak{F}i} \neq id_{\mathrm{ch}}\rangle$, F produces an arbitrary $\kappa_{\mathfrak{F}i} \in Z_q^*$ and processes $\mathcal{U}_{\mathfrak{F}i} = \mathcal{T}_{\kappa_{\mathfrak{F}i}}(y)(\mathrm{mod} q)$, else F sets $\kappa_{\mathfrak{F}i} = \mu$ and $\mathcal{U}_{\mathfrak{F}i} = u$. Here μ is a special symbol.

3. F adds the tuple $\langle id_{\mathfrak{F}i}, \mathcal{U}_{\mathfrak{F}i}, \kappa_{\mathfrak{F}i}\rangle$ to $\mathcal{L}$ and gives $\mathcal{U}_{\mathfrak{F}i}$ back to $\mathfrak{F}$.

Stage 1-Extraction inquiries: At the point when $\mathfrak{F}$ requests for the private key related to $id_{\mathfrak{F}i}$, F runs the above procedure and gets $\left(id_{\mathfrak{F}i}\right) = u_{\mathfrak{F}i}$, where $\langle id_{\mathfrak{F}i}, \mathcal{U}_{\mathfrak{F}i}, \kappa_{\mathfrak{F}i}\rangle$is the corresponding entry in $\mathcal{L}$. As $\mathcal{U}_{\mathfrak{F}i} = \mathcal{T}_{\kappa_{\mathfrak{F}i}}(y)(\mathrm{mod}q)$, F can recover the real private key $\kappa_{\mathfrak{F}i}$ for $id_{\mathfrak{F}i}$. The extraction inquiry on id_{ch} will be repudiated.

Stage 1-Decryption inquiries: Let $\langle id_{\mathfrak{F}i}, \mathcal{C}_i\rangle$ be a decryption inquiry delivered by $\mathfrak{F}$, where $\mathcal{C}$ is the ciphertext of the chaotic-map-based cryptosystem. F reacts to the inquiry as follows:

1. In the event that $\langle id_{\mathfrak{F}i} \neq id_{\mathrm{ch}}\rangle, \rangle$, then F runs the h-inquiry procedure with the end goal that $\langle id_{\mathfrak{F}i}, \mathcal{U}_{\mathfrak{F}i}, \kappa_{\mathfrak{F}i}\rangle$ be the relating tuple on $\mathcal{L}$. Then it utilizes $\kappa_{\mathfrak{F}i}$ to react to the decryption inquiry.
2. In the event that $\langle id_{\mathfrak{F}i} = id_{\mathrm{ch}}\rangle$, then F runs the decryption inquiry with $\langle \mathcal{C}_i\rangle$ and after that transfers the challenger's reply back to $\mathfrak{F}$.

Challenge: Once $\mathfrak{F}$ decides that Stage 1 is finished, it yields $\mathcal{M}_0$,$\mathcal{M}_1 \in (-\infty, +\infty)$, which it wants to be challenged on. F then reacts as follows:

1. F provides the challenger with $\mathcal{M}_0$ and $\mathcal{M}_1$. The challenger reacts with the cryptosystem's chaotic maps $\mathcal{C}$ s.t. $\mathcal{C}$ is the encryption of $\mathcal{M}_a$ for an arbitrary coin $a \in \{0, 1\}$.
2. F runs the h-inquiry procedure to get $u \in Z_q^*$ with the end goal that $\left(id_{\mathrm{ch}}\right) = u$ and replies $\mathcal{C}$ to $\mathfrak{F}$.

Stage 2-Extraction inquiries: F reacts the same way as in Stage 1, with the exception of the extraction inquiry on id_{ch}, which will be rejected.

Stage 2-Decryption inquiries: F reacts similarly as in Stage 1 with the exception of the decryption inquiry $\langle id_{\mathfrak{F}i}, \mathcal{C}\rangle$, which will be denied.

Guess: $\mathfrak{F}$ ultimately yields a guess a' for a. Foe F yields a' as its guess for a.

The reactions to h-inquiries are just the same as what will happen in real attacks. Meanwhile, every reaction is consistently and freely dispersed in Z_q^*. The entire reactions to SK extraction inquiries and decryption inquiries are legitimate, so F will not abort throughout the duration of the simulation; namely the probability of immaculate simulation is 1. After these, we can presume that foe $\mathfrak{F}$ has successfully played the role of the adversary and has launched a real attack. Through the explanation of procedure $\mathfrak{F}$, we have come to the result $\left|\Pr\left[a = a'\right] - 1/2\right| \geq \epsilon(k)$, along these lines F has at least advantage $\epsilon(k)$ against the cryptosystem using chaotic maps. This confirms hypothesis 1 and terminates the proof.

Table 1 Comparisons between our proposed transformation model and other models

Model	P_1	P_2 (ms)	P_3	P_4
Lee and Liao (2004)	$2\mathbb{T}_{\mathrm{mul}} + 3\mathbb{T}_{\mathrm{exp}} = 1805\mathbb{T}_{\mathrm{hash}}$	907.91	N	N
Meshram and Meshram (2013)	$2\mathbb{T}_{\mathrm{mul}} + 3\mathbb{T}_{\mathrm{exp}} + 3\mathbb{T}_{\mathrm{hash}} = 1808\mathbb{T}_{\mathrm{hash}}$	909.41	Y	Y
Purpose Model	$3\mathbb{T}_{\mathrm{hash}} + 3\mathbb{T}_{\mathrm{chaotic}} + \mathbb{T}_{\mathrm{mul}} = 8.5\mathcal{T}_h$	4.27	Y	Y

Y The scheme can resist to the risk and N the scheme cannot resist to the risk

P_1 computational cost for model execution (encryption and decryption); P_2 total time (ms); P_3 provides provable security in random oracle model; and P_4 provides security in CCA

6 Comparison to other schemes

In this section, we will compare a competing model such as Lee and Liao (2004) and Meshram and Meshram (2013) transformation model, and our proposed model. Notations utilized as a part of this analysis are as shown below: $\mathbb{T}_{\mathrm{mul}}$, $\mathbb{T}_{\mathrm{exp}}$,$\mathbb{T}_{\mathrm{hash}}$, and $\mathbb{T}_{\mathrm{chaotic}}$ denoted the time executing for a modular multiplication; a modular exponentiation in group; a one-way hash function and a Chebyshev chaotic map operation, respectively. It is to be noted that encryption and decryption procedures are the dominating processes in terms of computation cost than setup and extract phases as they are executed only once. Thus, we consider only the encryption and decryption phase as whole process of model and accordingly compare the proposed transformation model with Lee and Liao's transformation model (Lee and Liao 2004) and Meshram and Meshram transformation model (Meshram and Meshram 2013). The comparative results are shown in Table 1. Utilizing the experimental outcomes obtained in (Algehawi and Samsudin 2010; Ibrahim et al. 2016), we have the accompanying computation time, which are mapped to the hashing time as the time unit:$\mathbb{T}_{\mathrm{hash}} = \mathbb{T}_{\mathrm{chaotic}}$, $\mathbb{T}_{\mathrm{mul}} = 2.5\mathbb{T}_{\mathrm{hash}}$ and $\mathbb{T}_{\mathrm{exp}} = 600\mathbb{T}_{\mathrm{hash}}$. Therefore, in terms of computational complexity, we have the accompanying relationship: $\mathbb{T}_{\mathrm{hash}} \approx \mathbb{T}_{\mathrm{chaotic}} < \mathbb{T}_{\mathrm{mul}} < \mathbb{T}_{\mathrm{exp}}$. The executing time for $\mathbb{T}_{\mathrm{hash}}$ is 0.503 ms (Ibrahim et al. 2016). It may be noticed that the displayed transformation model using extended Chebyshev chaotic map devised in this paper exhibits lower computational cost than (Lee and Liao 2004; Meshram and Meshram 2013) and provably secure in random oracle than (Lee and Liao 2004).

7 Conclusion

In this article, we have shown how to develop an efficient ID-based cryptographic transformation technique that is built on the foundation of a chaotic-map-based cryptosystem without changing the original public key cryptosystem configuration. To avoid the trouble and possible threats of designing a new ID-based cryptographic technique over from the very beginning, we decided to use chaotic maps to help with ID-based cryptographic transformation. We have proved that our new model is secure under IND-sID-CCA in the ROM. This arrangement can be straightforwardly conveyed to an existing system at a very low computation cost. Combining the strengths and advantages of both chaotic maps and ID-based cryptography, our new model is vastly applicable and offers high level security.

Acknowledgements This work was supported by Dr. D.S. Kothari Post-Doctoral fellowship awarded by University Grants Commission, New Delhi, India.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

References

Algehawi MB, Samsudin A (2010) A new identity based encryption (IBE) scheme using extended Chebyshev polynomial over finite fields Zp. Phys Lett A 374:4670–4674

Bergamo P, D'Arco P, Santis A, Kocarev L (2005) Security of public key cryptosystems based on Chebyshev polynomials. IEEE Trans Circuits Syst I 52(7):1382–1393

Boneh D, Boyen X (2004) Efficient selective-id secure identity based encryption without random oracles. In: Advances in cryptology-EUROCRYPT 2004, lecture notes in computer science, vol 3027. Springer, Berlin, pp 223–238

Boneh D, Franklin MK (2003) Identity based encryption from the Weil pairing. SIAM J Comput 32(3):586–615

Canetti R, Halevi S, Katz J (2003) A forward-secure public-key encryption scheme. In: Advances in cryptology—Eurocrypt 2003, vol 2656, pp 255–271

Chen F, Liao X, Wong KW, Han Q, Li Y (2012) Period distribution analysis of some linear maps. Commun Nonlinear Sci Numer Simul 17:3848–3856

Cocks C (2001) An identity based encryption protocol based on quadratic residues. In: International conference on cryptography and coding (proceedings of IMA), lecture notes in computer science, vol 2260. Springer, pp 360–363

Diffie W, Hellman ME (1976) New directions in cryptography. IEEE Trans Inf Theory IT 22(4):454–644

ElGmal T (1995) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 31:469–472

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

Heng S, Kurosawa K (2006) k-Resilient identity-based encryption in the standard model. IEICE Trans Fundam E89CA(1):39–46

Hwan MS, Lo JW, Lin SC (2004) An efficient user identification scheme based on ID-based cryptosystem. Comput Stand Interfaces 26:565–569

Hwu F (1993) The interpolating random spline cryptosystem and the chaotic-map public-key cryptosystem. Ph.d. thesis, University of Missouri Rolla

Ibrahim MH, Kumari S, Das AK, Wazid M, Odelu V (2016) Secure anonymous mutual authentication for star two-tier wireless body area networks. Comput Methods Progr Biomed 135:37–50

Kiltz E, Vahlis Y (2008) CCA2 secure IBE: standard model efficiency through authenticated symmetric encryption. CT-RSA, lecture notes in computer science, vol 4964. Springer, pp 221–239

Kocarev L (2001) Chaos-based cryptography: a brief overview. IEEE Circuits Syst Mag 1:6–21

Kocarev L, Tasev Z (2003) Public-key encryption based on chebyshev maps. In: Proceedings of the 2003 international symposium on circuits and systems. https://doi.org/10.1109/iscas.2003.1204947

Lee CC, Hsu CW (2013) A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. Nonlinear Dyn 71(1–2):201–211

Lee WC, Liao KC (2004) Constructing identity-based cryptosystems for discrete logarithm based cryptosystems. J Netw Comput Appl 22:191–199

Lee CC, Chen CL, Wu CY, Huang SY (2012) An extended chaotic maps-based key agreement protocol with user anonymity. Nonlinear Dyn 69(1–2):79–87

Lee CC, Hsu CW, Lai YM, Vasilakos AV (2013a) An enhanced mobile-healthcare emergency system based on extended chaotic maps. J Med Syst 37(5):9973

Lee CC, Li CT, Hsu CW (2013b) A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps. Nonlinear Dyn 73(1–2):125–132

Lee CC, Li CT, Chiu ST, Lai YM (2014a) A new three-party-authenticated key agreement scheme based on chaotic maps without password table. Nonlinear Dyn 79(4):2485–2495

Lee CC, Lou DC, Li CT, Hsu CW (2014b) An extended chaotic-maps-based protocol with key agreement for multiserver environments. Nonlinear Dyn 76(1):853–866

Li CT, Lee CC, Weng CY (2014) A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. J Med Syst 38(9):77

Li CT, Chen CL, Lee CC et al (2017) A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps. Soft Comput. https://doi.org/10.1007/s00500-017-2504-z

Liu W, Liu J, Wu Q, Qin B, Naccache D, Ferradi H (2017) Efficient subtree-based encryption for fuzzy-entity data sharing. Soft Comput. https://doi.org/10.1007/s00500-017-2743-z

Mason JC, Handscomb DC (2003) Chebyshev polynomials. Chapman & Hall/CRC, Boca Raton

Menezes A, Oorschot PV, Vanstone S (1997) Handbook of applied cryptography. CRC, Boca Raton

Meshram C (2015a) An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem. Inf Process Lett 115(2):351–358

Meshram C (2015b) An efficient ID-based beta cryptosystem. Int J Secur Appl 9(2):189–202

Meshram C (2015c) Factoring and discrete logarithm using IBC. Int J Hybrid Inf Technol 8(3):121–132

Meshram C, Meshram S (2011) An identity based beta cryptosystem. In: IEEE Proceedings of 7th international conference on information assurance and security (IAS 2011) Dec 5–8, pp 298–303

Meshram C, Meshram S (2013) An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem. Inf Process Lett 113(10–11):375–380

Meshram C, Meshram SA (2017) Constructing new an ID-based cryptosystem for IFP and GDLP based cryptosystem. J Discrete Math Sci Cryptogr 20(5):1121–1134

Meshram C, Obaidat MS (2015) An ID-based quadratic-exponentiation randomized cryptographic scheme. In: IEEE proceeding of international conference on computer, information and telecommunication systems, pp 1–5

Meshram C, Meshram S, Zhang M (2012a) An ID-based cryptographic mechanisms based on GDLP and IFP. Inf Process Lett 112(19):753–758

Meshram C, Huang X, Meshram S (2012b) New Identity-based cryptographic scheme for IFP and DLP based cryptosystem. Int J Pure Appl Math 81(1):65–79

Meshram C, Meshram S, Ram C (2012c) Constructing identity-based cryptographic scheme for beta cryptosystem. Int J Appl Math 25(5):609–624

Meshram C, Powar PL, Obaidat MS, Lee CC (2016) An IBE technique using partial discrete logarithm. Procedia Comput Sci 93:735–741

Meshram C, Tseng YM, Lee CC, Meshram SG (2017a) An IND-ID-CPA secure ID-based cryptographic protocol using GDLP and IFP. Informatica 28(3):471–484

Meshram C, Lee CC, Li CT, Chen CL (2017b) A secure key authentication scheme for cryptosystems based on GDLP and IFP. Soft Comput 21(24):7285–7291

Meshram C, Li CT, Meshram SG (2018) An efficient online/offline ID-based short signature procedure using extended chaotic maps. Soft Comput. https://doi.org/10.1007/s00500-018-3112-2

Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21:120–126

Shamir A (1984) Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO'84, lecture notes in computer science, vol 196. Springer, pp 47–53

Shao Z (2007) A provably secure short signature scheme based on discrete logarithms. Inf Sci 177:5432–5440

Stinson D (2002) Cryptography: theory and practice, 2nd edn. CRC, Boca Raton

Tsujii S, Itoh T (1989) An ID-based cryptosystem based on the discrete logarithm problem. IEEE J Sel Areas Commun 7:467–473

Waters B (2005) Efficient identity-based encryption without random oracles. In: Advances in cryptology-CRYPTO 2005, lecture notes in computer science, vol 3494. Springer, Berlin, pp 114–127

Wei J, Hu X, Liu W et al (2017) Forward and backward secure fuzzy encryption for data sharing in cloud computing. Soft Comput. https://doi.org/10.1007/s00500-017-2834-x

Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fractals 37(3):669–674