




Article

An Efficient Fractional Chebyshev Chaotic Map-Based Three-Factor Session Initiation Protocol for the Human-Centered IoT Architecture

Chandrashekhar Meshram ¹, Cheng-Chi Lee ^{2,3,*} , Ismail Bahkali ⁴  and Agbotiname Lucky Imoize ^{5,6} 

- ¹ Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government, Post-Graduate College, College of Chhindwara University, Betul 460001, MP, India
- ² Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei City 24205, Taiwan
- ³ Department of Computer Science and Information Engineering, Asia University, Taichung City 41354, Taiwan
- ⁴ Department of Information Science, King Abdulaziz University, Jeddah 21589, Saudi Arabia
- ⁵ Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria
- ⁶ Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany
- * Correspondence: cclee@mail.fju.edu.tw

Abstract: One of the most frequently used signaling techniques for initiating, sustaining, and dismissing sessions on the internet is a session initiation protocol (SIP). Currently, SIPs are gaining widespread applications in the human-centered Internet of Things (HC-IoT) domain. In HC-IoT environments, sensitive user data are transmitted over open communication channels that require secure authentication to protect sensitive user information from unlawful exploitation. In order to provide robust authentication for critical user data, SIP-based authentication mechanisms have been proposed; however, these authentication schemes have not provided perfect authentication and effective security for users. Additionally, the existing schemes are computationally intensive and cost-prohibitive in design and implementation. In order to address this problem, especially in the human-centered IoT context, this work introduces a provably secure, lightweight, three-factor SIP-based scheme to tackle the shortcomings of traditional schemes. The presented scheme is based on an extended fractional Chebyshev chaotic map. A formal security verification of the session key in the real-or-random (ROR) model is conducted to evaluate the projected scheme. The investigation results indicate that the new scheme is SIP compatible and achieves secure mutual authentication with robust security features compared to the existing schemes. Therefore, the proposed SIP-enabled scheme can be deployed in the human-centered Internet of Things to secure critical user information.

Keywords: session initiation protocol; fractional Chebyshev chaotic map; secure key agreement; smart card; human-centered IoT environment; biometrics-assisted lightweight security systems

MSC: 34C28

Citation: Meshram, C.; Lee, C.-C.; Bahkali, I.; Imoize, A.L. An Efficient Fractional Chebyshev Chaotic Map-Based Three-Factor Session Initiation Protocol for the Human-Centered IoT Architecture. *Mathematics* **2023**, *11*, 2085. <https://doi.org/10.3390/math11092085>

Academic Editor: Lingfeng Liu

Received: 12 February 2023

Revised: 24 April 2023

Accepted: 25 April 2023

Published: 27 April 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In recent years, the session initiation protocol (SIP) has become the most widely used application layer control protocol [1–3]. Specifically, a SIP creates, modifies, and terminates sessions [4]. A SIP supports five key aspects required for establishing and maintaining the termination of a multimedia session; the five aspects are user location, user ability, user effectiveness, session management, and session initiation. Additionally, a SIP can define how to manage a session to meet expected outcomes in real time [5]. This flexible feature makes it possible to use a SIP in numerous applications and services such as music, videos, and web meetings [6,7].

In the literature, SIP-based schemes have been broadly categorized as one-factor SIP authentication [6,8–11], two-factor SIP authentication [2,12–15], and three-factor SIP authentication [16–20] schemes. One-factor SIP authentication schemes pose limited security against adversarial attacks since they only use passwords to prove user authenticity. The vulnerabilities identified include, but are not limited to, dictionary attacks, guessing attacks, and Trojan attacks [3]. Additionally, two-factor SIP authentication schemes use passwords and smart cards, making them safer. However, several drawbacks have been associated with two-factor SIP authentication schemes [21,22]; it is not unlikely that they are vulnerable to smart card loss attacks [12]. Three-factor SIP authentication schemes combine passwords, smart cards, and biometrics, which reinforces the security architecture of the schemes, making them suitable for applications in human-centered IoT environments [23–25]. These schemes have been used in medical decision support systems, smart homes, learning systems, and more [26,27]. Figure 1 depicts the network configuration and application scenarios for the session initiation protocol (SIP).

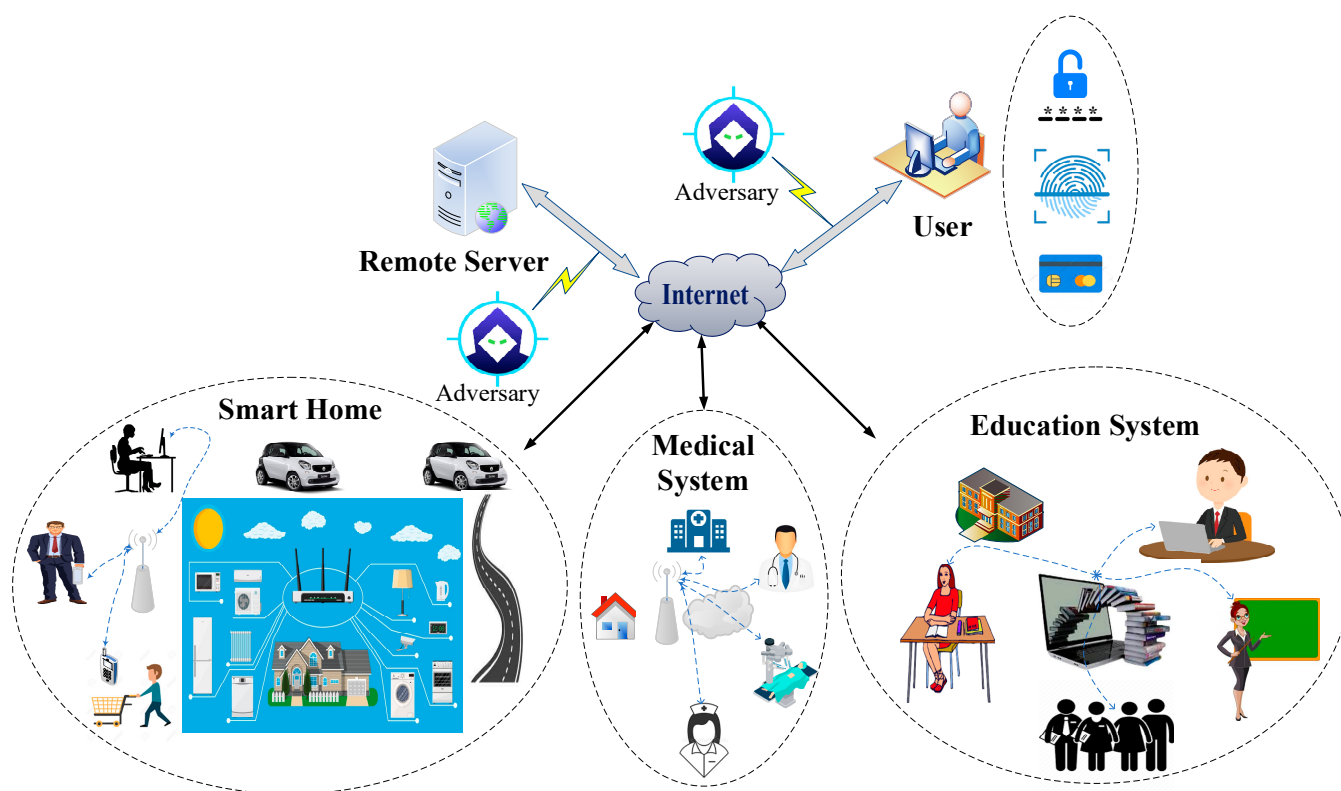


Figure 1. Network configuration and application scenarios for the session initiation protocol.

Whereas the services provided by a SIP are beneficial, the associated security challenges are enormous and require critical examination. Several SIP-based authentication schemes have been reported [14,22,28–30]. In addition, a few SIP-based key agreement schemes pose high resistance to sophisticated attacks [31]. However, most SIP-based authentication schemes are vulnerable to well-known threats. Thus, the need for robust security and a key agreement protocol for a SIP scheme that is not susceptible to any known attack is imperative, which is the basis for the current study.

1.1. Research Contributions

This article proposes a provably secure, lightweight, three-factor session initiation protocol using extended fractional Chebyshev chaotic maps (FCCM) in the HC-IoT environment. In particular, the key contributions of this paper are highlighted as follows.

- An efficient and secure remote authentication scheme for a SIP is proposed using extended FCCM, a smart card (SC), and user biometrics simultaneously in the HC-IoT environment.
- An informal security analysis of the projected protocol is demonstrated, and the results show that it is provably secure in the ROR model.
- A comparison of the projected protocol with related authentication protocols is conducted and it is found that it is cost-efficient and requires fewer computational resources. This is because the presented approach uses FCCM, which eliminates computationally intensive elliptic curve point multiplication.

1.2. Organization of Manuscript

The remainder of this work is organized as follows: In Section 2, we outline related works; in Section 3, we provide the background and material; In Section 4, we present our new SIP scheme based on FCCM; in Section 5, we provide a comprehensive security analysis of the projected technique; in Section 6, we demonstrate the performance evaluation of the projected technique; finally, in Section 7, we provide a concise conclusion to the paper.

2. Related Work

In wireless communication, especially in the human-centered IoT environment, guaranteeing a secure SIP for the communication requires secure authentication with a key agreement protocol executed before actual communication is initiated. In order to fulfill this criterion, several SIP-based schemes have been proposed [6,12,13,32,33]. Specifically, Arshad and Nikooghadam presented an effective authentication scheme for a SIP based on elliptic curve cryptography (ECC). In addition, Zhang et al. [12] reported a flexible authentication scheme for a SIP, leveraging smart cards. Interestingly, the scheme by Zhang et al. [12] showed impressive security features; however, the security of the scheme was not perfect, as claimed. In the work by Irshad et al. [13], the flaws in Zhang et al.'s scheme were highlighted, and solutions were offered to improve the scheme. In particular, one of the main limitations of Zhang et al.'s scheme was its vulnerability to a DoS attack. As a result, Irshad et al. [13] presented an improved SIP based on chaotic constructions. In another related study that examined the limitations of Irshad et al.'s protocol [13], Arshad et al. [6] mentioned that the protocol was vulnerable to client impersonation attacks. In order to address the limitations posed by Irshad et al.'s protocol, Arshad et al. projected a secure protocol that employed elliptic curve cryptography (ECC) [6]. In a recent analysis, Lin et al. [32] showed that the protocol, due to Arshad et al., was not secure against several attacks such as server spoofing, denial-of-service (DoS), and privilege insider attacks. Lin et al. [32] also demonstrated that Arshad et al.'s protocol failed the user anonymity test. In order to strengthen the security of Arshad et al.'s protocol [6], Lin et al. suggested a new scheme for a SIP using the ECC.

In [34], Chen et al. examined the security of the protocol presented by Lin et al. [32]. The SIP for anonymous authentication and key negotiation was shown to have various security issues. The protocol failed an offline password-guessing attack and could not sustain a stolen memory device attack. Furthermore, Lin et al.'s protocol could not verify a wrong password and showed a weak password updating procedure. In order to address the proliferating issues in Lin et al.'s protocol, Chen et al. [34] presented a new mutual authentication with a key agreement protocol with robust features compared to Lin et al.'s protocol. An authentication scheme for a SIP was presented by Islam et al. [35]. The authors claimed that the SIP-based scheme was immune to known attacks. However, the work conducted by Chen et al. [34] revealed that Islam et al.'s protocol [35] failed impersonation attacks and could not achieve user anonymity.

Chen et al.'s scheme [34] used an extended chaotic map that supported fast computation. Additionally, the scheme was tested using Burrows–Abadi–Needham (BAN) logic to demonstrate that it supported secure mutual authentication. The ROR model was also used to examine the formal security investigation of the session key. The most critical part

of a SIP is the authentication process required for a network user to access the SIP server. SIP security is becoming increasingly significant, and the need for a reliable authentication scheme for the SIP is not out of place.

However, the security of a SIP-based authentication protocol has been questioned, primarily as billions of sensitive user data are currently being conveyed in real time over open communication channels. In order to boost the security frameworks of these schemes, Zhang et al. [36] employed biometric identification technology to project a lightweight SIP authentication leveraging symmetric encryption. Zhang et al.'s scheme [36] showed good resilience to insider attacks, offline dictionary attacks, replay attacks, and it had lower computational costs. It should be emphasized that Zhang et al.'s scheme was not perfect. Recently, Naqvi et al. [16] revealed some security vulnerabilities in Zhang et al.'s scheme, such as limited resistance to replay attacks and failure to meet user anonymity requirements.

Naqvi et al. suggested a three-factor SIP-based protocol to address the vast limitations of Zhang et al.'s protocol. Furthermore, Mishra et al. [17] analyzed the protocol reported in [37] and showed that it was vulnerable to man-in-the-middle and impersonation attacks. A SIP protocol based on biometrics offering robust security against active and passive attacks has been demonstrated by Mishra et al. [17] to address the limitations of the scheme by Tu et al. [37]. Additionally, Mishra et al. [17] used the Automated Validation of Internet Security Protocols and Application (AVISPA) tool to investigate the formal security of the projected protocol. However, Islam et al. [20] observed that the SIP-based protocols reported by [16,17,36] were vulnerable to DoS attacks and lacked resiliency against clock synchronization issues. In order to improve the performance of this protocol, Islam et al. [20] suggested a robust and cost-effective scheme using hash functions and hard computational problems.

However, several vulnerabilities, such as limited resistance to impersonation attacks, forgery attacks, user anonymity issues, and lack of forward secrecy, limit the protocol's authenticity. In order to improve user anonymity and other problems identified in Islam et al.'s procedure [20], Wang et al. [38] put forward a public key scheme that provided robust security and supported user anonymity. Due to design deficiencies, most SIP-based protocols [27,39,40] have shown some security vulnerabilities. In addition, the application of scalar multiplication in SIP-based protocols has contributed to high computation overhead. Nevertheless, Chebyshev chaotic maps find useful applications in human-centered IoT environments in facilitating identity verification in healthcare information systems [41], cloud computing [42], and the Internet of Things (IoT) [43].

Another work closely related to the current study is the scheme reported in [3]. Specifically, the scheme is based on an extended chaotic map, which avoids computationally expensive elliptic curve point multiplication. In addition, the study aimed to enhance mutual authentication to eliminate the drawbacks of the existing schemes. The study applied Burrows–Abadi–Needham logic to prove that the proposed scheme achieved secure mutual authentication and was suitable for SIP applications. However, the work in [3] failed the clock synchronization attack, which is critical to protecting sensitive user information. In order to address this problem, there is a need for a more robust and enhanced security scheme for SIP applications. To this end, the current work proposes using fractional Chebyshev chaotic maps to address the prevailing issues in the existing SIP-based protocols. The proposed scheme successfully resolved the clock synchronization problem in the scheme reported in [3].

The preliminaries and background of fractional Chebyshev chaotic maps employed in designing our SIP-based protocol are briefed in this paper.

3. Background and Material

In this section, we briefly discuss the functionality and security requirements, the hash function [44], the Chebyshev chaotic map [45], the FCCM [46], and the biometrics and fuzzy extractor [47] which are described in this article. Table 1 lists the notations used for the protocol developed in this paper.

Table 1. The notations used in the development of the protocol.

Notation	Explanation
\mathcal{C}	Client
\mathcal{RS}	Remote server
$id_{\mathcal{C}}$	Identity of \mathcal{C}
\mathfrak{F}	Adversary
$pw_{\mathcal{C}}$	Password of \mathcal{C}
$BIO_{\mathcal{C}}$	Biometrics of \mathcal{C}
id_{sc}	Smart cards identity
s	\mathcal{RS} 's secret key
$\vartheta/y_r/a_{\mathcal{C}}/b_r$	Random number
$SK_{\mathcal{C}_r}$	Session key
δ	Random rational number from $[0, 1]$
F_q	A finite field, where q is a huge prime
$T_n(\cdot)$	A n th degree Chebyshev polynomial
$T_n^{\delta}(\cdot)$	A n th fractional Chebyshev polynomial
$h(\cdot)$	Cryptographic one-way hash function
\oplus	XOR operation
\parallel	Concatenation operation

3.1. Hash Function

A hash function of the form $h : \{0, 1\}^* \rightarrow \{0, 1\}^n$ accepts any binary length string $q \in \{0, 1\}^*$ as input and gives a binary string $h_q \in \{0, 1\}^n$ as yield. The following is the collision-resistance of $h(\cdot)$:

Definition 1. Assume that $Adv_{\mathcal{A}}^{Hash}(t)$ reflects an adversary \mathcal{A} 's advantage in locating a hash collision in polynomial time t , i.e., $Adv_{\mathcal{A}}^{Hash}(t) = Pr[(a, \mathfrak{A}) \leftarrow a \neq \mathfrak{A}, h(a) = h(\mathfrak{A})]$, where $Pr[E]$ denotes the probability of an E event occurring. When a (ζ, t) -adversary \mathcal{A} attacks the resistance of $h(\cdot)$, this indicates that \mathcal{A} 's runtime is, at most, t and that $Adv_{\mathcal{A}}^{Hash}(t) \leq \zeta$ is true for an adequately small $\zeta > 0$.

3.2. Chebyshev Chaotic Maps

Let $z \in [-1, 1]$ be a real number and n be an integer, the Chebyshev polynomial $T_n(z) : [-1, 1] \rightarrow [-1, 1]$ is then defined as follows:

$$T_n(z) = \cos(n \cdot \cos^{-1}(z))$$

The Chebyshev polynomial has the following recurrence relation:

$$T_n(z) = \begin{cases} 1 & \text{if } n = 0 \\ z & \text{if } n = 1 \\ 2z_{n-1}(z) - T_{n-2}(z) & \text{if } n \geq 2 \end{cases}$$

- Chaotic map-based discrete logarithm problem (CMDLP): For any given x and y , it is not computationally feasible to calculate the integer n such that $T_n(z) \bmod p = y$.
- Chaotic map-based computational Diffie–Hellman problem (CMDHP): It is not computationally feasible to compute $T_{rs}(z) \bmod p$, for three elements z , $T_r(z) \bmod p$, and $T_s(z) \bmod p$.

Where there is a large prime number, the Chebyshev polynomial with CMDHP has the following formal definition:

Definition 2. For any \mathcal{A} adversary with t execution time, the advantage probability $Adv_{\mathcal{A}}^{AS}(t)$ of the CMDHP is negligible, that is, $Adv_{\mathcal{A}}^{Hash}(t) \leq \varsigma$ for a sufficiently small $\varsigma > 0$.

3.3. Fractal Chaotic Maps (FCM)

Fractal calculus (FC) was formerly known as a local fractional calculus [45,48]. In addition, fractional calculus accepts holdings. The following preparation takes priority over FC:

Suppose that the fractional difference operator ξ^γ is defined by the formal equation for a random fractional-order $\gamma \in [0, 1]$. Then,

$$\xi^\gamma \psi(\mathfrak{z}) = \frac{\Delta^\gamma(\psi(\mathfrak{z}) - \psi(\mathfrak{z}_0))}{(\mathfrak{z} - \mathfrak{z}_0)^\alpha} = \Gamma(\gamma + 1)(\psi(\mathfrak{z}) - \psi(\mathfrak{z}_0))$$

and the fractal integral operator is the same as this:

$$I^\gamma \psi(\mathfrak{z}) = \frac{1}{\Gamma(\gamma + 1)} \int_a^b \psi(\mathfrak{z})(d)^\gamma.$$

By using the formula in (1), it can be approximated as:

$$I^\gamma \psi(\mathfrak{z}) = \frac{(b-a)^\gamma}{\Gamma(\gamma + 1)} \psi(\mathfrak{z}), \quad a \leq \mathfrak{z} \leq b. \quad (1)$$

By generalizing the polynomial $\mathbb{T}_n(\nu)$ with the FC notion, we obtain the following Equation (2):

$$I^\gamma \mathbb{T}_n(\nu) := \mathbb{T}_n^\gamma(\nu) = \frac{(2)^\gamma}{\Gamma(\gamma + 1)} \mathbb{T}_n(\nu), \quad (2)$$

The fractal Chebyshev polynomial is abbreviated as FCP (see Figure 2).

3.4. Possessions of Fractal Chaotic Maps with Extension

The following are two of the FCP's critical properties:

Definition 3 (Chaotic possessions of FCM). The fractal chaotic maps [45,49] satisfy the chaotic possessions recurrent relations, i.e., $\mathbb{T}_n^\gamma(\nu) = \frac{(2)^\gamma}{\Gamma(\gamma + 1)} (2\nu \mathbb{T}_{n-1}(\nu) - \mathbb{T}_{n-2}(\nu)) \pmod{q_1}$. The usual significant effect, as observed by Yang et al. [48], is well known when $\gamma \rightarrow 0$ is used.

Definition 4 (Semi-group possessions of FCM). For FCMs on the interval $(-\infty, \infty)$ (it is known as extended FCCM) [45], the semi-group possessions hold.

$$\mathbb{T}_k^\gamma(\mathbb{T}_n^\gamma(\nu)) \pmod{q_1} = \mathbb{T}_n^\gamma(\mathbb{T}_k^\gamma(\nu)) \pmod{q_1} = \mathbb{T}_{kn}^\gamma(\nu) \pmod{q_1}$$

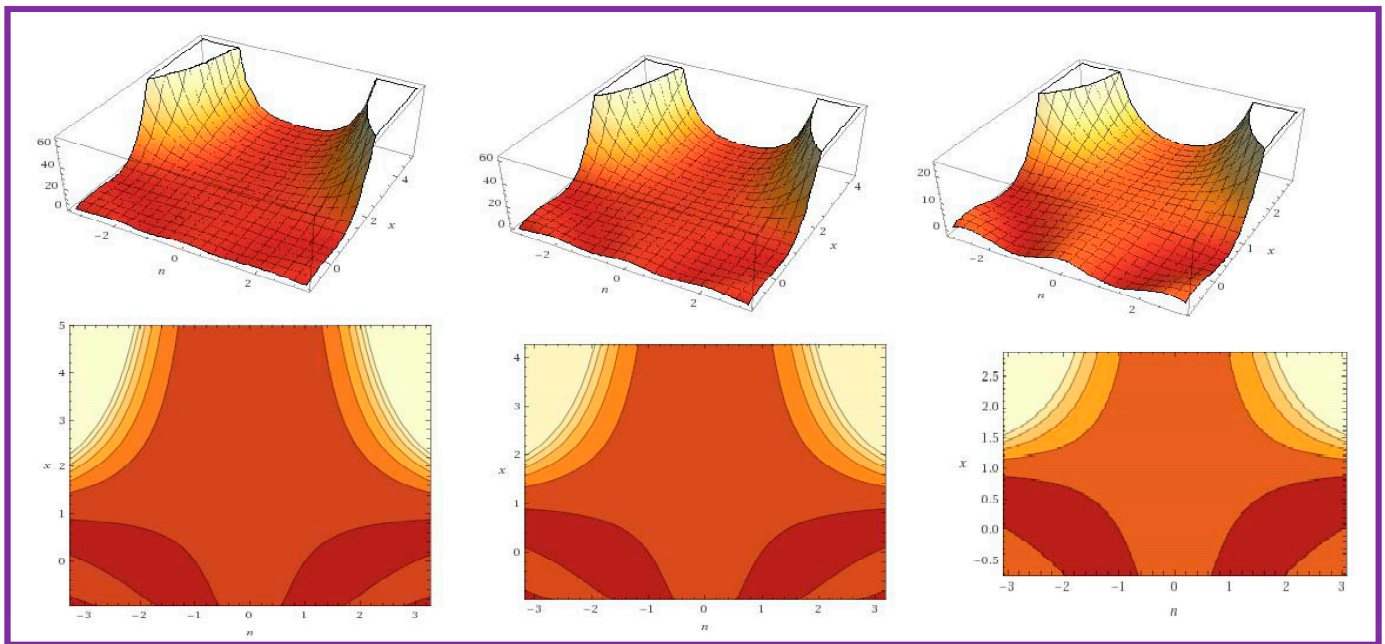


Figure 2. 3D-FCP when $\gamma = 0, 1/2$, and $3/4$.

3.5. Biometrics and Fuzzy Extractor

Because of their distinct qualities, biometric keys such as palm prints, fingerprints, and iris are being used in numerous authentication procedures. There are three significant advantages to using biometric keys: They are incredibly tough to fabricate or distribute, as well as duplicate or share, and they cannot be misplaced or forgotten.

The fuzzy extractor approach has recently been discovered to be effective in extracting the biometric key from the biometric input from users. The fuzzy extractor takes a user's biometric feature input, say BIO_C , and generates the unique random string, ζ_C , as well as the auxiliary string, ζ_C , in an error-tolerant manner using a probabilistic generation function. Furthermore, it uses a deterministic replication technique to construct the identical original string ζ_C , an auxiliary string ζ_C , and a noisy user biometric BIO'_C that differs from the original biometric BIO_C up to a threshold value.

Two algorithms, $Gen(\cdot)$ and $Rep(\cdot)$, are used in the fuzzy extraction method. $(\zeta_C, \zeta_C) = Gen(BIO_C)$ and $\zeta_C = Rep(BIO'_C, \zeta_C)$ are the definitions for the functions $Gen(\cdot)$ and $Rep(\cdot)$.

4. The Proposed Three-Factor SIP Scheme Based on FCCM under the HClIoT Environment

An efficient and secure SIP is projected in this segment. The proposed SIP is divided into five major stages: (1) setup, (2) registration, (3) login, (4) authentication and key formation, and (5) password and biometrics change. The specifics are listed as follows:

4.1. Setup Stage

During this stage, the \mathcal{RS} produces all systems' public constraints.

Step 1. The \mathcal{RS} picks $s \in F_q$ as its secret key.

Step 2. $\mathcal{T}^\delta(\cdot)(\vartheta)$ and a secure hash function $h(\cdot)$ are computed by the \mathcal{RS} using a random number $\vartheta \in (-\infty, +\infty)$ and rational number $\delta \in [0, 1]$.

Step 3. The \mathcal{RS} makes the constraints $\{h(\cdot), \vartheta, \mathcal{T}^\delta(\cdot)(\vartheta)\}$ available to all legal users.

4.2. Registration Stage

During this stage of the protocol, the C and the RS use a secure channel to complete the following tasks in order to publish a valid SC . It is worth noting that this is a one-time procedure.

- Step 1. The C scans her/his biometrics BIO_C using a biometric scanner gadget. The C picks an id_C , as well as a password pw_C . Then, he/she computes $Gen(BIO_C) = (\zeta_C, \zeta_C)$ and $\eta_C = h(id_C, pw_C, \zeta_C)$, and sends id_C, η_C through a secure channel to the RS .
- Step 2. When the registration message is received, the RS uses its private key s and id_C to calculate $Y_C = h(s, id_C)$, $U_C = Y_C \oplus \eta_C$, $T_s^\delta(\theta)$, and $O_C = h(id_C, \eta_C, Y_C)$. Then, the RS stores $\{U_C, O_C, \theta, T_s^\delta(\theta), h(\cdot), T^\delta(\cdot)(\theta), Rep(\cdot)\}$ into a SC and transmits it to the C over a protected channel.
- Step 3. When the C receives the SC , he/she writes ζ_C on it.

Finally, the SC contains the following info: $\{U_C, O_C, \zeta_C, \theta, T_s^\delta(\theta), h(\cdot), T^\delta(\cdot)(\theta), Rep(\cdot)\}$.

4.3. Login Stage

The C and their SC carry out the following steps:

- Step 1. The C enters his/her id_C and pw_C into the terminal contraption before allowing a scan to obtain his/her biometrics BIO'_C . In addition, the C must use the terminal card reader to input his/her SC .
- Step 2. The SC calculates $\zeta_C = Rep(BIO'_C, \zeta_C)$, $\eta_C = h(id_C, pw_C, \zeta_C)$, $Y_C = U_C \oplus \eta_C$, and $h(id_C, \eta_C, Y_C)$. If $h(id_C, pw_C, \zeta_C) \neq O_C$, the SC exits this stage, and the C 's login request is rejected. Otherwise, the next phase is carried out by both the C and the RS .

4.4. Authentication and Key Formation Stage

After a registered user successfully signs in, the authentication of a remote server is confirmed. The session key S_{C_r} is recognized among the C and the RS after the successful mutual authentication. The specific steps are outlined as follows:

- Step 1. The C 's SC picks an arbitrary number $a_C \in F_q$ and computes $\mu_C = T_{a_C}^\delta(\theta)$, $K\mu = T_{a_C}^\delta(T_s^\delta(\theta))$, $Did_C = id_C \oplus h(K\mu)$, and $W_C = h(\mu_C, Y_C)$. The SC uses a public channel to send a request message $\{Did_C, \mu_C, W_C\}$ to the RS .
- Step 2. The RS computes $\mu' = T_s^\delta(\mu_C)$, $id_C = Did_C \oplus h(K\mu')$, $Y_C = h(s, id_C)$, and $W'_C = h(\mu_C, Y_C)$ after receiving the request message $\{Did_C, \mu_C, W_C\}$. If W_C is equal to the computed value W'_C . If the verification fails, the RS immediately rejects this stage. Otherwise, the RS selects an arbitrary number $b_r \in F_q$ and computes $B_r = T_{b_r a_C}^\delta(\theta)$, $K_{C_r} = T_{b_r}^\delta(\theta)$, and $W_r = h(K_{C_r}, Y_C, B_r)$. Over a public channel, the RS sends W_r and B_r to the C .
- Step 3. When the C receives W_r and B_r , it computes $K_{C_r} = T_{a_C}^\delta(B_r) = T_{a_C b_r}^\delta(\theta)$ and $C_C = h(K_{C_r}, Y_C, B_r)$. The C validates the correctness of $\{W_r, B_r\}$ by comparing C_C to W_r . If $C_C \neq W_r$, the C aborts the session; otherwise, it calculates $D_C = h(K_{C_r}, Y_C)$ and transmits the D_C answer message to the RS through a public channel. Then, C calculates the $SK_{C_r} = h(\mu_C, B_r, K_{C_r}, Y_C)$.
- Step 4. When the RS gets D_C from the C 's smart card, it computes $h(K_{C_r}, Y_C)$ and compares D_C to the calculated value. If $h(K_{C_r}, Y_C) = D_C$, the RS calculates the $S_{C_r} = h(\mu_C, B_r, K_{C_r}, Y_C)$. Figure 3 depicts the registration, login, authentication, and key establishment processes.

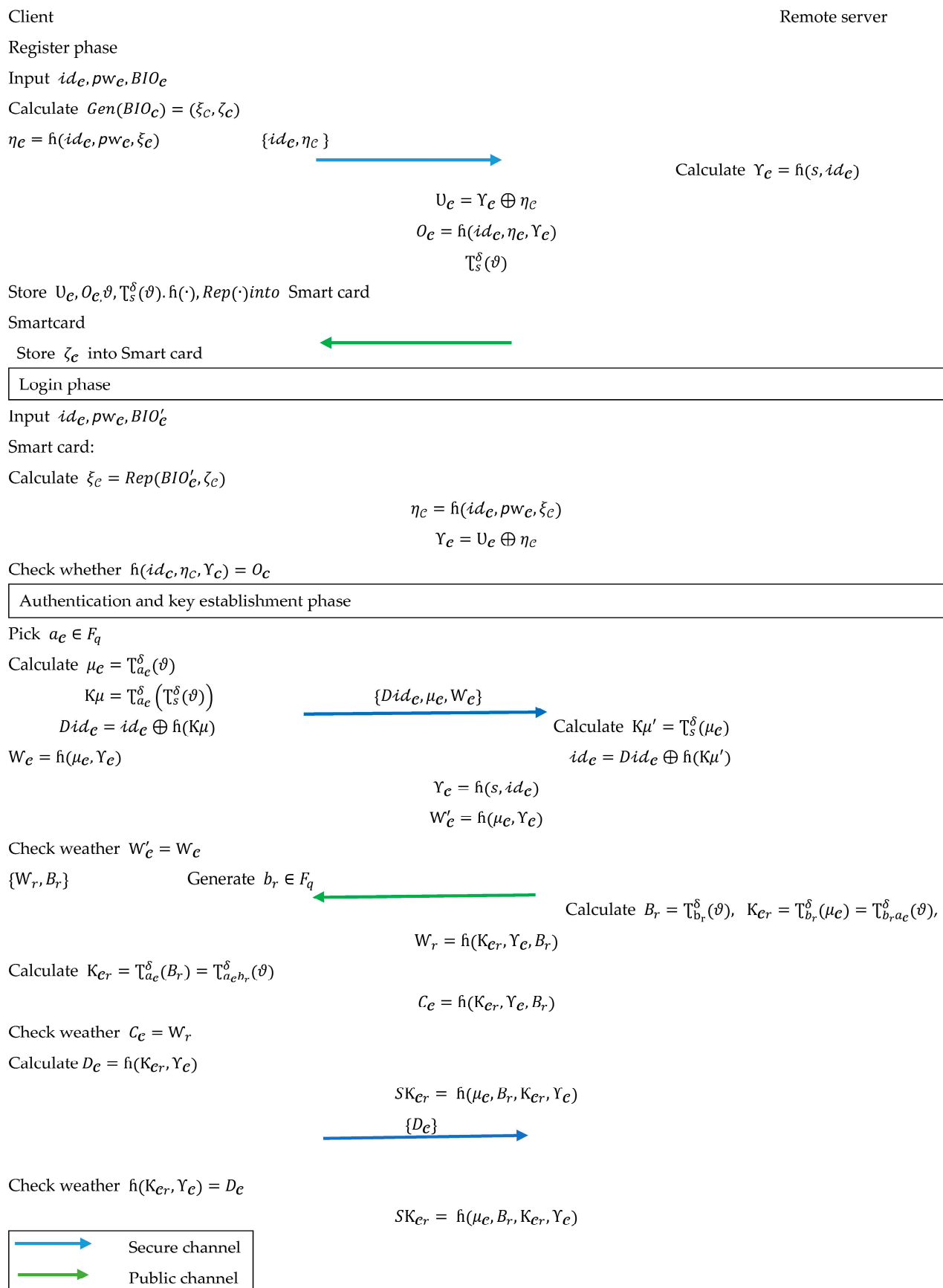


Figure 3. The registration, login, authentication, and key formation stages of the projected protocol.

4.5. Password and Biometrics Change Stage

The C can update her/his existing pw_C and BIO'_C without involving the \mathcal{RS} during this step, as indicated below:

- Step 1. The C inserts the SC into the card reader and enters the credentials id_C and pw_C . Then, the C uses a biometric scanner gadget to scan her/his biometrics BIO'_C .
- Step 2. The smart card calculates $\xi_C = Rep(BIO'_C, \zeta_C)$, $\eta_C = h(id_C, pw_C, \xi_C, Y_C) = U_C \oplus \eta_C$, and $h(id_C, \eta_C, Y_C)$. Then, the smart card checks to see if the calculated $h(id_C, \eta_C, Y_C)$ is similar to O_C . If the conditions are met, the C can change the existing pw_C and BIO'_C . Otherwise, the request can be denied.
- Step 3. The C updates the smart card with a new password \overline{pw}_C and biometrics \overline{BIO}_C . Then, the smart card computes $\bar{\xi}_C = Rep(\overline{BIO}_C, \zeta_C)$, as well as $\bar{\eta}_C = h(id_C, \overline{pw}_C, \bar{\xi}_C, Y_C)$, $\bar{U}_C = Y_C \oplus \bar{\eta}_C$, and $\bar{O}_C = h(id_C, \bar{\eta}_C, Y_C)$. The smart card replaces the tuple $\{U_C, O_C, \zeta_C, \theta, T_s^\delta(\theta), h(\cdot), T^\delta(\cdot)(\theta), Rep(\cdot)\}$ with the new tuple $\{\bar{U}_C, \bar{O}_C, \zeta_C, \theta, T_s^\delta(\theta), h(\cdot), T^\delta(\cdot)(\theta), Rep(\cdot)\}$.

5. Security Examination of the Proposed Protocol

We examine the introduced protocol from the standpoint of security analysis in this section, employing all available analyses. The session key's formal security is demonstrated using the widely established ROR model [50], and other known attacks are evaluated using informal (non-mathematical) security analysis.

5.1. The ROR Model for Session Key Security

In order to investigate the security of a session key, the ROR model [50] is extensively used in authentication based on key agreement techniques [51–57]. In order to prove the security of the session key, the introduced protocol also employs the ROR model.

Bellare et al. [58] introduced the security mechanism for the password-based authenticated key exchange procedure. By introducing a few new oracles to Abdalla et al.'s ROR model [50], we made it a three-factor model. The following are the definitions of the terms:

a. Participants

Let P stand for the proposed scheme. P polynomial times can be executed by both a genuine user C and a \mathcal{RS} . The symbols C_i and \mathcal{RS}_j denote the place of the C and the \mathcal{RS} , respectively.

b. Partnering

In practice, each key agreement conversation has its session identification (*sid*). If C_i and \mathcal{RS}_j have the same non-null session identifiers, we call them partnered.

c. Adversary

The widely established Dolev–Yao (DY) threat model [59] is used to model an adversary \mathcal{F} in the ROR model. \mathcal{F} can interrupt, remove, modify, or even insert some or all messages transmitted among the C_i and \mathcal{RS}_j communication participants using the following queries, according to the DY model:

Execute $\{C_i, \mathcal{RS}_j\}$: This inquiry simulates an eavesdropping attack and returns to its partner \mathcal{RS}_j a copy of the messages sent by C_i .

Send (C_i/\mathcal{RS}_j) : This inquiry executes an active attack. \mathcal{F} can transmit this inquiry to a participant instance C_i/\mathcal{RS}_j via message m . Then, they will respond to the \mathcal{F} with an analogous reply message.

Corrupt (C_i, z) : It represents the loss of C_i 's info. There are three available cases:

- $z = 0$: pw_C is obtained by \mathcal{F} via the query.
- $z = 1$: The query allows \mathcal{F} to obtain data from C_i 's Smart card.
- $z = 2$: Through the query, \mathcal{F} obtains C_i 's biometrics ξ_C .

This inquiry is depicted as an active attack in which \mathcal{F} can extract all of the sensitive secret info contained in its memory by using power analysis attacks.

Test (C_i, \mathcal{RS}_j): In the test inquiry, the session key's semantic security is emulated. In order to respond to the inquiry, the test oracle invokes *execute* (C_i, \mathcal{RS}_j) and flips a fair arbitrary coin $b \in \{0, 1\}$. If $b = 0$, the test oracle sends to the adversary \mathfrak{F} the yield of *execute* (C_i, \mathcal{RS}_j) and the session key S_{C_r} . If $b = 1$, the test oracle sends to the adversary \mathfrak{F} the yield of *execute* (C_i, \mathcal{RS}_j) and an arbitrary binary string. The random binary string must be a similar length as the session key in this scenario. If adversary \mathfrak{F} asks many test questions, all of the answers should depend on the same b value.

Hash ($\alpha, \mathfrak{h}(\alpha)$): When a query is issued to the hash oracle, it examines its table for x and proceeds $\mathfrak{h}(\alpha)$ if α exists; otherwise, it proceeds to a uniformly arbitrary string β and stores $\{\alpha, \beta\}$, in the table.

d. Semantic Security

If the above-noted inquiries are provided, the \mathfrak{F} may communicate with the situations to assist him/her in determining the value of bit b . If they guess properly, the strategy does not give semantic security. Let b' be \mathfrak{F} 's guessed bit. Then, a polynomial-time t , the \mathfrak{F} 's advantage in breaching the proposed scheme's session key security P , is defined as $Adv_{A, succ}^P(t) = |2Pr[b = b'] - 1|$, where $Pr[E]$ indicates the probability of an event E occurring.

5.2. The Proof of Security

Theorem 1. Let $Adv_{\mathfrak{F}, succ}^P(t)$ be the advantage that a \mathfrak{F} adversary with execution time t violates the semantic security of our projected protocol P . Then,

$$Adv_{\mathfrak{F}, succ}^P(t) \leq 2 \left(\frac{Q_h^2}{2^{\downarrow_h-1}} + \frac{Q_s}{2^{\downarrow_h-3}} + \frac{(Q_s + Q_e)^2}{2^{\downarrow_t-1}} + \frac{Q_h}{2q} + Q_h Adv_{\mathfrak{F}}^{FCMDHP}(t) + \max \left\{ \frac{Q_s}{|\mathfrak{X}|}, \frac{Q_s}{2^{\downarrow_b}}, Q_s \epsilon_{bm} \right\} \right)$$

where Q_e , Q_s , and Q_h represent the number of execute, send and hash queries, respectively. $|\mathfrak{X}|$, \downarrow_t , \downarrow_h , ϵ_{bm} , and \downarrow_b represent the size of the homogeneously distributed password dictionary \mathfrak{X} , the string length of the result of the Chebyshev polynomial, the string length of hash results, the probability of false positive, and the extracted string length of user biometrics, respectively. The advantage of \mathfrak{F} in breaching the FCMDHP with the t execution time is indicated by $Adv_{\mathfrak{F}}^{FCMDHP}(t)$.

Proof: Our proof establishes a series of hybrid games, beginning with the actual attack and ending with a game in which \mathfrak{F} has no advantage. S_i is an occurrence in which \mathfrak{F} has a chance to win the game G_i . Below is a detailed portrayal of the games. \square

Game G_0 : This game simulates an actual attack by \mathfrak{F} . We have, according to the preliminary definitions given by Equation (3),

$$Adv_{\mathfrak{F}, succ}^P(t) = |2Pr[S_0] - 1| \quad (3)$$

Game G_1 : The only difference between this game and the previous one is that \mathfrak{F} replicates the hash oracle \mathfrak{h} by keeping a list Y_h . If there is a record (α, β) in Y_h for a hash query $\mathfrak{h}(\alpha)$, the oracle proceeds β to the \mathfrak{F} . Otherwise, the oracle selects an arbitrary number β , proceeds to the \mathfrak{F} , and inserts the record (α, β) to Y_h . This accomplishment of the corrupt, send, execute, and test inquiries are similar to the execution of the actual attack. Thus, we have Equation (4):

$$Pr[S_1] = Pr[S_0] \quad (4)$$

Game G_2 : We simulate all inquiries in this game in the same way that we did in G_1 , except that we halt all simulations when a collision ensues in the documents $\{Di, d_C, \mu_C, W_C\}$, $\{W_r, B_r\}$, and $\{D_C\}$. The \mathfrak{h} oracles may clash with distinct input values if μ_C and B_r are the same locations in multiple documents. We stop the game if any of the above scenarios appear. The probability of collision in the oracle output is, at most, $Q_h^2/2^{l_h+1}$, according to the birthday paradox. In the documents simulation, the chance of

collisions is limited to $(Q_e + Q_s)^2 / 2^{l_t+1}$, because μ_C and B_r were arbitrarily selected from a uniform distribution F_q^* . As a result, (5):

$$|Pr[S_2] - Pr[S_1]| \leq \frac{Q_h^2}{2^{\ell_h+1}} + \frac{(Q_s + Q_e)^2}{2^{\ell_t+1}} \quad (5)$$

Game G_3 : We abort the executions in this game if the adversary \mathfrak{F} guesses the authentication values W_C, W_r , and D_C by chance (that is, without having to use the hash inquiry h). Except that the \mathcal{RS} (or the \mathcal{C}) discards a legal authentication assessment, there is no difference between G_3 and G_2 . Thus, we have Equation (6):

$$|Pr[S_3] - Pr[S_2]| \leq \frac{Q_s}{2^{\ell_h}} \quad (6)$$

Game G_4 : The adversary's situation is avoided in this game. \mathfrak{F} predicts the authentication value Y_C directly and correctly. At most, the probability is $Q_s / 2^{\ell_h}$. We arrive at Equation (7):

$$|Pr[S_4] - Pr[S_3]| \leq \frac{Q_s}{2^{\ell_h}} \quad (7)$$

Game G_5 : In this game, we try to prevent adversary \mathfrak{F} from using corrupt (C_i, z) to compute the authentication value Y_C . According to the premise, oracle corrupt (C_i, z) can only provide \mathfrak{F} with two factors. If \mathfrak{F} only has BIO_C and pw_C , she/he will be unable to find the session key. As a result, corrupt $(C_i, 1)$ is required for \mathfrak{F} , and we assume \mathfrak{F} has asked about it. The analysis that follows is split into two parts.

Case Assume \mathfrak{F} sends a query to corrupt $(C_i, 1)$ to guess the real password. The probability 1: is $Q_s / |x|$ because there are Q_s chances to send inquiries and $|x|$ passwords.

Case Assume \mathfrak{F} inquiries corrupt $(C_i, 0)$ to crack BIO_C . There are two subcases to consider:

- 2: (a) Within Q_s , \mathfrak{F} guesses BIO_C . Send queries. $Q_s / 2^{\ell_b}$ is the probability.
- (b) \mathfrak{F} tries the event of "false positive" with send inquiries using her/his biometrics. $Q_{s\epsilon_{bm}}$ is the probability.

In this game, adversary \mathfrak{F} can choose between Cases 1 and 2. The games G_5 and G_4 are indistinguishable without these guessing attacks, and therefore, we have Equation (8):

$$|Pr[S_5] - Pr[S_4]| \leq \max \left\{ \frac{Q_s}{|x|}, \frac{Q_s}{2^{\ell_b}}, Q_{s\epsilon_{bm}} \right\} \quad (8)$$

Game G_6 : In this game, instead of using the h , we include and use the private h' oracle to calculate the S_{C_r} . The adversary is unaware of h' because he/she is a private oracle. $Pr[S_6] = 1/2$ is the value we have. Except that the \mathfrak{F} makes a hash inquiry $h(\mu_C, B_r, K_{C_r}, Y_C)$, the games G_6 and G_5 are indistinguishable. We call this event $Query_{in-6}$. Therefore, we have Equation (9):

$$|Pr[S_6] - Pr[S_5]| \leq Pr[Query_{in-6}] \quad (9)$$

Game G_7 : In this game, we simulate FCMDHP's random self-reducibility. To build the session key K_{C_r} , hash entries with two chaotic map variables $\mu_C = T_{a_c}^\delta(\theta)$ and $B_r = T_{b_r}^\delta(\theta)$ are utilized. This game executes Y_C without running the h oracle or possessing the s or $i d_C$. As a result, the probability in this case is $Q_h Adv_A^{FCMDHP}(t) + Q_h/q$. As a result, we obtain Equation (10):

$$Pr[Query_{in-6}] \leq Q_h Adv_{\mathfrak{F}}^{FCMDHP}(t) + \frac{Q_h}{q} \quad (10)$$

As a result, we manipulated Equations (3)–(10) to give the following inequality:

$$Adv_{\mathfrak{F},succ}^P(\mathfrak{h}) \leq 2 \left(\frac{Q_{\mathfrak{h}}^2}{2^{\ell_{\mathfrak{h}}-1}} + \frac{Q_s}{2^{\ell_{\mathfrak{h}}-3}} + \frac{(Q_s + Q_e)^2}{2^{\ell_{\mathfrak{h}}-1}} + \frac{Q_{\mathfrak{h}}}{2q} + Q_{\mathfrak{h}} Adv_{\mathfrak{F}}^{ECMDHP}(\epsilon) + \max \left\{ \frac{Q_s}{|\mathfrak{X}|}, \frac{Q_s}{2^{\ell_b}}, Q_{s \in bm} \right\} \right)$$

5.3. Informal Security Examination and Discussion

In this area, we address the security of the presented protocol informally (non-mathematically) in terms of existing known attacks and some of the proposed protocol's core functionality characteristics.

5.3.1. User Anonymity

Due to privacy considerations, user anonymity becomes a major worry for authentication schemes. It stipulates that no one can reveal the user's true identity without the remote server's private key. Our technique ensures user anonymity because \mathfrak{F} cannot find $id_{\mathcal{C}}$ from any attacker login or authentication communication. In our design, the \mathcal{C} never conveys the $id_{\mathcal{C}}$ to the \mathcal{RS} over a public channel. Only $Did_{\mathcal{C}}$ and $Did_{\mathcal{C}} = id_{\mathcal{C}} \oplus \mathfrak{h}(\mathcal{T}_{a_{\mathcal{C}}}^{\delta}(\mathcal{T}_s^{\delta}(\theta)))$ are sent by the \mathcal{C} , and $id_{\mathcal{C}}$ is protected by the arbitrary number $a_{\mathcal{C}}$. As a result of $a_{\mathcal{C}}$, the \mathfrak{F} is unable to extract it from $Did_{\mathcal{C}}$. As a result, our proposed scheme protects user privacy.

5.3.2. User Untraceability

User untraceability specifies that no two messages from the same session will be identical. If it is, \mathfrak{F} will have little trouble tracing the \mathcal{C} . We suppose that the \mathfrak{F} catches two request messages, $\{Did_{\mathcal{C}}, \mu_{\mathcal{C}}, W_{\mathcal{C}}\}$ and $\{Did_{\mathcal{C}}^*, \mu_{\mathcal{C}}^*, W_{\mathcal{C}}^*\}$, which are created by the \mathcal{C} in two sessions, where $\mu_{\mathcal{C}} = \mathcal{T}_{a_{\mathcal{C}}}^{\delta}(\theta), K\mu = \mathcal{T}_{a_{\mathcal{C}}}^{\delta}(\mathcal{T}_s^{\delta}(\theta))$, $Did_{\mathcal{C}} = id_{\mathcal{C}} \oplus \mathfrak{h}(K\mu)$, $W_{\mathcal{C}} = \mathfrak{h}(\mu_{\mathcal{C}}, Y_{\mathcal{C}})$ and $\mu_{\mathcal{C}}^* = \mathcal{T}_{a_{\mathcal{C}}^*}^{\delta}(\theta), K\mu^* = \mathcal{T}_{a_{\mathcal{C}}^*}^{\delta}(\mathcal{T}_s^{\delta}(\theta))$, $Did_{\mathcal{C}}^* = id_{\mathcal{C}} \oplus \mathfrak{h}(K\mu^*)$, $W_{\mathcal{C}}^* = \mathfrak{h}(\mu_{\mathcal{C}}^*, Y_{\mathcal{C}})$. The messages $\{Did_{\mathcal{C}}, \mu_{\mathcal{C}}, W_{\mathcal{C}}\}$ and $\{Did_{\mathcal{C}}^*, \mu_{\mathcal{C}}^*, W_{\mathcal{C}}^*\}$ are different because of the random numbers $a_{\mathcal{C}}$ and $a_{\mathcal{C}}^*$. As a result, \mathfrak{F} will be unable to discover the relationship between $\{Did_{\mathcal{C}}, \mu_{\mathcal{C}}, W_{\mathcal{C}}\}$ and $\{Did_{\mathcal{C}}^*, \mu_{\mathcal{C}}^*, W_{\mathcal{C}}^*\}$. As a result, our suggested approach provides high user anonymity.

5.3.3. Impersonation Attack

The attacker \mathfrak{F} attempts to mimic either the \mathcal{C} or the \mathcal{RS} , or both, in this attack. If \mathfrak{F} achieves some sort of success, the system will not provide strong security. As a result, the \mathfrak{F} cannot imitate any of the \mathcal{C} or the \mathcal{RS} because the message $\{Did_{\mathcal{C}}, \mu_{\mathcal{C}}, W_{\mathcal{C}}\}$, $\{W_r, B_r\}$, and $\{D_{\mathcal{C}}\}$ cannot be fabricated by the \mathfrak{F} . If \mathfrak{F} intends to impersonate the user, she/he must first construct an arbitrary number in order to calculate a request message. $Did_{\mathcal{C}} = id_{\mathcal{C}} \oplus \mathfrak{h}(K\mu)$ and $W_{\mathcal{C}} = \mathfrak{h}(\mu_{\mathcal{C}}, Y_{\mathcal{C}})$ may be computed by the \mathfrak{F} . With a legitimate request message, to impersonate the user, the \mathfrak{F} must know the assessment of $Y_{\mathcal{C}} = \mathfrak{h}(s, id_{\mathcal{C}})$ and $id_{\mathcal{C}}$, that is, the \mathfrak{F} must know the s and $id_{\mathcal{C}}$. Authentication will fail if this is not done. Similarly, the \mathfrak{F} cannot deceive the user and the remote server by forging the messages $\{W_r, B_r\}$, and $\{D_{\mathcal{C}}\}$. As a result, under our suggested approach, impersonating the \mathcal{C} and the \mathcal{RS} is not possible.

5.3.4. Offline Password Guessing Attack

Assume you have a competitor. \mathfrak{F} obtains all of the recorded information $\{U_{\mathcal{C}}, O_{\mathcal{C}}, \zeta_{\mathcal{C}}, \theta, \mathcal{T}_s^{\delta}(\theta), \mathfrak{h}(\cdot), \mathcal{T}_{(\cdot)}^{\delta}(\theta), Rep(\cdot)\}$ from the memory of a stolen or lost SC of a legitimate user \mathcal{C} employing power analysis attacks. To properly guess $pw_{\mathcal{C}}$ from $U_{\mathcal{C}} = Y_{\mathcal{C}} \oplus \eta_{\mathcal{C}} = \mathfrak{h}(s, id_{\mathcal{C}}) \oplus \mathfrak{h}(id_{\mathcal{C}}, pw_{\mathcal{C}}, \theta_{\mathcal{C}})$, \mathfrak{F} must be aware of \mathcal{RS} 's private key s , as well as \mathcal{C} 's biometrics $\theta_{\mathcal{C}}$ and $id_{\mathcal{C}}$. In addition, knowledge of $\theta_{\mathcal{C}}$, $id_{\mathcal{C}}$, and s is required to accurately guess $pw_{\mathcal{C}}$ from $O_{\mathcal{C}} = \mathfrak{h}(id_{\mathcal{C}}, \mathfrak{h}(id_{\mathcal{C}}, pw_{\mathcal{C}}, \theta_{\mathcal{C}}), \mathfrak{h}(s, id_{\mathcal{C}}))$. However, only \mathcal{C}_i can supply its $\theta_{\mathcal{C}}$, only the \mathcal{C} and \mathcal{RS} involved in the authentication procedure are aware of the $id_{\mathcal{C}}$, and only \mathcal{RS} is aware of its secret key s . As a result, our technique is resistant to offline password-guessing attacks.

5.3.5. Known Key Secrecy

Even if a specific session key in the proposed technique is compromised, \mathfrak{F} will not be able to discover the other session keys. $S_{C_r} = \mathfrak{h}(\mu_C, B_r, K_{C_r}, Y_C)$, where $K_{C_r} = \mathcal{T}_{b_r a_C}^\delta(\theta)$ is how our technique computes the session key. a_C and b_r are generated at random and only once for each new session. As a result, in order to calculate future session keys, an attacker cannot extract any personal info from an obtained session key.

5.3.6. Temporary Information Attack on Known Sessions

In the projected system, the C and the RS estimate a mutual session key in each session as $S_{C_r} = \mathfrak{h}(\mu_C, B_r, K_{C_r}, Y_C)$. The secrecy of S_{C_r} is determined by the parameters $K_{C_r} = \mathcal{T}_{b_r a_C}^\delta(\theta)$ and $Y_C = \mathfrak{h}(s, id_C)$. The temporary secrets a_C and b_r are assumed to be known by \mathfrak{F} . By using this information, on the one hand, the \mathfrak{F} may compute $K_{C_r} = \mathcal{T}_{b_r a_C}^\delta(\theta)$. The \mathfrak{F} , on the other hand, cannot compute $Y_C = \mathfrak{h}(s, id_C)$ without being aware of the RS 's private key s and the C 's identification id_C . As a result, the \mathfrak{F} cannot compute $S_{C_r} = \mathfrak{h}(\mu_C, B_r, K_{C_r}, Y_C)$; thus, our suggested strategy is resistant to this type of attack.

5.3.7. Privileged-Insider Attack

The C selects an id_C and a pw_C during the user registration process. Then, they compute $Gen(BIO_C) = (\xi_C, \zeta_C)$ and $\eta_C = \mathfrak{h}(id_C, pw_C, \xi_C)$, and sends $\{id_C, \eta_C\}$ to the RS through a secure channel. Nevertheless, due to the one-way of $\mathfrak{h}(\cdot)$, an insider client of the RS who is an adversary is unable to extract pw_C and BIO_C from $\{id_C, \eta_C\}$. As a result, our suggested solution resolves the problem caused by the privileged-insider attack.

5.3.8. Password and Biometrics Change Attack

The SC of an approved registered user C first authenticates the user by computing $\xi_C = Rep(BIO'_C, \zeta_C)$, $Y_C = U_C \oplus \eta_C$ and, $\eta_C = \mathfrak{h}(id_C, pw_C, \xi_C)$, and then validating the condition $\mathfrak{h}(id_C, \eta_C, Y_C) = O_C$ based on the user's initiated identity id_C , pw_C , and BIO'_C . The SC will allow you to alter your password and biometrics if this condition is met. As a result, updating the password and biometrics of C without knowing the private integrity id_C, pw_C, BIO'_C is a computationally infeasible assignment for \mathfrak{F} . As a result, the presented protocol protects against password and biometrics change attacks.

5.3.9. Efficient Password and Biometrics Change

Through the password and biometrics change stage of the presented technique, a legitimately registered user C inserts her/his identification, biometrics, and current password into her/his smart card to update the recent password and biometrics. The C can update the password and biometrics if all of the secret integrity entered are correct. The password and biometrics are then updated locally in the smart card's memory, bypassing the remote server RS . As a result, the stage of changing passwords and biometrics goes smoothly.

5.3.10. Three-Factor Confidentiality

Three-factor confidentiality means that even if one or both authentication parameters are exposed, the adversary will not impersonate the user successfully. In the following three cases, we demonstrate that our technique ensures three-factor confidentiality:

- If the user's smart card and biometrics are revealed, the adversary \mathfrak{F} attempts to crack the password. On the one hand, the parameters $\{U_C, O_C, \zeta_C, \theta, \mathcal{T}_s^\delta(\theta), \mathfrak{h}(\cdot), \mathcal{T}_{(\cdot)}^\delta(\theta), Rep(\cdot)\}$ and ξ_C are obtained by the \mathfrak{F} , where $U_C = Y_C \oplus \eta_C$, and $O_C = \mathfrak{h}(id_C, \eta_C, Y_C)$. The \mathfrak{F} , on the other hand, is unable to reveal pw_C because $Y_C = \mathfrak{h}(s, id_C)$, where s is known only to the RS and id_C is known only to the user.
- If the user's smart card and password are revealed, on the one hand, the \mathfrak{F} obtains the parameters $\{U_C, O_C, \zeta_C, \theta, \mathcal{T}_s^\delta(\theta), \mathfrak{h}(\cdot), \mathcal{T}_{(\cdot)}^\delta(\theta), Rep(\cdot)\}$, and pw_C , where $U_C = Y_C \oplus \eta_C$ and

$O_C = h(i\mathcal{d}_C, \eta_C, Y_C)$. The \mathfrak{F} , on the other hand, is unable to deduce ξ_C from O_C and U_C because it must simultaneously guess correct $i\mathcal{d}_C$, ξ_C , and s .

- The \mathfrak{F} tries to crack the smart card's specifications if the biometrics and password are disclosed. Because Y_C is unavailable, retrieving the critical factor O_C is impossible.

5.3.11. Clock Synchronization Issue

Unlike many previous SIPs, the presented SIP might work even if the clock is out of sync, providing adequate communication between the recipient and the sender. Since the timestamp is merely relevant to the receiver's clock, synchronized clocks are not necessary. He/she only verifies the timestamp generated by the recipient.

6. Performance Evaluation

In this segment, we compare the proposed protocol's communication, computation, and smart card storage costs to those of other relevant SIPs, such as [3,6,13,18,19,35]. We state that the presented SIP involves two major stages: login/authentication and the key establishment, which must be completed each time the system is accessed. As a result, we simply look at the phases of login/ authentication and the key establishment in this segment. All of the comparisons are described in detail below.

6.1. Computation Cost Analysis

The notations used for comparison estimations are listed in Table 2. We signify certain notations and their implementation times on an Intel Pentium 4 2600 MHz processor with 1024 MB RAM, as conducted in [3], and given in Table 3. To estimate the effectiveness of the presented SIP and compare it to earlier SIPs, we ignore the bitwise XOR operation because it is insignificant.

Table 2. Syntaxes for making comparative estimates.

Syntaxes	Description
t_{hash}	The execution time of the hash function
t_{sym}	The execution time of symmetric key decryption/encryption
t_{mul}	The execution time of ellipse curve point multiplication
t_{chos}	The execution time of the Chebyshev map operation
t_{fchos}	The execution time of fractional Chebyshev map operation
t_{fuzzy}	The execution time of fuzzy extractor operation

Table 3. The computation costs comparison.

Protocols	Computational Cost	Running Time (In Milliseconds)
[6]	$7t_{mul} + 8t_{hash}$	445.6
[13]	$4(t_{mul} + 2t_{hash})$	256.4
[18]	$2(3t_{mul} + 5t_{hash})$	383.5
[19]	$7t_{mul} + 10t_{hash}$	446.6
[35]	$4t_{mul} + 10t_{hash} + 2t_{sym} + t_{fuzzy}$	337.8
[3]	$6t_{chos} + 9t_{hash} + t_{fuzzy}$	193.7
Proposed SIP	$6t_{fchos} + 9t_{hash} + t_{fuzzy}$	126.5

According to [3], the execution time for t_{hash} , t_{sym} , t_{mul} , t_{chos} , t_{fuzzy} , and t_{fchos} for $\delta = 0.75$ [45] are given by 0.5 ms, 8.7 ms, 63.08 ms, 63.08 ms, and 9.82 ms, respectively. We compare the computational cost of the presented protocol with the other associated SIPs [3,6,13,18,19,35]. Table 3 shows the comparison of computational cost results. These findings indicate that the presented protocol is more efficient than other SIP schemes.

6.2. Communication Cost and Smart Card Storage Assessment

In this subsection, we compare our proposed SIP to comparable SIPs in terms of smart card storage and communication costs. The SHA-1 hash function is used, and its output length is 160 bits. The identity/password/arbitrary number is 64 bits long. The output of the Chebyshev chaotic map (CCM) is 128 bits long. The function $Gen(\cdot)$ returns a tuple with 80 bits for each component. The smart card in our proposed SIP holds $\langle U_C, O_C, \zeta_C, T_s^\delta(\theta) \rangle$, and the storage cost is $2 \times 160 + 128 + 80 = 528$ bits. As a result, our proposed SIP significantly reduces smart card storage capacity. In our login, authentication and key formation process, the C first sends $Di d_C, \mu_C$, and W_C to the RS at a cost of $2 \times 160 + 128 = 448$ bits. Then, the RS sends W_r and B_r to the C at a cost of $128 + 160 = 288$ bits. Lastly, the C transmits D_C to the RS at a cost of 160 bits. As a result, the overall cost of communication is $448 + 288 + 160 = 896$ bits. We also compute the costs of communication and smart card storage [3,6,13,18,19,35], as shown in Figure 4.

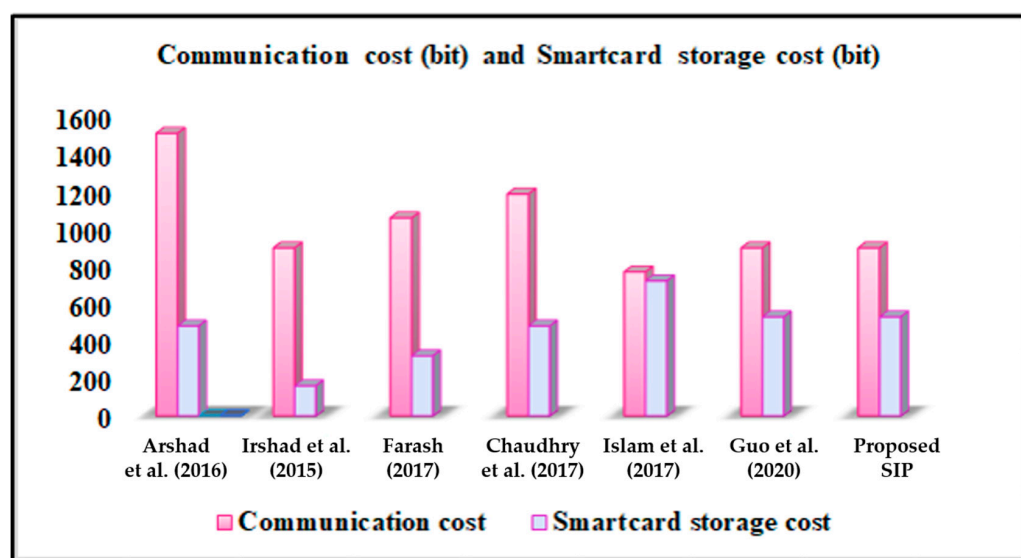


Figure 4. A comparison of the costs of communication and smart card storage.

6.3. Analysis of Security and Functionality

Table 4 provides a full comparison of various security attacks and functionality aspects. As shown in Table 4, our suggested SIP solves the security and functionality flaws prevalent in existing SIPs. Among the contenders, the work in [3] appears to show related results to the results of the current study. However, the work in [3] failed the clock synchronization attack, whereas our presented scheme successfully resolved the clock synchronization problem. Regarding running costs, our scheme also shows favorable costs compared to the scheme reported in [3], as shown in Table 4.

Table 4. Comparison of security and functionality attributes.

Security Features	[6]	[13]	[18]	[19]	[35]	[3]	Proposed SIP
SF_1	☒	☒	☑	☑	☑	☑	☑
SF_2	☑	☑	☑	☑	☒	☑	☑
SF_3	☑	☒	☒	☒	☑	☑	☑
SF_4	☑	☑	☑	☑	☑	☑	☑
SF_5	☒	☑	☑	☑	☒	☑	☑
SF_6	☒	☒	☒	☑	☒	☑	☑
SF_7	☑	☑	☑	☒	☑	☑	☑
SF_8	☑	☑	☒	☒	☑	☑	☑
SF_9	☒	☒	☒	☑	☑	☑	☑
SF_{10}	☒	☒	☑	☑	☑	☑	☑
SF_{11}	☒	☒	☒	☒	☒	☒	☑

SF_1 , stolen smart card attack; SF_2 , offline password guessing attack; SF_3 , strong replay attack; SF_4 , privileged insider attack; SF_5 , impersonation attack; SF_6 , user anonymity provision; SF_7 , efficient password change; SF_8 , login phase efficiency; SF_9 , mutual authentication; SF_{10} , stolen smart card attack; SF_{11} , clock synchronization problem. Note: ☑: Secure; ☒: Vulnerable.

7. Conclusions

In this paper, we proposed a lightweight, provably, protected three-factor session initiation protocol in human-centered IoT. We used the ROR model for formal security analysis, and the results indicated that our proposed SIP provides session key security. Additionally, we performed an informal security analysis to demonstrate that our proposed SIP could withstand various existing attacks. Based on the FCCM-CDH problem's hardness assumption, the proposed SIP is provably secure. Lastly, through a rigorous performance assessment, we showed that it significantly decreased total computing time, smart card storage, and communication costs compared to other associated protocols. Future studies will analyze the presented protocol in a simulated and real-world context to further investigate the performance characteristics. In addition, the projected technique would be tested using Bergamo's and other security attacks to demonstrate its efficacy.

Author Contributions: C.M. and C.-C.L. were responsible for the conceptualization of the topic; article gathering and sorting were carried out by C.M., C.-C.L. and A.L.I.; manuscript writing and original drafting and formal analysis were carried out by C.M., C.-C.L., I.B. and A.L.I.; writing of reviews and editing were carried out by C.M., C.-C.L., I.B. and A.L.I.; C.M. led the overall research activity. All authors have read and agreed to the published version of the manuscript.

Funding: The work of Agbotiname Lucky Imoize is supported by the Nigerian Petroleum Technology Development Fund (PTDF), the German Academic Exchange Service (DAAD), through the Nigerian-German Postgraduate Program under grant 57473408. This work was supported, in part, by the Ministry of Science and Technology (MOST), Taiwan, R.O.C., under contract no. MOST 110-2410-H-030-032.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data that support the findings of this paper are available from the corresponding author upon reasonable request.

Acknowledgments: The authors would like to thank anonymous reviewers of the *Mathematics* MDPI Journal for their careful and helpful comments.

Conflicts of Interest: The authors declare no conflict of interest related to this work.

References

1. Yeh, H.-L.; Chen, T.-H.; Shih, W.-K. Robust smart card secured authentication scheme on SIP using elliptic curve cryptography. *Comput. Stand. Interfaces* **2014**, *36*, 397–402. [\[CrossRef\]](#)
2. He, D.; Chen, J.; Chen, Y. A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography. *Secur. Commun. Netw.* **2012**, *5*, 1423–1429. [\[CrossRef\]](#)
3. Guo, X.Y.; Sun, D.Z.; Yang, Y. An Improved Three-Factor Session Initiation Protocol Using Chebyshev Chaotic Map. *IEEE Access* **2020**, *8*, 111265–111277. [\[CrossRef\]](#)
4. Yoon, E.-J.; Shin, Y.-N.; Jeon, I.-S.; Yoo, K.-Y. Robust mutual authentication with a key agreement scheme for the session initiation protocol. *IETE Tech. Rev.* **2010**, *27*, 203–213. [\[CrossRef\]](#)
5. Kilinc, H.H.; Yanik, T. A survey of SIP authentication and key agreement schemes. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 1005–1023. [\[CrossRef\]](#)
6. Arshad, H.; Nikooghdam, M. An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC. *Multimed. Tools Appl.* **2016**, *75*, 181–197. [\[CrossRef\]](#)
7. Febro, A.; Xiao, H.; Spring, J.; Christianson, B. Edge security for SIP-enabled IoT devices with P4. *Comput. Netw.* **2022**, *203*, 108698. [\[CrossRef\]](#)
8. Xie, Q.; Tang, Z. Biometrics based authentication scheme for session initiation protocol. *Springerplus* **2016**, *5*, 1–14. [\[CrossRef\]](#)
9. Arshad, R.; Ikram, N. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. *Multimed. Tools Appl.* **2013**, *66*, 165–178. [\[CrossRef\]](#)
10. Tang, H.; Liu, X. Cryptanalysis of Arshad et al.'s ECC-based mutual authentication scheme for session initiation protocol. *Multimed. Tools Appl.* **2013**, *65*, 321–333. [\[CrossRef\]](#)
11. Irshad, A.; Sher, M.; Faisal, M.S.; Ghani, A.; Ul Hassan, M.; Ashraf, C.S. A secure authentication scheme for session initiation protocol by using ECC on the basis of the Tang and Liu scheme. *Secur. Commun. Netw.* **2014**, *7*, 1210–1218. [\[CrossRef\]](#)
12. Zhang, L.; Tang, S.; Cai, Z. Efficient and flexible password authenticated key agreement for voice over internet protocol session initiation protocol using smart card. *Int. J. Commun. Syst.* **2014**, *27*, 2691–2702. [\[CrossRef\]](#)
13. Irshad, A.; Sher, M.; Rehman, E.; Ch, S.A.; Hassan, M.U.; Ghani, A. A single round-trip sip authentication scheme for voice over internet protocol using smart card. *Multimed. Tools Appl.* **2015**, *74*, 3967–3984. [\[CrossRef\]](#)
14. Kumari, S.; Chaudhry, S.A.; Wu, F.; Li, X.; Farash, M.S.; Khan, M.K. An improved smart card based authentication scheme for session initiation protocol. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 92–105. [\[CrossRef\]](#)
15. Farash, M.S. Security analysis and enhancements of an improved authentication for session initiation protocol with provable security. *Peer-to-Peer Netw. Appl.* **2016**, *9*, 82–91. [\[CrossRef\]](#)
16. Naqvi, H.; Chaudhry, S.A.; Mahmood, K. An improved authentication protocol for SIP-based VoIP. In Proceedings of the International Conference on Recent Advances in Computer Systems (RACS 2015), Hail, Saudi Arabia, 30 November–1 December 2015; pp. 7–12.
17. Mishra, D.; Das, A.K.; Mukhopadhyay, S. A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card. *Peer-to-Peer Netw. Appl.* **2016**, *9*, 171–192. [\[CrossRef\]](#)
18. Farash, M.S. An improved password-based authentication scheme for session initiation protocol using smart cards without verification table. *Int. J. Commun. Syst.* **2017**, *30*, e2879. [\[CrossRef\]](#)
19. Chaudhry, S.A.; Naqvi, H.; Sher, M.; Farash, M.S.; Hassan, M.U. An improved and provably secure privacy preserving authentication protocol for SIP. *Peer-to-Peer Netw. Appl.* **2017**, *10*, 1–15. [\[CrossRef\]](#)
20. Islam, S.K.H.; Rajeev, V.; Amin, R. A robust and efficient three-factor authentication and session key agreement mechanism for SIP. In Proceedings of the 2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM), IEEE, Tindivanam, India, 3–4 February 2017; pp. 286–291.
21. Reddy, A.G.; Yoon, E.-J.; Das, A.K.; Yoo, K.-Y. An enhanced anonymous two-factor mutual authentication with key-agreement scheme for session initiation protocol. In Proceedings of the 9th International Conference on Security of Information and Networks, Newark, NJ, USA, 20–22 July 2016; pp. 145–149.
22. Lu, Y.; Li, L.; Peng, H.; Yang, Y. An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography. *Multimed. Tools Appl.* **2017**, *76*, 1801–1815. [\[CrossRef\]](#)
23. Meshram, C.; Imoize, A.L.; Aljaedi, A.; Alharbi, A.R.; Jamal, S.S.; Barve, S.K. A Provably Secure IBE Transformation Model for PKC Using Conformable Chebyshev Chaotic Maps under Human-Centered IoT Environments. *Sensors* **2021**, *21*, 7227. [\[CrossRef\]](#)
24. Meshram, C.; Obaidat, M.S.; Tembhurne, J.V.; Shende, S.W.; Kalare, K.W.; Meshram, S.G. A Lightweight Provably Secure Digital Short-Signature Technique Using Extended Chaotic Maps for Human-Centered IoT Systems. *IEEE Syst. J.* **2020**, *15*, 5507–5515. [\[CrossRef\]](#)
25. Meshram, C.; Imoize, A.L.; Jamal, S.S.; Alharbi, A.R.; Meshram, S.G.; Hussain, I. CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps. *IEEE Access* **2022**, *10*, 39853–39863. [\[CrossRef\]](#)
26. Dharminder, D.; Kumar, U.; Gupta, P. A construction of a conformal Chebyshev chaotic map based authentication protocol for healthcare telemedicine services. *Complex Intell. Syst.* **2021**, *7*, 2531–2542. [\[CrossRef\]](#)
27. Dhillon, P.K.; Kalra, S. Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things. *Multimed. Tools Appl.* **2019**, *78*, 22199–22222. [\[CrossRef\]](#)

28. Farash, M.S.; Kumari, S.; Bakhtiari, M. Cryptanalysis and improvement of a robust smart card secured authentication scheme on SIP using elliptic curve cryptography. *Multimed. Tools Appl.* **2016**, *75*, 4485–4504. [\[CrossRef\]](#)
29. Azrou, M.; Ouanan, M.; Farhaoui, Y. A new secure SIP authentication scheme based on elliptic curve cryptography. In Proceedings of the International Conference on Information Technology and Communication Systems, Churibka, Morocco, 28–29 March 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 155–170.
30. Sureshkumar, V.; Amin, R.; Anitha, R. A robust mutual authentication scheme for session initiation protocol with key establishment. *Peer-to-Peer Netw. Appl.* **2018**, *11*, 900–916. [\[CrossRef\]](#)
31. Nikooghadam, M.; Amintoosi, H. A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol. *Secur. Priv.* **2020**, *3*, e92. [\[CrossRef\]](#)
32. Lin, H.; Wen, F.; Du, C. An anonymous and secure authentication and key agreement scheme for session initiation protocol. *Multimed. Tools Appl.* **2017**, *76*, 2315–2329. [\[CrossRef\]](#)
33. Wu, L.; Zhang, Y.; Wang, F. A new provably secure authentication and key agreement protocol for SIP using ECC. *Comput. Stand. Interfaces* **2009**, *31*, 286–291. [\[CrossRef\]](#)
34. Chen, C.-M.; Xiang, B.; Wang, K.-H.; Yeh, K.-H.; Wu, T.-Y. A robust mutual authentication with a key agreement scheme for session initiation protocol. *Appl. Sci.* **2018**, *8*, 1789. [\[CrossRef\]](#)
35. Islam, S.K.H.; Vijayakumar, P.; Bhuiyan, M.Z.A.; Amin, R.; Balusamy, B. A provably secure three-factor session initiation protocol for multimedia big data communications. *IEEE Internet Things J.* **2017**, *5*, 3408–3418. [\[CrossRef\]](#)
36. Zhang, L.; Tang, S.; Zhu, S. A lightweight privacy preserving authenticated key agreement protocol for SIP-based VoIP. *Peer-to-Peer Netw. Appl.* **2016**, *9*, 108–126. [\[CrossRef\]](#)
37. Tu, H.; Kumar, N.; Chilamkurti, N.; Rho, S. An improved authentication protocol for session initiation protocol using smart card. *Peer-to-Peer Netw. Appl.* **2015**, *8*, 903–910. [\[CrossRef\]](#)
38. Wang, D.; He, D.; Wang, P.; Chu, C.-H. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. *IEEE Trans. Dependable Secur. Comput.* **2014**, *12*, 428–442. [\[CrossRef\]](#)
39. Maitra, T.; Giri, D.; Mohapatra, R.N. SAS-SIP: A secure authentication scheme based on ECC and a fuzzy extractor for session initiation protocol. *Cryptologia* **2019**, *43*, 212–232. [\[CrossRef\]](#)
40. Hassan, M.U.; Chaudhry, S.A.; Irshad, A. An Improved SIP Authenticated Key Agreement Based on Dongqing et al. *Wirel. Pers. Commun.* **2020**, *110*, 2087–2107. [\[CrossRef\]](#)
41. Meshram, C.; Ibrahim, R.W.; Obaidat, M.S.; Sadoun, B.; Meshram, S.G.; Tembhurne, J. V An effective mobile-healthcare emerging emergency medical system using conformable chaotic maps. *Soft Comput.* **2021**, *25*, 8905–8920. [\[CrossRef\]](#)
42. Tiwari, D.; Gangadharan, G.R. SecAuth-SaaS: A hierarchical certificateless aggregate signature for secure collaborative SaaS authentication in cloud computing. *J. Ambient Intell. Humaniz. Comput.* **2021**, *12*, 10539–10563. [\[CrossRef\]](#)
43. Mandal, S.; Bera, B.; Sutrala, A.K.; Das, A.K.; Choo, K.K.R.; Park, Y.H. Certificateless-Signcryption-Based Three-Factor User Access Control Scheme for IoT Environment. *IEEE Internet Things J.* **2020**, *7*, 3184–3197. [\[CrossRef\]](#)
44. Gaikwad, V.P.; Tembhurne, J.V.; Meshram, C.; Lee, C.-C. Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function. *J. Supercomput.* **2021**, *77*, 8281–8304. [\[CrossRef\]](#)
45. Meshram, C.; Imoize, A.L.; Aljaedi, A.; Alharbi, A.R.; Jamal, S.S.; Barve, S.K. An Efficient Electronic Cash System Based on Certificateless Group Signcryption Scheme Using Conformable Chaotic Maps. *Sensors* **2021**, *21*, 7039. [\[CrossRef\]](#) [\[PubMed\]](#)
46. Meshram, C.; Ibrahim, R.W.; Obaid, A.J.; Meshram, S.G.; Meshram, A.; Abd El-Latif, A.M. Fractional chaotic maps based short signature scheme under human-centered IoT environments. *J. Adv. Res.* **2021**, *32*, 139–148. [\[CrossRef\]](#)
47. Meshram, C.; Obaidat, M.S.; Lee, C.-C.; Meshram, S.G. An Efficient, Robust, and Lightweight Subtree-Based Three-Factor Authentication Procedure for Large-Scale DWSN in Random Oracle. *IEEE Syst. J.* **2021**, *15*, 4927–4938. [\[CrossRef\]](#)
48. Yang, X.-J.; Baleanu, D.; Srivastava, H.M. *Local Fractional Integral Transforms and Their Applications*; Academic Press: Cambridge, MA, USA, 2015; ISBN 0128040327.
49. Han, S.; Chang, E. Chaotic map based key agreement with/out clock synchronization. *Chaos Solitons Fractals* **2009**, *39*, 1283–1289. [\[CrossRef\]](#)
50. Abdalla, M.; Fouque, P.-A.; Pointcheval, D. Password-based authenticated key exchange in the three-party setting. *IEEE Proc. Inf. Secur.* **2006**, *153*, 27–39. [\[CrossRef\]](#)
51. Dua, A.; Kumar, N.; Das, A.K.; Susilo, W. Secure message communication protocol among vehicles in smart city. *IEEE Trans. Veh. Technol.* **2017**, *67*, 4359–4373. [\[CrossRef\]](#)
52. Das, A.K.; Wazid, M.; Kumar, N.; Khan, M.K.; Choo, K.-K.R.; Park, Y. Design of secure and lightweight authentication protocol for wearable devices environment. *IEEE J. Biomed. Health Inform.* **2017**, *22*, 1310–1322. [\[CrossRef\]](#)
53. Wazid, M.; Das, A.K.; Odelu, V.; Kumar, N.; Susilo, W. Secure remote user authenticated key establishment protocol for smart home environment. *IEEE Trans. Dependable Secur. Comput.* **2017**, *17*, 391–406. [\[CrossRef\]](#)
54. Wazid, M.; Das, A.K.; Odelu, V.; Kumar, N.; Conti, M.; Jo, M. Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks. *IEEE Internet Things J.* **2018**, *5*, 269–282. [\[CrossRef\]](#)
55. Srinivas, J.; Das, A.K.; Kumar, N.; Rodrigues, J.J.P.C. Cloud centric authentication for wearable healthcare monitoring system. *IEEE Trans. Dependable Secur. Comput.* **2018**, *17*, 942–956. [\[CrossRef\]](#)
56. Chang, C.-C.; Le, H.-D. A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. *IEEE Trans. Wirel. Commun.* **2015**, *15*, 357–366. [\[CrossRef\]](#)

57. Chattaraj, D.; Sarma, M.; Das, A.K. A new two-server authentication and key agreement protocol for accessing secure cloud services. *Comput. Netw.* **2018**, *131*, 144–164. [[CrossRef](#)]
58. Bellare, M.; Pointcheval, D.; Rogaway, P. Authenticated key exchange secure against dictionary attacks. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Bruges, Belgium, 14–18 May 2000; Springer: Berlin/Heidelberg, Germany, 2000; pp. 139–155.
59. Shoup, V. Sequences of games: A tool for taming complexity in security proofs. *IACR Cryptol. ePrint Arch.* **2004**, *2004*, 332.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.