Complex & Intelligent Systems (2022) 8:973–987
https://doi.org/10.1007/s40747-021-00555-y

ORIGINAL ARTICLE

Conformal Chebyshev chaotic map-based remote user password authentication protocol using smart card

Chandrashekhar Meshram[1] · Sarita Gajbhiye Meshram[2] · Rabha W. Ibrahim[3] · Hamid A. Jalab[4] · Sajjad Shaukat Jamal[5] · Sharad Kumar Barve[2]

Received: 25 October 2020 / Accepted: 21 September 2021 / Published online: 29 October 2021

Abstract
With the rapid advancement and growth of computer networks, there have been greater and greater demands for remote user password authentication protocols. In current ages, smartcard-based authentication protocol has formed the standard with their incredibly insubstantial, user-friendly equipment and low-cost apps. In this study, we proposed an effective robust authentication protocol using the conformable chaotic map, where a conformable calculus is a branch of newly appearing fractional calculus. It has a magnificent property, because it formulates using a controller term. We shall also offer formal proof of smooth execution of the proposed authenticated protocol. Our new protocol is more secure as compared to several comparable protocols.

Keywords Mutual authentication · Smart card · Session key · Conformable chaotic map · Fractional calculus · Conformable calculus · Perfect forward secrecy · Hash function · Cryptography

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Rabha W. Ibrahim
rabhaibrahim@yahoo.com

Hamid A. Jalab
hamidjalab@um.edu.my

Sajjad Shaukat Jamal
shussain@kku.edu.sa

Sharad Kumar Barve
drsharadbarve@gmail.com

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

[2] Water Resources & Applied Mathematics Research Lab, Nagpur, India

[3] IEEE: 94086547, Kuala Lumpur 59200, Malaysia

[4] Department of Computer System and Technology -Multimedia Unit, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

[5] Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

Introduction

In recent years, research in chaotic maps and their applications within the field of cryptography has acquired significant attention Chaotic frameworks are defined by subtle need on initial situations and proximity to random behavior; features that appear to be fundamentally analogous to those needed by certain cryptographic primitives [1, 2]. In his doctoral thesis in 1993, Hwu [3] introduced the idea of chaos theory to public-key cryptography (PKC). He defined his chaotic development of a PKC with a quadratic equation of difference and a one-dimensional equation of difference (1DDE), which is a well-qualified one-way function. In contrast, Hwu's scheme uses ElGmal's method [4] to execute the cycle of encryption. The security of this scheme is based on the infeasibility of resolving the given discrete logarithm over finite fields. Nonetheless, it is possible to work out a trapdoor by letting the true owner know the reiteration times of the distinguishing condition.

The smartcard-founded remote client authentication system allows a device to authenticate a remote client through open, unsafe networks. In general, one of the two approaches next is used by a system to identify a client such as (a) use something that is accessible only to the client, like a password, (b) single client has permitted admission to

use something, like a smart card (SC). The smartcard-founded authentication utilizes both methods and, therefore, it occasionally mentioned to as two-factor authentication. An authentication protocol based on a smartcard password requires an Authentication Server (AS) and a Client (C). The protocol typically has three main phases: the phase of registration, the phase of login and the phase of authentication. However, sometimes using the smart card, usually with the aid of AS, there may also be an additional stage for changing the password of the user. To date, a number of remote client password authentication protocols using SC have been published [5–7, 9, 10] with the purpose of providing stable and well-organized authentication services to connected clients. Nevertheless, furthermost of such systems are vulnerable to cryptographic occurrences online.

Xu et al. [7] planned a password confirmation procedure using SC. Nonetheless, Song et al. [9] and Sood et al. [10] recognized certain limitations in the template of Xu et al. [7]. Song et al. [9] demonstrated that an attacker can collect information from the SC of a legal client and thus launch an impersonation attack [11–13]. Song [8] suggested an improved form of the design of Xu et al. to solve the problem. Sood et al. [10] also introduced the upgraded form of the protocol of Xu et al. in 2010, by solving the problems of off-line password guessing and the spoofing attacks contained in the protocol of Xu et al. In 2013, yet, Chen et al. [5] found that both the protocol of Song et al. [8] and the protocol of Sood et al. [10] consumed security errors. Song's device is vulnerable to check the stolen smartcard attack besides offline password guessing attack, while Sood et al.'s protocol cannot do the shared authentication. An improved remote user password authentication protocol based on a SC was subsequently projected by Chen et al. [14]. Li et al. [15] argued at about the same time that the protocol of Chen et al. was unable to recognize incorrect passwords and during the login process did not provide security. He also argued that the password change process of Chen et al. was not feasible, because the database had to upgrade the old passwords.

In 2016, Islam [16] demonstrated that Li et al.'s [15] protocol is not single susceptible to a recognized session-specific provisional knowledge occurrence, a stolen smart card attack and an insider attack, but correspondingly lacks a mechanism to withdraw the stolen smart card. The proposed protocol of Islam has a noteworthy performance in falling the cost of computation. Li et al. [17] established in the random oracle (RO) model using chaotic maps based on computational Diffie-Hellman hypothesis, novel client authentication and key agreement procedure using chaotic maps for multi-server settings with known security. Luo et al. [18] introduced a dual-party strategic contract rules using chaos map with proven protection and outcomes show that the protocol could solve off-line password-guessing attacks. Li et al. [19] introduced a new triple-party password-based valid strategic argument procedure using chaotic maps with operator secrecy and demonstrated that the protocol is protect with appropriate computational complexity and overhead communication. In 2019, Zhao et al. [20] demonstrated an active three-factor remote user confirmation procedure using chaotic maps and demonstrated that the protocol offers a solider safety security at the charge of appropriate directly above computing and is suitable for secure mobile network communication. Dharminder and Gupta [21] discussed the security evaluation-related issues and application of Chebyshev chaotic map in the authentication protocols. In 2020, Mishra et al. [22] demonstrated a mutual authentication protocol using chaotic maps for vehicular cloud computing, with the goal of ensuring security and efficient communication while preserving anonymity. In 2021, Meshram et al. [23] presented efficient password-based authentication protocol for smart cities environments.

Fractional calculus (FC) and its presentations are essential in quite a lot of fields of mathematical sciences. The actual presentation of FC is considering the nonlinearity. It extended the concepts of integer order derivation. FC introduces an outstanding mechanism for the sketch the common possessions of different materials and developments. The benefits of FC converted specious in information technology, signal and vision processing and fractional chaotic map (see [24, 25]). Recently, different types of FC have imposed. One of these recent calculi is calling the conformable calculus (CC).

Our contribution

As outline mention above, we proposed a new protocol in this paper that assists the client to modify the password directly deprived of any assistance from AS. Furthermore, we provide the ability to reject a lost/stolen smartcard in order to reissue another card to the same client. All remote-related internet transactions require authentication mechanisms. As a result, it is vital to ensure that these protocols work properly so that the entire system can run smoothly. Despite the fact that the various approaches outlined above have had significant success in lowering the cost of computation, security flaws and inconvenience have been identified. To achieve the conformable calculus, we devised a new authentication mechanism based on conformable chaotic-map (CCM). The main security and presentation analysis confirms that the suggested approach has the following advantages (shown in Fig. 1):

(i) Identification of a wrong password by the smart-card without the involvement of the authentic server;

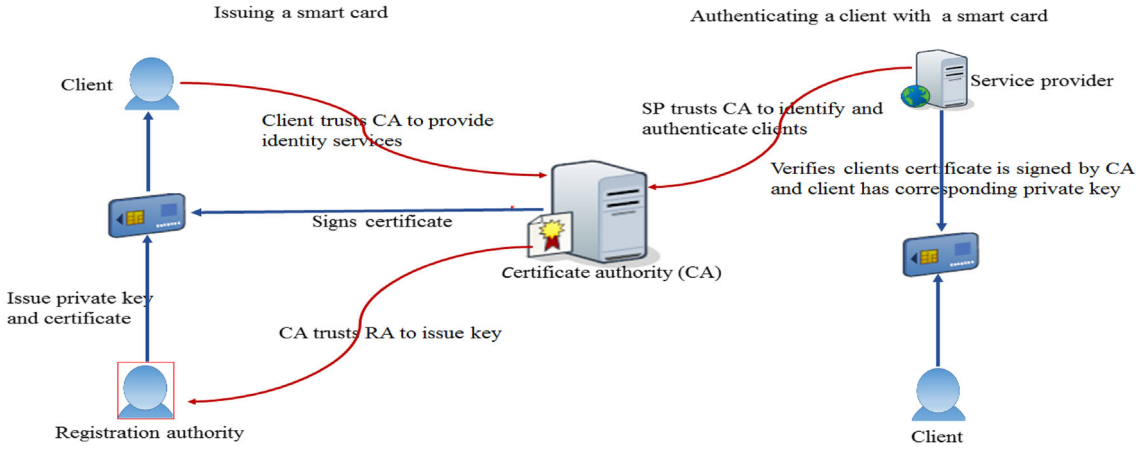

Fig. 1 Graphical overview of protocol

(ii) Replacement and selection of a password by client without the participation of the authentic server;
(iii) Protection of the session key from known active/passive attacks;
(iv) The security evaluation proof is done by utilizing the Real-Or-Random (ROR) model;
(v) Lower computation cost and adds better security aspects.

Road map of the article

The remainder of the paper is laid out as follows. "Mathematical backgrounds" describes the basic info, which includes a brief summary of the associated methods and a list of representations employed throughout this work. "Proposed authentication protocol" illustrates our presented authentication protocol. In "Security analysis in ROR model", we will determine the security evaluation under the ROR Model. The suggested protocol's security investigation is shown in "Other security examination and discussion of the proposed protocol". "Contrast with other protocols with experimental complexity evaluation" displays the results of our security argument as well as the proposed protocol's computing cost. "Conclusion" is where the conclusion is reached.

Mathematical backgrounds

This segment includes a brief outline of a few algorithms used by our presented protocol, Conformable Chebyshev polynomial, conformable chaotic maps and a list of notations (see Table 1) used throughout this paper.

Chebyshev chaotic transforms

Basically, we review Chebyshev successive polynomials (CP) (see [26]) and evaluate their functionality. CP $\mathcal{T}_r(z)$ is a polynomial of n-degree in the variable z. Let $z \in [-1, 1]$ be the type, and let n be an integer. CP mentioned the following in general:

$$\mathcal{T}_n(z) = \cos(n \times \arccos(z)),$$
$$\mathcal{T}_0(z) = 1$$
$$\mathcal{T}_1(z) = z$$
$$\mathcal{T}_n(z) = 2z\mathcal{T}_{n-1}(z) - \mathcal{T}_{n-2}(z); n \geq 2$$

In this circumstance, the functionals $\arccos(z)$ and $\cos(z)$ characterized as $\arccos : [-1, 1] \rightarrow [0, \pi]$ and $\cos : R \rightarrow [-1, 1]$.

There are two primary characteristics of CP [27–29] and [40, 41]: bisection-group and chaotic properties.

Table 1 Symbolization to use in our new procedure

Symbolization	Significance
$\mathcal{C}_i$	The ith client
id_i	Special identity of $\mathcal{C}_i$
pw_i	Special pw_i of $\mathcal{C}_i$
AS	Authentication Server
SC	Smartcard
α, δ	Temporary values created, respectively, by client and server
q_1	Big safe prime number
ΔT	Total delay of transmission
$\hbar(.)$	One way hash function
$\mathfrak{s}id_i$	Client $\mathcal{C}_i$'s smartcard id
x	The client retains private key
$\oplus$	The XOR operation
$\|\|$	The operation of string concatenation
SK	Session key

(1) The chaotic properties: The CP transform fixed as $\mathcal{T}_r : [-1, 1] \to [-1, 1]$ with degree$n > 1$, is a chaotic transform associated the functional (invariant density) $f^*(z) = \frac{1}{\left(\pi\sqrt{1-z^2}\right)}$ for some positive Lyapunov exponent exponent $\lambda = \text{In } n > 0$.
(2) The properties of what is calling semi-group satisfy the subsequent impartialities: $\mathcal{T}_w(\mathcal{T}_\ell(z)) = \cos\left(w\cos^{-1}\left(\cos\left(\ell\cos^{-1}(z)\right)\right)\right) = \cos(w\ell\cos^{-1}(z)) = \mathcal{T}_{\ell w}(z) = \mathcal{T}_\ell(\mathcal{T}_w(z))$, where w and ℓ are positive integers and $z \in [-1, 1]$.

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

(1) The DL's task is to discover w an integer with the final aim of $\mathcal{T}_w(z) = y$ given two components, z and y.
(2) For three variables z, $\mathcal{T}_w(z)$, and $\mathcal{T}_\ell(z)$, the Diffie-Hellman problems (DHP) task is to measure the $\mathcal{T}_{w\ell}(z)$ element.

Conformable chaotic maps (CCM)

The conformable calculus (CC) previously stated to as a conformable fractional calculus [41]. However, it strains definite of the established upon properties for fractional calculus (derivatives of non-integer power). CC works on the basis of the following arrangement. Let $\beta \in [0, 1]$. If and only if δ^0 is the identity operator and δ^1 is the classical differential operator, a differential operator δ^β is conformable. δ^β is conformable if and only if $\vartheta = \vartheta(x)$ given a differentiable function.

$$\delta^0\vartheta(x) = \vartheta(x), \quad \delta^1\vartheta(x) = \vartheta'(x).$$

Newly, Anderson and Ulness [42] presented a novel formulation of CC founded by the control theory to designate the performance of proportional-differentiation controller conforming to error function. The formula has the next definition.

Definition 2.1 Let $\beta \in [0, 1]$ then CC has in the succeeding formal

$$\delta^\beta\vartheta(x) = \mu_1(\beta, x)\vartheta(x) + \mu_0(\beta, x)\vartheta'(x),$$

where the functions μ_0 and μ_1 attain the boundaries

$$\lim_{\beta\to 0}\mu_1(\beta, x) = 1, \lim_{\beta\to 1}\mu_1(\beta, x) = 0,$$
$$\lim_{\beta\to 0}\mu_0(\beta, x) = 0, \lim_{\beta\to 1}\mu_0(\beta, x) = 1.$$

We will deliberate to obtain the overhead description.

$$\mu_1(\beta, x) = (1-\beta)x^\beta \text{ and } \mu_0(\beta, x) = \beta x^{1-\beta}, \text{ or}$$

$$\mu_1(\beta, x) = \frac{(1-\beta)}{\Gamma(1+\beta)} \text{ and } \mu_0(\beta, x) = \frac{\beta}{\Gamma(1+\beta)},$$

where the conformable differential operator for the function $\vartheta(x)$ is $\delta^\beta\vartheta(x)$. As a result, μ_1, μ_0 correspond to the fractional tuning connections of the function ϑ and its derivative.

We get the following construction by using the idea of CC to generalize the polynomial $\mathcal{T}_n(z)$:

Since $\mathcal{T}_n'(z) = 2n\mathcal{T}_{n-1}(z)$, then $\delta^\beta\mathcal{T}_n(z)$ has the following formal

$$\mathcal{T}_n{}^\beta(z) := \delta^\beta\mathcal{T}_n(z) = \mu_1(\beta, z)\mathcal{T}_n(z) + \mu_0(\beta, z)\mathcal{T}_n'(z). \quad (1)$$

In frequent formula (1) can replace by

$$\mathcal{T}_n{}^\beta(z) = \mu_1(\beta, z)\mathcal{T}_n(z) + 2n\mu_0(\beta, z) * \omega(z)\mathcal{T}_{n-1}(z), \quad (2)$$

where $\omega(z) = 1 + 2z + (4z^2 - 1) + \cdots + (n-1)$-times. Equation (2) is called the Conformable Chebyshev polynomials (CCP). Figure 2 displays the dynamic plot of the offered CCP. The following is the consequence of the formula that is used more frequently.

Proposition 2.1 *The CCP satisfies the most common relationships.*

$$\mathcal{T}_n{}^\beta(z) = [2z\mu_1(\beta, z) + 2n\mu_0(\beta, z) * \omega(z)]\mathcal{T}_{n-1}(z) - \mu_1(\beta, z)\mathcal{T}_{n-2}(z). \quad (3)$$

Proof Linking (2) with the frequent formula $\mathcal{T}_n(z) = 2z\mathcal{T}_{n-1}(z) - \mathcal{T}_{n-2}(z); n \geq 2$, we have

$$\begin{aligned}\mathcal{T}_n{}^\beta(z) &= \mu_1(\beta, z)\mathcal{T}_n(z) + 2n\mu_0(\beta, z) * \omega(z)\mathcal{T}_{n-1}(z)\\ &= \mu_1(\beta, z)[2z\mathcal{T}_{n-1}(z) - \mathcal{T}_{n-2}(z)]\\ &\quad + 2n\mu_0(\beta, z) * \omega(z)\mathcal{T}_{n-1}(z)\\ &= [2z\mu_1(\beta, z) + 2n\mu_0(\beta, z) * \omega(z)]\mathcal{T}_{n-1}(z)\\ &\quad - \mu_1(\beta, z)\mathcal{T}_{n-2}(z).\end{aligned}$$

It's worth noting that when $\beta \to 0$, we get the main ordinary result, as shown in [29].

Proposition 2.2 *The semi-group properties clamps for CCP situated on interval* $(-\infty, \infty)$.

Proof Let $H = z\mu_1(\beta, z) + n\mu_0(\beta, z) * \omega(z)z\mu_1(\beta, z)$. By Proposition 2.1, we obtain

$$\mathcal{T}_{n+2}{}^\beta(z) = 2H\mathcal{T}_{n+1}(z) - \mu_1(\beta, z)\mathcal{T}_n(z).$$

The overhead formulation implies a modification equation (disconnected equation) with a well-known principle.

$$\sigma^2 - 2H\sigma + \mu_1 = 0.$$

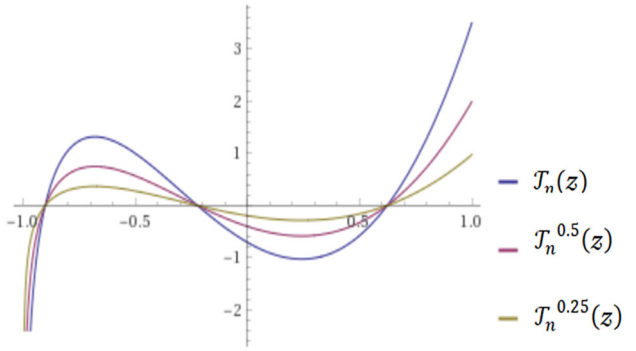

Fig. 2 CCP for different values of β with $\mu_1(\beta, x) = \frac{(1-\beta)}{\Gamma(1+\beta)}$ and $\mu_0(\beta, x) = \frac{\beta}{\Gamma(1+\beta)}$ [55]

Satisfying the relations

$$\sigma_1 + \sigma_2 = 2H, \sigma_1\sigma_2 = \mu_1, \sigma_{1,2} = H \pm \sqrt{H^2 - \mu_1}.$$

A computation yields that

$$\begin{aligned}\mathcal{T}_n{}^{\beta}(z) &= ({\sigma_1}^n + {\sigma_2}^n)/2 \\ &= \frac{(H + \sqrt{H^2-\mu_1})^n + (H - \sqrt{H^2-\mu_1})^n}{2} \\ &= \sum_{m=0}^{[n/2]} \binom{n}{m} H^{n-2m}(H^2 - \mu_1)^m.\end{aligned}$$

Resulting the proof in [31] on the overhead summation, we get

$$\mathcal{T}_k{}^{\beta}\left(\mathcal{T}_n{}^{\beta}(z)\right) = ({\tau_1}^k + {\tau_2}^k)/2$$
$$\tau_1 + \tau_2 = 2\mathcal{T}_n{}^{\beta}(z), \sigma_1\sigma_2 = \mu_1.$$

Hence, we have the important relation

$$\mathcal{T}_k{}^{\beta}\left(\mathcal{T}_n{}^{\beta}(z)\right) = \mathcal{T}_n{}^{\beta}\left(\mathcal{T}_k{}^{\beta}(z)\right) = \mathcal{T}_{kn}{}^{\beta}(z).$$

When $\beta \to 0$ is used, we get the original case of Proposition 2.2, which is described in [29] (Fig. 2).

The DL and assignments for the CCP are approximately DHP occur at this point.

Proposed authentication protocol

We will present the new password authentication protocol in this section. As mentioned below, our proposed protocol includes five different phases. Figure 3 is the workflow of the planned protocol. The stages for every of the five phases are conferred in next investigation.

Registration phase

This is a preliminary phase that arises when a client interacts with the remote AS database for only one time. The steps that must be taken are:

$\mathscr{R}1$: First, a $\mathcal{C}_i$ client picks an identity like id_i and a secure password like pw_i. Otherwise, the client will measure $\mathcal{R}pw_i = \hbar(b_i \oplus pw_i)$, wherever b_i an arbitrary numeral charge is.

$\mathscr{R}2$: $\mathcal{C}_i \to AS : \{id_i, \mathcal{R}pw_i\}$ is a secure channel of communication.

$\mathscr{R}3$: Upon getting the demand for registration after the local $\mathcal{C}_i$ at time T_i, AS will verify whether it exists. If it occurs then mater AS will reject the application for recording; Else it will continue to produce a SC individuality $\mathfrak{s}id_i$ detailed to $\mathcal{C}_i$ and measure $\mathcal{V}_i = \hbar(id_i||x||\mathfrak{s}id_i)$, $Tid_i = \hbar(T_i||x)$ and $SD_i = \mathfrak{s}id_i \oplus Tid_i$.

Note that AS stores $\{Tid_i, \hbar(id_i), SD_i\}$ in its database for each $\mathcal{C}_i$ user, where x is a hidden key to the server.

$\mathscr{R}4$: $AS \to \mathcal{C}_i$, a SC containing $\{\mathcal{V}_i, q_1, \hbar(.)\}$ along with T_i and $\mathfrak{s}id_i$ to the client $\mathcal{C}_i$ by incomes of a protected network of correspondence.

$\mathscr{R}5$: $\mathcal{C}_i$ computes B_i, $\mathcal{A}_i$, $\mathcal{R}_i$, S_i and inscribes these tenets to the SC after obtaining the SC. Currently the SC covers $\{\mathcal{A}_i, B_i, \mathcal{R}_i, S_i, q_1, \hbar(.)\}$, where $B_i = \mathcal{V}_i \oplus \hbar(pw_i||b_i||id_i)$, $\mathcal{A}_i = \hbar(b_i||id_i||pw_i||\mathcal{V}_i)$,$\mathcal{R}_i = b_i \oplus \hbar(pw_i||id_i)$, $S_i = T_i \oplus \hbar(id_i||b_i||pw_i)$.

Login phase

To obtain facility from AS, a $\mathcal{C}_i$ client has to lodge his/her SC into the card peruse and consent their id_i and pw_i. SC then completes the steps that result.

$\mathcal{L}1$: Calculate: $b_i = \mathcal{R}_i \oplus \hbar(pw_i||id_i)$, $\mathcal{V}_i^{'} = B_i \oplus \hbar(pw_i||b_i||id_i)$, $\mathcal{A}_i^* = \hbar(b_i||id_i||pw_i||\mathcal{V}_i)$.

$\mathcal{L}2$: Relate the measured A_i^* and A_i stowed in SC of $\mathcal{C}_i$. If together are the same, the credibility of the client's will be remembered, and SC will income the following move.

$\mathcal{L}3$: For a session, pick an arbitrary α number and evaluate: $D_i = \mathcal{T}_{\alpha b_i}^{\beta}(\mathcal{V}_i)(mod q_1)$,$T_i = S_i \oplus \hbar(id_i||b_i||pw_i)$,$M_i = \hbar(id_i||\mathcal{V}_i||D_i||T_i||T_1)$, where T_1 is the existing time, $Did_i = id_i \oplus \hbar(\mathfrak{s}id_i||T_1||T_i)$.

$\mathcal{L}4$: SC sends the message $\{Did_i, D_i, M_i, T_i, T_1\}$ of the login query to AS.

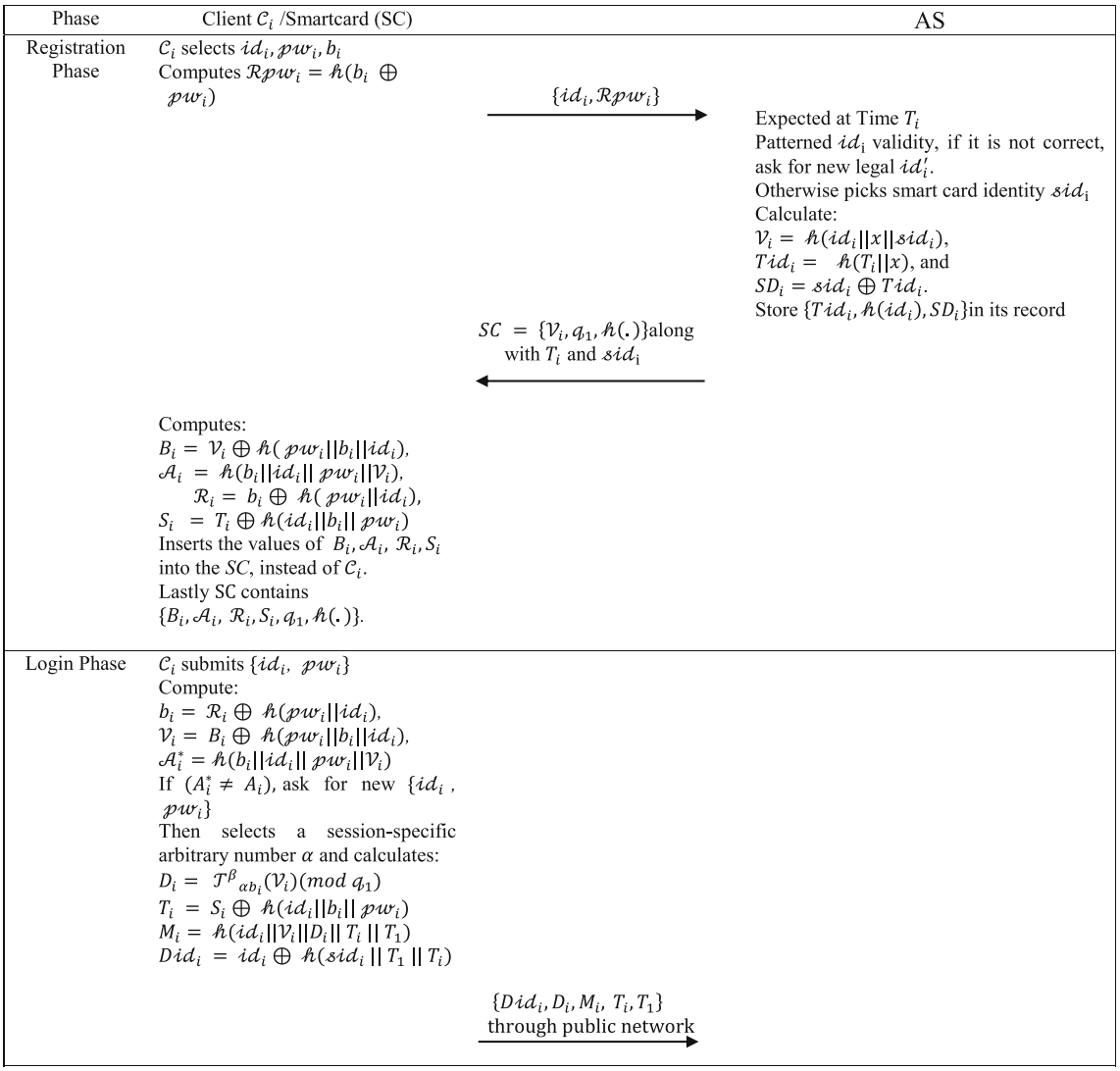

Fig. 3 Proposed authentication protocol

Authentication stage

After getting the access demand email from $\mathcal{C}_i$, AS carries out the following undertakings at the time $T_1^{'}$:

$\mathbb{A}1$: Check the time stamp validity by checking if $(T_1^{'} - T_1) \leq \Delta t$. If the time stamp checks out, the following steps will be performed by AS.

$\mathbb{A}2$: To authenticate $\mathcal{C}_i$, AS calculates: $Tid_i = h(x||T_i)$, $sid_i^* = SD_i \oplus Tid_i$, $id_i{}^* = Did_i \oplus h(sid_i^*||T_1||T_i)$ and verifies $h(id_i{}^*) =? h(id_i)$
If the above confirmation is correct, then $\mathcal{C}_i$ is a valid client; otherwise the login for authentication will be immediately terminated.

$\mathbb{A}3$: For a session, AS selects an arbitrary number δ and assesses the following:

$$
\begin{aligned}
V_i^* &= h(id_i||x||sid_i)\\
M_i^* &= h(id_i||\mathcal{V}_i^*||D_i||T_i||T_1)\\
\mathcal{W}_i &= \mathcal{T}^{\beta}_{\delta id_i}(\mathcal{V}_i^*)(\mathrm{mod} q_1)\\
SK &= \mathcal{T}^{\beta}_{\delta id_i}(D_i)(\mathrm{mod} q_1) = \mathcal{T}^{\beta}_{\alpha b_i \delta id_i}(\mathcal{V}_i)(\mathrm{mod} q_1)\\
M_s &= h(id_i||\mathcal{V}_i^*||\mathcal{W}_i||SK||T_2)\\
sDid_i &= Did_i \oplus h(\mathcal{V}_i||T_2)\\
T_i^* &= T_i \oplus h(T_1||\delta)\\
T_i^{\mathrm{new}} &= T_i^* \oplus h(T_2||id_i).
\end{aligned}
$$

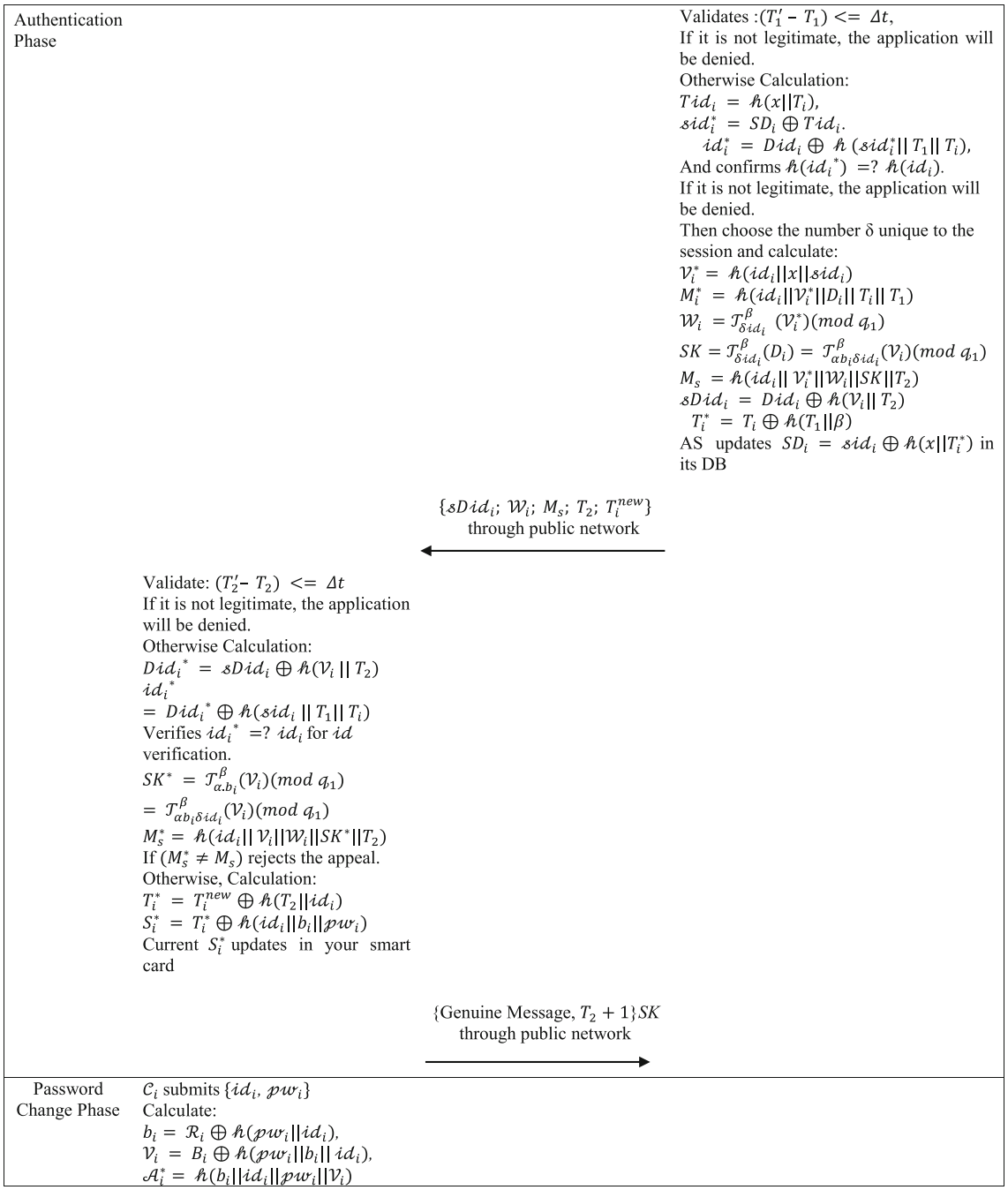

Fig. 3 continued

AS modifies $SD_i = sid_i \oplus h(x||T_i^*)$ in its database in response to the new timestamp T_i^*.

𝔸4 : $AS \rightarrow \mathcal{C}_i$ sends an access response message $\{sDid_i; \mathcal{W}_i; M_s; T_2; T_i^{\text{new}}\}$ at period T_2.

𝔸5 : $\mathcal{C}_i$ checks time validity $(T_2^{'} - T_2) \leq \Delta t$, when receiving the account response message

$$\left(T_2^{'} - T_2\right) \leq \Delta t.$$

𝔸6 If the interval of time is verified, it calculates: $Did_i^* = sDid_i \oplus h(\mathcal{V}_i||T_2)$,$id_i^* = Did_i^* \oplus h(sid_i||T_1||T_i)$.$\mathcal{C}_i$ verifies $id_i^* =? id_i$ for id verification and calculates

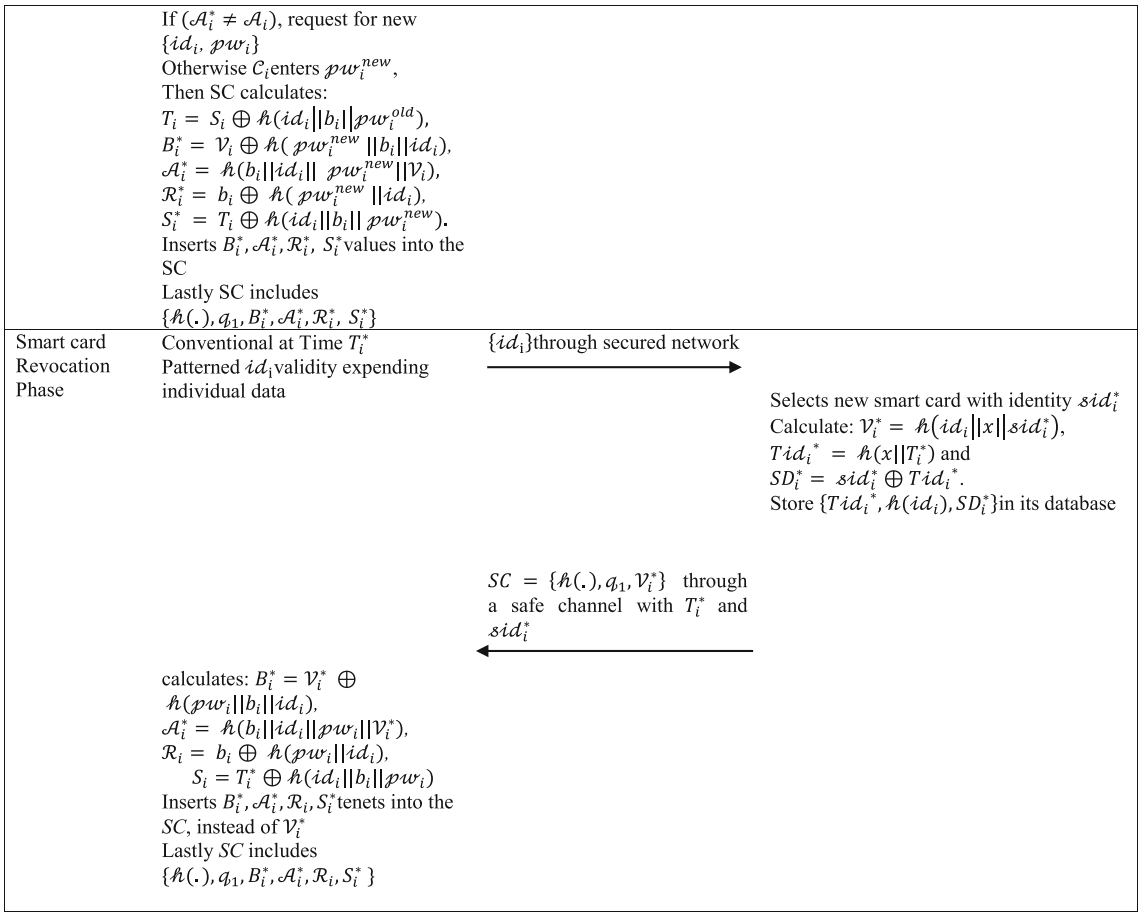

Fig. 3 continued

$$SK^* = \mathcal{T}^{\beta}_{\alpha b_i}(\mathcal{W}_i)(\mathrm{mod} q_1) = \mathcal{T}^{\beta}_{\alpha b_i \delta i d_i}(\mathcal{V}_i)(\mathrm{mod} q_1)$$
$$M_s^* = h(id_i||\mathcal{V}_i||\mathcal{W}_i||SK^*||T_2).$$

$\mathbb{A}7$ $\mathcal{C}_i$ associates the calculated M_s^* esteem and the established M_s value. If they contest, the authentication of the server will be completed; otherwise, the session will be closed immediately.

$\mathbb{A}8$ $\mathcal{C}_i$ computes $T_i^* = T_i^{\text{new}} \oplus h(T_2||id_i)$, as $\mathcal{C}_i$ can deliver his/her own id_i and T_2.
Then, $\mathcal{C}_i$ modifies $S_i^* = T_i^* \oplus h(id_i||b_i||pw_i)$ in reference to the novel times fill T_i^* in his/her SC.

$\mathbb{A}9$ The framed session key SK encrypts all further communications between $\mathcal{C}_i$ and AS.

Password change stage

In this phase, without the aid of the server, $\mathcal{C}_i$ changes her/his old password pw_i in the form of a new password pw_i^{new} in the form of a new password. Taking the following steps:

$\mathcal{P}1$ $\mathcal{C}_i$ presents his/her SC addicted to a pass reader inters his/her deserted (id_i, pw_i), and chooses for an application for a password update.

$\mathcal{P}2$ The SC calculates $b_i = \mathcal{R}_i \oplus h(pw_i||id_i), \mathcal{V}_i = B_i \oplus h(pw_i||b_i||id_i)$ and $\mathcal{A}_i^* = h(b_i||id_i||pw_i||\mathcal{V}_i)$.

$\mathcal{P}3$ Next, SC tests $\mathcal{A}_i^* =? \mathcal{A}_i$. If both organize not competition, the SC refuses $\mathcal{C}_i$'s call; otherwise, the client is permissible to select a other password pw_i^{new}.

$\mathcal{P}4$ Now, SC calculates $T_i = S_i \oplus h(id_i||b_i||pw_i^{\text{old}}), B_i^* = \mathcal{V}_i \oplus h(pw_i^{\text{new}}||b_i||id_i)$, $\mathcal{A}_i^* = h(b_i||id_i||pw_i^{\text{new}}||\mathcal{V}_i)$, $\mathcal{R}_i^* = b_i \oplus h(pw_i^{\text{new}}||id_i)$, $S_i^* = T_i \oplus h(id_i||b_i||pw_i^{\text{new}})$, and the modified values $B_i^*, \mathcal{A}_i^*, \mathcal{R}_i^*, S_i^*$ are embedded into the SC. Currently the SC includes $\{h(.), q_1, B_i^*, \mathcal{A}_i^*, \mathcal{R}_i^*, S_i^*\}$, and C_i can log in with pw_i^{new}.

SC revocation stage

If the client has lost her/his SC, she/he will be able to revoke the missing card and reissue the same account id.

R1: $\mathcal{C}_i$ refers his/her old id_i to AS.
R2: AS check the id_i of $\mathcal{C}_i$ and additional individual details (e.g. PAN card, Voter card, Aadhaar card, birth information, etc.) through which $\mathcal{C}_i$ described perfectly.
R3: AS subjects an original SC with a $\mathfrak{s}id_i^*$ identity and calculates:$\mathcal{V}_i^* = \hbar(id_i||x||\mathfrak{s}id_i^*)$,$Tid_i{}^* = \hbar(x|\left|T_i^*\right)$ and $SD_i^* = \mathfrak{s}id_i^* \oplus Tid_i{}^*$.
R4: AS keeps $\{Tid_i{}^*, \hbar(id_i), SD_i^*\}$ in its record.
R5: $AS \rightarrow \mathcal{C}_i$, send an SC containing $\{\hbar(.), q_1, \mathcal{V}_i^*\}$ along with T_i^* and $\mathfrak{s}id_i^*$ via a protected network.
R6: After obtaining the SC, $\mathcal{C}_i$ calculates $B_i^* = \mathcal{V}_i^* \oplus \hbar(pw_i||b_i||id_i)$, $\mathcal{A}_i^* = \hbar(b_i||id_i||pw_i||\mathcal{V}_i^*)$, $\mathcal{R}_i = b_i \oplus \hbar(pw_i||id_i)$, $S_i = T_i^* \oplus \hbar(id_i||b_i||pw_i)$.
R7 Replace in place of V_i^* with $B_i^*, \mathcal{A}_i^*, \mathcal{R}_i, S_i^*$ in the SC. Now the $\{\hbar(.), q_1, B_i^*, \mathcal{A}_i^*, \mathcal{R}_i, S_i^*\}$ includes the SC.

Security analysis in ROR model

In this segment, we analyze the projected authentication protocol from the standpoint of security analysis, including structured security under the widely recognized Real-Or-Random (ROR) model [30, 31].

Formal security using the ROR model

The object of the ROR model [30, 31] formal security analysis of the proposed authentication protocol is to show that it provides session key (SK) security against an active/passive adversary, say . The ROR model-based structured security examination has recently gained notoriety and has been used in a variety of authentication key exchange protocols [32–35]. To begin the formal security, we will go over the ROR model briefly before presenting the key proof in Theorem 1.

(1) ROR Model: The projected authentication protocol has two parties during the shared authentication and key agreement process: a server AS_j and a client $\mathcal{C}_i$. The following sections go through the main components of the ROR model for the proposed authentication protocol.

a: Participants: $\mathcal{I}_{\mathcal{C}_i}^{\mathfrak{c}}$ and $\mathcal{I}_{AS_j}^{\mathfrak{s}}$ are represented as the illustrations $\mathfrak{c}$ and $\mathfrak{s}$ of $\mathcal{C}_i$ and AS_j, respectively. The oracles are another name for these.

b: Accepted state: After receiving the final message, placed the instance $\mathcal{I}^t$ in the accept state. The accepted state is then referred to as $\mathcal{I}^t$. All contact messages, including those sent and received by $\mathcal{I}^t$, form the session identification for $\mathcal{I}^t$ for the existing session if they are arranged in order.

c: Partnering: If the subsequent three circumstances are met instantaneously, the instances $\mathcal{I}^{\mathfrak{c}}$ and $\mathcal{I}^{\mathfrak{s}}$ are considered partners: (1) they are in an accept state, (2) they mutually authenticate between themselves and share the same session identity, and (3) they are reciprocal associates of each other.

d: Freshness: We refer to $\mathcal{I}_{\mathcal{C}_i}^{\mathfrak{c}}$ or $\mathcal{I}_{AS_j}^{\mathfrak{s}}$ as fresh if the SK formed among $\mathcal{C}_i$ and AS_j is not leaked through the reveal oracle *Reveal* described below.

e: Adversary: In the ROR model, an opponent is modeled using the widely known Dolev-Yao (DY) threat model, as defined in [SB-IEEE ACC]. According to the DY model, $\mathcal{A}$ can intercept, alter, delete, or even inject any or entirely messages exchanged among the cooperative players $\mathcal{C}_i$ and AS_j using the following queries.

Execute $\left(\mathcal{I}^{\mathfrak{c}}, \mathcal{I}^{\mathfrak{s}}\right)$: This inquiry apparatuses a snooping attack that consents $\mathcal{A}$ to recite the messages exchanged among $\mathcal{C}_i$ and AS_j.

Send $\left(\mathcal{I}^t, M\right)$: This query implements an active attack in which $\mathcal{A}$ sends a message M to a participant instance $\mathcal{I}^t$ and receives a response from $\mathcal{I}^t$ in return.

Reveal $(\mathcal{I}^t)$: $\mathcal{A}$ can find out the session key SK formed among $\mathcal{I}^t$ and its partner in the current session using this inquiry.

Corrupt Smart Card $\left(\mathcal{I}_{\mathcal{C}_i}^{\mathfrak{c}}\right)$: This inquiry is showed as an active attack, in which $\mathcal{A}$ uses power analysis attacks to retrieve all of the sensitive secret information contained in its memory [36, 37].

Test $\left(\mathcal{I}^t\right)$: Formerly, the game starts, an impartial coin ς is flipped, and the result is used as a decider in this query. Allow to run this inquiry. If the shared session key SK among $\mathcal{C}_i$ and AS_j is valid, $\mathcal{I}^t$ returns SK when $\varsigma = 1$ and an arbitrary number when $\varsigma = 0$. Else, a null value $(\perp)$ is returned.

We restrict $\mathcal{A}$ in this formal security review to only allow a limited number of *Corrupt Smart Card* $\left(\mathcal{I}_{\mathcal{C}_i}^{\mathfrak{c}}\right)$ queries. $\mathcal{A}$, on the other hand, is allowed to run an infinite number of *Test* $\left(\mathcal{I}^t\right)$ queries.

f: Semantic security: It is required by semantic security that $\mathcal{A}$ is unable to distinguish the real SK session key from a random number. The performance of *Test* $(\mathcal{I}^t)$ is compared to a random bit ς for consistency checking. Let $\varsigma^{'}$ be $\mathcal{A}$'s guessed bit, and Succ be the game's winning probability. The advantage of a polynomial time t adversary $\mathcal{A}$ in breaking the proposed authentication protocol's session key (SK) security, say p, is described as $\mathrm{Adv}_p^{\mathcal{A}}(t) = |2.\Pr[\mathrm{Succ}] - 1| = \left|2.Pr\left[\varsigma^{'} = \varsigma\right] - 1\right|$, where $\Pr[Y]$ represents the probability of an incident Y.

g: Random oracle: We usage the one-way hash function $\hbar(\bullet)$ in our protocol, which is open to all participants,

including adversary . $\hbar(\bullet)$ is modeled as a random oracle, say $\hbar$.

(2) Security proof
Theorem 1 gives the SK protection of the proposed authentication protocol under the ROR model.

Theorem 1 *Let* $Adv_{\mathfrak{p}}^{\mathcal{A}}(t)$ *be the polynomial-time* t*-adversary's function in breaking the proposed protocol* $\mathfrak{p}$*'s SK security. After that,*

$$Adv_{\mathfrak{p}}^{\mathcal{A}}(t) \leq \left(\frac{2\mathcal{Q}_s}{2^{\ell}.|\eta|} + \frac{\mathcal{Q}_{\hbar}^2}{|\hbar|}\right),$$

where $\mathcal{Q}_{\hbar}$, ℓ, $\mathcal{Q}_s$, $|\eta|$ *and* $|\hbar|$ *represent the number of* $\hbar$*-queries, bits in the private key, Send queries, the size of a uniformly distributed password dictionary* η*, and the range space of the hash function* $\hbar(\bullet)$*, respectively.*

Proof This theorem uses a formal security proof close to those found in [32–35]. In this proof, we need the following four games i.e., $\mathcal{G}_{m_j}(j = 0, 1, 2, 3)$. We represent $\text{Succ}_{\mathcal{G}_{m_j}}^{\mathcal{A}}$ as an incident in which the $\mathcal{A}$ adversary can win the $\mathcal{G}_{m_j}$ game. Additionally, $\text{Adv}_{\mathcal{G}_{m_j}}^{\mathcal{A}} = \Pr\left[\text{Succ}_{\mathcal{G}_{m_j}}^{\mathcal{A}}\right]$ denotes and defines $\mathcal{A}$'s advantage in winning $\mathcal{G}_{m_j}$.

- *Game* $\mathcal{G}_{m_0}$*:* Bit ς is chosen first in the initial game $\mathcal{G}_{m_0}$ by a polynomial-time t adversary $\mathcal{A}$. Since the $\mathcal{G}_{m_0}$ and the ROR's actual procedure are virtually identical, it follows that

$$\text{Adv}_{\mathfrak{p}}^{\mathcal{A}}(t) = \left|2.\text{Adv}_{\mathcal{G}_{m_0}}^{\mathcal{A}} - 1\right|. \tag{4}$$

- *Game* $\mathcal{G}_{m_1}$*:* In the game, the eavesdropping attack is carried out by $\mathcal{A}$, who uses the *Execute* query. After the game is over, $\mathcal{A}$ invokes the *Test* query. Notice that the *Test* query's output serves as a decider between a real SK and a random number in a session. The SK creation is as follows. AS_j calculates the $SK = \mathcal{T}^{\beta}_{\alpha b_i \delta i d_i}(\mathcal{V}_i)(\text{mod} q_1)$ shared with $\mathcal{C}_i$, where $\mathcal{V}_i = \hbar(i d_i||x||\mathfrak{s} i d_i)$ and the same SK calculated by $\mathcal{C}_i$ is shared with AS_j as $SK^* = \mathcal{T}^{\beta}_{\alpha b_i \delta i d_i}(\mathcal{V}_i^*)(\text{mod} q_1)(= SK)$. Presume $\mathcal{A}$ interrupts message $M_s = \hbar(i d_i||\mathcal{V}_i^*||\mathcal{W}_i||SK||T_2)$. The long-term secrets $i d_i$, $\mathfrak{s} i d_i$ and $\mathcal{W}_i$ are needed for the computation of the SK by $\mathcal{A}$. The probability of winning game $\mathcal{G}_{m_1}$ by intercepting messages M_s is not augmented without these secret identifications. We have the following since both games $\mathcal{G}_{m_0}$ and $\mathcal{G}_{m_1}$ are virtually indistinguishable:

$$\text{Adv}_{\mathcal{G}_{m_1}}^{\mathcal{A}} = \text{Adv}_{\mathcal{G}_{m_0}}^{\mathcal{A}}. \tag{5}$$

- *Game* $\mathcal{G}_{m_2}$*:* In this game, the *Send* and $\hbar$-queries are simulated. This game is modeled as an active attack, in which $\mathcal{A}$ tries to calculate the SK among $\mathcal{C}_i$ and AS_j by intercepting the message $M_s = \hbar(i d_i||\mathcal{V}_i^*||\mathcal{W}_i||SK||T_2)$. The random numbers α, β and δ, as well as the current time stamp T_2, are included in the messages M_s. As a consequence, when $\mathcal{A}$ makes $\hbar$ queries on these interrupted messages, there is no collision in hash yields. Due to the collision resistant possessions of the one-way hash function $\hbar(\bullet)$, computing the long-term secrets $i d_i$, $\mathfrak{s} i d_i$ and $\mathcal{W}_i$, as well as the short-term secrets α, β and δ, is computationally unfeasible. Since the $\mathcal{G}_{m_2}$ game is comparable to the $\mathcal{G}_{m_1}$ game when the simulation of *Send* and $\hbar$-queries is not involved, the birthday paradox outcomes are as follows:

$$\left|\text{Adv}_{\mathcal{G}_{m_2}}^{\mathcal{A}} - \text{Adv}_{\mathcal{G}_{m_1}}^{\mathcal{A}}\right| \leq \frac{\mathcal{Q}_{\hbar}^2}{2|\hbar|}. \tag{6}$$

- *Game*$\mathcal{G}_{m_3}$*:* The Corrupt Smart Card query is simulated in this game. Consequently, $\mathcal{A}$ has the secret identifications $\{\hbar(.), q_1, B_i^*, \mathcal{A}_i^*, \mathcal{R}_i, S_i^*\}$ from $\mathcal{C}_i^{'}$ smart cardSC's memory, where$B_i^* = \mathcal{V}_i^* \oplus \hbar(\mathfrak{p}w_i||b_i||i d_i)$, $\mathcal{A}_i^* = \hbar(b_i||i d_i||\mathfrak{p}w_i||\mathcal{V}_i^*)$,$\mathcal{R}_i = b_i \oplus \hbar(\mathfrak{p}w_i||i d_i)$, and$S_i = T_i^* \oplus \hbar(i d_i||b_i||\mathfrak{p}w_i)$. It is computationally impossible to derive the x private key and the password $\mathfrak{p}w_i$ of client $\mathcal{C}_i$ without the secret credentials b_i and$\mathcal{V}_i$. The guessing probability of $x \in \{0, 1\}^{\ell}$ by $\mathcal{A}$ is approximately $\frac{1}{2^{\ell}}$ [38], assuming x is ℓ bits. Furthermore, it is believed that the opponent $\mathcal{A}$ will be allowed to enter a limited number of incorrect passwords. When guessing attacks and password are not involved, the games G_{m_2} and G_{m_3} are similar. As a result, we arrive at the following conclusion:

$$\left|\text{Adv}_{\mathcal{G}_{m_3}}^{\mathcal{A}} - \text{Adv}_{\mathcal{G}_{m_2}}^{\mathcal{A}}\right| \leq \frac{\mathcal{Q}_s}{2^{\ell}.|\eta|}. \tag{7}$$

Due to the fact that all the games have been completed, $\mathcal{A}$ can only guess the accurate ς bit. After that, it follows that

$$\text{Adv}_{\mathcal{G}_{m_3}}^{\mathcal{A}} = \frac{1}{2}. \tag{8}$$

The following is the consequence of Eqs. (4), (6), and (7):

$$\begin{aligned}\frac{1}{2}\text{Adv}_{\mathfrak{p}}^{\mathcal{A}}(t) &= \left|\text{Adv}_{\mathcal{G}_{m_0}}^{\mathcal{A}} - \frac{1}{2}\right| \\ &= \left|\text{Adv}_{\mathcal{G}_{m_1}}^{\mathcal{A}} - \frac{1}{2}\right| \\ &= \left|\text{Adv}_{\mathcal{G}_{m_1}}^{\mathcal{A}} - \text{Adv}_{\mathcal{G}_{m_3}}^{\mathcal{A}}\right|. \end{aligned} \tag{9}$$

The triangular inequality yields the following result:

$$\begin{aligned}\left|\text{Adv}_{\mathcal{G}_{m_1}}^{\mathcal{A}} - \text{Adv}_{\mathcal{G}_{m_3}}^{\mathcal{A}}\right| &\leq \left|\text{Adv}_{\mathcal{G}_{m_1}}^{\mathcal{A}} - \text{Adv}_{\mathcal{G}_{m_2}}^{\mathcal{A}}\right| + \left|\text{Adv}_{\mathcal{G}_{m_2}}^{\mathcal{A}} - \text{Adv}_{\mathcal{G}_{m_3}}^{\mathcal{A}}\right| \\ &\leq \frac{\mathcal{Q}_{\hbar}^2}{2|\hbar|} + \frac{\mathcal{Q}_s}{2^{\ell}.|\eta|}. \end{aligned} \tag{10}$$

The following is the consequence of Eqs. (9) and (10):

$$\frac{1}{2}\mathrm{Adv}_{p}^{\mathcal{A}}(t) \leq \left(\frac{\mathcal{Q}_{\hbar}^{2}}{2|\hbar|} + \frac{\mathcal{Q}_{s}}{2^{\ell}.|\eta|}\right). \tag{11}$$

Finally, by multiplying the factor of 2 on both sides of Eq. (8) and simplifying the equations, we get the required result:

$$\mathrm{Adv}_{p}^{\mathcal{A}}(t) \leq \left(\frac{2\mathcal{Q}_{s}}{2^{\ell}.|\eta|} + \frac{\mathcal{Q}_{\hbar}^{2}}{|\hbar|}\right).$$

Other security examination and discussion of the proposed protocol

We show in this segment that the proposed protocol is free from the below detailed attacks. Also, we demonstrate that it is not enough to deliver client anonymity and control of the password by the client.

Proposition 5.1 *The proposed protocol could withstand round and stolen/lost SC round by the off-line /on-line key guessing*.

Proof Several researchers claimed that the information stored in the SC might be segregated in a variety of ways, including file structure with secret keys and encryption methods, power usage analysis, and so on [11–13, 43–47]. Assume that an attacker E robs $\mathcal{C}_i$ of her/his SC and collect data$\{\hbar(.), q_1, \mathcal{A}_i, B_i, \mathcal{R}_i, S_i\}$, where$B_i = \mathcal{V}_i \oplus \hbar(pw_i||b_i||id_{\mathrm{i}})$, $\mathcal{A}_i = \hbar(b_i||id_{\mathrm{i}}||pw_i||\mathcal{V}_i)$, $\mathcal{R}_i = b_i \oplus \hbar(pw_i||id_{\mathrm{i}})$, and $S_i = T_i \oplus \hbar(id_{\mathrm{i}}||b_i||pw_i)$. Even the attacker E cannot determine the password of $\mathcal{C}_i$ from the above calculations, because he/she does not have id_{i}, pw_i, $\mathcal{V}_i$ and b_i. If the attacker had all the required standards excluding for pw_i suddenly, then there may remain a small casual to guess it appropriately. However, it is not feasible to guess more than one worth at the same time (i.e.$(pw_i||id_{\mathrm{i}})$, or $(pw_i||b_i||id_{\mathrm{i}})$, or $(b_i||id_{\mathrm{i}}||pw_i||\mathcal{V}_i)$. As a result, we can say that our approach protected against off-line password guessing's round and stolen/lost SC attacks.

In a round that guessing online password, the attacker challenges to log in to the database by adding one phrase after additional starting a dictionary in an effort to contest the client's login $\mathfrak{z}id_i$ as well as pw. This type of round is essentially not practical, because the task of estimating a solitary worth within the polynomial time (i.e., Δt) is usually deliberated difficult, let unaided when there are more than one parameter to handle at the same time (e.g., $(pw_i||id_{\mathrm{i}})$, or $(pw_i||b_i||id_{\mathrm{i}})$, or $(b_i||id_{\mathrm{i}}||pw_i||\mathcal{V}_i)$. The attacker is only allowed three trials in total, and if all three fails, the SC will be locked up. Consequently, the online pw solving occurrence can touch our procedure.

Proposition 5.2 *The presented protocol protected against known key attacks using session-specific random numbers*.

Proof In particular, a common session key SK will exchange by the server and client pair for all terms. To deliver adequate defense beside the identified key occurrence, we must confirm that the novel SK can never extracted from earlier session keys. That is, we remain need to confirm the security of forthcoming and/or former session keys with one SK exposed somewhere. In presented protocol, if the $SK = \mathcal{T}^{\beta}_{\alpha b_i \delta id_i}(\mathcal{V}_i)(\mathrm{mod} q_1)$ would leakage out of a current session, the attacker will still not be able to use this information to disclose other SKs since the session-specific random numbers α, δ are unlike for changed sittings as well as id_{i} and b_i are unknown.

Proposition 5.3 *The presented protocol can avoid the attack on the restate*.

Proof This type of round chances when an invader tries to sign in to the database by referring communications previously trapped between the legal client and the server. Because the SC of the client and the server will utilize the current timestamps T_1 and T_2 in all inventive assemblies, the values of M_i, Did_{i}, and M_s will be dynamic in our procedure, there will be no effort in relaying messages from one assembly to another. T_i Value is also variable in each session and will modify in both the storage of the server and the SC of the client. Our presented protocol therefore protected in contradiction of the attack of the message replay.

Proposition 5.4 *The proposed protocol could withstand the attack of forgery/modification and the attack of the masquerade client/server*.

Proof Assume an attacker had some communications interrupted among the user and the server (e.g. authentication and login information) and now has $\{Did_{\mathrm{i}}, D_i, M_i, T_i, T_1\}$ and$\{Did_{\mathrm{i}}; \mathcal{W}_i; M_s; T_2; T_i^{\mathrm{new}}\}$, where $M_i = \hbar(id_{\mathrm{i}}||\mathcal{V}_i||D_i||T_i||T_1)$ and $M_s = \hbar(id_{\mathrm{i}}||\mathcal{V}_i^*||\mathcal{W}_i||SK||T_2)$. Because he/she lacks $\mathcal{V}_i$, the attacker E is unable to interfere with M_i and M_s. As a result, we can state that our protocol is secure from modification/forgery attacks. To impersonate a server, an attacker E must appropriately frame a login request message $\{Did_{\mathrm{i}}, D_i, M_i, T_i, T_1\}$. To be able to frame $Did_{\mathrm{i}} = id_{\mathrm{i}} \oplus \hbar(\mathfrak{z}id_i||T_1||T_i)$, an attacker must have id_{i} and $\mathfrak{z}id_i$. Such two values, however, are unidentified to E. This indicates that presented protocol is secure from a masquerade attack on the server. To imitate a server, the attacker must create a login answer message that includes$\{\mathfrak{z}Did_{\mathrm{i}}; \mathcal{W}_i; M_s; T_2; T_i^{\mathrm{new}}\}$. The attacker must

have id_i and $\mathcal{V}_i$ to frame $\mathfrak{z}Did_i$, $\mathcal{W}_i$ and M_s. The attacker, on the other hand, is completely oblivious of these two principles. This demonstrates that presented protocol can thwart a database masquerade attack.

Proposition 5.5 *The presented protocol could withstand the session's detection of a temporary information attack.*

Proof Let's examine whether an attacker could cooperation the session-specific random numbers (α, δ) that are chosen by AS and $\mathcal{C}_i$. In this situation, the session key $SK = \mathcal{T}^{\beta}_{\delta id_i}(D_i)(\mathrm{mod}q_1)$(or) $\mathcal{T}^{\beta}_{\alpha.b_i}(\mathcal{W}_i)(\mathrm{mod}q_1)$(or) $\mathcal{T}^{\beta}_{\alpha b_i \delta id_i}(\mathcal{V}_i)(\mathrm{mod}q_1)$ has not yet been accessed by an attacker. An attacker may be able to get a public communication channel from D_i or $\mathcal{W}_i$ over, but in order to frame SK, he/she requests to have either id_i, or b_i, or $\mathcal{V}_i$, which she/he does not have, sideways with δ, α. In this sense, we can say that our protocol prevents the known session-specific temporary information attack.

Proposition 5.6 *The proposed protocol maintains perfect forward secrecy for the security of the session key.*

Proof To say that this feature is in our protocol, we must prove that no session keys are uncovered even if some attacker E knows the server's private key x. The following fact demonstrates this: In our protocol, $SK = \mathcal{T}^{\beta}_{\alpha b_i \delta id_i}(\mathcal{V}_i)(\mathrm{mod}q_1)$, where $\mathcal{V}_i = \hbar(id_i||x||\mathfrak{z}id_i)$ is generated by $\mathcal{C}_i$ and AS in our protocol. An attacker E is unable to extract SK from the overheard note $\{D_i, \mathcal{W}_i\}$ even though x is on hand, since E does not have id_i and b_i at all.

Proposition 5.7 *The proposed procedure grants the user anonymity.*

Proof: The anonymity of the user guarantees that the id_i identity of a client like $\mathcal{C}_i$ is appropriately secured so that no attacker has access to it and can connect it to passwords. In our proposed protocol, the client's id_i tremendous communicated over a community message network, so the attacker E has no mode to get anywhere near tremendous id_i. In other words, only the login message contains the user's identity in the proposed protocol. The login message, on the other hand, is encrypted with the server's public key, whose security is based on the hardness of conformal Chebyshev chaotic maps. As a result, the login message cannot be used to determine the user's identity. In addition, the login message contains a random number that is different for each session. As a result, an attacker will be unable to determine the connection between transmitted login messages. The user's anonymity is ensured by the unlinkability and encryption of the login message. This means that the conditions for client anonymity fulfilled by the recent procedure.

Table 2 Functionality examination with other different protocols of the proposed protocol

Protocols/security features	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8
[5]	√	×	×	×	×	×	×	√
[9]	No(×)	×	×	×	×	×	×	√
[16]	×	√	×	√	√	×	×	×
[10]	Yes(√)	×	×	×	×	×	×	×
[15]	×	×	×	√	√	×	√	√
[49]	×	×	√	√	√	√	√	×
[48]	√	×	√	√	√	√	√	√
[50]	×	×	√	√	√	√	√	√
Proposed protocol	√	√	√	√	√	√	√	√

F_1 stolen SC attack, F_2 cancellation of lost smartcard, F_3 session specific temporary information attack, F_4 detection of the wrong password, F_5 perfect forward secrecy, F_6 insider attack, F_7 client impersonation attack, F_8 mutual authentication

Contrast with other protocols with experimental complexity evaluation

In this section, we will compare our presented authentication protocol with five other protocols introduced by Chen et al. [5], Song et al. [9], Sood et al. [10], Li et al. [15], Islam [16], Reddy et al. [48], Moon et al. [49] and Pan et al. [50], respectively, to demonstrate the security performance (see Table 2) and efficiency of our new design. Notations used to present our evaluation results include $\mathbb{t}_{ec}$, $\mathbb{t}_m$,$\mathbb{t}_s$,, $\mathbb{t}_e$,$\mathbb{t}_c$, and $\mathbb{t}_h$, which to represent the execution time essential for elliptic curve scale multiplication, modular multiplication, symmetric encryption/decryption operation, group modular exponentiation, chaotic map operation, and one-way hash function in the password change, authentication, registration and login, phases. Please note that only phases of password change, registration, authentication and login are the dominant processes which need more computing possessions compared to the extraction phase and the setup phase. Therefore, in our computational cost comparison, we concentrate only on the phases of login, registration, password change and authentication as we contrast our current authentication protocols with the work of Chen et al. [5], the work of Song et al. [9], the work of Sood et al. [10], the work of Li et al. [15], the work of Islam [16], the work of Reddy et al. [48], the work of Moon et al. [49] and the work of Pan et al. [50]. The functionality analysis of the proposed protocol is shown in Table 3 with other related protocols [5, 9, 10, 15, 16]. Table 3, Figs. 4, and 5 show how our novel approach compares in terms of computing costs to similar techniques [5, 9, 10, 15, 16, 48–50]. Based on the experimental findings in [51–53], we reach at the following computation time figures with unit hashing time: $\mathbb{t}_e = 600\mathbb{t}_h$,

Table 3 Computational cost analysis of the planned protocol with other related protocols

Protocols/phases	Registration	Login	Authentication	PW change
[5]	$\mathbb{t}_h + \mathbb{t}_e \approx 302.31$ ms	$2(\mathbb{t}_h + \mathbb{t}_e) \approx 604.61$ ms	$2(3\mathbb{t}_h + \mathbb{t}_e) \approx 606.38$ ms	$2(3\mathbb{t}_h + 2\mathbb{t}_e) \approx 1210.22$ ms
[9]	$\mathbb{t}_h + \mathbb{t}_e \approx 302.31$ ms	$2(\mathbb{t}_h + \mathbb{t}_e) \approx 604.61$ ms	$4\mathbb{t}_h + \mathbb{t}_e \approx 303.82$ ms	$2(\mathbb{t}_h + \mathbb{t}_e) \approx 604.61$ ms
[16]	$2\mathbb{t}_h + \mathbb{t}_e \approx 302.81$ ms	$2(\mathbb{t}_h + \mathbb{t}_e) \approx 604.61$ ms	$4\mathbb{t}_h + 3\mathbb{t}_e \approx 907.42$ ms	$2\mathbb{t}_h + \mathbb{t}_e \approx 302.81$ ms
[10]	$2(\mathbb{t}_h + \mathbb{t}_e) \approx 604.61$ ms	$2\mathbb{t}_h + 3\mathbb{t}_e \approx 906.41$ ms	$2(2\mathbb{t}_h + \mathbb{t}_e) \approx 605.62$ ms	$2(\mathbb{t}_h + \mathbb{t}_e) \approx 604.61$ ms
[15]	$2(\mathbb{t}_h + \mathbb{t}_e) \approx 604.61$ ms	$3\mathbb{t}_h + 3\mathbb{t}_e \approx 906.91$ ms	$4\mathbb{t}_h + 4\mathbb{t}_e \approx 1209.22$ ms	$3\mathbb{t}_h + 4\mathbb{t}_e \approx 1208.71$ ms
[49]	$5\mathbb{t}_h + \mathbb{t}_m \approx 3.78$ ms	$5\mathbb{t}_h + \mathbb{t}_m + 2\mathbb{t}_{ec} \approx 76.71$ ms	$4\mathbb{t}_h + \mathbb{t}_m + 2\mathbb{t}_{ec} \approx 76.21$ ms	$3\mathbb{t}_h + \mathbb{t}_m \approx 2.77$ ms
[48]	$2(\mathbb{t}_h + \mathbb{t}_m) \approx 3.521$ ms	$3\mathbb{t}_h + \mathbb{t}_m + \mathbb{t}_{ec} \approx 39.24$ ms	$2\mathbb{t}_h + \mathbb{t}_m \approx 2.27$ ms	$\mathbb{t}_h + 2\mathbb{t}_m \approx 3.02$ ms
[50]	$5\mathbb{t}_h + \mathbb{t}_m \approx 3.78$ ms	$6\mathbb{t}_h + \mathbb{t}_m + 2\mathbb{t}_{ec} \approx 77.22$ ms	$5\mathbb{t}_h + \mathbb{t}_m + 2\mathbb{t}_{ec} \approx 76.71$ ms	$3\mathbb{t}_h + \mathbb{t}_m \approx 2.77$ ms
Proposed protocol	$7\mathbb{t}_h \approx 3.53$ ms	$6\mathbb{t}_h + \mathbb{t}_c \approx 3.53$ ms	$16\mathbb{t}_h + 3\mathbb{t}_c \approx 9.56$ ms	$8\mathbb{t}_h \approx 4.03$ ms

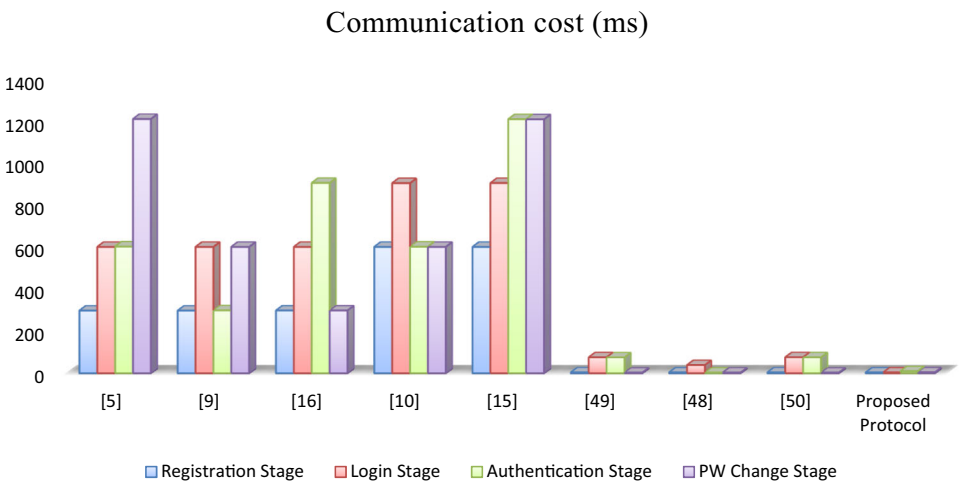

Fig. 4 Communication costs (ms) in different phases

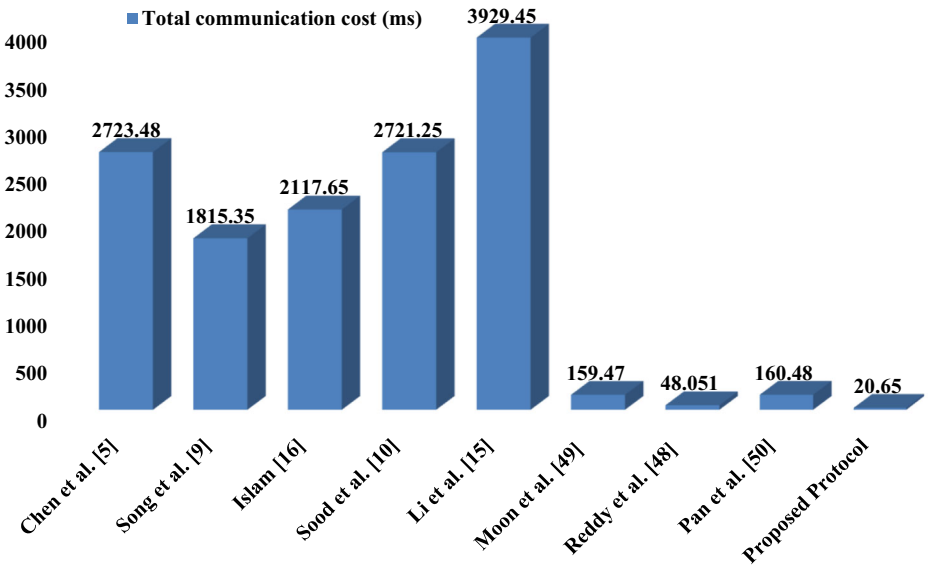

Fig. 5 Total communication costs (ms)

$\mathbb{t}_m = 2.5\mathbb{t}_h, \mathbb{t}_{ec} = 72.5\mathbb{t}_h, \mathbb{t}_s = \mathbb{t}_h$ and $\mathbb{t}_h = \mathbb{t}_c$. In this method, we obtain the following order of computational complexity: $\mathbb{t}_h \approx \mathbb{t}_c \approx \mathbb{t}_s < \mathbb{t}_m < \mathbb{t}_{ec} < \mathbb{t}_e$. By the way, we know that 0.503 ms [51] is running time of$\mathbb{t}_h$. The total communication costs of the work of Chen et al. [5], the work of Song et al. [9], the work of Islam [16], the work of Sood et al. [10], the work of Li et al. [15], the work of Pan et al. [50], the work of Reddy et al. [48] and the work of Moon et al.

[49] and the proposed protocol are 2723.48 ms, 1815.35 ms, 2117.65 ms, 2721.25 ms, 3929.45 ms, 160.48 ms, 48.06 ms, 159.47 ms and 20.65 ms, respectively. The suggested protocol has by far the lowest interaction value, as evidenced by the study findings in Fig. 5. The proposed protocol frequently results in tests that outperform the rest of the protocols in terms of runtime.

Conclusion

In this paper, we proposed an effective remote user password authentication protocol based on CCM using smart card, where the client can get relief from several types of attacks. The projected protocol is more efficient, has reduced computing costs, and, most importantly, provides a higher level of security for smart card-based password authentication. The ROR model is also used to demonstrate the security evaluation of our proposed protocol. However, the other security and applied features of the proposed authentication protocol are examined. The proposed protocol is a more suitable and stable authentication protocol for genuine use compared to previous protocols. In the future, we plan to provide a security framework for CCM-based authentication and key agreement protocols, as well as develop authentication protocols using this mechanism. When establishing security protocols, we will also look into privacy protection and the most effective approach for client authentication and key agreement.

Acknowledgements The authors would like to thank anonymous reviewers of Complex and Intelligent Systems for their careful and helpful comments and extend their gratitude to the Deanship of Scientific Research at King Khalid University for funding this work through research groups program under Grant Number R. G. P. 1/72/42

Declarations

Conflict of interest The authors have declared no conflict of interest.

Compliance with ethics requirements This article does not contain any studies with human or animal subjects.

References

1. Kocarev L (2001) Chaos-based cryptography: a brief overview. IEEE Circ Syst Mag 1:6–21
2. Han S, Chang E (2009) Chaotic map based key agreement with/out clock synchronization. Choas Solit Fract 39(3):1283–1289
3. Hwu F (1993) The interpolating random spline cryptosystem and the chaotic-map public-key cryptosystem. Ph.D. thesis, University of Missouri Rolla
4. ElGmal T (1995) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 31:469–472
5. Chen BL, Kuo WC, Wu LC (2014) Robust smartcard-based remote user password authentication scheme. Int J Commun Syst 27:377–389
6. Ma CG, Wang D, Zhao SD (2014) Security flaws in two improved remote user authentication schemes using smart cards. Int J Commun Syst 27(10):2215–2227
7. Xu J, Zhu WT, Feng DG (2009) An improved smartcard-based password authentication scheme with provable security. Comput Stand Interfaces 31(4):723–728
8. Song R (2010) Advanced smartcard-based password authentication protocol. Comput Stand Interfaces 32(5):321–325
9. Song R, Korba L, Yee G (2007) Analysis of smart card-based remote user authentication schemes. In: Proceedings of the 2007 International Conference on Security and Management. Las Vegas, USA, pp 323–329
10. Sood SK, Sarje AK, Singh K (2010) An improvement of Xu et al.'s authentication scheme using smartcards. In: Proceedings of the Third Annual ACM Bangalore Conference, Bangalore, Karnataka, India, pp 17–25
11. Joye M, Olivier F (2010) Side-channel analysis, encyclopedia of cryptography and security. Kluwer Academic Publishers Springer, Berlin, pp 571–576
12. Kocher P, Jaffe J, Jun B (1999) Differential power analysis. In: Proceedings of Advances in Cryptology (Crypto'99), LNCS. Springer Berlin Heidelberg, pp 388–397
13. Messerges TS, Dabbish EA, Sloan RH (2002) Examining smart card security under the threat of power analysis attacks. IEEE Trans Comput 51(5):541–552
14. Chen C, He DJ, Chan SM, Bu JJ, Gao Y, Fan R (2011) Lightweight and provably secure user authentication with anonymity for the global mobility network. Int J Commun Syst 24(3):347–362
15. Li X, Niu J, Khan MK, Liao J (2013) An enhanced smartcard based remote user password authentication scheme. J Netw Comput Appl 36:1365–1371
16. Islam SKH (2016) Design and analysis of an improved smartcard–based remote user password authentication scheme. Int J Commun Syst 29(11):1708–1719
17. Li X, Niu J, Kumari S, Islam SKH, Wu F, Khan MK, Das AK (2016) A novel chaotic maps-based user authentication and key agreement protocol for multi-server environments with provable security. Wirel Pers Commun 89(2):569–597
18. Luo M, Zhang Y, Khan MK, He D (2017) An efficient chaos-based two-party key agreement protocol with provable security. Int J Commun Syst 30(14):e3288
19. Li CT, Chen CL, Lee CC, Weng CY, Chen CM (2018) A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps. Soft Comput 22:2495–2506
20. Zhao Y, Li S, Jiang L, Liu T (2019) Security-enhanced three-factor remote user authentication scheme based on Chebyshev chaotic maps. Int J Distrib Sens Netw 15(4):1–12
21. Dharminder D, Gupta P (2019) Security analysis and application of Chebyshev Chaotic map in the authentication protocols. Int J Comput Appl. https://doi.org/10.1080/1206212X.2019.1682238

22. Mishra D, Kumar V, Dharminder D, Rana S (2020) SFVCC: chaotic map-based security framework for vehicular cloud computing. IET Intel Transp Syst 14(4):241–249
23. Meshram C, Ibrahim RW, Deng L, Shende SW, Meshram SG, Barve SK (2021) A Robust smart card and remote user password-based authentication protocol using extended chaotic-maps under smart cities environment, soft computing. Accepted
24. Wu GC, Baleanu D, Xie HP, Chen FL (2016) Chaos synchronization of fractional chaotic maps based on the stability condition. Physica A 460:374–383
25. Bai YR, Baleanu D, Wu GC (2018) A novel shuffling technique based on fractional chaotic maps. Optik 168:553–562
26. Wu GC, Deng ZG, Baleanu D, Zeng DQ (2019) New variable-order fractional chaotic systems for fast image encryption. Chaos 29(8):083–103
27. Mason JC, Handscomb DC (2003) Chebyshev polynomials. Chapman & Hall/CRC, Boca Raton
28. Bergamo P, D'Arco P, Santis A, Kocarev L (2005) Security of public key cryptosystems based on Chebyshev polynomials. IEEE Trans Circ Syst I 52(7):1382–1393
29. Han S, Chang E (2009) Chaotic map based key agreement with/out clock synchronization. Choas Solit Fractals 39(3):1283–1289
30. Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solit Fractals 37(3):669–674
31. Canetti R, Krawczyk H (2001) Analysis of key-exchange protocols and their use for building secure channels. In: Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol. (EUROCRYPT). Tyrol, Austria: Springer, pp 453–474
32. Canetti R, Krawczyk H (2002) Universally composable notions of key exchange and secure channels. In: Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol. (EUROCRYPT), Amsterdam, The Netherlands, pp 337–351
33. Chatterjee S, Roy S, Das AK, Chattopadhyay S, Kumar N, Vasilakos AV (2018) Secure biometric-based authentication scheme using chebyshev chaotic map for multi-server environment. IEEE Trans Depend Secure Comput 15(5):824–839
34. Dua A, Kumar N, Das AK, Susilo W (2018) Secure message communication protocol among vehicles in smart city. IEEE Trans Veh Technol 67(5):4359–4373
35. Srinivas J, Das AK, Kumar N, Rodrigues J (2020) Cloud centric authentication for wearable healthcare monitoring system. IEEE Trans Depend Secure Comput 17(5):942–956
36. Chattaraj D, Sarma M, Das AK (2018) A new two-server authentication and key agreement protocol for accessing secure cloud services. Comput Netw 131:144–164
37. Kocher P, Jaffe J, Jun B (1999) Differential power analysis. In advances in cryptology—CRYPTO. Springer, Santa Barbara, pp 388–397
38. Messerges TS, Dabbish EA, Sloan RH (2002) Examining smart-card security under the threat of power analysis attacks. IEEE Trans Comput 51(5):541–552
39. Odelu V, Das AK, Goswami A (2015) A secure biometrics-based multiserver authentication protocol using smart cards. IEEE Trans Inf Foren Secur 10(9):1953–1966
40. 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
41. Meshram C, Li CT, Meshram SG (2019) An efficient online/offline ID-based short signature procedure using extended chaotic maps. Soft Comput 23(3):747–753
42. Meshram C, Lee CC, Meshram SG, Li CT (2019) An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem. Soft Comput 23(16):6937–6946
43. Anderson DR, Camrud E, Ulness DJ. On the nature of the conformable derivative and its applications to physics. *arXiv preprint* arXiv:1810.02005*, 2018*.
44. Burrows M, Abadi M, Needham R (1990) A logic of authentication. ACM Trans Comput Syst 8(1):18–36
45. Das AK, Odelu V, Goswami A (2014) A Robust and Effective Smart-Card-Based Remote User Authentication Mechanism Using Hash Function. Sci World J. https://doi.org/10.1155/2014/719470
46. Chang CC, Cheng TF, Hsueh WY (2016) A robust and efficient dynamic identity-based multi-server authentication scheme using smart cards. Int J Commun Syst 29(2):290–306
47. Tang HB, Liu XS (2012) Cryptanalysis of a dynamic ID-based remote user authentication with key agreement scheme. Int J Commun Syst 25(12):1639–1644
48. Farash MS (2017) An improved password-based authentication scheme for session initiation protocol using smart cards without verification table. Int J Commun Syst 30(1):e2879
49. Reddy AG, Suresh D, Phaneendra K, Ji SS, Odelu V (2018) Provably secure pseudo-identity based device authentication for smart cities environment. Sustain Cities Soc 41:878–885
50. Moon J, Lee D, Jung J, Won D (2017) Improvement of efficient and secure smart card-based password authentication scheme. Int J Netw Secur 19(6):1053–1061
51. Pan H-T, Yang H-W, Hwang M-S (2020) An enhanced secure smart card-based password authentication scheme. Int J Netw Secur 22(2):358–363
52. Kumari S, Khan MK (2014) Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme. Int J Commun Syst 27(12):3939–3955
53. 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
54. 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 Programs Biomed 135:37–50
55. Meshram C, Ibrahim RW, Obaidat MS, Sadoun B, Meshram SG, Tembhurne JV (2021) An effective mobile-healthcare emerging emergency medical system using conformable chaotic maps. Soft Comput 25(14):8905–8920