An Improved Authentication Protocol for Telecare Medical Information System

Wan-Rong Liu[12], Xin He[2], Zhi-Yong Ji[1]
(Corresponding author: Zhi-Yong Ji)

Shanghai Sixth People's Hospital East affiliated to Shanghai University of Medicine & Health Sciences[1]
Shanghai 201306, China
Department of Engineering Science and Technology, Shanghai Ocean University[2]
Shanghai 201306, China
(Email: joyer99@126.com) *(Received Apr. 6, 2020; revised and accepted Nov. 15, 2020)*

Abstract

In the telecare medicine information system, the importance of patient information system security and mutual authentication is self-evident. In 2017, Aslam et al. considered Kumari et al.'s protocol to be the better of the two-factor authentication protocols they analyzed. We analyze the agreements of Kumari et al. and find some shortcomings. Based on the Computational Diffie-Hellman problem and the timestamp mechanism, we improve the protocol to improve security and use elliptic curves to speed up the calculation. In the comparative analysis of performance and efficiency, we can see that our improved protocol has a smaller calculation amount and higher security.

Keywords: Anonymity; Authentication; Password; Telecare Medicine Information System

1 Introduction

Telemedicine information system (TMIS) is an information system built by integrated use of electronic information technology, computer communication technology, medical technology and other advanced technologies. In the telemedicine information system, patients send their own medical information data to doctors through the Internet, and doctors use these data to diagnose the patient's condition, thereby reducing extra travel for patients [11]. In the late 1950s, two-way television system was applied by American scholars in the field of medical treatment, which realized telemedicine image transmission by means of cable. Such as radiology. At the same time, a technology called " STARPAHC (Space Technology Applied to Rural Papago Advanced Health Care)" was developed between Lockheed and NASA and the public health service [22]. The technology could provide telemedicine for astronauts in space. Since the 1960s, telemedicine system has moved into other areas, providing interactive videos and transmitting electrocardiograms, blood pressure, and services such as tele-psychiatry and radiology. On this basis, telemedicine was subsequently created. In addition, some scholars have creatively introduced the electronic communication technology in the field of communication into the field of medical treatment.

In the late 1960s, remote ECG monitoring [10, 21] appeared. In 2004, Anliker et al. [3] developed a wearable medical monitoring and warning system that regularly collected multiple physiological parameters over a period of time and sent the data of these parameters to the hospital warning center. As one of the important applications of medical informatization, telemedicine integrates and utilizes the medical resources in the region to provide better medical services for patients. These systems reduce the cost of hospitalization, treatment costs and commuting time. In the telemedicine information system, patients send their own medical information data to doctors through the Internet, and doctors use these data to diagnose the patient's condition, thereby reducing extra travel for patients. This approach allows medical resources to be used effectively, especially for patients who unable to go to the hospital due to disability and other reasons. However, in telemedicine information system, medical information security and mutual authentication of patients are very important. So far, scholars have proposed many improved protocols to make the information transmitted by patients more secure and ensure that the information is not maliciously stolen [1,12,13]. In addition, Masdari et al. suggest that in some TMIS, a patient communicates with more than just a doctor. In some cases, a patient needs to communicate with multiple doctors, but group identity authentication rarely exists in current identity authentication [20]. There are generally three ways for users to conduct identity authentication. The first way is to use password only to authenticate users; the second way is to use smart card to authenticate users on the basis of password; the third way is to add biometric authentication on the basis of the former.

The first remote computer authentication scheme was proposed by Lamport [18]. The first single factor and password-based identity authentication comes out in the period when the Internet efficiency is not very high. Secondly, the password leakage in the single factor authentication protocol is a common problem. With the development of the Internet, the efficiency of computers is getting higher and higher, and researchers have proposed more lightweight but more secure authentication protocols. The first two-factor authentication scheme was proposed by Hwang in 1990 [14]. The scheme is based on Shamir's ID-based signature scheme [23] to solve the password storage problem. Then, the authentication scheme proposed by Chang [6] in 1991 is a two-factor. Compared with single-factor, two-factor authentication protocols are increasingly favored by scholars [**?**,**?**,4–8,14,15,17,19,23–27]. In 2012, both Wu et al. [25] and He et al. [8] proposed an authentication scheme for TMIS. Wei et al. [24] pointed out that not only the scheme of Wu et al. cannot achieve two-factor authentication, but also the scheme of He et al. In 2013, Xu et al. [26] proposed an ECC-based authentication protocol. Next year, Islam et al. [15] proposed their own scheme and thought that they solved all the problems in Xu et al.'s scheme. Chaudhry et al. [7] and Zhang et al. [27] proved that Islam et al.'s scheme cannot resist against the sever and user impersonation. In 2018, Qiu et al. [22] found some important limitations in both Islam et al.'s scheme and Chaudhry et al.'s. In Aslam et al.' [4] survey, they thought Kumari et al.'s [17] scheme did not have extensive cryptanalysis, Xu et al.' [26] scheme did not validate the user's legitimacy with the end user.

However, we analyzed that Kumari et al.'s scheme does not provide forward confidentiality and is also vulnerable to smart card loss attacks. The clock synchronization problem also exists in their scheme. According to the scheme of Kumari et al., we improve it and get a more secure two-factor authentication protocol. Our improved protocols are based on Computational Diffie-Hellman (CDH) problem and timestamp mechanism to improve security primarily. We employed elliptic curves (ECC) in our protocol. The use of elliptic curves in cryptography was independently proposed by Neal Koblitz and Victor Miller in 1985 [5]. One of the advantages of ECC is the use of smaller keys than other methods [16]. In addition, ECC-based protocols have advantages over other cryptographic systems in computation and communication. We use dynamic identity to keep user information confidential and untraceable. Through performance comparison and efficiency analysis, it can be seen from the analysis that the improved protocol has less computation and higher security.

2 Review of Kumari et al.'s Scheme

We review of Kumari et al.'s scheme. All notations which used are described in Table 3. There are four phases in Kumari et al.'s scheme: Registration phase (See Figure 1), login and authentication phase (See Figure 2), password change phase (See Figure 3), and revocation phase. When a smart card is lost or stolen, users can deregister their corresponding smart cards in the revocation phase.

Table 1: Notations

Symbol	Definition
U	User
Ms/S	Medical Server
ID	Identify of U
PW	Password of U
x	Secret key
r,R	a random number
P	a point on the elliptic curve
$P \cdot x$	the value of on x-axis
A	The adversary
SC	The smart card
$E_k(\cdot)/D_k(\cdot)$	Symmetric key encryption/decryption by key k
$h(\cdot)$	One-way hash functionr
$\oplus$	Bitwise XOR operatio
$\|$	Concatenation operation
T	The current time of system
SK	Session-key
ΔT	The maximum time interval for transmission delay
$H(\cdot)$	Bio-hash function
B	Biological characteristics

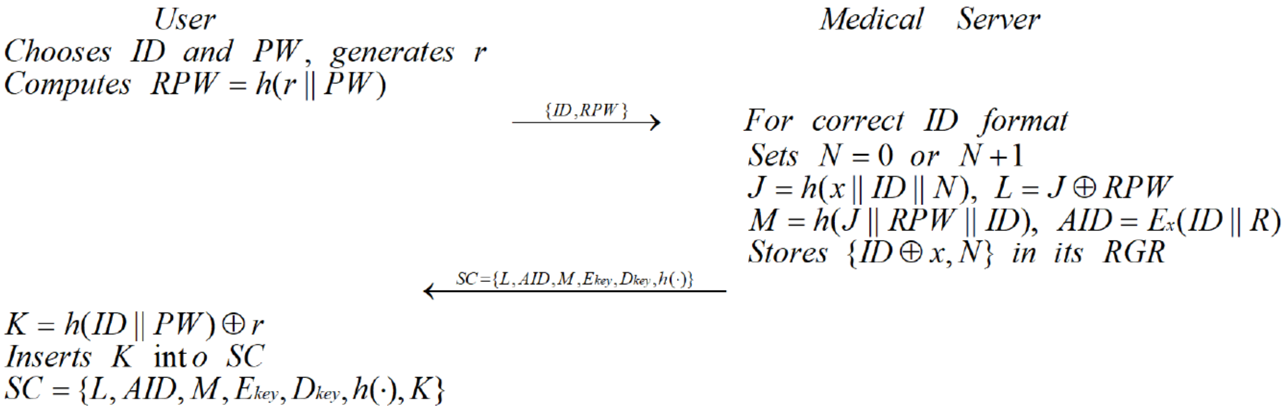
User
Chooses ID and PW, generates r
Computes $RPW = h(r \| PW)$
$\{ID, RPW\}$
Medical Server
For correct ID format
Sets $N = 0$ or $N+1$
$J = h(x \| ID \| N)$, $L = J \oplus RPW$
$M = h(J \| RPW \| ID)$, $AID = E_x(ID \| R)$
Stores $\{ID \oplus x, N\}$ in its RGR
$SC = \{L, AID, M, E_{key}, D_{key}, h(\cdot)\}$
$K = h(ID \| PW) \oplus r$
Inserts K into SC
$SC = \{L, AID, M, E_{key}, D_{key}, h(\cdot), K\}$

Figure 1: Registration Phase

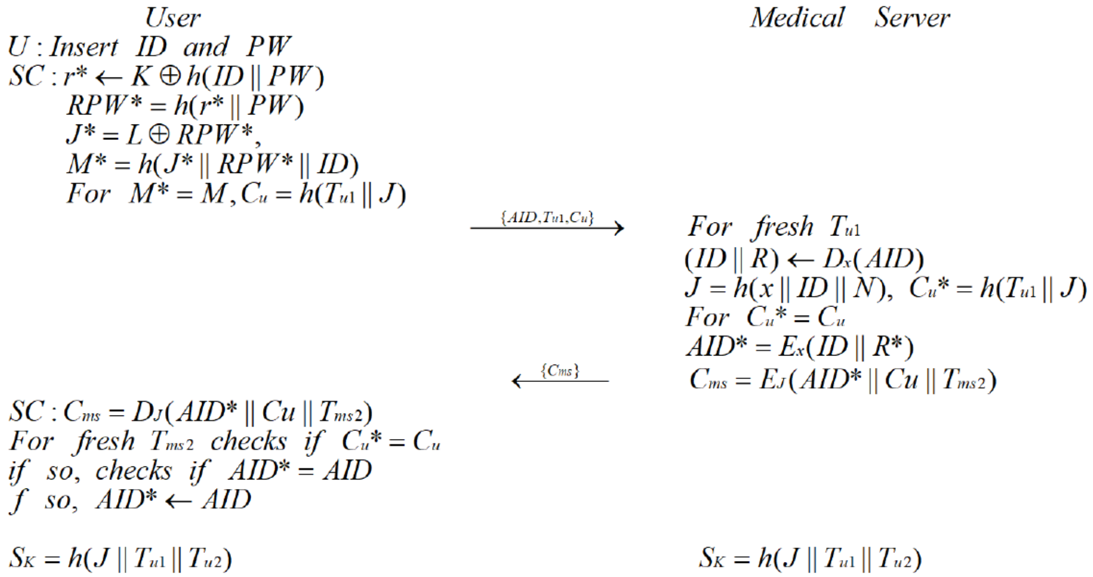
User
Medical Server
$U : Insert\ ID\ and\ PW$
$SC : r^* \leftarrow K \oplus h(ID \| PW)$
$RPW^* = h(r^* \| PW)$
$J^* = L \oplus RPW^*,$
$M^* = h(J^* \| RPW^* \| ID)$
$For\ M^* = M, C_u = h(T_{u1} \| J)$
$\{AID, T_{u1}, C_u\}$
$For\ fresh\ T_{u1}$
$(ID \| R) \leftarrow D_x(AID)$
$J = h(x \| ID \| N),\ C_u^* = h(T_{u1} \| J)$
$For\ C_u^* = C_u$
$AID^* = E_x(ID \| R^*)$
$\{C_{ms}\}$
$C_{ms} = E_J(AID^* \| Cu \| T_{ms2})$
$SC : C_{ms} = D_J(AID^* \| Cu \| T_{ms2})$
$For\ fresh\ T_{ms2}\ checks\ if\ C_u^* = C_u$
$if\ so,\ checks\ if\ AID^* = AID$
$f\ so,\ AID^* \leftarrow AID$
$S_K = h(J \| T_{u1} \| T_{u2})$
$S_K = h(J \| T_{u1} \| T_{u2})$

Figure 2: Login and Authentication Phase

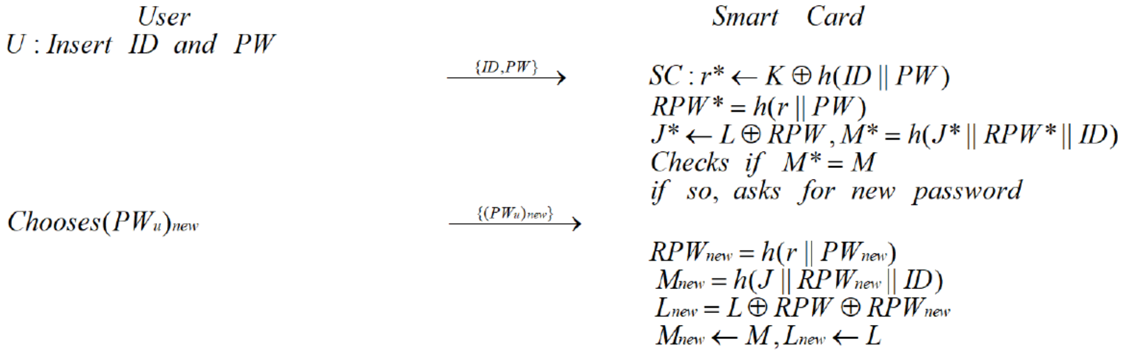
User
Smart Card
$U : Insert\ ID\ and\ PW$
$\{ID, PW\}$
$SC : r^* \leftarrow K \oplus h(ID \| PW)$
$RPW^* = h(r \| PW)$
$J^* \leftarrow L \oplus RPW, M^* = h(J^* \| RPW^* \| ID)$
$Checks\ if\ M^* = M$
$if\ so,\ asks\ for\ new\ password$
$Chooses(PW_u)_{new}$
$\{(PW_u)_{new}\}$
$RPW_{new} = h(r \| PW_{new})$
$M_{new} = h(J \| RPW_{new} \| ID)$
$L_{new} = L \oplus RPW \oplus RPW_{new}$
$M_{new} \leftarrow M, L_{new} \leftarrow L$

Figure 3: Password Change Phase

3 Weaknesses of Kumari et al.'s Scheme

3.1 Weakness 1: Lack of Forward Secrecy

First,We assume that A has obtained the master secret key x from the compromised server. And A eavesdropped messages $\{AID, T_{u1}, C_u\}$ and obtain the identity of U by decrypting AID.AID=$E_x(ID \| R)$,$D_x(AID) = (ID \| R)$. Then,A chooses a candidate N^* in sequence to check if $C_u = h(T_{u1} \| h(x \| ID \| N^*))$,where $C_u = h(T_{u1} \| J)$ and $J = h(x \| ID \| N)$. If it does not, the attacker repeats the process until the correct one is found. We think this discovery process is feasible because that the registration time as per user is very short integer.Next, the attacker can compute $J = h(x \| ID \| N)$,

$C_{ms} = E_J(AID* \parallel C_u \parallel T_{ms2})$,$D_J(C_{ms}) = (AID* \parallel C_u \parallel T_{ms2})$.Finally,$A$ can compute $S_k = h(J \parallel T_{u1}) \parallel T_{ms2})$.

3.2 Weakness 2: Stolen Smart Card Attack

We suppose that A has stolen SC. A can extract the message { L,AID,M,E_{key},D_{key},$h(\cdot)$,K} by differential power analysis.$J = L \oplus RPW$,$RPW = h(r \parallel PW)$ and $r = K \oplus h(ID \parallel PW)$ in registration phase. And A knows $M = h(J \parallel RPW \parallel ID) = h(L \oplus h(K \oplus h(ID \parallel PW) \parallel PW)) \parallel h(K \oplus h(ID \parallel PW) \parallel PW \parallel ID)$. Furthermore A computes $M^* = h(L \oplus h(K \oplus h(ID^{ast} \parallel PW^{ast}) \parallel PW^*) \parallel h(K \oplus h(ID^* \parallel PW^{ast}) \parallel PW^*) \parallel ID^*)$,where A selects an identity ID^* and a password PW^* respectively. If they are equal. A gets the correct identity and password. Otherwise, chooses another identity, password and repeats until he/she finds the correct answer.

3.3 Weakness 3: The Clock Synchronization Problem

As we know, there is no way to determine whether there is a delay in network traffic, so the timestamp does not protect the user from replay attacks. So, just use timestamp mechanism to resist replay attack is not suitable.

4 The Proposed Protocol

4.1 Registration Phase

During the registration phase, he/she will perform the following steps complete the registration (See Figure 4).

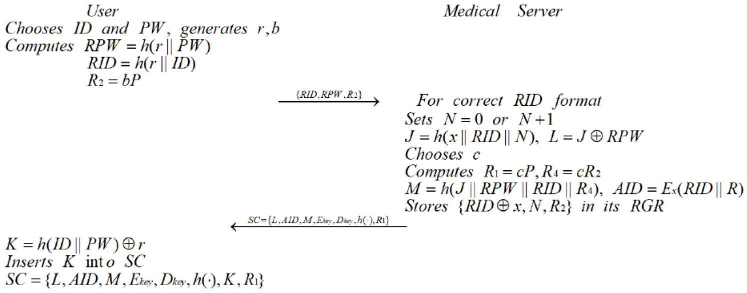
User
Medical Server
Chooses ID and PW, generates r,b
Computes RPW = h(r || PW)
RID = h(r || ID)
R2 = bP
{RID,RPW,R2}
For correct RID format
Sets N = 0 or N+1
J = h(x || RID || N), L = J ⊕ RPW
Chooses c
Computes R1 = cP, R4 = cR2
M = h(J || RPW || RID || R4), AID = Ex(RID || R)
Stores {RID ⊕ x, N, R2} in its RGR
SC={L,AID,M,Ekey,Dkey,h(·),R1}
K = h(ID || PW) ⊕ r
Inserts K int o SC
SC = {L, AID, M, Ekey, Dkey, h(·), K, R1}

Figure 4: Registration Phase

4.2 Login and Authentication Phase

Once M_S receives the login request from U, M_S and U will achieve mutual authentication (See Figure 5).

4.3 Password Change Phase

Figure 6 shows the password change phase of the proposed scheme.

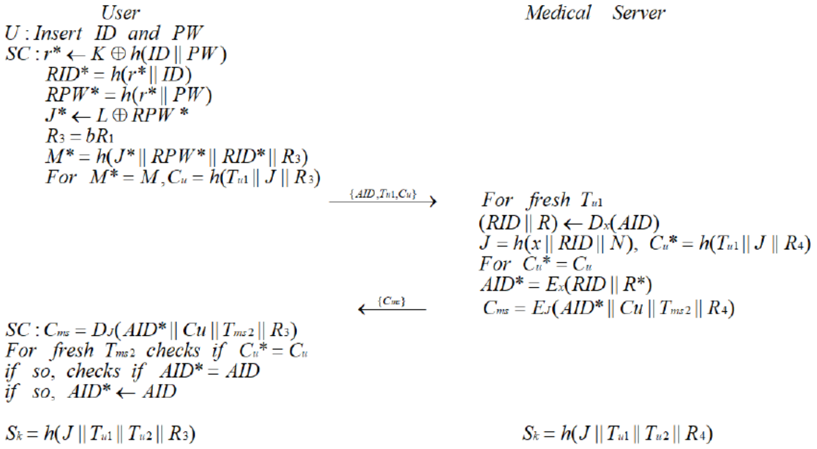
User
Medical Server
U : Insert ID and PW
SC : r* ← K ⊕ h(ID || PW)
RID* = h(r* || ID)
RPW* = h(r* || PW)
J* ← L ⊕ RPW *
R3 = bR1
M* = h(J* || RPW* || RID* || R3)
For M* = M, Cu = h(Tu1 || J || R3)
{AID, Tu1, Cu}
For fresh Tu1
(RID || R) ← Dx(AID)
J = h(x || RID || N), Cu* = h(Tu1 || J || R4)
For Cu* = Cu
AID* = Ex(RID || R*)
Cms = EJ(AID* || Cu || Tms2 || R4)
{Cms}
SC : Cms = DJ(AID* || Cu || Tms2 || R3)
For fresh Tms2 checks if Cu* = Cu
if so, checks if AID* = AID
if so, AID* ← AID
Sk = h(J || Tu1 || Tu2 || R3)
Sk = h(J || Tu1 || Tu2 || R4)

Figure 5: Login and Authentication Phase

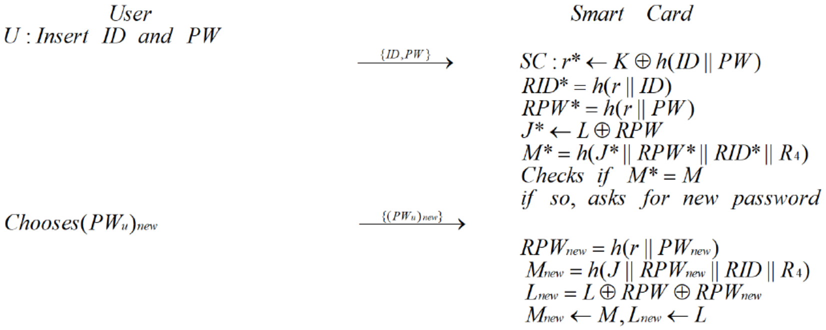

Figure 6: Password Change Phase

4.4 Revocation Phase

This part is the same as Kumari et al.'s scheme.

5 Security Analysis of the Proposed Scheme

1) Stolen smart card attack:
   We suppose that A has stolen SC,A can extract the message { L,AID,M,E_{key},D_{key},$h(\cdot)$,k,R_1} by differential power analysis. And A knows $M = h(J \parallel RPW \parallel RID \parallel R_4) = h(L \oplus h(K \oplus h(ID \parallel PW) \parallel PW)) \parallel h(K \oplus h(ID \parallel PW) \parallel PW \parallel RID \parallel R_4)$. Furthermore, A computes $M^* = h(L \oplus h(K \oplus h(ID^* \parallel PW^*) \parallel PW^*) \parallel h(K \oplus h(ID^* \parallel PW^*) \parallel PW^*) \parallel RID^* \parallel R_4)$,where $R_4 = bcP$.

2) Forward secrecy:
   The session key $SK = h(J \parallel T_{u1} \parallel T_{u2} \parallel bcP)$,where b,c are fresh in every conversation. In addition, the timestamp mechanism means that session messages are not maliciously delayed.

   The verifying of T_{u1}, T_{u2} and bcP can ensureare SK are valid. There will not be a problem that the attacker A can compute the session key.

3) Anonymous:
In this phase,$RPW = h(r \parallel PW), RID = h(r \parallel ID)$. ID is encrypted using a hash function, only $RPW$and RID are transmitted over secure channel. A cannot derive ID from RID.

4) Privileged insider attack:
The user only transmits the information {RID,RPW} security during the registration phase. A needs to know ID and r. But ID are not stored in SC and $r$is a random nonce.

5) Password change attack:
The user inserts ID and PW. The SC computes RPW^*, RID^*,and checks $M^* = M$ for equality. If A wants to change the password of SC, he/she has to know $M = h(J \parallel RPW \parallel RID \parallel R_4)$ .As mentioned above, it is impossible to guess bcP.

6) Session specific temporary information attack:
The timestamp mechanism ensures that the messages are instant. The verifying of T_{u1}, T_{u2} and bcP can ensure the attacker is not effective.

6 Security Analysis Using BAN Logic

In this section, the proposed protocol is formally security analyzed using BAN logic. Goals We use the BAN logic structure to prove that our proposed scheme can achieve mutual authentication.

Goal 1: User $\models (User \leftarrow \frac{SK}{} \rightarrow M_S)$.

Goal 2: Ms $\models (User \leftarrow \frac{SK}{} \rightarrow M_S)$.

Idealized form. The arrangement of proposed scheme to idealized form is as follows.

Message1:

$$User \rightarrow Ms : \{User \leftarrow \frac{SK}{} \rightarrow M_S, T_{u1}\}RID.$$

Message2:

$$Ms \rightarrow User : \{User \leftarrow \frac{SK}{} \rightarrow M_S, T_{u2}\}J.$$

Assumptions: We make the following assumptions to analyze our proposed scheme.

A1: User $\models (User \leftarrow \frac{J}{} \rightarrow M_S)$.

A2: $Ms \models (User \leftarrow \frac{J}{} \rightarrow M_S)$.

A3: $User \models \#(T_{u2})$.

A4: $Ms \models \#(T_{u1})$.

A5: $User \models M_S \Rightarrow (User \leftarrow \frac{SK}{} \rightarrow M_S)$.

A6: $Ms \models User \Rightarrow (User \leftarrow \frac{SK}{} \rightarrow M_S)$.

Based on the above assumptions and the rules of BAN logic, we will analyze the idealized form of the proposed scheme and the main steps of proof. From message1,we have:

$$Ms < \{User \leftarrow \frac{J}{} \rightarrow Ms, Tu\}RID.$$

From A2 and message-meaning rule, we have:

$$Ms \models User| : (User \leftarrow \overset{J}{-} \rightarrow M_S).$$

From A4 and freshnesss rules,we have:

$$Ms \models \#(User \leftarrow \overset{SK}{-} \rightarrow M_S, T_{u1}).$$

From $Ms \models User| : (User \leftarrow \overset{Sk}{-} \rightarrow Ms, T_{u1})$ and nonce verification rule, we have:

$$Ms \models User \models (User \leftarrow \overset{Sk}{-} \rightarrow M_S, T_{u1}).$$

From message judgement rule, we have:

$$Ms \models User \models (User \leftarrow \overset{Sk}{-} \rightarrow M_S).$$

From A6 and message judgement rule, we have:

$$Ms \models (User \leftarrow \overset{Sk}{-} \rightarrow Ms). \quad \text{(Goal 2)}$$

From message2, we have:

$$User < | : (User \leftarrow \overset{Sk}{-} \rightarrow Ms, T_{u2}J.$$

From A1 and message-meaning rule, we have:

$$User \models Ms| : (User \leftarrow \overset{Sk}{-} \rightarrow Ms, T_{u2}).$$

From A3 and freshness rules, we have:

$$User \models \#Ms| : (User \leftarrow \overset{Sk}{-} \rightarrow Ms, T_{u2}).$$

From $User \models Ms| : (User \leftarrow \overset{Sk}{-} \rightarrow Ms, T_{u2})$ and nonce verification rule, we have:

$$User \models Ms \models (User \leftarrow \overset{Sk}{-} \rightarrow Ms, T_{u2}).$$

From message judgment rule, we have:

$$User \models Ms \models (User \leftarrow \overset{Sk}{-} \rightarrow Ms).$$

From A5 and message judgment rule, we have:

$$User \models (User \leftarrow \overset{Sk}{-} \rightarrow Ms). \quad \text{(Goal 1)}$$

7 Performance Comparison and Efficiency Analysis

According to the Tables 2 and 3, the proposed agreement adds a small amount of computing and provides more security.

Table 2: Performance comparison

Performance	Kumari et al.(2013)	Islam and Khan(2014)	Chaudhry et al.(2015)	Ours
F1	No	No	No	Yes
F2	No	Yes	No	Yes
F3	Yes	No	No	Yes
F4	Yes	No	No	Yes
F5	Yes	Yes	No	Yes
F6	Yes	Yes	Yes	Yes
F7	Yes	No	Yes	Yes
F8	Yes	No	Yes	Yes
F9	Yes	Yes	Yes	Yes
F10	Yes	No	No	Yes
F11	Yes	No	No	Yes
F12	Yes	No	Yes	Yes

F1: Forward secrecy; F2: Stolen smart card attack; F3: Man-in-middle attack; F4: User impersonation attack; F5: Stolen verifier attack; F6: Ensure user anonymity; F7: Replay attack; F8: Insider attack; F9: Mutual Authentication; F10: Off-line password guessing attack; F11: Server impersonation attack; F12: On-line password guessing attack.

Table 3: Comparison regarding computation costs

Performance	Kumari et al.(2013)	Islam and Khan(2014)	Chaudhry et al.(2015)	Ours
User	$5T_h + T_{fun}$	$5T_h + T_{fun}$	$5T_h + T_{fun}$	$5T_h + T_{fun}$
Solver	$5T_h + T_{fun}$	$5T_h + T_{fun}$	$5T_h + T_{fun}$	$5T_h + T_{fun}$
Total	$5T_h + T_{fun}$	$5T_h + T_{fun}$	$5T_h + T_{fun}$	$5T_h + T_{fun}$

T_h=Time to compute a one-way hash function; T_{fun}=Time to compute a symmetric encryption or decryption function [9]; T_{mul}=Time complexity of a point multiplication operation on elliptic [2].

8 Conclusions

In this paper, we analyze Kumari et al.'s scheme. First of all, it goes without saying that their schemes are very worthy of our learning, but we believe that both of them can be further improved. Kumari et al.'s solution has several problems, such as the inability to provide forward confidentiality, clock synchronization problems, and so on. Through the analysis of Kumari et al.'s scheme, we further improved it and proposed our own scheme. Our improved protocols are based on CDH and timestamp mechanisms, primarily to improve security. We use elliptic curves to speed up the calculation. Compared with the analysis of other protocols, it can be seen that the improved authentication protocol has higher security.

Acknowledgments

This work was supported in part by the 2018 "Research and Development and Application of Limb Local Drug Delivery Dialysis Device" of the seed fund program of Shanghai university of medicine & health Sciences (SFP-18-21-14-001). The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] D. S. AbdElminaam, "Improving the security of cloud computing by building new hybrid cryptography algorithms," *International Journal of of Electronics and Information Engineering*, vol. 8, no. 1, pp. 40-48, 2018.

[2] G. R. Alavalapati, G. Reddy, A. K. Das, E. J. Yoon, and K. Y. YOO, "A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptography," *IEEE Access*, vol. 4, pp. 4394-4407, 2016.

[3] U. Anliker, A. Ward J, P. Lukowicz, *et al.*, "AMON: A wearable multiparameter medical monitoring and alert system," *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 4, pp. 415-427, 2004.

[4] M. U. Aslam, A. Derhab, *et al.*, "A survey of authentication schemes in telecare medicine information systems," *Journal of Network and Computer Applications*, vol. 41, 2017.

[5] M. Bedoui, B. Bouallegue, B. Hamdi, Mohsen Machhout, "An Efficient Fault Detection Method for Elliptic Curve Scalar Multiplication Montgomery Algorithm," in *IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS'19)*, 2019.

[6] C. C. Chang, and T. C. Wu, "A password authentication scheme without verification tables," in *8th IASTED International Symposium of Applied Informatics*, Innsbruck, Austria, pp. 202–204, 1990.

[7] S. A. Chaudhry, "Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems," *Journal of Medical Systems*, vol. 39, no. 6, pp.1–11, 2015.

[8] H. Debiao, C. Jianhua, and Z. Rui, "A more secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1989–1995, 2012.

[9] W. Fan, H. T. Pai, X. X. Zhu, P.Y. Hsueh and Y. H. Hu, "An adaptable and scalable group access control scheme for managing wireless sensor networks," *Telematics and Informatics*, vol. 30, no. 2, pp. 144-157, 2013.

[10] S. Gradl, P. Kugler, C. Lohmuller, *et al.*, "Real-time ECG monitoring and arrhythmia detection using Android-based mobile devices," in *34th Annual International Conference of the IEEE Engineering-in-Medicine-and-Biology-Society (EMBS)*, San Diego, CA, pp. 2452-2455, 2012.

[11] C. Hutchinson, J. Ward, K. Castilon, "Navigating the next-generation application architecture," *IT Professional*, vol. 1, no. 2, pp. 18–22, 2009.

[12] M. S. Hwang, H. W. Yang and C. Y. Yang, "An Improved Hou-Wang's User Authentication Scheme," in *Information Science and Applications*, Lecture Notes in Electrical Engineering, vol. 514, 2018.

[13] M. S. Hwang, E. F. Cahyadi, Y. C. Chou, C. Y. Yang, "Cryptanalysis of Kumar's Remote User Authentication Scheme with Smart Cards," in *14th International Conference on Computational Intelligence and Security (CIS'18)*, pp. 416-420, 2018.

[14] T. Hwang, Y. Chen, and C. J. Laih, "Non-interactive password authentications without password tables," in *IEEE Region 10 Conference on Computer and Communication Systems (IEEE TENCON'90)*, pp. 429–431, 1990.

[15] S. K. H. Islam, and M. K. Khan, "Cryptanalysis and improvement of authentication and key agreement protocols for telecare medicine information systems," *Journal of Medical Systems*, vol. 38, no. 10, pp. 1–16, 2014.

[16] S. G. Jin, G. J. Wang, "Design of Digital Signature Scheme Based on Elliptic Curve Cryptosystem," *Applied Mechanics and Materials*, vol. 685, pp. 579-582, 2014.

[17] S. Kumari, M. K. Khan, and R. Kumar, "Cryptanalysis and improvement of a privacy enhanced scheme for telecare medical information systems," *Journal of Medical Systems*, vol. 37, no. 4, pp. 1–11, 2013.

[18] L. Lamport, "Password authentication with insecure communication," *Communications of ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[19] L. Liu, Z. Z. Guo, *et al.*, "An improvement of one anonymous identity-based encryption scheme," *International Journal of of Electronics and Information Engineering*, vol. 9, no.1, pp. 11-21, 2018.

[20] M. Masdari, S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems," *Journal of Network Computation Applications*, vol. 87, pp. 1-19, 2017.

[21] U. Qidwai, J. Chaudhry, S. Jabbar, *et al.*, "Using casual reasoning for anomaly detection among ECG live data streams in ubiquitous healthcare monitoring systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 10, pp. 4085-4097, 2018.

[22] S. Qiu, G. Xu, H. Ahmad, *et al.*, "A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems," *IEEE Access*, vol. 6, pp. 7452-7463, 2017.

[23] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[24] J. Wei, X. Hu, and W. Liu, "An improved authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 6, pp. 3597–3604, 2012.

[25] Z. Y. Wu, *et al.*, "A secure authentication scheme for telecare medicine information systems," *Journal of Medical Systems*, vol. 36, no. 3, pp. 1529–1535, 2012.

[26] X. Xu, *et al.*, "A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems," *Journal of Medical Systems*, vol. 38, no. 1, pp.1–7, 2013.

[27] L. Zhang, S. Tang, Z. Cai, "Efficient and flexible password authenticated key agreement for voice over internet protocol session initiation protocol using smart card," *International Journal of Commun. Syst.*, vol. 27, no. 11, pp. 2691–2702, 2014.

Biography

Liu Wanrong received her bachelor's degree in electrical engineering and automation from Luoyang Institute of Technology in 2018. Now, she is a student at the College of Engineering Science and

Technology, Shanghai Ocean University. Her main research is communication security and Internet of things technology.

He Xin received his bachelor's degree in mechanical engineering from Anhui Polytechnic University in 2018. Now, he is a student at the College of Engineering Science and Technology, Shanghai Ocean University. He main research is Internet of things technology.

Ji Zhiyong received his bachelor's degree from Nanjing University of Aeronautics and Astronautics in 2012. He received his MS degree Jiangsu University in 2017. He is the master's supervisor of mechanical engineering of Shanghai Ocean University. He is also the medical equipment senior engineer and deputy director of Shanghai Sixth People's Hospital East. His research directions include the development and application of wearable medical devices based on the Internet of things and the information security of the medical Internet of things.