Hindawi
Security and Communication Networks
Volume 2023, Article ID 9839023, 1 page
https://doi.org/10.1155/2023/9839023

Retraction

Retracted: A Chaotic-Map-Based Password-Authenticated Key Exchange Protocol for Telecare Medicine Information Systems

Security and Communication Networks

Received 5 December 2023; Accepted 5 December 2023; Published 6 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] Y. Lu and D. Zhao, "A Chaotic-Map-Based Password-Authenticated Key Exchange Protocol for Telecare Medicine Information Systems," *Security and Communication Networks*, vol. 2021, Article ID 7568538, 8 pages, 2021.

Hindawi
Security and Communication Networks
Volume 2021, Article ID 7568538, 8 pages
https://doi.org/10.1155/2021/7568538

Research Article

A Chaotic-Map-Based Password-Authenticated Key Exchange Protocol for Telecare Medicine Information Systems

Yanrong Lu [1] **and Dawei Zhao** [2]

[1]*School of Safety Science and Engineering, Civil Aviation University of China, Tianjin, China*
[2]*Shandong Provincial Key Laboratory of Computer Networks, Shandong Computer Science Center (National Supercomputer Center in Jinan) Qilu University of Technology (Shandong Academy of Sciences), Jinan, China*

Correspondence should be addressed to Yanrong Lu; yr_lu@cauc.edu.cn and Dawei Zhao; zhaodw@sdas.org

Received 22 July 2021; Revised 23 August 2021; Accepted 30 October 2021; Published 30 November 2021

Academic Editor: Chinmay Chakraborty

Telecare medicine information systems (TMISs) provide e-health services such that patients can access medical resources conveniently and doctors can prescribe treatments rapidly. Authentication is an essential security requirement in TMISs. In particular, the growth of password-based remote patient authenticated key exchange combining extended chaotic maps has enhanced the level of secure communications for TMISs. Recently, Lee suggested an improved random-number-based password-authenticated key exchange (PAKE) using extended chaotic maps and synchronized-clock-based PAKE using extended chaotic maps on Guo and Zhang and Xiao et al.'s PAKE. Unfortunately, we found that the nonce-based scheme of Lee is insecure against known session-specific temporary information and server spoofing attacks. To cope with the aforementioned defects, this study aims to provide a new secure PAKE based on extended chaotic maps with more security functionalities for TMISs. Additionally, we show that the proposed scheme for TMISs provides high security along with low communication cost, computational cost, and a variety of security features.

1. Introduction

At present, the researches on the cloud assisted e-health are more and more in-depth. It facilitates health condition monitoring and improves efficiency for medical resources [1]. As one of the most popular applications of e-health care service, telecare medical information systems (TMISs) provide the medical or healthcare for those patients who are disabled or cannot attend hospital normally [2, 3]. With the openness of wireless environment, the security of TMISs is highlighted. How to authenticate the communication entities and thus securely transmit sensitive medical data related with patients is an urgent problem that needs to be researched and solved.

Key exchange schemes aim at establishing a shared session key between two or more communicating entities. The shared session key is used in securing subsequent communication over an insecure channel. Therefore, the key challenge of designing such a scheme is how to securely and efficiently derive a session key that is only known to the communicated entities. Hitherto, a large number of related authenticated key agreement schemes have been presented with different structures such as pure password schemes, password schemes with smart cards, dynamic schemes, and dynamic schemes with smart cards.

With the extremely studied and widely applied Chebyshev polynomials by the cryptographic research community, various password authenticated key exchange (PAKE) based on chaotic maps and related approaches have been developed recently [4–10]. Kocarev-Tasev [11] presented the first chaotic maps-based public key encryption scheme. Unfortunately, according to the periodicity of cosine function, the scheme of Kocarev-Tasev was demonstrated to be insecure by Bergamo et al. [12]. After that, Xiao

et al. [13] suggested an authenticated key agreement scheme using chaotic map. Nevertheless, Alvarez [14] pointed out that the scheme of Xiao et al. could not withstand man-in-the-middle attack. Shortly after, Xiao et al. [15] introduced an enhanced PAKE to prevent the security threats. Guo-Chang [16] raised a smart card based PAKE using chaotic maps. Later, Lin [17] claimed that the Guo-Chang's scheme might easily leak the identity of communicating user by intercepting the transmitted messages. In addition, Lin [17] also pointed that the session key could be derived by an adversary during the communication in the Guo-Chang's scheme [16]. In order to negate these risks, Lin also developed an improved variant without sacrificing the efficiency.

Recently, Guo and Zhang [18] identified that the drawbacks of Xiao et al.'s scheme [13] and found that Xiao et al.'s scheme failed to satisfy the requirements with the contributory nature of key agreement. Subsequently, Guo and Zhang developed their own improved version of the remote user PAKE. Recently, Lee [19] observed that both Xiao et al. [13] and Guo and Zhangs' schemes [18] were unable to free from offline password guessing attack and achieve the session key security. As a counter measure to these sufferings, Lee developed two PAKE; that is, one uses random numbers, while the other uses timestamp. However, this study shows that Lee (the nonce based) fails to resist known session-specific temporary information and server spoofing attacks.

The merits of this paper are as follows.

(i) Our proposed scheme demonstrates that Lee's scheme has several drawbacks once the private information is leaked.

(ii) Our proposed scheme for TMISs withstands an unauthorized patient to deceive the service provided by the telecare medical server.

(iii) Our proposed scheme for TMISs satisfies high security along with a variety of attributes compared with Xiao et al. [13], Guo and Zhang [18], and Lee schemes. Extensive comparisons are conducted with related schemes to verify the performance of our schemes in terms of security and efficiency.

The remainder of this paper is organized as follows. Section 2 introduces preliminary knowledge of some Chebyshev chaotic maps that we use in our system. We describe Lee's scheme in Section 3. In Section 4, we show that Lee's scheme [19] is vulnerable to various attacks. The proposed scheme for TMISs is presented in detail in Section 5, followed by the security analysis in Section 6. In Section 7, we compare the performance and security of our scheme for TMISs with related schemes. Finally, Section 8 concludes the paper.

2. Preliminaries

This section lists the used definitions and defines Chebyshev chaotic maps and corresponding chaotic properties that are used in this paper [11, 12, 20–22].

The Chebyshev polynomial $T_s(x)$: $[-1, 1] \longrightarrow [-1, 1]$ is defined as follows:

$$T_s(x) = 2xT_{s-1}(x) - T_{s-2}(x), \quad (1)$$

where s be an integer with $s \geq 2$, $x \in [-1, 1]$, $T_0(x) = 1, T_1(x) = x$.

The Chebyshev polynomial satisfies the semigroup property:

$$T_{st}(x) = T_s(T_t(x)) = T_t(T_s(x)). \quad (2)$$

Chaotic property:

When $a > 1$, Chebyshev polynomial map T_s: $[-1, 1] \longrightarrow [-1, 1]$ of degree s is a chaotic map with invariant density $f^*(x) = 1/(\pi\sqrt{[2]}\,1 - x^2)$ for Lyapunov exponent $\lambda = \ln s > 0$.

Quadratic residue assumption:

If $y = x^2 \bmod n$ has a solution, that is, $\exists$ a square root for y, then y is named as a quadratic residue modulo n. It is computationally unfeasible to derive x such that $y = x^2 \bmod n$ under the condition of not knowing the parameters p and q because of the factoring problem $n = pq$ is NP-hard problem.

3. Review of Lee's PAKE

Lee [19] presented two authentication schemes, which are based on nonce and timestamp, respectively. Without loss of generality, we briefly review the nonce based PAKE of Lee, which includes system initialization, authentication and key agreement phases.

3.1. System Initialization.

Step 1: Server B chooses two large primes p and q as its private keys.

Step 2: B calculates $n = pq$.

Step 3: B publishes h_1: $\{0, 1\}^* \longrightarrow \{-\infty, +\infty\}$, h_2: $\{0, 1\}^* \longrightarrow \{0, 1\}^\tau$ and n, where τ is the fixed size.

3.2. Authentication and Key Agreement

Step 1: User A computes $x = h_1(y), X_1 = (y, pw)^2 \bmod n, TID_A = ID_A \oplus h_2(y, pw)$, and $X_2 = h_2(TID_A, (y, pw), T_r(x))$, where r and y are the random numbers. A then sends the message $M_1 = \{TID_A, X_1, X_2, T_r(x)\}$ to B.

Step 2: Once receiving M_1, B retrieves the four solutions $(y_i, pw_i)\,(0 \leq i \leq 3)$ from X_1 by using the Chinese remainder theorem (CRT) and checks whether $h_2(TID_A, (y_i, pw_i), T_r(x)) \stackrel{?}{=} X_2$. If successful, it means B has gotten the correct y' and pw'. After that, B checks if $pw' \stackrel{?}{=} pw$. If the equation is true, B derives ID_A by computing $TID_A \oplus h_2(y', pw')$ and computes $x = h_1(y'), sk = h_2(T_r(x), T_s(x), T_s(T_r(x)))$ and $Auth_B = h_2(sk, pw, ID_B, ID_A)$. Next, B sends back $M_2 = \{ID_B, T_s(x), Auth_B\}$ to A.

Step 3: When receiving M_2, A computes $sk = h_2(T_r(x), T_s(x), T_r(T_s(x))$ and $Auth_B' \stackrel{?}{=} h_2(sk, pw, ID_B, ID_A)$. Next, A checks whether $Auth_B' \stackrel{?}{=} Auth_B$. If it holds, A computes $Auth_A = h_2(sk, ID_A, ID_B)$ and sends $M_3 = \{Auth_A\}$ to B.

Step 4: After receiving M_3, B verifies whether $h_2(sk, ID_A, ID_B)$ is equal to the received $Auth_A$. If it does not hold, B terminates the session; otherwise, A and B have a common session key $sk = h_2(T_r(x), T_s(x), T_{rs}(x))$.

4. Security Analysis on Lee's Scheme

Lee [19] found some severe security pitfalls in Xiao et al. [13] and Guo and Zhang's schemes [18, 21] and proposed new chaotic-based authenticated key schemes. It is claimed that their new scheme achieves many security attributes while being secure against general threats. In this part, however, we will demonstrate that Lee's nonce based scheme [19] is actually vulnerable to known session-specific temporary information attack [23], which is one of the most important security properties that most of schemes shall attain. In addition, as the result of overlooking the server is a semi-trusted party, this scheme is subject to server spoofing attack.

4.1. Known Session-Specific Temporary Information Attack. Assume the user's session random number y is corrupted by an adversary $\mathbb{U}$. The scheme will suffer the following attack.

Step 1: $\mathbb{U}$ guesses a candidate password pw^* and checks whether $h_2(TID_A, (y, pw^*), T_r(x)) \stackrel{?}{=} X_2$, where TID_A and $T_r(x)$ are intercepted information through the public channel by $\mathbb{U}$. If the result is true, the correct password has been gotten. Otherwise, $\mathbb{U}$ continues to execute the aforementioned procedure until he succeeds.

Step 2: Once $\mathbb{U}$ successfully owns the user A's password pw. There can be no real defense against attacks from $\mathbb{U}$. First, $\mathbb{U}$ derives ID_A by computing $TID_A \oplus (y, pw)$ and computes $X_1 = (y, pw)^2 \bmod n$. Next, $\mathbb{U}$ sends the counterfeited message $M_1 = \{TID_A, X_1, X_2, T_r^*(h_1(y))\}$ to the server B, where r^* is the random number chosen by $\mathbb{U}$.

Step 3: When the server B receives M_1, it performs the scheme without any detection since all the verification information derived from the user "A." Finally, the server B sends back the message $M_2 = \{ID_B, T_s(h_1(y)), Auth_B\}$ to $\mathbb{U}$ who masquerades as a legal user A, where $Auth_B = h_2(ID_B, ID_A, pw, sk)$ and $sk = h_2(T_r^*(h_1(y)), T_s(h_1(y)), T_s(T_r^*(h_1(y))))$.

Step 4: After receiving the message M_2, $\mathbb{U}$ computes $sk = h_2(T_r^*(h_1(y)), T_s(h_1(y)), T_{r^*}(T_s(h_1(y))))$ and verifies whether the equation $h(ID_B, ID_A, pw, sk)$ is equal to the received $Auth_B$. If the result is correct, $\mathbb{U}$ computes $Auth_A = h_2(ID_B, ID_A, sk)$ and returns $M_3 = \{Auth_A\}$ to the server B.

Step 5: Once receiving the message M_3, server B validates the correctness of the value $Auth_A$. Then, server B accepts the communication request from user "A" and agrees on the session key sk as a "confidential" session key for concealing the following messages. In this way, the subsequent communication messages seem like plain text such that $\mathbb{U}$ could do whatever he wants. This shows that, in Lee's scheme, $\mathbb{U}$ can use the unexpectedly disclosed session random number to successfully complete mutual authentication. This concludes that their scheme lacks strongly the SK-security, which is very essential in the security critical applications.

4.2. Server Spoofing Attack. In Lee's scheme, server B masters the sensitive information pw of user A, which leads to a malicious spoofing attack because the legal but malicious server B could monitor the authentication process of user A and gather information related to user A and thus become an adversary. The malicious server $\mathbb{B}$ can forge the valid request message by performing the following procedures.

Step 1: The malicious server $\mathbb{B}$ can eavesdrop the message $M_1 = \{TID_A, X_1, X_2, T_r^*(h_1(y))\}$ during authentication and key agreement phase corresponding to the legitimate user A. Then, $\mathbb{B}$ generates two random numbers r^*, y^* and calculates $x = h_1(y^*), T_r^*(x), z = (y^*, pw), X_1 = z^2 \bmod n, TID_A = ID_A^* \oplus h_2(z)$ and $X_2 = h_2(TID_A, z, T_r^*(x))$. Next, $\mathbb{B}$ sends an imitative message $M_1 = \{TID_A, X_1, X_2, T_r^*(x)\}$ to server B.

Step 2: When receiving M_1, server B derives (y', pw') from X_1 by using the Chinese remainder theorem (CRT) and examines whether $h_2(TID_A, (y', pw'), T_r^*(x))$. Because the computed result equals the received X_2, B will accept $\mathbb{B}$'s request. Next, B derives ID_A^* by computing $TID_A \oplus h_2(y', pw')$ and checks whether $pw' \stackrel{?}{=} pw$. If it holds, server B computes $x = h_1(y'), T_s(x), sk = h_2(T_r^*(x), T_s(x), T_s(T_r^*(x))$ and $Auth_B = h(sk, pw, ID_B, ID_A^*)$. At last, B sends the message $M_2 = \{ID_B, T_s(x), Auth_B\}$ to $\mathbb{B}$ who is masquerading as user A.

Step 3: Once receiving M_2, $\mathbb{B}$ computes $h_2(sk, pw, ID_B, ID_A^*)$ and checks it with $Auth_B$, where $sk = h_2(T_r^*(x), T_s(x), T_s(T_r^*(x))$. If they are equivalent, $\mathbb{B}$ computes $Auth_A = h_2(sk, ID_A^*, ID_B)$ and sends back $M_3 = \{Auth_A\}$ to server B.

Step 4: When receiving M_3, server B computes $h_2(sk, ID_A^*, ID_B)$ and compares it with M_3. If they are equal, B authenticates $\mathbb{B}$. In this regard, $\mathbb{B}$ and B share a common session key $sk = h_2(T_r^*(x), T_s(x), T_s(T_r^*(x))$ for securing communication. Therefore, a legal but malicious server can masquerade as a legal user to log into a remote server.

The same flaw can be applied to the timestamp based scheme of Lee. Since they work on the same principle, only nonce-based scheme is analyzed above.

5. The Proposed PAKE Scheme for TMISs

To overcome the security pitfalls found in Lee's scheme, we present efficient and secure PAKE using chaotic maps for TMISs. To achieve the patient anonymity and reduce the computation overhead at the patient's side who may take mobile device, the proposed scheme leverages the encryption function to find a trade-off between the security and the cost. The proposed scheme has the following phases: system initialization phase, patient registration phase (Algorithm 1), and authentication and key agreement phase (Algorithm 2).

5.1. System Initialization.

Step 1: The telecare medical server B chooses two large primes p and q as its private keys.

Step 2: B calculates $n = pq$.

Step 3: B publishes h: $\{0,1\}^* \longrightarrow \{0,1\}^\tau$ and n, where τ is the fixed size.

5.2. Patient Registration

Step 1: Patient A computes $h(pw, ra)$ and sends $\{ID_A, h(pw, ra)\}$ to the telecare medical server B over a private channel, where ra is a random nonce and pw is A's password.

Step 2: When B receives the message, B computes $A_{pw} = E_{K_B}[h(ID_A, h(pw, ra))]$ and stores A_{pw} in its database, where K_B is the secret key of B.

5.3. Authentication and Key Agreement

Step 1: A computes $x = h(ID_A, h(pw, ra))$, $z = (ID_A, r)^2 \bmod n$, $X_1 = h(ID_A, x, r)$ and $X_2 = E_x[T_r(x), z, X_1]$, where r is a random nonce. Next, A transmits the messages $M_1 = \{X_2\}$ to B.

Step 2: Upon receiving the message, B first derives $x = h(ID_A, h(pw, ra))$ by decrypting A_{pw} and then retrieves $[T_r(x), z, X_1]$ by decrypting X_2. Subsequently, B solves z by CRT and verifies whether $h(ID'_A, r', x) \stackrel{?}{=} X_1$. If true, B computes $X_3 = E_{T_r(x)}[T_s(x), SID_B, h(ID'_A, r')]$ and sends $M_2 = \{X_3\}$ to A.

Step 3: On receiving the message, A retrieves $[T_s(x), SID_B, h(ID'_A, r')]$ by decrypting X_3, computes $h(ID_A, r)$, and checks whether $h(ID'_A, r') \stackrel{?}{=} h(ID_A, r)$. If successful, A computes $sk = h(T_u(x), T_s(x), T_{us}(x))$, $X_4 = E_{T_{r(x)}}[T_{u(x)}]$, and $Auth_A = h(sk, T_u(x), T_s(x))$. Next, A sends back $M_3 = \{Auth_A, X_4\}$ to B.

Step 4: When receiving the message, B retrieves $T_u(x)$ by decrypting X_4 with computed $T_r(x)$. After that, B computes $sk = h(T_s(x), T_u(x), T_s(T_u(x)))$ and checks whether $h(T_s(x), T_u(x), T_s(T_u(x))) \stackrel{?}{=} Auth_A$. If correct, B computes $Auth_B = h(sk, T_s(x), T_u(x), 00)$ and sends $M_4 = \{Auth_B\}$ to A.

Step 5: A verifies the correctness of the value $Auth_B$. If not, A aborts the session. Otherwise, A and B share a common session key $sk = h(T_s(x), T_u(x), T_{su}(x)))$ with each other.

6. Cryptanalysis of Our Enhancement

In this section, we provide an in-depth analysis on the security features of our enhanced remote user PAKE scheme for TMISs. We will show that the proposed scheme not only provides anonymity and mutual authentication and but could also withstand the aforementioned attacks.

6.1. Full Protection for Patient's Identity. Obviously, the proposed scheme for TMISs provides patient anonymity because patient A's identity ID_A is not transmitted in plaintext via any messages traveling over insecure network. For one thing, ID_A is protected by hash function as a symmetric key only known by the patient A and the corresponding telecare medical server B. The telecare medical server could not know the real identity even if it intends to decrypt the stored value or the legal telecare medical server's private key is embezzled by an illegitimate patient or an illegitimate server to derive the hash value. The real identity ID_A is concealed by the quadratic residue assumption. As we know, the assumption is secure for chosen-plaintext attack and the identity is always a short string which could not be known by the unauthorized third-party unless it is completely learnt. Besides, the random number r is not an uncertain number which is not easily guessed. All in all, the proposed scheme for TMISs can be categorized as one preserving the patient privacy.

6.2. Mutual Authentication Thwarting Man-in-the-Middle Attack. The mutual authentication between correspondents is a basic security features for a remote PAKE. Only on the basis of the trust, two unfamiliar participates, that is, the patient and the server, are able to establish the session key for securing the following communication messages. In the proposed scheme for TMISs, patient A is authenticated by the telecare medical server by verifying the validity of X_1. This verification needs two indispensable conditions. One is the private key of the telecare medical server B to derive the hashed value including the identity ID_A, the password pw, and the random number r_a. Another are the two private values p and q, which are used to retrieve the plain-text identity ID_A and the random number r. The telecare medical server is not able to examine the received message $M_1 = \{X_2\}$ without the knowledge of the two secrets. In other words, not anyone could generate the valid message $\{X_2\}$ unless they know all the private information, such as the identity ID_A, the password pw, and even the random number r_a of the registered patient, only known by the patient itself. Additionally, the message $M_3 = \{Auth_A, X_4\}$ further consolidates the authenticity of patient A since only the real patient knows the value $T_r(x)$, which is employed to compute the authenticated messages. On the other side, following the previously mentioned discussion, only the legitimate telecare medical server retrieves the plain-text identity ID_A, the random number r, and the value $T_r(x)$,

Input: pw, h, p, q, n
Output: Store A_{pw}.
(1) Select ra,
(2) Compute $h(pw, ra)$,
(3) $A_{pw} = E_{K_B}[h(ID_A, h(pw, r_a))]$.

Algorithm 1: Patient registration.

which are used for checking by patient A. Similarly, message $M_4 = \{Auth_B\}$ is utilized to further confirm the legitimacy of the telecare medical server. According to the previously mentioned analysis, the man-in-the-middle attack is not launched due to lack of personal information. Any forged messages could be detected by the receivers since they have the symmetric key which is unknown by any third party. This confirms that our PAKE scheme for TMISs achieves the property of mutual authentication and thus resists man-in-the middle attack.

6.3. Resistance to Known Session-Specific Temporary Information Attack. From Algorithm 2, patient A and telecare medical server B use $T_r(x)$ to encrypt the session key $SK = h(T_u(x), T_s(x), T_{us}(x))$, where $x = h(ID_A, h(pw, r_a))$. Clearly, even if an adversary gets the temporary information r and r_a, it is incapable of computing $T_u(x)$ without having the knowledge of either ID_A or pw [19]. In this way, the proposed scheme for TMISs overcomes the drawbacks found in Lee's scheme. Moreover, without revealing the identity pw of A to B, B authenticates A through decrypting A's registered message $A_{pw} = E_{K_B}[h(ID_A, h(pw, r_a))]$. Thus, the proposed PAKE scheme for TMISs can withstand this type of attack.

6.4. Perfect Forward Session Key Secrecy. Even if the password pw of the patient A is lost, the session key is still secure since the password is not related with the computed session key. Actually, if the important values $T_u(x)$ and $T_s(x)$ are compromised, an adversary could derive the correct u and s using the approach [12]. However, the adversary has no opportunity to get the two values unless they know user A's private information, such as the identity ID_A, password pw, and the random number r_a or the private keys of the telecare medical server B, such as K_B and two large primes p, q. Unfortunately, the patient anonymity has guaranteed that it is impossible for the adversary to obtain the patient's personal information. As we know, the telecare medical server's private keys are not easily exposed. These features along with the patient anonymity confirm forward secrecy and known-key secrecy capability of our PAKE scheme.

6.5. Resistance to Patient Impersonation Attack. Evidently, the most essential goal of a secure PAKE scheme is to withstand impersonation attack, which means an interception of the transmitted messages from both sides will not lead to the serious threats on the system. In the proposed PAKE scheme for TMISs, no adversaries are able to impersonate patient A by eavesdropping the communication messages, since the secret parameters including A's identity ID_A, password pw, and random number r_a are unknown to the adversary. Additionally, it is computationally infeasible to find ID_A and r from $z = (ID_A, r)^2 \bmod n$ without the knowledge of p and q, where $n = p * q$. Therefore, the proposed PAKE scheme for TMISs provides the resilience against patient impersonation attack.

6.6. Resistance to Telecare Medical Server Spoofing Attack. Suppose an adversary plans to impersonate the telecare medical server B by eavesdropping the communication message: $M_1 = X_2 = E_x[T_r(x), z, X_1]$, where $x = h(ID_A, h(pw, r_a)), z = (r, ID_A)^2 \bmod n$ and $X_1 = h(x, ID_A, r)$. They could not pass the authentication by patient A without knowing the telecare medical server B's secret key K_B. How easy will it be to get hold of patient A's identity ID_A and r without the help of the correct value x? Hence, the proposed PAKE scheme for TMISs can withstand telecare medical server spoofing attack.

6.7. Resistance to Bergamo et al.'s Attack. The implementation of the Bergamo et al.'s attack [12] is based on the following facts: (i) Chebyshev polynomials can be alternatively defined as the cosine function, which leads to the same value due to the periodicity of the cosine function; (ii) $T_u(x), T_s(x)$, and x as the public keys are transmitted in an open channel, which can be intercepted by an adversary. However, in the proposed scheme for TMISs, patient A and the telecare medical server B transmitted the encrypted messages $Auth_A$ and $Auth_B$ over a public channel, where $Auth_A = h(sk, T_u(x), T_s(x))$, $Auth_A = h(sk, T_s(x), 00, T_u(x))$, respectively. Without knowing $T_r(x)$, no adversaries can decrypt the message X_4 and thus they cannot recover $T_u(x)$. Additionally, the value $x = h(ID_A, h(pw, r_a))$ is related with the patient A's sensitive information, and adversaries are incapable of getting such sensitive information. Therefore, the proposed PAKE scheme for TMISs is free from Bergamo et al.'s attack [12].

6.8. Resistance to Replay Attack. With the purposing of free from replay attack, we use a random number r which is only recovered by the telecare medical server S. If an adversary attempts to masquerade A by immediately replaying the previous authentication messages $M_1 = \{X_2\}$ after eavesdropping, the telecare medical server S would obviously refuse the request because the invalid random number r will be detected by checking $h(x, ID_A, r) \stackrel{?}{=} X_1$. Moreover, the

Input: ID_A, pw, ra
Output: true: success; false: failure
1: Generate r,
2: Compute $x = h(ID_A, h(pw.ra))$, $y = (ID_A, r)$
3: $Z = y^2 \bmod n$, $X_1 = h(x, ID_A, r)$, $X_2 = E_X[T_r(x), z, X_1]$.
4: Transmit $M_1 = \{X_2\}$ to B.
5: Decrypt $A_{pw} \longrightarrow x = h(ID_A, h(pw, ra))$, $X_2 \longrightarrow [T_r(x), z, X_1]$.
6: Solve z by CRT, determinate (ID'_A, r')
7: if $h(x, ID'_A, r') \stackrel{?}{=} X_1$ then
8: Generate s, $X_3 = E_{T_r(x)}[T_s(x), SID_B, h(ID_A, r)]$
9: Transmit X_3 to Patient A.
10: Decrypt $X_3 \longrightarrow [T_s(x), SID_B, h(ID_A, r)]$
11: if $h(ID_A, r) \stackrel{?}{=} h(ID'_A, r')$ then
12: Generate u, $sk = h(T_u(x), T_s(x), T_{us}(x))$
13: $X_4 = E_{T_r(x)}[T_u(x), ID_A]$, $Auth_A = h(sk, T_u(x), T_s(x))$.
14: Transmit $Auth_A$ and X_4 to B.
15: Decrypt $X_4 \longrightarrow [T_u(x), ID_A]$.
16: $sk = h(T_s(x), T_u(x), T_s(T_u(x)))$.
17: if $h(sk, T_s(x), T_u(x)) \stackrel{?}{=} Auth_A$ then
18: $Auth_B = h(sk, T_s(x), T_u(x), 00)$
19: Transmit $Auth_B$ to $M_4 = \{Auth_B\}$.
20: if $Auth_B \stackrel{?}{=} h(sk, T_s(x), T_u(x), 00)$then
21: return true
22: else
23: return false
24: else
25: return false
26: else
27: return false
28: else
29: return false
30: end if

Algorithm 2: Authentication and Key agreement.

patient also checks the random number which is sent from the telecare medical server to prevent the replay attack.

7. Security Attributes and Performance Comparison

In the following section, we analyze the security attributes and the computational efficiency of the proposed PAKE scheme for TMISs and compare to Xiao et al. [15], Guo and Zhang [18], and Lee [19] since they are all based on chaotic-maps PAKE schemes. Table 1 shows the security attributes comparison among our presented scheme and other schemes [15, 18, 19]. Compared with other schemes, both Guo and Zhang and Xiao et al.'s schemes cannot achieve user anonymity and perfect forward session key secrecy. Furthermore, both of their schemes cannot withstand patient impersonation attack. In addition, Lee's scheme fails to prevent known session-specific temporary information and server spoofing attacks.

Table 2 lists the computational complexity comparison of our proposed PAKE scheme with other schemes, where T_c denotes the time of executing a Chebyshev polynomial computing; T_h denotes the time of executing a hash operation; T_s denotes the time of executing a symmetric key encryption/decryption; T_{sq} denotes the time of executing a squaring; T_{sr} denotes the time of executing a squaring root solving. According to [15], the execution time for T_s is about 70 times than T_c, and T_s is almost equal to T_h in software. Therefore, our proposed PAKE scheme consumes a slightly higher computation cost than others. We think it is worth slightly sacrificing the efficiency in the hope of guaranteeing a high level security for TMISs.

Table 1: Comparison of security attributes.

	Ours	Lee [19]	Guo and Zhang [18]	Xiao et al. [15]
Provide anonymity	Yes	Yes	No	No
Provide perfect forward session key secrecy	Yes	Yes	No	No
Provide mutual authentication	Yes	Yes	Yes	Yes
Resist man-in-the-middle attack	Yes	Yes	Yes	Yes
Resist replay attack	Yes	Yes	Yes	Yes
Resist known session-specific temporary information attack	Yes	No	—	—
Resist Bergamo et al.'s attack	Yes	Yes	No	Yes
Resist patient impersonation attack	Yes	Yes	No	No
Resist server spoofing attack	Yes	No	Yes	No

Table 2: Comparison of computational cost.

	Ours	Lee [19]	Guo and Zhang [18]	Xiao et al. [15]
User	$3T_c + 7T_h + 3T_s + 1T_{sq}$	$2T_c + 6T_h + 1T_{sq}$	$2T_c + 8T_h$	$2T_c + 2T_h$
Server	$2T_c + 8T_h + 4T_s + 1T_{sr}$	$2T_c + 9T_h + 1T_{sr}$	$2T_c + 10T_h$	$2T_c + 2T_h$
No. of message communications	4	3	6	5

8. Conclusion

In this paper, we first reviewed Lee's scheme and then demonstrated that Lee's scheme is vulnerable to the known session-specific temporary information and server spoofing attacks. With the purpose of remedy of these security loopholes, we presented an improved PAKE scheme using extended chaotic maps for TMISs. We showed that our design is secure and provides more functionalities compared with the related schemes. Performance analysis showed the proposed PAKE scheme for TMISs is secure and efficient. In the future, we will further optimize the proposed scheme regarding security and performance using encryption and machine learning in order to apply to network structure to improve its availability.

Data Availability

The data are included in the manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This paper was supported in part by the National Natural Science Foundation of China under grant 61802276 and the Fundamental Research Funds for the Central Universities of China (no. 3122021027).

References

[1] Z. Yu, C. Y. Zhang, and J. X. Yu, "Research on mathematical model of characteristic curve of surface perception by PVDF array based on Ferguson function," *International Journal of Engineering Systems Modelling and Simulation*, vol. 12, no. 1, p. 17, 2021.

[2] X. Li, F. Wu, M. K. Khan, L. Xu, J. Shen, and M. Jo, "A secure chaotic map-based remote authentication scheme for telecare medicine information systems," *Future Generation Computer Systems*, vol. 84, pp. 149–159, 2017.

[3] A. K. Sutrala, A. K. Das, V. Odelu, M. Wazid, and S. Kumari, "Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems," *Computer Methods and Programs in Biomedicine*, vol. 135, pp. 167–185, 2016.

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

[5] J.-L. Tsai and N.-W. Lo, "A chaotic map-based anonymous multi-server authenticated key agreement protocol using smart card," *International Journal of Communication Systems*, vol. 28, no. 13, pp. 1955–1963, 2015.

[6] X. Li, J. Niu, S. Kumari, M. K. Khan, J. Liao, and W. Liang, "Design and analysis of a chaotic maps-based three-party authenticated key agreement protocol," *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1209–1220, 2015.

[7] X. Wang, W. Zhang, W. Guo, and J. Zhang, "Secure chaotic system with application to chaotic ciphers," *Information Sciences*, vol. 221, pp. 555–570, 2013.

[8] W.-C. Yau and R. C.-W. Phan, "Cryptanalysis of a chaotic map-based password-authenticated key agreement protocol using smart cards," *Nonlinear Dynamics*, vol. 79, no. 2, pp. 809–821, 2014.

[9] Y. Lu, L. Li, H. Peng, and Y. Yang, "Cryptanalysis and improvement of a chaotic maps-based anonymous authenticated key agreement protocol for multiserver architecture," *Security and Communication Networks*, vol. 9, no. 11, pp. 1321–1330, 2016.

[10] D. Abbasinezhad-Mood, A. Ostad-Sharif, S. M. Mazinani, and M. Nikooghadam, "Provably secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 12, pp. 7287–7294, 2020.

[11] L. Kocarev and Z. Tasev, "Public key encryption based on Chebyshev maps," in *Proceedings of the IEEE Symposium on Circuits and Systems*, pp. 28–31, IEEE, Bangkok, Thailand, May 2003.

[12] P. Bergamo, P. D'Arco, A. De Santis, and L. Kocarev, "Security of public-key cryptosystems based on Chebyshev

polynomials," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 52, no. 7, pp. 1382–1393, 2005.
[13] D. Xiao, X. Liao, and K. Wong, "An efficient entire chaos-based scheme for deniable authentication," *Chaos, Solitons & Fractals*, vol. 23, no. 4, pp. 1327–1331, 2005.
[14] G. Alvarez, "Security problems with a chaos-based deniable authentication scheme," *Chaos, Solitons & Fractals*, vol. 26, no. 1, pp. 7–11, 2005.
[15] D. Xiao, X. Liao, and S. Deng, "A novel key agreement protocol based on chaotic maps," *Information Sciences*, vol. 177, no. 4, pp. 1136–1142, 2007.
[16] C. Guo and C.-C. Chang, "Chaotic maps-based password-authenticated key agreement using smart cards," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 6, pp. 1433–1440, 2013.
[17] H.-Y. Lin, "Improved chaotic maps-based password-authenticated key agreement using smart cards," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 482–488, 2015.
[18] X. Guo and J. Zhang, "Secure group key agreement protocol based on chaotic hash," *Information Sciences*, vol. 180, no. 20, pp. 4069–4074, 2010.
[19] T.-F. Lee, "Enhancing the security of password authenticated key agreement protocols based on chaotic maps," *Information Sciences*, vol. 290, pp. 63–71, 2015.
[20] Y. Chen, J.-S. Chou, and H.-M. Sun, "A novel mutual authentication scheme based on quadratic residues for RFID systems," *Computer Networks*, vol. 52, no. 12, pp. 2373–2380, 2008.
[21] W. Patterson, *Mathematical Cryptology for Computer Scientists and Mathematicians*, ACM Digital Library, Ingolstadt, Germany, 1987.
[22] L. Zhang, "Cryptanalysis of the public key encryption based on multiple chaotic systems," *Chaos, Solitons & Fractals*, vol. 37, no. 3, pp. 669–674, 2008.
[23] V. Odelu, A. K. Das, and A. Goswami, "A secure biometrics-based multi-server authentication protocol using smart cards," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 9, pp. 1953–1966, 2015.