ECC-Based Lightweight Authentication And Access Control Scheme For IoT E-Healthcare

Hailong Yao (hailong.yao@outlook.com)
Lanzhou City University https://orcid.org/0000-0002-0638-8494
Qiao Yan
Shenzhen University
Xingbing Fu
Hangzhou Dianzi University
Zhibin Zhang
Lanzhou City University
Caihui Lan
Lanzhou City University

Research Article

Keywords: authentication, key agreement, access control, healthcare

Posted Date: April 26th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-210016/v1

Version of Record: A version of this preprint was published at Soft Computing on November 26th, 2021.
See the published version at https://doi.org/10.1007/s00500-021-06512-8.

Noname manuscript No.
(will be inserted by the editor)

ECC-based lightweight authentication and access control scheme for IoT E-healthcare

Hailong Yao[1] · Qiao Yan[2] · Xingbing Fu[3] · Zhibin Zhang[1] · Caihui Lan[1]

Received: date / Accepted: date

Abstract The E-healthcare system has a complex architecture, diverse business types, and sensitive data security. To meet the secure communication and access control requirements in the user-medical server, user-patient, patient-medical server and other scenarios in the E-healthcare system, secure and efficient authenticated key agreement and access authorization scheme need to be studied. However, the existing multi-server solutions do not consider the authentication requirements of the Wireless Body Area Network(WBAN), and are not suitable for user-patient, patient-medical server scenarios; most of the existing WBAN authentication scheme are single-server type, which are difficult to meet the requirements of multi-server applications; the study of user-patient real-time scenarios has not received due attention. This work first reveals the structural flaws and security vulnerabilities of the existing typical schemes, and then proposes an authentication and access control architecture suitable for multiple scenarios of the E-healthcare system with separate management and business, and designs a novel ECC-based multi-factor remote authentication and access control scheme for E-healthcare using physically uncloneable function (PUF) and hash. Security analysis and efficiency analysis show that the new scheme has achieved improved functionality and higher security while maintaining low computational and communication overhead.

Keywords authentication · key agreement · access control · healthcare

✉ Qiao Yan
yanq@szu.edu.cn

[1] School of Electronic and Information Engineering, Lanzhou City University, 730070, Lanzhou, China

[2] College of Computer Science and Software Engineering, Shenzhen University, 518060, Shenzhen, China

[3] School of Cyberspace, Hangzhou Dianzi University, 310018, Hangzhou, China

1 Introduction

In the near future, the medical industry will incorporate more artificial intelligence, sensor technology and other high technologies to create smart hospital systems, regional health systems and home health systems. They will use advanced Internet of Things technology, cloud computing technology, big data technology and artificial intelligence technology to achieve seamless interaction between patients and medical staff, medical institutions, medical equipment, and make medical services truly digital and intelligent. Through the wireless network, the portable PDA is used to easily connect various diagnostic and therapeutic instruments, so that medical staff can grasp the patient's medical record information and the latest diagnostic report at any time, and quickly formulate a diagnostic program anytime, anywhere; authorized medical staff and family members of patients can access the telemedicine server at any time and any place to query medical image data and medical orders; the patient's referral information and medical records can be accessed through medical networking at any hospital; special groups such as chronic diseases, old and young patients, mental retardation, disability, and infectious diseases can be monitored and taken care of through the telemedicine system.

For secure communication and access control among all these entities, we need a secure mutual authenticated key agreement and access authorization mechanism which can provide authentication among body sensors and personal gateways, personal gateways and health servers, personal gateways and users (i.e. medical staff and family members of patients), and health servers and users, and can provide authorization for users and patients to access medical servers, and users to access patient sensors. However, due to the complex network structure of E-healthcare system (the server side is mostly secure and stable Ethernet, the user side is mostly WLAN or cellular mobile communication network, and the patient side is wireless sensor network), some nodes are resource-constrained devices (most medical servers are high-performance server cluster or cloud server, the user-side devices are mostly personal computers or mobile smart terminals, except for the relatively rich gateway on the patient side, the remaining sensors and other devices are cheap terminals with limited batteries, storage and computing power, the interaction data involves individuals privacy (such as patient's name, home address, medical records, blood test results, DNA sequence and other sensitive data) and other characteristics, so existing authentication and authorization scheme cannot be directly applied to E-healthcare system.

1.1 Motivation

The drawbacks of existing scheme include tow aspects: architecture flaws and security vulnerability.

1) Session key initialization between users and patients require the assistance of a particular medical server, which is not in line with the design concept of separation of management and application.
2) Single server mode, can not meet the application needs of a multi-server environment. Common multi-server authentication schemes [33,38,30,8,23,39,21, 36,15,14] can meet the authentication or authorization requirements of the user-server scenario, but no multiple solution is proposed, and many schemes [33,23,36] that do not use the public key system suffer from the vulnerability of anonymity [11,10].
3) There are fewer schemes for the patient-server scenario, and most existing schemes [13,32,5,17,22,19] are in the WBAN-server mode.
4) There are few schemes for the patient-user scenario. The only few schemes also adopt the patient-server-user mode, which does not meet the requirements of separation of management and business [22,40].
5) There are still some general security flaws in the existing schemes. Most schemes [33,23] that do not use public key cryptography suffer from the vulnerability of anonymity [36,10]. Some schemes [30,23] have lost their forward security due to ephemeral secrets being acquired by adversary [15]. Some schemes [30, 23,37] are vulnerable to smart card loss attacks due to poor secret packaging in smart card, which can lead to offline dictionary attack, causing the schemes can not resist user impersonation attack or device impersonation attack [9,15,16].

To overcome the above challenges, this work uses PUF and biohash based on ECC cryptography to propose a secure and efficient multi-server authentication and access control scheme for E-healthcare. This proposal can provide mutual authentication and access authorization for entities in the E-healthcare systems.

1.2 Our Contributions

The contributions of this article are summarized below.

1) We cryptanalyze existing authentication schemes such as LACO [13], revealing the reasons why their anonymity and forward security are vulnerable and cannot resist user impersonation or device impersonation attacks.
2) We first proposed a multiple solution architecture for authentication and authorization in user-server, patient-server, user-patient and other scenarios in E-healthcare.
3) Based on the above architecture, we combine PUF-based patient WBAN authentication with ECC-based remote multi-server authentication, and use a hash function to design a remote authentication and access control scheme that integrates three factors of identity, password and biometric, named SEMAS.
4) Formal security proof, non-formal security analysis, comparative analysis of functional and security properties, comparative analysis of computing efficiency and communication efficiency are given.

1.3 Paper Outline

The rest of this work is organized as follows. In Section 2, we briefly discuss the related work. Basic notations, ECC security assumptions, physically uncloneable function, communication model and threat model definition will be described in Section 3. The LACO is reviewed and its weaknesses are analyzed in Sections 4 and 5, respectively. We describe the details of our

scheme in Section 6. The security analysis and performance evaluation will be given in Sections 7 and 8, respectively.Finally, we present our conclusions in Section 9.

2 Literature Review

Authentication and access control schemes can be classified into symmetric cryptography based schemes and public key cryptography based schemes according to the cryptography they rely on. Although symmetric cryptography based schemes is generally computationally efficient, it is almost difficult to effectively achieve strong anonymity[10,16]. Therefore, authentication and access control schemes with privacy protection are usually designed based on public key cryptography. However, most public key cryptography based schemes are difficult to apply to the IoT environment due to high overhead, such as RSA-based schemes[23,24], bilinear-pairing-based schemes[25,26], and chaotic-maps-based schemes[27,28]. In the IoT scenario, the short key feature of ECC cryptography gives it an advantage in balancing resources and efficiency.

In 2010, Yang and Yang propose the first three-factor [6] EDLP-based authenticated key exchange scheme. In the same year, Yoon and Yoo propose another EDLP-based three-factor authenticated key exchange scheme [12]. However, He et al. show that Yoon and Yoo's scheme cannot resist insider attack and hardware factor loss attack [7], and give an improvement [8]. In 2015, Odelu et al. show that He et al. scheme's anonymity is vulnerable and cannot resist replay attack and user impersonation attack [39]. Chuang et al. also show that the anonymity problem of Yoon-Yoo's scheme and use a random number and hash function to construct a lightweight improvement scheme [2]. In 2017, Kumari et al. show that Chuang et al.'s scheme can not resist intermediate data attacks, user impersonation attack and forward security attack, and propose an improvement using digital signature [34,35]. In 2018, Feng et al. [30] show that Kumari et al.'s scheme [35] is vulnerable to user anonymity and impersonation attacks, and an improvement is given. However, Yao et al. show that Feng et al.'s scheme is vulnerable to anonymity and cannot resist ephemeral secrets leak attacks, and causing replay attacks and session key security attacks [14]. In 2018, Lwamo et al.[23] find that Kumari-Om's scheme[35] used too many exponential operations, resulting in excessive computational overhead. They propose a new RSA based remote authentication scheme for the single and multi-server environments to achieve lower computational overhead and higher security. However, Yao et al. show that the anonymity of Lwamo et al.'s scheme is vulnerable and can not resist hardware loss attack, so incurred offline dictionary attack and user impersonation attack [15]. In 2018, Zhang et al. [19] propose a three-factor authenticated key agreement scheme for E-health systems to protect user privacy through the use of a dynamic authentication mechanism. In 2019, Aghili et al. [13] show that Zhang et al.'s scheme suffers from several attacks including de-synchronization attack, denial of service attack, and insider attacks, and propose an improvement scheme named LACO. Recently, we find that although LACO solve some of the security problems of Zhang et al.'s scheme, and also consider the ownership transfer in access control, there are security vulnerability and algorithm errors.

Table 1: Notations Used in This Paper

Notations	Descriptions
ID_i / PW_i / B_i	i^{th} user's ID/Password/Biometric
Cr_i / UD_i	i^{th} user's Credential/Device
ID_j / Cr_j	j^{th} server's ID/Credential
ID_k / PW_k	k^{th} patient's ID/Password
B_k / Cr_k	k^{th} patient's Biometric/Credential
ID_l^k	l^{th} device of k^{th} patient
$R = PUF_l(C)$	device's physically uncloneable function
RA / pk / sk	Registration center/Public & secret key
L_P / L_U / L_S	Registry of patient, user and sever
$h(\cdot)$	Cryptographic hash algorithm
$h_b(\cdot)$	Biohash algorithm
$HD(\cdot)$	Hamming distance
δ	Hamming distance threshold
D_{PW} / D_H	Distribution of password and hash value
T_i / ΔT / ΔL	i^{th} Timestamp/Time threshold/TTL
$\oplus$ / $\|$	XOR operator/Concatenation operator
$\leftarrow$ / $\perp$	Normal output/Abnormal output
$\xleftarrow{\$}$	Random sampling from the distribution

3 Preliminaries and Background

In this section, we describe the preliminaries which is necessary to understand the rest of this work.

3.1 Notation

Notations used in this paper and their descriptions are shown in Table 1.

3.2 EDLP & ECDH

The elliptic curve over the finite field F_p is a finite cyclic group G satisfying $y^2 = x^3 + ax + b\,(modp)$ and containing the infinity point $\mathcal{O}$. Where, $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0\,(\mathrm{mod}p)$ [29]. There are two operations of

addition and scalar multiplication on G, and the scalar multiplication is defined as the same point accumulation.

The cryptosystem constructed using the elliptic curve discrete logarithm problem (EDLP) and the elliptic curve Diffie-Hellman problem (ECDH) is widely used in security protocols. The security assumptions of the EDLP and ECDH are given by the following two lemmas, for any Probability Polynomial Time (PPT) adversary $\mathcal{A}$:

Definition 3.1 EDLP Security Assumption: Given $k \in Z_p$ and $P \in G$, it is easy to calculate $Q = kP \in G$, but given P, $Q \in G$, the advantage $Adv_{DELP}(\mathcal{A})$ for solving $k \in Z_p$ is bounded by the negligible probability $negl(\lambda)$.

Definition 3.2 ECDH Security Assumption: Given P, yP and $xP \in G$, but unknown x or $y \in Z_p$, the advantage $Adv_{ECDH}(\mathcal{A})$ for solving $xyP \in G$ is bounded by the negligible probability $negl(\lambda)$.

3.3 Physically Uncloneable Function

A physically uncloneable function is a physical circuit that maps unique challenge C to unique response R based on the random variations introduced by the chip manufacturing process [3]. The $R = PUF_l(C)$ of device l is correct if:

1) $Pr\left[HD\left(PUF_l(C_i), PUF_l(C_j)\right)_{1\le i,j\le n, i=j} > \delta\right] < negl(\lambda)$;
2) For any $PUF_l(\cdot)$ and $PUF_{l'}(\cdot)$, $Pr\left[HD\left(PUF_l(C_i), PUF_{l'}(C_j)\right)_{1\le i,j\le n, i=j} \le \delta\right] \ge 1 - negl(\lambda)$.

The $R = PUF_l(C)$ of device l is secure if:

1) $Pr\left[\hat{H}\left(PUF_l(C_i), PUF_l(C_j)\right)_{1\le i,j\le n, i\ne j} > \epsilon\right] > 1 - negl(\lambda)$, which means that the min-entropy of the $PUF_l(\cdot)$ output is always larger than ϵ with high probability.

3.4 Communication Model

In a multi-server scenario, medical servers, patients, and users need to register with a registration authority (RA). The local RA is responsible for the management and access authorization of servers, users, and patients in the region, and the central RA (CRA) is responsible for the management of region AR and the authentication and authorization between regions. Medical servers such as Electronic Medical Records (EMR) and Hospital Information Systems (HIS) work in central computer rooms with relatively high security. Users such as medical staff, academics, and patients in wards, homes, jobs, and streets need to access the medical server or access each other through the Internet. As shown in Figure 1, Patients and users can access the medical servers after the authentication and authorization obtained by the RA, and users can access the patient's sensors after the authentication and authorization obtained by the RA.

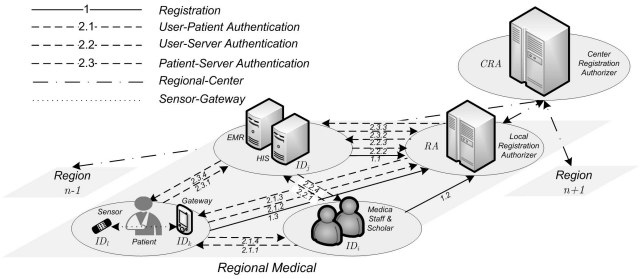

Fig. 1: Communication Model of This Proposal

3.5 Threat Model

According to the widely accepted Dolev-Yao threat model [4] and the Canetti-Krawczyk adversary model [31], the adversary $\mathcal{A}$ attacking E-healthcare multi-server scheme has the ability to fully control the channel and get ephemeral secrets of the session. Adversary capabilities include:

1) $\mathcal{A}$ can interfere with communication between entities by means of interception, modification, deletion, insertion, etc.
2) Medical server, patient gateway, and sensor are unreliable, and $\mathcal{A}$ can learn long-term secrets from the captured devices.
3) $\mathcal{A}$ has the ability to obtain ephemeral secrets of the incompletely corrupted object.
4) All servers are honest and curious.

4 Review of LACO Scheme

In order to facilitate the understanding of the subsequent cryptanalysis of LACO, in this section we briefly review the registration and authentication process of it [13].

4.1 Registration

As shown in Figure 2, when the LACO system is initialized, the server generates system parameters and issues

written secrets sensor to the patient. When the user registers, the server issues the smart card for subsequent authentication.

4.2 Authentication and Session Key Agreement

As shown in Figure 3, LACO needs to perform smart card login authentication locally before initiating remote authentication, and then sends an authentication request to the server after login. If the authentication passes, the server forwards the relevant information to the sensor. If the authentication passes, the sensor calculates the session key and directly sends an authentication key agreement request to the user. If the authentication passes, the user calculates the session key.

5 Cryptanalysis of LACO Scheme

The drawbacks of LACO scheme include three aspects: architecture flaws, fatal algorithm error and security vulnerability.

5.1 The Architecture Flaws of LACO

A lame system architecture does not meet the needs of future E-healthcare applications.

1) Session key initialization between medical staff and patients requires the assistance of a particular medical server, which is not in line with the design concept of separation of management and application.
2) Single server mode, can not meet the application needs of a multi-server environment. And dynamic updates and revocations of medical staff, patients, and medical servers are not considered.

5.2 Fatal Algorithm Error in LACO

There is fatal algorithm error in the LACO scheme, causing the protocol to fail to run as expected. In *Step2*, the server needs to find the $\{X_{ni}, Z_{nl}\}$ that satisfies $h_3 = X_{ni}\|Z_{nl}$ or $h_3 = h\left(r_i\|X_{ni}\|Y_{ni}^{'}\right)\|h\left(r_i\|Y_{ni}^{'}\|Z_{nl}\right)$ from the user registration information, calculates $K_u^{'} = h_1 \oplus h\left(X_{ni}\|Y_{ni}\|T_1\right)$ and $ID_l^{'} = h_2 \oplus h\left(X_{ni}\|Y_{ni}\|Z_{nl}\|T_1\right)$ to verify whether $h_4 \leftarrow h\left(h_1\|h_2\|h_3\|K_u\|ID_l\|T_1\|r_i\right)$ is true, and then achieves authentication of ID_i. Although, ID_j and ID_i updated

$$X_{(n+1)i} = h\left(h\left(r_i\|X_{ni}\right) \oplus r_i \oplus Y_{ni}^{'}\right),$$
$$Z_{(n+1)l} = h\left(Y_{ni}^{'}\|X_{ni}\right) \oplus A_l$$

in *Step4* and *Step5* respectively. However, B_{ni} has not been updated in the user's smart card, which means that ID_i calculates

$$h_3^{n+1} = h\left(r_i\|X_{(n+1)i}\|Y_{ni}^{'}\right)\|h\left(r_i\|Y_{ni}^{'}\|Z_{(n+1)l}\right)$$

in n+1 rounds because $Y_{ni}^{'} = B_{ni} \oplus h\left(ID_i^{'}\|PW_i^{'}\|h_b\left(B_i^{'}\right)\right)$ and B_{ni} is still the old one. However, the server calculates

$$h_3^{n+1} = h\left(r_i\|X_{(n+1)i}\|Y_{(n+1)i}^{'}\right)\|h\left(r_i\|Y_{(n+1)i}^{'}\|Z_{(n+1)l}\right)$$

because it calculates

$$Y_{(n+1)i}^{'} = h\left(X_{(n+1)i}\|sk\right).$$

Obviously

$$h\left(r_i\|X_{(n+1)i}\|Y_{ni}^{'}\right)\|h\left(r_i\|Y_{ni}^{'}\|Z_{(n+1)l}\right) \neq$$
$$h\left(r_i\|X_{(n+1)i}\|Y_{(n+1)i}^{'}\right)\|h\left(r_i\|Y_{(n+1)i}^{'}\|Z_{(n+1)l}\right)$$

, so the protocol is aborted here.

5.3 The Security Drawbacks of LACO

In addition to architectural flaws and algorithm error, LACO also has security flaws such as lack of session key privacy, can not resist user impersonation attack, multi-factor security and forward security vulnerability.

1) **Lack of session key privacy**: During the authentication and key agreement phase of LACO, The server is able to calculate the session key $ss_s = h\left(A_l\|ID_l^{'}\|K_u^{'}\|K_p^{'}\right)$ between the user and the patient.
2) **Can not resist user impersonation attack**: If the adversary $\mathcal{A}$ obtains the secret $\{ID_l, Cr_l\}$ in the sensor's memory, s/he can bypass the server authentication, impersonating the server to forge M_2^* to pass the ID_l authentication and establish a session with it. Details are as follows:
Step1: $\mathcal{A}$ generates A_l^* and K_u^*;
Step2: $\mathcal{A}$ calculates

$$h_5^* = A_l^* \oplus h\left(Cr_l\|T_2\right),$$
$$h_6^* = A_l^* \oplus K_u^*,$$
$$h_7^* = h\left(A_l^*\|ID_l\|K_u^*\|T_2\right),$$
$$M_2^* = \{h_5^*, h_6^*, h_7^*, T_2\},$$

and sends M_2^* to ID_l;
Step3: If $T_3 - T_2 \leq \Delta T$, ID_l calculates

$$A_l^* = h_5^* \oplus h\left(Cr_l\|T_2\right),$$
$$K_u^* = A_l^* \oplus h_6^*,$$

and if $h_7^* = h\left(A_l^*\|ID_l\|K_u^*\|T_2\right)$ is true, then generates K_p and calculates

Patient's sensor$(NULL)$	**Medical server**(sk)
registration request	
	selects device identity ID_l, $Cr_l \leftarrow h(ID_l \| sk)$ writes $\{ ID_l, Cr_l \}$ into ID_l's memory and issue it
User(ID_i, PW_i, B_i)	**Medical server**(sk)
selects identity ID_i $\xrightarrow[ID_i \ 2 \ ID_j]{ID_i}$	
	if ID_i is valid generates r_s $X_{0i}, Z_{0l} \leftarrow NULL$ $X_{1i} \leftarrow h(UD_i \| ID_i \| r_s)$ $Y_{1i} \leftarrow h(X_{0i} \| sk)$ $Z_{1l} \leftarrow h(X_{0i} \| Y_{0i}) \oplus A_l$ writes $\{ X_{0i}, Z_{0l}, X_{1i}, Z_{1l} \}$ into R_U writes $\{ X_{1i}, Y_{1i}, Z_{1l}, h_b(\cdot) \}$ into smart card UD_i and issues it to ID_i
$A_{1i} \leftarrow h_b(B_i) \oplus h(PW_i \| ID_i)$ $B_{1i} \leftarrow Y_{1i} \oplus h(ID_i \| PW_i \| h_b(B_i))$ $flag \leftarrow 0$ writes $\{ A_{1i}, B_{1i}, flag \}$ into UD_i and deletes Y_{1i}	

Fig. 2: Registration Phase of LACO Scheme

$$ss_p = h(A_l^* \| ID_l \| K_u^* \| K_p),$$
$$h_8 = h(ss_p \| Cr_l \| T_3),$$
$$h_9 = K_u^* \oplus K_p,$$
$$M_3 \leftarrow \{h_8, h_9, T_3\},$$

and sends M_3 to $\mathcal{A}$;

Step4: $\mathcal{A}$ calculates $K_p = h_9 \oplus K_u^*$ and $ss_{\mathcal{A}} = h(A_l^* \| ID_l \| K_u^* \| K_p)$ after receiving M_3, A session between $\mathcal{A}$ and the patient is established.

3) **Multi-factor security vulnerability**: When $\mathcal{A}$ knows the biometric B_i and the smart card secret $\{A_{1i}, B_{1i}, X_{ni}, Y_{ni}\}$, although LACO has anonymity, since the user ID and password are low-entropy short strings, the probability that $\mathcal{A}$ guesses the user password 100 times is 32% – 73% [11]. When $\mathcal{A}$ knows the user password PW_i and the smart card secrets $\{A_{1i}, B_{1i}, X_{ni}, Y_{ni}\}$, $\mathcal{A}$ can use a centre search attack to derive the user's biometric information [18].
4) **Forward security vulnerability**: Once the sensor's secret information is leaked, $\mathcal{A}$ will be able to derive the session key between the user and the patient from the captured M_3 and M_4. Details are as follows:

Step1: $\mathcal{A}$ calculates $A_l = h_5 \oplus h(Cr_l \| T_2)$, $K_u = A_l \oplus h_6$, $K_p = K_u \oplus h_9$; and $M_2^* = \{h_5^*, h_6^*, h_7^*, T_2\}$, and sends M_2^* to ID_l;

Step2: If $h_7 = h(A_l \| ID_l \| K_u \| T_2)$ and $h_8 = h(ss_p \| Cr_l \| T_3)$, there must be $ss_{\mathcal{A}} = h(A_l \| ID_l \| K_u \| K_p)$.

6 Proposed Scheme

To overcome the security architecture flaws and security drawbacks of previous authentication protocols such as the LACO [13] adopted for E-health systems, we propose a secure and efficient protocol called SEMAS. In addition to providing preserving-privacy mutual authentication, key agreement, and access control, resisting known Internet attacks, the proposal also meets the authentication and access control requirements of the E-healthcare multi-server scenario.

The proposed scheme consists of six important phases: Initialization, Registration, Authentication and Key Agreement, Password Update and Ownership Transfer.

6.1 Initialization

RA initializes the system parameters, it selects a finite field F_p with a large prime p as the order, and defines an elliptic curve E_p over it, then selects an additive group $\mathbf{G}$ with order q and generator P over E_p, and then selects the system private key $sk \in F_p$, and computes the public key $PK = skP$; finally, RA selects the secure hash algorithm $h(\cdot)$, the biohash algorithm $h_b(\cdot)$ and physically uncloneable function algorithm $PUF(\cdot)$, and publishes the public parameters $\{P, PK, E_p, h(\cdot), h_b(\cdot)\}$.

6.2 Registration

As shown in Figure 4, during the registration phase, medical servers, users, and patients need to register with the RA in a secure manner. Details are as follows:

6.2.1 Medical Server Registration

1) Server selects ID ID_j and sends tuple $\{ID_j\}$ to RA.

User(ID_i, PW_i, B_i)	**Medical server**(sk)	**Patient's sensor**(ID_l, Cr_l)
Step1		
inserts UD_i, inputs $ID_i^{'}, PW_i^{'}, B_i^{'}$		
$A_{ni}^{'} \leftarrow h_b\left(B_i^{'}\right) \oplus h\left(PW_i^{'} \| ID_i^{'}\right)$		
if $A_{ni}^{'} = A_{ni}$, generates K_u, r_i		
$Y_{ni}^{'} \leftarrow B_{ni} \oplus h\left(ID_i^{'} \| PW_i^{'} \| h_b\left(B_i^{'}\right)\right)$		
$h_1 \leftarrow K_u \oplus h\left(X_{ni} \| Y_{ni}^{'} \| T_1\right)$		
$h_2 \leftarrow ID_l \oplus h\left(X_{ni} \| Y_{ni}^{'} \| Z_{nl} \| T_1\right)$		
if $flag = 0$, $h_3 \leftarrow X_{ni} \| Z_{nl}$ else h_3	**Step2**	
$= h\left(r_i \| X_{ni} \| Y_{ni}^{'}\right) \| h\left(r_i \| Y_{ni}^{'} \| Z_{nl}\right)$	if $T_2 - T_1 \leq \Delta T$	
$h_4 \leftarrow h\left(h_1 \| h_2 \| h_3 \| K_u \| ID_l \| T_1 \| r_i\right)$	for $i = 1, i++, i \leq I$	
$M_1 = \{h_1, h_2, h_3, h_4, r_i, T_1\}$	$Y_{ni} \leftarrow h\left(X_{ni} \| sk\right)$	
$\xrightarrow[ID_i \ 2 \ ID_j]{M_1}$	if h_3 is valid	
	$K_u^{'} \leftarrow h_1 \oplus h\left(X_{ni} \| Y_{ni} \| T_1\right)$	
	$ID_l^{'} \leftarrow h_2 \oplus h\left(X_{ni} \| Y_{ni} \| Z_{nl} \| T_1\right)$, if	
	$h_4 = h\left(h_1 \| h_2 \| h_3 \| K_u^{'} \| ID_l^{'} \| T_1 \| r_i\right)$	
	$A_l \leftarrow h\left(X_{ni} \| Y_{ni}\right) \oplus Z_{nl}$	
	$Cr_l^{'} \leftarrow h\left(ID_l^{'} \| sk\right)$	
	$h_5 \leftarrow A_l \oplus h\left(Cr_l^{'} \| T_2\right)$	**Step3**
	$h_6 \leftarrow A_l \oplus K_u^{'}$	if $T_3 - T_2 \leq \Delta T$
	$h_7 \leftarrow h\left(A_l \| ID_l^{'} \| K_u^{'} \| T_2\right)$	$A_l^{'} \leftarrow h_5 \oplus h\left(Cr_l \| T_2\right)$
	$M_2 = \{h_5, h_6, h_7, T_2\}$	$K_u^{'} \leftarrow A_l^{'} \oplus h_6$
	$\xrightarrow[ID_j \ 2 \ ID_l]{M_2}$	if $h_7 = h\left(A_l^{'} \| ID_l \| K_u^{'} \| T_2\right)$
		generates K_p
		$ss_p \leftarrow h\left(A_l^{'} \| ID_l \| K_u^{'} \| K_p\right)$
	Step4	$h_8 \leftarrow h\left(ss_p \| Crl \| T_3\right)$
	if $T_4 - T_3 \leq \Delta T$, $K_p^{'} \leftarrow h_9 \oplus K_u^{'}$	$h_9 \leftarrow K_u^{'} \oplus K_p$
	$ss_s \leftarrow h\left(A_l \| ID_l^{'} \| K_u^{'} \| K_p^{'}\right)$	$M_3 \leftarrow \{h_8, h_9, T_3\}$
	if $h_8 = h\left(ss_s \| Cr_l^{'} \| T_3\right)$	$\xleftarrow[ID_l \ 2 \ ID_j]{M_3}$
Step5	$h_{10} \leftarrow h\left(ss_s \| K_u^{'} \| K_p^{'} \| T_4\right)$, updates	
if $T_5 - T_4 \leq \Delta T$, $K_p^{'} \leftarrow h_9 \oplus K_u$	$X_{(n+1)i} \leftarrow h\left(h\left(r_i \| X_{ni}\right) \oplus r_i \oplus Y_{ni}\right)$	
$ss_u \leftarrow h\left(A_l^{'} \| ID_l \| K_u \| K_p^{'}\right)$	$Z_{(n+1)l} \leftarrow h\left(Y_{ni} \| X_{ni}\right) \oplus A_l$	
if $h_{10} = h\left(ss_u \| K_u \| K_p^{'} \| T_4\right)$	$M_4 = \{h_9, h_{10}, T_4\}$	
$flag \leftarrow 0$ and updates	$\xleftarrow[ID_j \ 2 \ ID_i]{M_4}$	
$X_{(n+1)i} \leftarrow h\left(h\left(r_i \| X_{ni}\right) \oplus r_i \oplus Y_{ni}^{'}\right)$		
$Z_{(n+1)l} \leftarrow h\left(Y_{ni}^{'} \| X_{ni}\right) \oplus A_l$		

Fig. 3: Authentication Phase of LACO Scheme

2) After RA verifies that ID_j is valid, it selects random number r_j, calculates credential Cr_j and sends tuple $\{Cr_j\}$ to ID_j, and writes $\{ID_j, r_j\}$ to the server registration list L_S.
3) ID_j writes $\{ID_j, Cr_j\}$ to its memory.

6.2.2 User Registration

1) User selects ID ID_i and password PW_i, generates biometric B_i, calculates α_i, β_i and sends $\{ID_i, \alpha_i, \beta_i\}$ to RA.
2) After RA verifies that ID_i is valid, it selects random number r_i, calculates credential Cr_i, η_i and γ_i, returns the message of successful registration, and writes $\{ID_i, r_i, \eta_i, \gamma_i\}$ to the user registration list L_U.

6.2.3 Patient Registration

1) Patient selects ID ID_k and password PW_k, generates biometric B_k, calculates α_k, β_k and sends tuple $\{ID_k, \alpha_k, \beta_k\}$ to RA.
2) After RA verifies that ID_k is valid, it selects random number r_k, calculates credential Cr_k, η_k and γ_k; RA selects sensor ID_l according to the needs of ID_k, generates random number C_l and writes $\{h_b(\cdot), PUF(\cdot)\}$ to ID_l's memory.
3) ID_l calculates $R_l = h_b(PUF(C_l))$ and $\alpha_l = R_l \oplus ID_l$, and inserts α_l into ID_l's memory and issues it to ID_k.

Server$(NULL)$	**RA**(sk)
selects ID_j sends $\{ID_j\}$ to RA	
	if ID_j is valid, $r_j \xleftarrow{\$} \mathbf{Z}_q^*$ $Cr_j \leftarrow h\left(ID_j \| r_j \| sk\right)$ writes $\{ ID_j, r_j \}$ to L_S sends $\{ Cr_j \}$ to ID_j
writes $\{ ID_j, Cr_j \}$ to it's memory	
User$(NULL)$	**RA**(sk)
selects ID_i, PW_i, generates B_i $\alpha_i \leftarrow h\left(ID_i \| PW_i\right)$ $\beta_i \leftarrow h_b\left(B_i\right) \oplus h\left(ID_i \| PW_i\right)$ sends $\{ID_i, \alpha_i, \beta_i\}$ to RA	
	if ID_i is valid, $r_i \xleftarrow{\$} \mathbf{Z}_q^*$ $Cr_i \leftarrow h\left(ID_i \| r_i \| sk\right)$ $\eta_i \leftarrow \alpha_i \oplus Cr_i$ $\gamma_i \leftarrow \beta_i \oplus Cr_i$ writes $\{ ID_i, r_i, \eta_i, \gamma_i \}$ to L_U
Patient$(NULL)$	**RA**(sk)
selects ID_k, PW_k, generates B_k $\alpha_k \leftarrow h\left(ID_k \| PW_k\right)$ $\beta_k \leftarrow h_b\left(B_k\right) \oplus h\left(ID_k \| PW_k\right)$ sends $\{ID_k, \alpha_k, \beta_k\}$ to RA	
	if ID_k is valid, $r_k \xleftarrow{\$} \mathbf{Z}_q^*$ $Cr_k \leftarrow h\left(ID_k \| r_k \| sk\right)$ $\eta_k \leftarrow \alpha_k \oplus Cr_k$ $\gamma_k \leftarrow \beta_k \oplus Cr_k$ selects device identity ID_l, $C_l \xleftarrow{\$} \{0,1\}^{128}$ writes $\{h_b\left(\cdot\right), PUF\left(\cdot\right)\}$ to ID_l's memory ID_l calculates $R_l \leftarrow h_b\left(PUF_l\left(C_l\right)\right)$, $\alpha_l \leftarrow R_l \oplus ID_l$ inserts α_l into ID_l's memory and issues it to ID_k writes $\{ ID_k, r_k, \eta_k, \gamma_k, \{ID_l\} \}$ to L_P sends $\{ Cr_k, \{ID_l, R_l, C_l\} \}$ to ID_k
$\kappa_k \leftarrow Cr_k \oplus h\left(ID_k \| PW_k \| h_b\left(B_k\right)\right)$ $\beta_l \leftarrow R_l \oplus Cr_k$, $\gamma_l \leftarrow C_l \oplus Cr_k$ writes $\{ \kappa_k, \{ID_l, \beta_l, \gamma_l\} \}$ to it's memory	

Fig. 4: Registration Phase of Our Scheme

4) RA writes $\{ID_k, r_k, \eta_k, \gamma_k, \{ID_l\}\}$ to the patient registration list L_P and sends tuple $\{Cr_k, \{ID_l, R_l, C_l\}\}$ to ID_k.
5) Patient gateway ID_k calculates κ_k, β_l and γ_l, and writes $\{\kappa_k, \{ID_l, \beta_l, \gamma_l\}\}$ to its memory.

6.3 Authentication and Session Key Agreement

As shown in Figures 5 and 6, during the authentication and key agreement phase, users and servers, users and patients can achieve authentication key agreement and access authorization under RA authentication and authorization. The patient-server authentication is similar to the user-server and will not be repeated here. The process of user ID_i and patient ID_k's sensor ID_l mutual authentication and establishing a secure session is as follows:

1) User inputs $ID_i^{'}$ and password $PW_i^{'}$, generates biometric $B_i^{'}$, and calculates $\beta_i^{'}$; User selects random number r_4, and calculates A_i, A_i^*, h_{14}, h_{15}, h_{16}, h_{17} and h_{18}, and sends tuple $\{h_{14}, h_{15}, h_{16}, h_{17}, h_{18}, T_6\}$ to patient ID_k.
2) After ID_k verifies that timestamp is valid, s/he inputs $ID_k^{'}$ and password $PW_k^{'}$, generates biometric $B_k^{'}$, and calculates $\beta_i^{'}$; ID_k selects random number r_5, and calculates credential A_k, A_k^*, h_{19}, h_{20}, h_{21} and h_{22}, and sends tuple $\{h_{14}, h_{15}, h_{16}, h_{17}, h_{18}, h_{19}, h_{20}, h_{21}, h_{22}, T_7\}$ to RA to request authentication.
3) After RA verifies that timestamp is valid, it calculates $A_k^* = skh_{19}$ and $ID_k^{'} = h_{20} \oplus h\left(\left(A_j^*\right)_x \| 1\right)$, and if searching for $ID_k^{'}$ in patient registration list L_P is false, abort the protocol, else if $h_{22} = h\left(ID_k \| h_{18} \| h_{19} \| h_{20} \| h_{21} \| T_7\right)$ is false, abort the protocol, else calculates $\beta_k^{'} = h_{21} \oplus h\left(\left(A_j^*\right)_x \| 2\right)$, Cr_k and $\beta_k = Cr_k \oplus \gamma_k$; If $HD\left(\beta_k, \beta_k^{'}\right) \leq \delta$ is false, abort the protocol, else calculates $A_i^* = skh_{14}$ and $ID_i^{'} = h_{15} \oplus h\left(\left(A_i^*\right)_x \| 1\right)$, and if searching for $ID_i^{'}$ in user registration list L_U is false, abort the protocol, else if $h_{18} = h\left(ID_i \| ID_j \| \ h_{14} \| h_{15} \| h_{16} \| h_{17} \| T_6\right)$ is false, abort the protocol, else calculates $\beta_i^{'}$, Cr_i and β_i; if $HD\left(\beta_i, \beta_i^{'}\right) \leq \delta$ is false, abort the protocol, else calculates $ID_l^{'} = h_{16} \oplus h\left(\left(A_i^*\right)_x \| 2\right)$, and if searching for ID_i in ID_l's access control list AL_l^k is false, abort the protocol, else selects random number r_6, and cal-

User$(ID_i, PW_i, B_i, \gamma_i)$	**Medical server**(ID_j, Cr_j)	**RA**(sk)
Step1		
inputs $ID_i^{'}, PW_i^{'}, B_i^{'}$		
$\beta_i^{'} \leftarrow h_b\left(B_i^{'}\right) \oplus h\left(ID_i^{'} \| PW_i^{'}\right)$		
$r_1 \xleftarrow{\$} Z_q^*$, $A_i \leftarrow r_1 P, h_0 \leftarrow A_i$	**Step2**	
$A_i^* \leftarrow r_1 PK = \left(\left(A_i^*\right)_x, \left(A_i^*\right)_y\right)$	if $T_2 - T_1 \leq \Delta T$	**Step3**
$h_1 \leftarrow ID_i^{'} \oplus h\left(\left(A_i^*\right)_x \| 1\right)$	$r_2 \xleftarrow{\$} Z_q^*$, $A_j \leftarrow r_2 P, h_4 \leftarrow A_j$	if $T_3 - T_2 \leq \Delta T$
$h_2 \leftarrow \beta_i^{'} \oplus h\left(\left(A_i^*\right)_x \| 2\right)$	$A_j^* \leftarrow r_2 PK = \left(\left(A_j^*\right)_x, \left(A_j^*\right)_y\right)$	$A_j^* \leftarrow skA_j = \left(\left(A_j^*\right)_x, \left(A_j^*\right)_y\right)$
$h_3 \leftarrow h\left(ID_i^{'} \| ID_j \| h_0 \| h_1 \| h_2 \| T_1\right)$	$h_5 \leftarrow ID_j \oplus h\left(\left(A_j^*\right)_x\right)$	$ID_j^{'} \leftarrow h_5 \oplus h\left(\left(A_j^*\right)_x\right)$
$M_1 = \{h_0, h_1, h_2, h_3, T_1\}$	$h_6 \leftarrow h\left(ID_j \| h_3 \| h_4 \| h_5 \| T_2 \| Cr_j^{'}\right)$	search for $ID_j^{'}$ in L_S
$\xrightarrow[ID_i \ 2 \ ID_j]{M_1}$	$M2 = \{h_0, h_1, h_2, h_3, h_4, h_5, h_6, T_2\}$	if $ID_j^{'} = ID_j$
	$\xrightarrow[ID_j \ 2 \ RA]{M_2}$	$Cr_j \leftarrow h\left(ID_j \| r_k \| sk\right)$
		if $h_6 \leftarrow h\left(ID_j \| h_3 \| h_4 \| h_5 \| T_2 \| Cr_j^{'}\right)$
		$A_i^* \leftarrow skA_i = \left(\left(A_i^*\right)_x, \left(A_i^*\right)_y\right)$
		$ID_i^{'} = h_1 \oplus h\left(\left(A_i^*\right)_x \| 1\right)$
		search for $ID_i^{'}$ in L_U
		if $ID_i^{'} = ID_i$
		if $h_3 = h\left(ID_i \| ID_j \| h_0 \| h_1 \| h_2 \| T_1\right)$
		$\beta_i^{'} = h_2 \oplus h\left(\left(A_i^*\right)_x \| 2\right)$
		$Cr_i \leftarrow h\left(ID_i \| r_i \| sk\right)$
		$\beta_i \leftarrow \gamma_i \oplus Cr_i$
		if $HD\left(\beta_i, \beta_i^{'}\right) \leq \delta$ and
	Step4	if ID_i in AL_j
Step5	if $T_4 - T_3 \leq \Delta T$	$r_3 \xleftarrow{\$} Z_q^*$, $\alpha_i \leftarrow \eta_i \oplus Cr_i$
if $T_5 - T_4 \leq \Delta T$	$ID_i^{'} \leftarrow h_7 \oplus h\left(\left(A_j^*\right)_y \| Cr_j \| 1\right)$	$r_{ij} \leftarrow h\left(ID_i \| ID_j \| \beta_i \| Cr_j \| r_3\right)$
$r_{ij}^{'} \leftarrow h_9 \oplus h\left(\left(A_i^*\right)_y \| \alpha_i \| \beta_i^{'}\right)$	$r_{ij}^{'} \leftarrow h_8 \oplus h\left(\left(A_j^*\right)_y \| Cr_j^{'} \| 2\right)$	$h_7 \leftarrow ID_i \oplus h\left(\left(A_j^*\right)_y \| Cr_j \| 1\right)$
if $h_{11} = h\left(h_9 \| r_{ij}^{'} \| \left(A_i^*\right)_y \| \beta_i^{'}\right)$	if $h_{10} = h\left(h_8 \| h_9 \| r_{ij}^{'} \| \left(A_j^*\right)_y \| Cr_j\right)$	$h_8 \leftarrow r_{ij} \oplus h\left(\left(A_j^*\right)_y \| Cr_j \| 2\right)$
$ss_{ij} \leftarrow h\left(ID_i \| r_{ij}^{'} \| r_1 h_4\right)$	$ss_{ji} \leftarrow h\left(ID_i^{'} \| r_{ij}^{'} \| r_2 h_0\right)$	$h_9 \leftarrow r_{ij} \oplus h\left(\left(A_i^*\right)_y \| \alpha_i \| \beta_i^{'}\right)$
if $h_{12} = h\left(r_{ij}^{'} \| h_4 \| h_9 \| h_{11} \| ss_{ij}\right)$	sets $T_{ij} = T_4$ and writes	$h_{10} \leftarrow h\left(h_8 \| h_9 \| r_{ij} \| \left(A_j^*\right)_y \| Cr_j\right)$
sets $T_{ij} = T_5$ and writes	$\{A_{ij}, ID_i, T_{ij}, r_{ij}^{'}\}$ to cache	$h_{11} \leftarrow h\left(h_9 \| r_{ij} \| \left(A_i^*\right)_y \| \beta_i^{'}\right)$
$\{A_{ij}, ID_j, T_{ij}, r_{ij}^{'}\}$ to cache	$h_{12} \leftarrow h\left(r_{ij}^{'} \| h_4 \| h_9 \| h_{11} \| ss_{ji}\right)$	$M3 = \{h_8, h_9, h_{10}, h_{11}, T_3\}$
$h_{13} \leftarrow h\left(r_{ij}^{'} \| ss_{ij} \| T_5\right)$	$M4 = \{h_4, h_9, h_{11}, h_{12}, T_4\}$	$\xleftarrow[RA \ 2 \ ID_j]{M_3}$
$M5 = \{h_{13}, T_5\}$	$\xleftarrow[ID_j \ 2 \ ID_i]{M_4}$	
$\xrightarrow[ID_i \ 2 \ ID_j]{M_5}$	**Step6**	
	if $T_6 - T_5 \leq \Delta T$	
	if $h_{13} = h\left(r_{ij}^{'} \| ss_{ij} \| T_5\right)$	
	session key is established	

Fig. 5: User-Server Authentication Phase of Our Scheme

culates access control string $r_{ik} = h\left(ID_i^{'} \| ID_k^{'} \| ID_l^{'} \| \beta_i^{'} \| \beta_k^{'} \| r_6\right)$, and calculates h_{23}, h_{24}, h_{25}, h_{26}, h_{27} and h_{28}, and sends tuple $\{h_{23}, h_{24}, h_{25}, h_{26}, h_{27}, h_{28}, T_8\}$ to ID_k to request authentication.

4) After patient gateway ID_k verifies that timestamp is valid, it derives ID_l and ID_i from h_{23} and h_{24}, and calculates Cr_k and derives R_l and C_l from β_l and γ_l, respectively; ID_k calculates $h_{29} = h\left(ID_l \| C_l \| R_l \| T_9\right)$ and sends tuple $\{C_l, h_{29}, T_9\}$ to sensor ID_l.
5) After ID_l verifies that timestamp is valid, it calculates $R_l^{'} = h_b\left(PUF_l\left(C_l\right)\right)$, if $h_{29} = h\left(\left(R_l^{'} \oplus \alpha_l\right) \| C_l \| R_l \| T_9\right)$ is false, abort the protocol, else calculates session key $ss_{lk} = h\left(R_l \| T_{10}\right)$ between ID_l and ID_k, and calculates $R_l^* = h_b\left(PUF_l\left(h\left(C_l \| T_9\right)\right)\right)$ and updates $\alpha_l = \alpha_l^* = R_l^* \oplus R_l^{'} \oplus \alpha_l$, and calculates h_{30} and sends tuple $\left\{R_l^* \oplus R_l^{'}, h_{30}, T_{10}\right\}$ to ID_K.
6) After verifying that timestamp is valid, ID_k calculates session key $ss_{kl} = h\left(R_l \| T_{10}\right)$ between ID_k and ID_l, and updates $\beta_l^* = R_l^* \oplus R_l^{'} \oplus Cr_k \oplus R_l^{'}$, $\gamma_l^* = h\left(C_l \| T_9\right) \oplus Cr_k$.
7) If $h_{30} = h\left(ID_l \| C_l \| R_l \| R_l^* \| ss_{kl} \| T_{10}\right)$ is false, ID_k abort the protocol and returns $\perp$, else derives access

User(ID_i, PW_i, B_i)	**Patient with Sensor**$(ID_k, PW_k, B_k, \{ID_l\})$	**RA**(sk)
Step1		
$\beta_i^{'} \leftarrow h_b\left(B_i^{'}\right) \oplus h\left(ID_i^{'} \| PW_i^{'}\right)$	**Step2** if $T_7 - T_6 \leq \Delta T$	
$r_4 \xleftarrow{\$} Z_q^*$, $A_i \leftarrow r_4 P, h_{14} \leftarrow A_i$	$\beta_k^{'} \leftarrow h_b\left(B_k^{'}\right) \oplus h\left(ID_k^{'} \| PW_k^{'}\right)$	**Step3** if $T_8 - T_7 \leq \Delta T$
$A_i^* \leftarrow r_4 PK = \left((A_i^*)_x, (A_i^*)_y\right)$	$r_5 \xleftarrow{\$} Z_q^*$, $A_k \leftarrow r_5 P, h_{19} \leftarrow A_k$	$A_k^* \leftarrow skA_k = \left((A_k^*)_x, (A_k^*)_y\right)$
$h_{15} \leftarrow ID_i^{'} \oplus h\left((A_i^*)_x \| 1\right)$	$A_k^* \leftarrow r_5 PK = \left((A_k^*)_x, (A_k^*)_y\right)$	$ID_k^{'} \leftarrow h_{20} \oplus h\left(\left(A_j^*\right)_x \| 1\right)$
$h_{16} \leftarrow ID_l \oplus h\left((A_i^*)_x \| 2\right)$	$h_{20} \leftarrow ID_k \oplus h\left(\left(A_j^*\right)_x \| 1\right)$	search for $ID_k^{'}$ in L_P
$h_{17} \leftarrow \beta_i^{'} \oplus h\left((A_i^*)_x \| 3\right)$	$h_{21} \leftarrow \beta_k \oplus h\left(\left(A_j^*\right)_x \| 2\right)$	if $ID_k^{'} = ID_k$ and if
$h_{18} \leftarrow h\left(ID_i^{'} \| ID_j \| h_{14} \|\right.$	$h_{22} \leftarrow h\left(ID_k \| h_{18} \| h_{19} \| h_{20} \| h_{21} \| T_7\right)$	$h_{22} = h\left(ID_k \| h_{18} \| h_{19} \| h_{20} \| h_{21} \| T_7\right)$
$\left.h_{15} \| h_{16} \| h_{17} \| T_6\right)$	$M_7 = \{ h_{14}, h_{15}, h_{16}, h_{17},$	$\beta_k^{'} = h_{21} \oplus h\left((A_k^*)_x \| 2\right)$
$M_6 = \{h_{14}, h_{15}, h_{16}, h_{17}, h_{18}, T_6\}$	$h_{18}, h_{19}, h_{20}, h_{21}, h_{22}, T_7 \}$	$Cr_k \leftarrow h\left(ID_k \| r_i \| sk\right)$
$\xrightarrow[ID_i \ 2 \ ID_k]{M_6}$	$\xrightarrow[ID_k \ 2 \ RA]{M_7}$	$\beta_k \leftarrow \gamma_k \oplus Cr_k$
	Step4 if $T_9 - T_8 \leq \Delta T$	if $HD\left(\beta_k, \beta_k^{'}\right) \leq \delta$
	$ID_l^{'} \leftarrow h_{23} \oplus h\left(\left(A_k^*\right)_y \| \alpha_k \| \beta_k^{'} \| 1\right)$	$A_i^* \leftarrow skA_i = \left((A_i^*)_x, (A_i^*)_y\right)$
	$ID_i^{'} \leftarrow h_{24} \oplus h\left(\left(A_k^*\right)_y \| \alpha_k \| \beta_k^{'} \| 2\right)$	$ID_i^{'} = h_{15} \oplus h\left((A_i^*)_x \| 1\right)$
	$Cr_k \leftarrow \kappa_k \oplus h\left(ID_k \| PW_k \| h_b\left(B_k\right)\right)$	search for $ID_i^{'}$ in L_U
	$R_l \leftarrow \beta_l \oplus Cr_k$, $C_l \leftarrow \gamma_l \oplus Cr_k$	if $ID_i^{'} = ID_i$ and h_{18} is valid
	$h_{29} \leftarrow h\left(ID_l \| C_l \| R_l \| T_9\right)$	$\beta_i^{'} = h_{17} \oplus h\left((A_i^*)_x \| 2\right)$
	sends $\{ C_l, h_{29}, T_9 \}$ to ID_l *if*	$Cr_i \leftarrow h\left(ID_i \| r_i \| sk\right)$
	$T_{10} - T_9 \leq \Delta T$, $R_l^{'} \leftarrow h_b\left(PUF_l\left(C_l\right)\right)$	$\beta_i \leftarrow \gamma_i \oplus Cr_i$
	if $h_{29} = h\left(\left(R_l^{'} \oplus \alpha_l\right) \| C_l \| R_l \| T_9\right)$	if $HD\left(\beta_i, \beta_i^{'}\right) \leq \delta$
	$R_l^* \leftarrow h_b\left(PUF_l\left(h\left(C_l \| T_9\right)\right)\right)$	$ID_l^{'} = h_{16} \oplus h\left((A_i^*)_x \| 2\right)$
	updates $\alpha_l^* \leftarrow R_l^* \oplus R_l^{'} \oplus \alpha_l$	if ID_i in AL_l^k, $\alpha_k \leftarrow \eta_k \oplus Cr_k$
	$h_{30} = h\left(ID_l \| C_l \| R_l \| R_l^* \| ss_{lk} \| T_{10}\right)$	$h_{23} \leftarrow ID_l^{'} \oplus h\left(\left(A_k^*\right)_y \| \alpha_k \| \beta_k^{'} \| 1\right)$
	sends $\{ R_l^* \oplus R_l^{'}, h_{30}, T_{10} \}$ to ID_k	$h_{24} \leftarrow ID_i^{'} \oplus h\left(\left(A_k^*\right)_y \| \alpha_k \| \beta_k^{'} \| 2\right)$
Step5	if T_{10} and h_{30} are valid, updates	$r_6 \xleftarrow{\$} Z_q^*$, $\alpha_i \leftarrow \eta_i \oplus Cr_i$
if $T_{12} - T_{11} \leq \Delta T$	$\beta_l^* \leftarrow R_l^* \oplus Cr_k$, $\gamma_l^* \leftarrow C_l^* \oplus Cr_k$	$r_{ik} \leftarrow h\left(ID_i^{'} \| ID_k^{'} \| ID_l^{'} \| \beta_i^{'} \| \beta_k^{'} \| r_6\right)$
$r_{ik}^{'} \leftarrow h_{26} \oplus h\left(\left(A_i^*\right)_y \| \alpha_i \| \beta_i^{'}\right)$	$r_{ik}^{'} \leftarrow h_{25} \oplus h\left(\left(A_k^*\right)_y \| \alpha_k \| \beta_k^{'} \| 3\right)$	$h_{25} \leftarrow r_{ik} \oplus h\left(\left(A_k^*\right)_y \| \alpha_k \| \beta_k^{'} \| 3\right)$
if $h_{28} = h\left(h_{26} \| r_{ik}^{'} \| \beta_i^{'}\right)$	if $h_{27} = h\left(h_{23} \| h_{24} \| h_{25} \| r_{ik} \| \beta_k^{'}\right)$	$h_{26} \leftarrow r_{ik} \oplus h\left(\left(A_i^*\right)_y \| \alpha_i \| \beta_i^{'}\right)$
$ss_{ik} \leftarrow h\left(ID_i \| r_{ik}^{'} \| r_4 h_{19}\right)$ if	$ss_{ki} \leftarrow h\left(ID_i^{'} \| r_{ik}^{'} \| r_5 h_{14}\right)$	$h_{27} \leftarrow h\left(h_{23} \| h_{24} \| h_{25} \| r_{ik} \| \beta_k^{'}\right)$
$h_{31} = h\left(r_{ik}^{'} \| h_{19} \| h_{26} \| h_{28} \| ss_{ik}\right)$	sets $T_{ikl} = T_{11}$ and writes	$h_{28} \leftarrow h\left(h_{26} \| r_{ik} \| \beta_i^{'}\right)$
sets $T_{ikl} = T_{12}$ and writes $\{A_{ikl},$	$\{A_{ikl}, ID_i, ID_l, T_{ikl}, r_{ik}^{'}\}$ to cache	$M_8 = \{h_{23}, h_{24}, h_{25}, h_{26}, h_{27}, h_{28}, T_8\}$
$ID_k, ID_l, T_{ikl}, r_{ik}^{'}\}$ to cache	$h_{31} \leftarrow h\left(r_{ik}^{'} \| h_{19} \| h_{26} \| h_{28} \| ss_{ki}\right)$	$\xleftarrow[RA \ 2 \ ID_j]{M_8}$
$h_{32} \leftarrow h\left(r_{ij}^{'} \| ss_{ik} \| T_{12}\right)$	$M_9 = \{h_{19}, h_{26}, h_{28}, h_{31}, T_{11}\}$	
$M_{10} = \{h_{32}, T_{12}\}$	$\xleftarrow[ID_k \ 2 \ ID_i]{M_9}$	
$\xrightarrow[ID_i \ 2 \ ID_k]{M_{10}}$	**Step6** if T_{12} and h_{32} are valid, accepts	

Fig. 6: User-Patient Authentication Phase of Our Scheme

control string $r_{ik}^{'}$, and if $h_{27} = h\left(h_{23} \| h_{24} \| h_{25} \| r_{ik} \| \beta_k^{'}\right)$ is false, abort the protocol, else calculates session key $ss_{ki} = h\left(ID_i^{'} \| r_{ik}^{'} \| r_5 h_{14}\right)$ and digest h_{31}, and sends tuple $\{h_{19}, h_{26}, h_{28}, h_{31}, T_{11}\}$ to ID_i request authentication, and initializes the value of the time to live of access control string $r_{ik}^{'}$ to $T_{ikl} = T_{11}$, and calculates access control label $A_{ikl} = h\left(ID_i^{'} \| ID_l \| r_{ik}^{'}\right)$ and writes tuple $\left\{A_{ikl}, ID_i, ID_l, T_{ikl}, r_{ik}^{'}\right\}$ to cache.

8) After ID_i verifies that timestamp is valid, ID_i derives $r_{ik}^{'}$ from h_{26}, and if $h_{28} = h\left(h_{26} \| r_{ik}^{'} \| \beta_i^{'}\right)$ is false, abort the protocol, else calculates session key $ss_{ik} = h\left(ID_i \| r_{ik}^{'} \| r_4 h_{19}\right)$, and if $h_{31} = h\left(r_{ik}^{'} \| h_{19} \| h_{26} \| h_{28} \| ss_{ik}\right)$ is false, abort the protocol, else initializes the value of the time to live of access control string $r_{ik}^{'}$ to $T_{ikl} = T_{12}$, and calculates access control label $A_{ikl} = h\left(ID_i \| ID_l \| r_{ik}^{'}\right)$ and writes tuple $\left\{A_{ikl}, ID_k, ID_l, T_{ikl}, r_{ik}^{'}\right\}$ to cache.
9) ID_i calculates digest h_{32}, and sends tuple $\{h_{32}, T_{12}\}$ to ID_k request authentication.
10) If ID_k verifies that timestamp and h_{32} are valid, then ss_{ki} is accepted.

In fact, the user checks the validity of the relevant access control authorization before initiating a authentication request, that is, if $T_{current} - T_{ikl} \leq \Delta L$ is true, the session key is negotiated directly by r_{ik}, otherwise

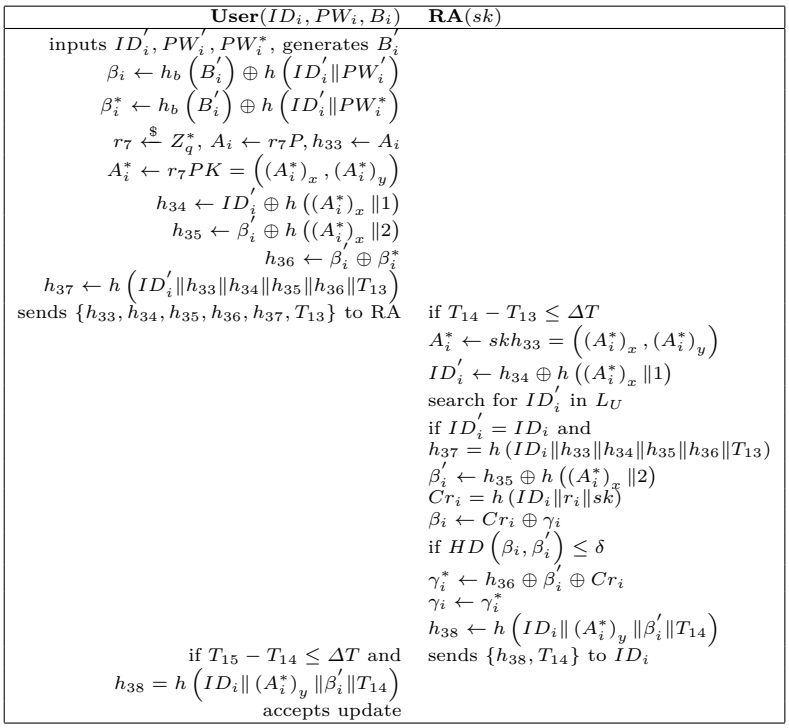

Fig. 7: Password Update Phase of Our Scheme

the authentication and authorization requests are initiated according to the algorithm shown in Figure 6, and ID_k and ID_l still use the dynamic shared secret R_l to achieve authentication key agreement. Details are as follows:

1) If $T_6 - T_{ikl} \leq \Delta L$ is true, ID_k selects random number r_4 and inputs $ID_i^{'}$, and calculates $h_{14} = r_4 P$, $h_{15} = ID_i^{'} \oplus h\left(r_{ik} \| 1\right)$, $h_{16} = ID_l \oplus h\left(r_{ik} \| 2\right)$ and $h_{18} = h\left(ID_i^{'} \| ID_l \| h_{14} \| h_{15} \| h_{16} \| A_{ikl} \| T_6\right)$, and sends tuple $\{h_{14}, h_{15}, h_{16}, h_{18}, A_{ikl}, T_6\}$ to patient ID_k.
2) After verifying that the timestamp is valid, if searching for A_{ikl} in cache is false, ID_k abort the protocol and returns $\perp$, else derives $ID_i^{'}$ and ID_l from h_{15} and h_{16}, and if verifying that $T_{11} - T_{ikl} \leq \Delta L$ or h_{18} is false, ID_k abort the protocol and returns $\perp$, else ID_k selects random number r_5 and calculates $h_{19} = r_5 P$, and calculates session key $ss_{ki} = h\left(ID_i^{'} \| r_{ik}^{'} \| r_5 h_{14}\right)$, and sets the value of the time to live of access control string $r_{ik}^{'}$ to $T_{ikl} = T_{11}$, and updates access control label $A_{ikl} = h\left(A_{ikl}\right)$ and updates tuple $\left\{A_{ikl}, ID_i^{'}, ID_l, T_{ikl}, r_{ik}^{'}\right\}$ in cache; ID_k calculates $h_{31} = h\left(r_{ik}^{'} \| h_{19} \| A_{ikl} \| ID_i^{'} \| ss_{ik} \| T_{11}\right)$ and sends tuple $\{h_{19}, h_{31}, T_{11}\}$ to ID_i.
3) After verifying that the timestamp is valid, ID_i calculates session key $ss_{ik} = h\left(ID_i \| r_{ik}^{'} \| \ r_4 h_{19}\right)$, and sets the value of the time to live of $r_{ik}^{'}$ to $T_{ikl} = T_{12}$, and updates $A_{ikl} = h\left(A_{ikl}\right)$ and updates tuple $\left\{A_{ikl}, ID_k, ID_l, T_{ikl}, r_{ik}^{'}\right\}$ in cache; if $h_{31} = h\left(r_{ik}^{'} \| h_{19} \| A_{ikl} \| ID_i \| ss_{ik} \| T_{11}\right)$ is true, ID_i calculates $h_{32} = h\left(A_{ikl} \| ss_{ik} \| T_{12}\right)$ and sends tuple $\{h_{32}, T_{12}\}$ to ID_k.
4) If ID_k verifies that timestamp and h_{32} are valid, then ss_{ki} is accepted.

6.4 Password Update

As shown in Figure 7, users or patients can update their passwords online at any time, anywhere. Details are as follows:

1) User inputs $ID_i^{'}$, old password $PW_i^{'}$ and new password PW_i^{*}, generates biometric $B_i^{'}$, and calculates $\beta_i^{'}$ and β_i^{*}; $ID_i^{'}$ selects random number r_7, and calculates $h_{33} = r_7 P$, $A_i^{*} = r_7 PK$, $h_{34} = ID_i^{'} \oplus h\left((A_i^{*})_x \| 1\right)$, $h_{35} = \beta_i^{'} \oplus h\left((A_i^{*})_x \| 2\right)$, $h_{36} = \beta_i^{'} \oplus \beta_i^{*}$ and h_{37}, and sends tuple $\{h_{33}, h_{34}, h_{35}, h_{35}, h_{37}, T_{13}\}$ to RA.
2) After verifying that timestamp is valid, RA calculates $A_i^{*} = skh_{33}$ and $ID_i^{'} = h_{34} \oplus h\left((A_i^{*})_x \| 1\right)$, and if searching for $ID_i^{'}$ in user registration list L_U is false, abort the protocol, else if $h_{37} = h\left(ID_i^{'} \| h_{33} \| h_{34} \| h_{35} \| h_{36} \| T_{13}\right)$ is false, returns $\perp$, else calculates $\beta_i^{'} =$

$h_{35} \oplus h\left(\left(A_i^*\right)_x \| 2\right), Cr_i$ and $\beta_i = Cr_i \oplus \gamma_i$; if $HD\left(\beta_i, \beta_i^{'}\right) \leq \delta$ is false, returns $\perp$, else updates $\gamma_i = \gamma_i^* = h_{36} \oplus \beta_i \oplus Cr_i$ and calculates $h_{38} = h\left(ID_i \| \left(A_i^*\right)_y \| \beta_i^{'} \| T_{14}\right)$, and sends tuple $\{h_{38}, T_{14}\}$ to ID_i.

3) After verifying that the timestamp and h_{38} are valid, ID_i accepts the update.

6.5 Ownership Transfer

In this proposal, users can transfer ownership after passing RA authentication and authorization. Suppose ID_{i1} wants to transfer ownership of patient ID_k to ID_{i2}, the details are as follows:

1) ID_{i1} generates a transfer request according to the algorithm **FIG.6.Step1** and sends it to ID_{i2}.
2) After verifying that the timestamp is valid, ID_{i2} also generates a transfer request according to the algorithm **FIG.6.Step1** and sends it to RA.
3) After verifying that the timestamp is valid, the RA verifies the identity of ID_{i1} and ID_{i2} according to the algorithm **FIG.6.Step3**. If it is false, aborts the protocol, else if searches for ID_{i1} in the access control list AL_k of ID_k is false, aborts the protocol, else writes ID_{i2} to AL_k, and returns the message of successful transfer.

7 Security Analysis

In this section, we will discuss how this proposal (SEMAS) provides mutual authentication, access control, session key privacy and forward security, and how to resist known Internet attacks such as insider attacks, multi-factor security attacks, and impersonation attacks. Moreover, we show that the proposed scheme is provably secure under the security model defined in section 3.5, the details are shown in Appendix A.

- **Mutual Authentication** In SEMAS, the user (or patient) mutually authenticates with the RA by β_i, the server mutually authenticates with RA by Cr_j, and the user and server mutually authenticate with the shared secret r_{ij} issued by the RA. ID_i encapsulates ID_i and β_i with the public key of RA. If h_3 and β_i are valid, RA believes that ID_i is a legitimate user. RA encapsulates the shared secret r_{ij} with β_i. If h_{11} is valid, ID_i believes that RA is the holder of the private key corresponding to the system public key. ID_j encapsulates ID with the public key of RA. If h_6 is valid, RA believes that ID_j is a legitimate server. RA encapsulates the shared secret r_{ij} with Cr_j. If h_{10} is valid, ID_j believes that RA is the holder of the private key corresponding to the system public key. On the basis of mutual authentication with RA, if h_{12} is valid, ID_i believes that ID_j is the common secret holder of RA certificated; if h_{13} is valid, ID_j believes that ID_i is the common secret holder of RA certificated.
- **Access Control** In SEMAS, the RA manages access authorization of server (or patient's sensor). The RA periodically generates an access control string r_{ij} for an authenticated and authorized user ID_i. A session can be established only if ID_i and ID_j hold the same access control string that meets the time limit.
- **Session Key Security** In SEMAS, the user ID_i and the server ID_j independently compute the session key $ss_{ij} = h\left(ID_i \| r_{ij} \| r_1 r_2 P\right)$, and the random numbers r_1, r_2 and r_{ij} are selected freshly each session, and the advantage of the enemy $\mathcal{A}$ to solve r_1, r_2 and r_{ij} is the advantage of attacking the EDLP security assumption, it is negligible. So $\mathcal{A}$ needs to know all the random numbers and ID_i to calculate ss_{ij}, and RA needs to know the random number r_1 and r_2 to calculate ss_{ij}.
- **Forward Security** In SEMAS, the user ID_i and the server ID_j independently compute the session key $ss_{ij} = h\left(ID_i \| r_{ij} \| r_1 r_2 P\right)$, and the random numbers r_1, r_2 and r_{ij} are selected freshly each session, and the advantage of the enemy $\mathcal{A}$ to solve r_1, r_2 and r_{ij} is the advantage of attacking the EDLP security assumption, it is negligible. So $\mathcal{A}$ can't calculate the previously generated session key even if it obtains all the long-term secrets of all protocol entities.
- **Privacy Protection** In the authentication and key agreement phase of the protocol, both ID_i and ID_j are transmitted in random pseudonym form h_1 and h_5, and the advantage of adversary $\mathcal{A}$ attacking these pseudonyms is equivalent to the advantage of attacking EDLP security assumption, which is negligible, so the advantage of $\mathcal{A}$ obtains ID_i and ID_j also is negligible. In addition, the information exchanged in the protocol are ECC ciphertexts and hash values generated by fresh random numbers. Therefore, the advantage of adversary tracking session is equivalent to the advantage of attacking EDLP security assumptions, which is negligible. In SEMAS, the biometric vector in the registration phase is encapsulated in γ_i by the RA's private key. According to the hash security assumption, the adversary's advantage of getting β_i from RA's L_U is $\frac{1}{(D_H)^{\frac{1}{2}}}$, which is negligible; during the authentication phase, the biometric vector is encapsulated in h_2 by a random number and RA's private key. According to

the ECC security assumption, the adversary's advantage in obtaining β_i from h_2 is negligible.

- **Against Privileged Insider Attack** In SEMAS, the password PW_i and biometric B_i of ID_i are encapsulated by a hash function. According to the one-way security of the secure hash, the curious RA cannot obtain the user's password and biometric.
- **Against Multi-factor Security Attack** In SEMAS, it is assumed that ID_i has been leaked. When PW_i is leaked, according to the hash security assumption and birthday paradox, the advantage of the adversary attack scheme multi-factor security is $\frac{1}{(D_H)^{\frac{1}{2}}}$. When B_i is leaked, the advantage of the adversary attack scheme multi-factor security by guessing password is $\frac{1}{D_{PW}}$.
- **Against Impersonation Attack** In SEMAS, mutual agreement is achieved between each agreement entity, and the premise of an adversary to impersonate the agreement entity is to obtain all the long-term secrets of the entity. All the information exchanged in the protocol are ECC ciphertexts and hash values generated from fresh random values. According to the ECC security assumption and hash security assumption, the advantage of adversary deriving the entity's long-term secret from $\{M_1, M_2, M_3, M_4, M_5\}$ is negligible.
- **Against Intermediate Data Attack** In SEMAS, the communication link between sever and RA is relatively secure. The intermediate data attack mainly occurs on the open link between user (patient) and server. SEMAS introduces a timestamp authentication mechanism and has good anonymity, adversary can't get ID_i and ID_j, and can't track the session, so the replay attack against SEMAS is difficult to work. In addition, only hash values and ECC ciphertexts are forwarded between protocol entities, and the secrets that generates these values are freshly selected for each session, so the man-in-the-middle attack against SEMAS is also difficult to work.

8 Performance Analysis

This section demonstrates that SEMAS how to satisfy the security goals and application requirements from the security and functionality properties, computational complexity and communication overhead.

8.1 Security and Functionality Properties Comparison

We evaluate the security and functionality features (P1: Mutual authentication, P2: Access Control, P3: Session key security, P4: Forward security, P5: Anonymity, P6: Against Insider Attack, P7: Against Multi-factor Security Attack, P8: Against User Impersonation Attack, P9: Against Server Impersonation Attack, P10: Against Patient Impersonation Attack, P11: Against Sensor Impersonation Attack, P12: Against Replay Attack, P13: Against Man-in-the-middle Attack, P14: Against Offline Password Attack, P15: Against Smart card loss Attack.) of our SEMAS and compare it with six recently proposed typical multi-server authentication schemes in the literature. The details are shown in Table 2.

Table 2: Security and Functionality Features Comparison

Features	[8]	[39]	[21]	[30]	[23]	[36]	SEMAS
P1	✓	✓	✓	✓	✓	✓	✓
P2	×	×	×	×	×	×	✓
P3	×	✓	✓	✓	✓	✓	✓
P4	✓	✓	✓	×	×	×	✓
P5	×	✓	×	×	×	✓	✓
P6	✓	✓	✓	✓	✓	✓	✓
P7	✓	✓	✓	✓	✓	✓	✓
P8	×	✓	✓	✓	✓	✓	✓
P9	✓	✓	✓	✓	×	✓	✓
P10	×	✓	✓	✓	×	✓	✓
P11	–	–	–	–	–	×	✓
P12	×	✓	✓	✓	✓	✓	✓
P13	✓	✓	✓	✓	✓	✓	✓
P14	✓	✓	✓	×	×	✓	✓
P15	✓	✓	×	×	×	×	✓

The results show that Feng et al.[30], Qi et al.[21], Lwamo et al. [23] and Roy et al. [36] are vulnerable to hardware loss attack. In turn, offline password guessing attack is caused, which leads to user impersonation attack and even loss of anonymity and forward security.

8.2 Computation Cost Comparison

To evaluate the computational efficiency of SEMAS, we calculate and compare the computation overhead of authentication key agreement phases of discussed protocols, including SEMAS, as shown in Table 4. The time-consuming overhead of the basic operations involved in these protocols is shown in Table 3 [1], the notations T_H, T_S, T_M and T_E represent the computational cost of hash operation, symmetric encryption/decryption operation, modulo operation and ECC scalar point multiplication operation, respectively. We assume that the computational complexity of the fuzzy extractor and ECC scalar point multiplication are close. Regardless of the overhead of XOR and hash operation, and the computation overhead of SEMAS is the lowest of the five online schemes [8,21,30,39].

Table 3: Runtime of Related Operation (ms)

Operation	T_H	T_S	T_M	T_E
Runtime	0.0003	0.0056	0.0027	0.0177

Table 4: Computation Cost Comparison (ms)

Scheme	Problem	User	Server & RA	Total
[8]	ECC	$3T_E$	$5T_E$	0.1416
[39]	ECC	$T_S + 3T_E$	$5T_S + 3T_E$	0.1398
[21]	ECC	$3T_E$	$5T_S + 2T_E$	0.1165
[30]	ECC	$3T_E$	$5T_E$	0.1416
[23]	Pairing	$2T_S$	$3T_S$	0.0280
[36]	Pairing	$T_S + T_E + T_M$	T_S	0.0316
SEMAS	ECC	$2T_E$	$4T_E$	0.1062

8.3 Communication Overhead Comparison

To evaluate the communication efficiency of SEMAS, we calculate and compare the communication overhead of authentication key agreement phases of discussed protocols, including SEMAS, as shown in Table 6. The byte length of the data structure transferred in these protocols is shown in Table 5. The notations T_I, T_H, T_E, T_S and T_N represent the byte length of identity, hash string, ECC block, symmetric ciphertext, random string, respectively. As in [39], we also assume that the length of the identity (ID_i, ID_j, ID_k, ID_l) (the time stamp is equal to the length), the hash value (e.g. SHA-1) and an elliptic curve point $P = (P_x, P_y)$ are 8 bytes, 20 bytes, and 40 bytes, respectively. In addition, we assume that the block size of symmetric ciphertext (e.g. AES) and a random number are 16 bytes, respectively.

Table 5: Byte Length of Related Metadata (bytes)

Metadata	L_I	L_H	L_E	L_S	L_N
Length	8	20	40	16	16

Table 6: Communication Cost Comparison (bytes)

Scheme	User	Server & RA	Total
[8]	$3L_H + L_E$	$11L_H + 3L_E$	440
[39]	$3L_H + L_E + L_S$	$3L_H + 3L_E + 3L_S$	344
[21]	$3L_H + L_I + L_E$	$2L_H + L_I + L_E + 7L_S$	308
[30]	$3L_H + L_E$	$11L_H + 3L_E$	440
[23]	$2L_H + 2L_I + 2L_S$	$L_H + L_I + 7L_S$	228
[36]	$3L_H + L_I$	$3L_H + L_I + L_S$	152
SEMAS	$4L_H + 2L_I + L_E$	$12L_H + 3L_I + 3L_E$	520

It can be seen from Figure 6 that the user side overhead of SEMAS is almost the same as that of other online protocols, but the total communication overhead is higher than that of other protocols. The main reason is that in order to achieve access control, anonymity and forward security, immune to offline password attack and smart card loss attack, SEMAS introduces time stamp authentication mechanism and the user sends one more ECC block.

9 Conclusion

The secure communication and access control in the E-healthcare systems are very important, and the key means to achieve this goal is the authenticated key agreement and access authorization mechanism. This work first performs a cryptanalysis of existing schemes such as LACO, and reveals the main reasons for the vulnerability of anonymity and forward security of these schemes, which can lead to impersonation attacks. Second, we proposed a multiple solution architecture for authentication and authorization in user-server, patient-server, user-patient and other scenarios in E-healthcare. Third, Based on the architecture, we design a secure and efficient multi-server authentication and access control scheme for E-Healthcare. Security analysis shows that the proposed scheme can provide mutual authentication, access control, session key security, anonymity and forward security, and can resist known Internet attack such as insider attack, multi-factor security attacks, impersonation attacks, intermediate data attacks, etc. Efficiency analysis shows that under the premise of higher security, the proposed scheme has better computational efficiency than similar typical schemes. Due to high security, the communication efficiency is slightly lower than similar typical schemes. Nevertheless, the total communication overhead of the proposed scheme is only 520 bytes, while the user side communication overhead is almost the same as other schemes.

Acknowledgments

This work was funded by the National Natural Science Foundation of China No. 61976142; the Zhejiang Province Natural Science Foundation of China under Grant No. LY19F020045. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

Declarations

Funding This work was funded by the National Natural Science Foundation of China No. 61976142; the Zhejiang Province Natural Science Foundation of China under Grant No. LY19F020045.

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

Availability of data and material Not applicable.

Code availability The code that support the findings of this study are available from the corresponding author, upon reasonable request.

Authors' contributions Qiao Yan: Supervision; Hailong Yao: Conceptualization, Methodology, Writing-Original draft preparation; Xingbing Fu: Writing-Reviewing and Editing; Zhibin Zhang, Caihui Lan: Software.

References

1. Kumari A, Jangirala S, Abbasi M, Kumar V, Alam M, (2020) ESEAP: ECC based secure and efficient mutual authentication protocol using smart card. Journal of Information Security and Applications 51:102443. https://doi.org/10.1016/j.jisa.2019.102443
2. Chuang MC and Chen MC (2014) An anonymous multi-server authenticated key agreement scheme based on trust computing using smart cards and biometrics. Expert Systems with Applications 41(4):1411–1418. https://doi.org/10.1016/j.eswa.2013.08.040
3. Böhm C, Hofer M (2012) Physical unclonable functions in theory and practice. Springer, NY. https://doi.org/10.1007/978-1-4614-5040-5
4. Dolev D, Yao A (1983) On the security of public key protocols. IEEE Transactions on Information Theory, 29(2):198–208. https://doi.org/10.1109/TIT.1983.1056650
5. He D, Kumar N, Chen J, Lee C, Chilamkurti N, and Yeo S (2015) Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks. Multimedia Syst., 21(1):49–-60. https://doi.org/10.1007/s00530-013-0346-9
6. Yang D, Yang B (2010) A biometric password-based multi-server authentication scheme with smart card. In: 2010 International Conference On Computer Design and Applications, IEEE, NY, pp 554–559. https://doi.org/10.1109/ICCDA.2010.5541128
7. He D (2011) Security flaws in a biometrics-based multi-server authentication with key agreement scheme. Cryptology ePrint Archive, Report 2011/365, https://eprint.iacr.org/2011/365.pdf. Accessed 26 Apr 2020
8. He D, Wang D (2015) Robust biometrics-based authentication scheme for multiserver environment. IEEE Systems Journal, 9(3):816–823. https://doi.org/10.1109/JSYST.2014.2301517
9. Wang C, Wang D, Tu Y, Xu G, Wang H (2020) Understanding node capture attacks in user authentication schemes for wireless sensor networks. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2020.2974220
10. Wang D, Zhang X, Zhang Z, Wang P (2020) Understanding security failures of multi-factor authentication schemes for multi-server environments. Computers & Security, 88:101619. https://doi.org/10.1016/j.cose.2019.101619
11. Wang D, Zhang Z, Wang P, Yan J, Huang X (2016) Targeted online password guessing: An underestimated threat. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security(CCS'16), ACM, 1242–1254. https://doi.org/10.1145/2976749.2978339
12. Yoon EJ, Yoo KY (2013) Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. The Journal of Supercomputing, 63:235–-255. https://doi.org/10.1007/s11227-010-0512-1
13. Aghili SF, Mala H, Shojafar M, Peris-Lopez P (2019) LACO: Lightweight three-Factor authentication, access control and ownership transfer scheme for E-health systems in IoT. Future Generation Computer Systems 96:410–424. https://doi.org/10.1016/j.future.2019.02.020
14. Yao H, Fu X, Wang C, Meng C,Hai B, Zhu S (2019) Cryptanalysis and improvement of a remote anonymous authentication protocol for mobile multi-server environments. 2019 IEEE Fourth International Conference on Data Science in Cyberspac. IEEE, NY, pp 19222220. https://doi.org/10.1109/DSC.2019.00015
15. Yao H, Wang C, Fu X, Liu C, Wu B, Li F (2019) A privacy-preserving RLWE-based remote biometric authentication scheme for single and multi-server environments. IEEE Access, 7:109597–109611. https://doi.org/10.1109/ACCESS.2019.2933576
16. Yao H, Wang C, Fu X, Liu C, Wu B, Li F (2020) Impersonation attacks on lightweight anonymous authenticated key exchange scheme for IoT. Cryptology ePrint Archive, Report 2020/143, https://eprint.iacr.org/2020/143.pdf. Accessed 26 Apr. 2020
17. Kirsal Ever Y (2018) Secure-anonymous user authentication scheme for E-healthcare application using wireless medical sensor networks. IEEE Systems Journal, 13(1):456–467. https://doi.org/10.1109/JSYST.2018.2866067
18. Simoens K, Bringer J, Chabanne H, Seys S (2012) A Framework for Analyzing Template Security and Privacy in Biometric Authentication Systems. IEEE Transactions on Information Forensics and Security, 7(2):833–841. https://doi.org/10.1109/TIFS.2012.2184092
19. Zhang L, Zhang Y, Tang S, Luo H (2018) Privacy protection for E-health systems by means of dynamic authentication and three-factor key agreement. IEEE Transactions on Industrial Electronics, 65(3):2795–2805. https://doi.org/10.1109/TIE.2017.2739683
20. Burrows M, Abadi M, Needham R (1990) A logic of authentication. ACM Transactions on Computer Systems, 8(1):18–36. https://doi.org/10.1098/rspa.1989.0125
21. Qi Mingping and Chen Jianhua and Chen Yitao (2018) A secure biometrics-based authentication key exchange protocol for multi-server TMIS using ECC. Computer Methods and Programs in Biomedicine, 164, pp 101–109. https://doi.org/10.1016/j.cmpb.2018.07.008
22. Wazid M, Das Ashok K, Vasilakos Athanasios V (2018) Authenticated key management protocol for cloud-assisted body area sensor networks. Journal of Network and Computer Applications, 123, pp 112–126. https://doi.org/10.1016/j.jnca.2018.09.008
23. Lwamo Nassoro MR, Zhu L, Xu C, Sharif K, Liu X, Zhang C (2019) SUAA: A secure user authentication scheme with anonymity for the single & multi-server environments. Information Sciences, 447, pp 369–385. https://doi.org/10.1016/j.ins.2018.10.037
24. Dharminder D, Mishra D, Li X (2020) Construction of RSA-based authentication scheme in authorized access to healthcare services. Journal of Medical Systems, 44:6. https://doi.org/10.1007/s10916-019-1471-6

25. Amin R, Biswas GP (2015) Design and analysis of bilinear pairing based mutual authentication and key agreement protocol usable in multi-server environment. Wireless Personal Communications, 84, pp 439–462. https://doi.org/10.1007/s11277-015-2616-7
26. Nikravan M, Reza AA (2020) Multi-factor user authentication and key agreement protocol based on bilinear pairing for the Internet of things. Wireless Personal Communications, 111, pp 463–494. https://doi.org/10.1007/s11277-019-06869-y
27. Chatterjee S, Roy S, Das AK, Chattopadhyay S, Kumar N, Vasilakos AV (2016) Secure biometric-based authentication scheme using Chebyshev chaotic map for multi-server environment. IEEE Transactions on Dependable and Secure Computing, 15(5):824–839. https://doi.org/10.1109/TDSC.2016.2616876
28. Roy S, Chatterjee S, Das AK, Chattopadhyay S, Kumari S, Jo M (2018) Chaotic map-based anonymous user authentication scheme with user biometrics and fuzzy extractor for crowdsourcing Internet of things. IEEE Internet of Things Journal, 5(4):2884–2895. https://doi.org/10.1109/JIOT.2017.2714179
29. Koblitz N (1987) Elliptic curve cryptosystems. Mathematics of computation, 48(177):203–209. https://doi.org/10.2307/2007884
30. Feng Q, He D, Zeadally S, Wang H (2018) Anonymous biometrics-based authentication scheme with key distribution for mobile multi-server environment. Future Generation Computer Systems, 84, pp 239–251. https://doi.org/10.1016/j.future.2017.07.040
31. Canetti R, Krawczyk H (2002) Universally composable notions of key exchange and secure channels. In: International Conference on the Theory and Applications of Cryptographic Techniques(Advances in Cryptology — EUROCRYPT 2002), Springer, Berlin/Heidelberg, 2332, pp 337–351. https://doi.org/10.1007/3-540-46035-7_22
32. Amin R, Hafizul Islamb S, Biswas GP, Khurram Khan M, Kumar N (2018) A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Generation Computer Systems, 80, pp 483–495. https://doi.org/10.1016/j.future.2016.05.032
33. Amin R, Hafizul Islamb S, Gope P, Raymond Choo KK, Tapas N (2019) Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system. IEEE Journal of Biomedical and Health Informatics, 23(4):1749–1759. https://doi.org/10.1109/JBHI.2018.2870319
34. Kumari S, Om H (2017) Cryptanalysis and improvement of an anonymous multi-server authenticated key agreement scheme. Wireless Personal Communications, 96, pp 2513-–2537. https://doi.org/10.1007/s11277-017-4310-4
35. Kumari S, Li X, Wu F, Das A, Choo K, Shen J (2017) Design of a provably secure biometrics-based multi-cloud-server authentication scheme. Future Generation Computer Systems, 68, 320-–330. https://doi.org/10.1016/j.future.2016.10.004
36. Roy S, Das AK, Chatterjee S, Kumar N, Chattopadhyay S, Rodrigues Joel JPC (2019) Provably Secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. IEEE Transactions on Industrial Informatics, 5(1):457–468. https://doi.org/10.1109/TII.2018.2824815
37. Banerjee Soumya and Odelu Vanga and Das Ashok Kumar and Srinivas Jangirala and Kumar Neeraj and Chattopadhyay Samiran (2019) A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of things deployment. IEEE Internet of Things Journal, 6(5):8739–8752. https://doi.org/110.1109/JIOT.2019.2923373
38. Barman S, Shum Hubert PH, Chattopadhyay S, Samanta D (2019) A secure authentication protocol for multi-server-based E-healthcare using a fuzzy commitment scheme. IEEE Access, 7, pp 12557–12574. https://doi.org/10.1109/ACCESS.2019.2893185
39. Odelu V, Das AK, Goswami A (2015) A secure biometrics-based multi-server authentication protocol using smart cards. IEEE Transactions on Information Forensics and Security, 10(9):1953–1966. https://doi.org/10.1109/TIFS.2015.2439964
40. Fu X, Nie X, Li F, Wu T (2018) Large universe attribute based access control with efficient decryption in cloud storage system. Journal of Systems and Software, 135, pp 157–164. https://doi.org/10.1016/j.jss.2017.10.020

A Formal Security Proof With the BAN Logic

We utilize the widely recognized BAN logic [20] to prove that in the proposed scheme the mutual authentication between a registered legitimate user ID_i and medical server ID_j is achieved with the help of RA. Notations used in the BAN Logic are shown in Table 7.

Table 7: Notations Used in the BAN Logic

Notations	Descriptions
$P\| \equiv X$	P believes a statement X
$\#(X)$	The statement X is fresh
$P \lhd X$	P sees the statement X
$P\| \sim X$	P once said the statement X
$P\| \Rightarrow X$	P has jurisdiction over statement X
$P \overset{K}{\leftrightarrow} Q$	K is a secret shared by P and Q
$P \overset{X}{\rightleftharpoons} Q$	X is a secret shared by P and Q and TTP
(X, Y)	X or Y is one part of (X, Y)
$\{X\}_K$	X is encrypted under the key K
$(X)_K$	X is hashed with the key K
$\langle X \rangle_K$	X is XORed with the key K

A.1 Rules

In this section, we present some of the main BAN logic rules for security proof.

Rul_1.Message meaning rule :

$$\frac{P| \equiv P \overset{K}{\leftrightarrow} Q, P \lhd \{X\}_K}{P| \equiv Q| \sim X} \text{and} \frac{P| \equiv P \overset{X}{\rightleftharpoons} Q, \langle X \rangle_K}{P| \equiv Q| \sim X}.$$

Rul_2.Nonce verification rule :

$$\frac{P| \equiv \#(X), P| \equiv Q| \sim X}{P| \equiv Q| \equiv X}.$$

Rul_3.Jurisdiction rule :

$$\frac{P| \equiv Q| \Rightarrow X, P| \equiv Q| \equiv X}{P| \equiv X}.$$

Rul_4.Freshness-conjuncatenation rule :

$$\frac{P| \equiv \#(X)}{P| \equiv \#(X,Y)}.$$

Rul_5.Believe rule :

$$\frac{P| \equiv (X), P| \equiv (Y)}{P| \equiv (X,Y)}.$$

A.2 Goals

According to the BAN logic, our scheme need to achieve the following five main goals:

$Goa_1 : ID_i| \equiv ID_j \overset{X}{\rightleftharpoons} ID_i.$

$Goa_2 : ID_j| \equiv ID_i \overset{X}{\rightleftharpoons} ID_j.$

$Goa_3 : ID_i| \equiv ID_j| \equiv ID_i \overset{K}{\leftrightarrow} ID_j.$

$Goa_4 : ID_j| \equiv ID_i| \equiv ID_j \overset{K}{\leftrightarrow} ID_i.$

A.3 Hypotheses

According to the BAN logic, the initialization conditions of our scheme are assumed as follows:

$Hyp_1 : ID_i| \equiv \#(r_1), ID_i| \equiv \#(r_1 P).$

$Hyp_2 : ID_j| \equiv \#(r_2), ID_j| \equiv \#(r_2 P).$

$Hyp_3 : ID_i| \equiv ID_i \overset{\beta_i}{\rightleftharpoons} RA.$

$Hyp_4 : RA| \equiv ID_i \overset{\beta_i}{\rightleftharpoons} RA.$

$Hyp_5 : ID_i| \equiv ID_i \overset{r_{ij}}{\leftrightarrow} RA.$

$Hyp_6 : ID_j| \equiv ID_j \overset{Cr_j}{\rightleftharpoons} RA.$

$Hyp_7 : RA| \equiv ID_j \overset{Cr_j}{\rightleftharpoons} RA.$

$Hyp_8 : ID_j| \equiv ID_j \overset{r_{ij}}{\leftrightarrow} RA.$

$Hyp_9 : ID_i| \equiv RA| \Rightarrow ID_i \overset{r_{ij}}{\leftrightarrow} ID_j.$

$Hyp_{10} : ID_j| \equiv RA| \Rightarrow ID_j \overset{r_{ij}}{\leftrightarrow} ID_i.$

$Hyp_{11} : ID_i| \equiv RA| \Rightarrow ID_j| \sim r_2 P.$

$Hyp_{12} : ID_j| \equiv RA| \Rightarrow ID_i| \sim r_1 P.$

$Hyp_{13} : ID_i| \equiv ID_j| \Rightarrow ID_i \overset{SS}{\leftrightarrow} ID_j.$

$Hyp_{14} : ID_j| \equiv ID_i| \Rightarrow ID_j \overset{SS}{\leftrightarrow} ID_i.$

A.4 The Idealized Form of Messages

In this section, we transform the general form of messages in our scheme into idealized ones.

M_1: From

$$h_0 = A_i,$$
$$h_1 = ID_i^{'} \oplus h\left(\left(A_i^*\right)_x \| 1\right),$$
$$h_2 = \beta_i^{'} \oplus h\left(\left(A_i^*\right)_x \| 2\right),$$
$$h_3 = h\left(ID_i^{'} \| ID_j \| h_0 \| h_1 \| h_2 \| T_1\right) \text{ to}$$

$$\left(ID_i\right)_{ID_i \overset{(A_i^*)_x}{\leftrightarrow} RA} \text{and} \left(ID_i, A_i, (A_i^*)_x\right)_{ID_i \overset{\beta_i}{\rightleftharpoons} RA}. \quad (1)$$

M_2: From

$$h_0, h_1, h_2, h_3,$$
$$h_4 = A_j,$$
$$h_5 = ID_j \oplus h\left(\left(A_j^*\right)_x\right),$$
$$h_6 = h\left(ID_j \| h_3 \| h_4 \| h_5 \| T_2 \| Cr_j^{'}\right) \text{ to}$$

$$\left(ID_j\right)_{ID_j \overset{(A_j^*)_x}{\leftrightarrow} RA} \text{and}$$
$$\left(ID_i, A_i, (A_i^*)_x, ID_j, A_j, (A_j^*)_x\right)_{ID_j \overset{Cr_j}{\rightleftharpoons} RA}. \quad (2)$$

M_3: From

$$h_8 = r_{ij} \oplus h\left(\left(A_j^*\right)_y \| Cr_j\right),$$
$$h_9 = r_{ij} \oplus h\left(\left(A_i^*\right)_y \| \alpha_i \| \beta_i^{'}\right),$$
$$h_{10} = h\left(h_8 \| h_9 \| r_{ij} \| \left(A_j^*\right)_y \| Cr_j\right),$$
$$h_{11} \leftarrow h\left(h_9 \| r_{ij} \| \left(A_i^*\right)_y \| \beta_i^{'}\right) \text{ to}$$

$$(r_{ij})_{RA \overset{(A_j^*)_y}{\leftrightarrow} ID_j} \text{ and } \left(ID_j, (A_j^*)_y\right)_{RA \overset{Cr_j}{\rightleftharpoons} ID_j}. \tag{3}$$

M_4: From

$h_5, h_9, h_{11},$

$h_{12} = h\left(r_{ij}^{'} \| h_5 \| h_9 \| h_{11} \| ss_{ji}\right)$ to

$$(r_{ij})_{RA \overset{(A_i^*)_y}{\leftrightarrow} ID_i} \text{ and } (ID_i, (A_i^*)_y, A_j)_{RA \overset{\beta_i}{\rightleftharpoons} ID_i}. \tag{4}$$

M_5: From

$h_{13} = h\left(r_{ij}^{'} \| ss_{ij} \| T_5\right)$ to

$$(ss_{ij})_{ID_i \overset{r_{ij}}{\rightleftharpoons} ID_i}. \tag{5}$$

A.5 Analysis

Based on the idealized message, BAN logic rules and initial condition hypotheses, the security analysis of our scheme is as follows:
According to the message M_1, hypothesis Hyp_4 and rule Rul_1, we have

$$RA \lhd \left((ID_i)_{ID_i \overset{(A_i^*)_x}{\leftrightarrow} RA}, A_i\right)_{ID_i \overset{\beta_i}{\rightleftharpoons} RA},$$
$$RA| \equiv ID_i| \sim (ID_i, A_i). \tag{6}$$

According to the message M_2, hypothesis Hyp_7 and Rul_1, we have

$$RA \lhd \left((ID_j)_{ID_j \overset{(A_j^*)_x}{\leftrightarrow} RA}, A_j\right)_{ID_j \overset{Cr_j}{\rightleftharpoons} RA},$$
$$RA| \equiv ID_j| \sim (ID_j, A_j). \tag{7}$$

According to the message M_3, hypothesis Hyp_6 and rule Rul_1, we have

$$ID_j \lhd \left((r_{ij})_{ID_j \overset{(A_j^*)_y}{\leftrightarrow} RA, A_i}\right)_{ID_j \overset{Cr_j}{\rightleftharpoons} RA},$$
$$ID_j| \equiv RA| \sim (r_{ij}, A_i). \tag{8}$$

According to the conclusions (7) and (8), hypothesis Hyp_6, rules Rul_2 and Rul_4, we have

$$ID_j| \equiv RA| \equiv ID_j \overset{r_{ij}}{\leftrightarrow} RA. \tag{9}$$

According to the conclusions (9), hypothesis Hyp_{10}, rules Rul_2 and Rul_4, we have

$$ID_j| \equiv ID_i \overset{r_{ij}}{\leftrightarrow} ID_j. \tag{10}$$

According to the conclusion (9) and (10), hypothesis Hyp_6, rules Rul_3, we achieve goal Goa_2

$$ID_j| \equiv ID_i \overset{r_{ij}}{\rightleftharpoons} ID_j. \tag{11}$$

According to the message M_4, hypothesis Hyp_3 and rule Rul_1, we have

$$ID_i \lhd \left((r_{ij})_{ID_i \overset{(A_i^*)_y}{\leftrightarrow} RA}, A_j\right)_{ID_i \overset{\beta_i}{\rightleftharpoons} RA},$$
$$ID_i| \equiv RA| \sim (r_{ij}, A_j). \tag{12}$$

According to the conclusion (12), hypothesis Hyp_3, rules Rul_2 and Rul_4, we have

$$ID_i| \equiv RA| \equiv ID_i \overset{r_{ij}}{\leftrightarrow} RA. \tag{13}$$

According to the conclusion (12) and (13), hypothesis Hyp_5, rules Rul_2 and Rul_4, we have

$$ID_i| \equiv ID_j \overset{r_{ij}}{\leftrightarrow} ID_i. \tag{14}$$

According to the conclusion (13) and (14), hypothesis Hyp_3, rules Rul_3, we achieve goal Goa_1

$$ID_i| \equiv ID_j \overset{r_{ij}}{\rightleftharpoons} ID_i. \tag{15}$$

According to the conclusion (12), (13), (14) and (15), hypothesis Hyp_9 and Hyp_{11}, rules Rul_3, we achieve goal Goa_3

$$ID_i| \equiv ID_j| \equiv ID_i \overset{ss_{ij}}{\leftrightarrow} ID_j. \tag{16}$$

According to the message Mes_5, conclusion (11) and rule Rul_1, we have

$$ID_j \lhd \left((T_5)_{ID_j \overset{ss_{ij}}{\leftrightarrow} ID_i}\right)_{ID_j \overset{r_{ij}}{\rightleftharpoons} ID_i},$$
$$ID_j| \equiv ID_i| \sim (T_5). \tag{17}$$

According to the conclusion (11) and (17), hypothesis Hyp_{12}, rules Rul_3, we achieve goal Goa_4

$$ID_j| \equiv ID_i| \equiv ID_j \overset{ss_{ij}}{\leftrightarrow} ID_i. \tag{18}$$

Figures

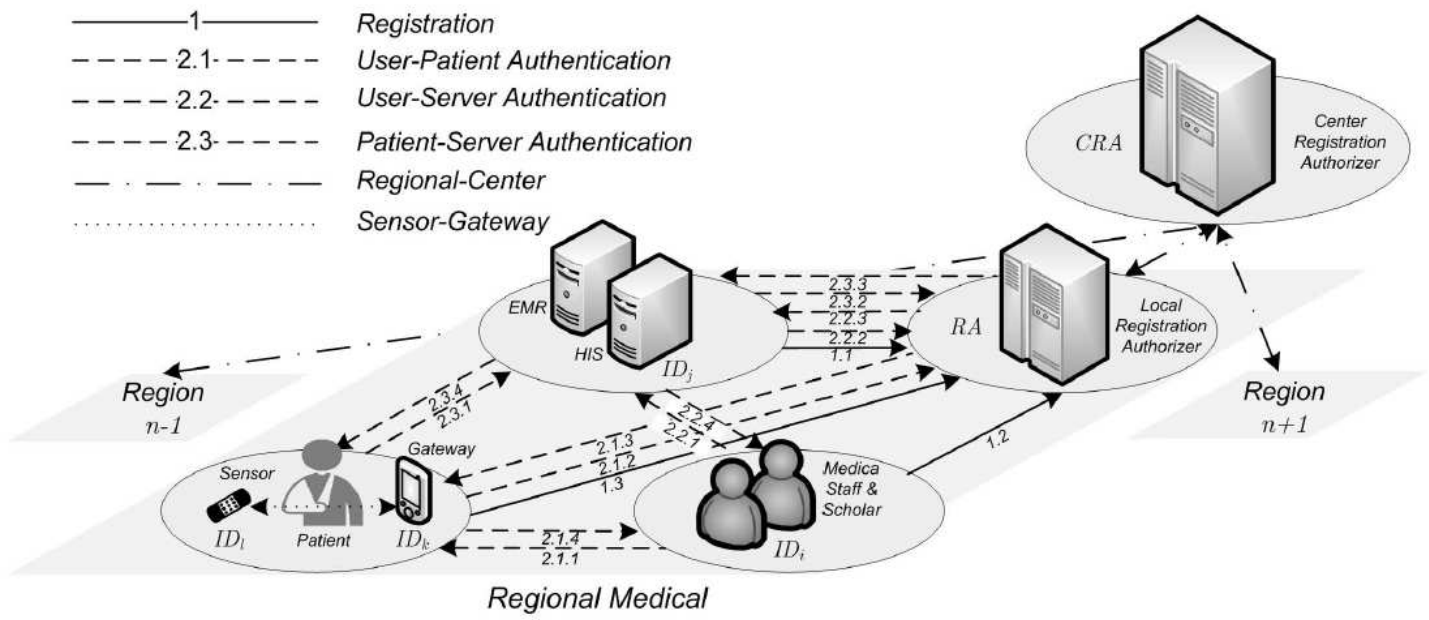

Figure 1

Communication Model of This Proposal

Patient's sensor$(NULL)$	**Medical server**(sk)
registration request	
	selects device identity ID_l, $Cr_l \leftarrow h\left(ID_l \| sk\right)$ writes $\{ ID_l, Cr_l \}$ into ID_l's memory and issue it
User(ID_i, PW_i, B_i)	**Medical server**(sk)
selects identity ID_i	
$\xrightarrow[ID_i \ 2 \ ID_j]{ID_i}$	
	if ID_i is valid generates r_s $X_{0i}, Z_{0l} \leftarrow NULL$ $X_{1i} \leftarrow h\left(UD_i \| ID_i \| r_s\right)$ $Y_{1i} \leftarrow h\left(X_{0i} \| sk\right)$ $Z_{1l} \leftarrow h\left(X_{0i} \| Y_{0i}\right) \oplus A_l$ writes $\{ X_{0i}, Z_{0l}, X_{1i}, Z_{1l} \}$ into R_U writes $\{ X_{1i}, Y_{1i}, Z_{1l}, h_b\left(\cdot\right) \}$ into smart card UD_i and issues it to ID_i
$A_{1i} \leftarrow h_b\left(B_i\right) \oplus h\left(PW_i \| ID_i\right)$ $B_{1i} \leftarrow Y_{1i} \oplus h\left(ID_i \| PW_i \| h_b\left(B_i\right)\right)$ $flag \leftarrow 0$ writes $\{ A_{1i}, B_{1i}, flag \}$ into UD_i and deletes Y_{1i}	

Figure 2

Registration Phase of LACO Scheme

User(ID_i, PW_i, B_i)	Medical server(sk)	Patient's sensor(ID_l, Cr_l)
Step1		
inserts UD_i, inputs $ID_i^{'}, PW_i^{'}, B_i^{'}$		
$A_{ni}^{'} \leftarrow h_b\left(B_i^{'}\right) \oplus h\left(PW_i^{'} \| ID_i^{'}\right)$		
if $A_{ni}^{'} = A_{ni}$, generates K_u, r_i		
$Y_{ni}^{'} \leftarrow B_{ni} \oplus h\left(ID_i^{'} \| PW_i^{'} \| h_b\left(B_i^{'}\right)\right)$		
$h_1 \leftarrow K_u \oplus h\left(X_{ni} \| Y_{ni}^{'} \| T_1\right)$		
$h_2 \leftarrow ID_l \oplus h\left(X_{ni} \| Y_{ni}^{'} \| Z_{nl} \| T_1\right)$		
if $flag = 0$, $h_3 \leftarrow X_{ni} \| Z_{nl}$ else h_3	**Step2**	
$= h\left(r_i \| X_{ni} \| Y_{ni}^{'}\right) \| h\left(r_i \| Y_{ni}^{'} \| Z_{nl}\right)$	if $T_2 - T_1 \leq \Delta T$	
$h_4 \leftarrow h\left(h_1 \| h_2 \| h_3 \| K_u \| ID_l \| T_1 \| r_i\right)$	for $i = 1, i++, i \leq I$	
$M_1 = \{h_1, h_2, h_3, h_4, r_i, T_1\}$	$Y_{ni} \leftarrow h\left(X_{ni} \| sk\right)$	
$\xrightarrow[ID_i \ 2 \ ID_j]{M_1}$	if h_3 is valid	
	$K_u^{'} \leftarrow h_1 \oplus h\left(X_{ni} \| Y_{ni} \| T_1\right)$	
	$ID_l \leftarrow h_2 \oplus h\left(X_{ni} \| Y_{ni} \| Z_{nl} \| T_1\right)$, if	
	$h_4 = h\left(h_1 \| h_2 \| h_3 \| K_u^{'} \| ID_l^{'} \| T_1 \| r_i\right)$	
	$A_l \leftarrow h\left(X_{ni} \| Y_{ni}\right) \oplus Z_{nl}$	
	$Cr_l^{'} \leftarrow h\left(ID_l^{'} \| sk\right)$	
	$h_5 \leftarrow A_l \oplus h\left(Cr_l^{'} \| T_2\right)$	**Step3**
	$h_6 \leftarrow A_l \oplus K_u^{'}$	if $T_3 - T_2 \leq \Delta T$
	$h_7 \leftarrow h\left(A_l \| ID_l^{'} \| K_u^{'} \| T_2\right)$	$A_l^{'} \leftarrow h_5 \oplus h\left(Cr_l \| T_2\right)$
	$M_2 = \{h_5, h_6, h_7, T_2\}$	$K_u^{'} \leftarrow A_l^{'} \oplus h_6$
	$\xrightarrow[ID_j \ 2 \ ID_l]{M_2}$	if $h_7 = h\left(A_l^{'} \| ID_l \| K_u^{'} \| T_2\right)$
		generates K_p
		$ss_p \leftarrow h\left(A_l^{'} \| ID_l \| K_u^{'} \| K_p\right)$
	Step4	$h_8 \leftarrow h\left(ss_p \| Cr_l \| T_3\right)$
	if $T_4 - T_3 \leq \Delta T$, $K_p^{'} \leftarrow h_9 \oplus K_u^{'}$	$h_9 \leftarrow K_u^{'} \oplus K_p$
	$ss_s \leftarrow h\left(A_l \| ID_l^{'} \| K_u^{'} \| K_p^{'}\right)$	$M_3 \leftarrow \{h_8, h_9, T_3\}$
	if $h_8 = h\left(ss_s \| Cr_l^{'} \| T_3\right)$	$\xleftarrow[ID_l \ 2 \ ID_j]{M_3}$
Step5	$h_{10} \leftarrow h\left(ss_s \| K_u^{'} \| K_p^{'} \| T_4\right)$, updates	
if $T_5 - T_4 \leq \Delta T$, $K_p^{'} \leftarrow h_9 \oplus K_u$	$X_{(n+1)i} \leftarrow h\left(h\left(r_i \| X_{ni}\right) \oplus r_i \oplus Y_{ni}\right)$	
$ss_u \leftarrow h\left(A_l^{'} \| ID_l \| K_u \| K_p^{'}\right)$	$Z_{(n+1)l} \leftarrow h\left(Y_{ni} \| X_{ni}\right) \oplus A_l$	
if $h_{10} = h\left(ss_u \| K_u \| K_p^{'} \| T_4\right)$	$M_4 = \{h_9, h_{10}, T_4\}$	
$flag \leftarrow 0$ and updates	$\xleftarrow[ID_j \ 2 \ ID_i]{M_4}$	
$X_{(n+1)i} \leftarrow h\left(h\left(r_i \| X_{ni}\right) \oplus r_i \oplus Y_{ni}^{'}\right)$		
$Z_{(n+1)l} \leftarrow h\left(Y_{ni}^{'} \| X_{ni}\right) \oplus A_l$		

Figure 3

Authentication Phase of LACO Scheme

Server($NULL$)	RA(sk)
selects ID_j	
sends $\{ID_j\}$ to RA	
	if ID_j is valid, $r_j \xleftarrow{\$} \mathbf{Z}_q^*$
	$Cr_j \leftarrow h(ID_j \| r_j \| sk)$
	writes $\{ ID_j, r_j \}$ to L_S
	sends $\{ Cr_j \}$ to ID_j
writes $\{ ID_j, Cr_j \}$ to it's memory	
User($NULL$)	**RA**(sk)
selects ID_i, PW_i, generates B_i	
$\alpha_i \leftarrow h(ID_i \| PW_i)$	
$\beta_i \leftarrow h_b(B_i) \oplus h(ID_i \| PW_i)$	
sends $\{ID_i, \alpha_i, \beta_i\}$ to RA	
	if ID_i is valid, $r_i \xleftarrow{\$} \mathbf{Z}_q^*$
	$Cr_i \leftarrow h(ID_i \| r_i \| sk)$
	$\eta_i \leftarrow \alpha_i \oplus Cr_i$
	$\gamma_i \leftarrow \beta_i \oplus Cr_i$
	writes $\{ ID_i, r_i, \eta_i, \gamma_i \}$ to L_U
Patient($NULL$)	**RA**(sk)
selects ID_k, PW_k, generates B_k	
$\alpha_k \leftarrow h(ID_k \| PW_k)$	
$\beta_k \leftarrow h_b(B_k) \oplus h(ID_k \| PW_k)$	
sends $\{ID_k, \alpha_k, \beta_k\}$ to RA	
	if ID_k is valid, $r_k \xleftarrow{\$} \mathbf{Z}_q^*$
	$Cr_k \leftarrow h(ID_k \| r_k \| sk)$
	$\eta_k \leftarrow \alpha_k \oplus Cr_k$
	$\gamma_k \leftarrow \beta_k \oplus Cr_k$
	selects device identity ID_l, $C_l \xleftarrow{\$} \{0,1\}^{128}$
	writes $\{h_b(\cdot), PUF(\cdot)\}$ to ID_l's memory
	ID_l calculates $R_l \leftarrow h_b(PUF_l(C_l))$, $\alpha_l \leftarrow R_l \oplus ID_l$
	inserts α_l into ID_l's memory and issues it to ID_k
	writes $\{ ID_k, r_k, \eta_k, \gamma_k, \{ID_l\} \}$ to L_P
	sends $\{ Cr_k, \{ID_l, R_l, C_l\} \}$ to ID_k
$\kappa_k \leftarrow Cr_k \oplus h(ID_k \| PW_k \| h_b(B_k))$	
$\beta_l \leftarrow R_l \oplus Cr_k$, $\gamma_l \leftarrow C_l \oplus Cr_k$	
writes $\{ \kappa_k, \{ID_l, \beta_l, \gamma_l\} \}$ to it's memory	

Figure 4

Registration Phase of Our Scheme

User$(ID_i, PW_i, B_i, \gamma_i)$	Medical server(ID_j, Cr_j)	RA(sk)
Step1		
inputs $ID_i^{'}, PW_i^{'}, B_i^{'}$		
$\beta_i^{'} \leftarrow h_b\left(B_i^{'}\right) \oplus h\left(ID_i^{'} \| PW_i^{'}\right)$		
$r_1 \xleftarrow{\$} Z_q^*$, $A_i \leftarrow r_1 P, h_0 \leftarrow A_i$	**Step2**	
$A_i^* \leftarrow r_1 PK = \left(\left(A_i^*\right)_x, \left(A_i^*\right)_y\right)$	if $T_2 - T_1 \leq \Delta T$	**Step3**
$h_1 \leftarrow ID_i^{'} \oplus h\left(\left(A_i^*\right)_x \| 1\right)$	$r_2 \xleftarrow{\$} Z_q^*$, $A_j \leftarrow r_2 P, h_4 \leftarrow A_j$	if $T_3 - T_2 \leq \Delta T$
$h_2 \leftarrow \beta_i^{'} \oplus h\left(\left(A_i^*\right)_x \| 2\right)$	$A_j^* \leftarrow r_2 PK = \left(\left(A_j^*\right)_x, \left(A_j^*\right)_y\right)$	$A_j^* \leftarrow skA_j = \left(\left(A_j^*\right)_x, \left(A_j^*\right)_y\right)$
$h_3 \leftarrow h\left(ID_i^{'} \| ID_j \| h_0 \| h_1 \| h_2 \| T_1\right)$	$h_5 \leftarrow ID_j \oplus h\left(\left(A_j^*\right)_x\right)$	$ID_j^{'} \leftarrow h_5 \oplus h\left(\left(A_j^*\right)_x\right)$
$M_1 = \{h_0, h_1, h_2, h_3, T_1\}$	$h_6 \leftarrow h\left(ID_j \| h_3 \| h_4 \| h_5 \| T_2 \| Cr_j^{'}\right)$	search for $ID_j^{'}$ in L_S
$\xrightarrow[ID_i \ 2 \ ID_j]{M_1}$	$M2 = \{h_0, h_1, h_2, h_3, h_4, h_5, h_6, T_2\}$	if $ID_j^{'} = ID_j$
	$\xrightarrow[ID_j \ 2 \ RA]{M_2}$	$Cr_j \leftarrow h\left(ID_j \| r_k \| sk\right)$
		if $h_6 \leftarrow h\left(ID_j \| h_3 \| h_4 \| h_5 \| T_2 \| Cr_j^{'}\right)$
		$A_i^* \leftarrow skA_i = \left(\left(A_i^*\right)_x, \left(A_i^*\right)_y\right)$
		$ID_i^{'} = h_1 \oplus h\left(\left(A_i^*\right)_x \| 1\right)$
		search for $ID_i^{'}$ in L_U
		if $ID_i^{'} = ID_i$
		if $h_3 = h\left(ID_i \| ID_j \| h_0 \| h_1 \| h_2 \| T_1\right)$
		$\beta_i^{'} = h_2 \oplus h\left(\left(A_i^*\right)_x \| 2\right)$
		$Cr_i \leftarrow h\left(ID_i \| r_i \| sk\right)$
		$\beta_i \leftarrow \gamma_i \oplus Cr_i$
		if $HD\left(\beta_i, \beta_i^{'}\right) \leq \delta$ and
	Step4	if ID_i in AL_j
Step5	if $T_4 - T_3 \leq \Delta T$	$r_3 \xleftarrow{\$} Z_q^*$, $\alpha_i \leftarrow \eta_i \oplus Cr_i$
if $T_5 - T_4 \leq \Delta T$	$ID_i^{'} \leftarrow h_7 \oplus h\left(\left(A_j^*\right)_y \| Cr_j \| 1\right)$	$r_{ij} \leftarrow h\left(ID_i \| ID_j \| \beta_i \| Cr_j \| r_3\right)$
$r_{ij}^{'} \leftarrow h_9 \oplus h\left(\left(A_i^*\right)_y \| \alpha_i \| \beta_i^{'}\right)$	$r_{ij}^{'} \leftarrow h_8 \oplus h\left(\left(A_j^*\right)_y \| Cr_j^{'} \| 2\right)$	$h_7 \leftarrow ID_i \oplus h\left(\left(A_j^*\right)_y \| Cr_j \| 1\right)$
if $h_{11} = h\left(h_9 \| r_{ij}^{'} \| \left(A_i^*\right)_y \| \beta_i^{'}\right)$	if $h_{10} = h\left(h_8 \| h_9 \| r_{ij}^{'} \| \left(A_j^*\right)_y \| Cr_j\right)$	$h_8 \leftarrow r_{ij} \oplus h\left(\left(A_j^*\right)_y \| Cr_j \| 2\right)$
$ss_{ij} \leftarrow h\left(ID_i \| r_{ij}^{'} \| r_1 h_4\right)$	$ss_{ji} \leftarrow h\left(ID_i^{'} \| r_{ij}^{'} \| r_2 h_0\right)$	$h_9 \leftarrow r_{ij} \oplus h\left(\left(A_i^*\right)_y \| \alpha_i \| \beta_i^{'}\right)$
if $h_{12} = h\left(r_{ij}^{'} \| h_4 \| h_9 \| h_{11} \| ss_{ij}\right)$	sets $T_{ij} = T_4$ and writes	$h_{10} \leftarrow h\left(h_8 \| h_9 \| r_{ij} \| \left(A_j^*\right)_y \| Cr_j\right)$
sets $T_{ij} = T_5$ and writes	$\{A_{ij}, ID_i, T_{ij}, r_{ij}^{'}\}$ to cache	$h_{11} \leftarrow h\left(h_9 \| r_{ij} \| \left(A_i^*\right)_y \| \beta_i^{'}\right)$
$\{A_{ij}, ID_j, T_{ij}, r_{ij}^{'}\}$ to cache	$h_{12} \leftarrow h\left(r_{ij}^{'} \| h_4 \| h_9 \| h_{11} \| ss_{ji}\right)$	$M3 = \{h_8, h_9, h_{10}, h_{11}, T_3\}$
$h_{13} \leftarrow h\left(r_{ij}^{'} \| ss_{ij} \| T_5\right)$	$M4 = \{h_4, h_9, h_{11}, h_{12}, T_4\}$	$\xleftarrow[RA \ 2 \ ID_j]{M_3}$
$M5 = \{h_{13}, T_5\}$	$\xleftarrow[ID_j \ 2 \ ID_i]{M_4}$	
$\xrightarrow[ID_i \ 2 \ ID_j]{M_5}$	**Step6**	
	if $T_6 - T_5 \leq \Delta T$	
	if $h_{13} = h\left(r_{ij}^{'} \| ss_{ij} \| T_5\right)$	
	session key is established	

Figure 5

User-Server Authentication Phase of Our Scheme

User(ID_i, PW_i, B_i)	Patient with Sensor$(ID_k, PW_k, B_k, \{ID_l\})$	RA(sk)
Step1		
$\beta_i^{'} \leftarrow h_b\left(B_i^{'}\right) \oplus h\left(ID_i^{'} \| PW_i^{'}\right)$	**Step2** if $T_7 - T_6 \leq \Delta T$	
$r_4 \xleftarrow{\$} Z_q^*$, $A_i \leftarrow r_4 P, h_{14} \leftarrow A_i$	$\beta_k^{'} \leftarrow h_b\left(B_k^{'}\right) \oplus h\left(ID_k^{'} \| PW_k^{'}\right)$	**Step3** if $T_8 - T_7 \leq \Delta T$
$A_i^* \leftarrow r_4 PK = \left((A_i^*)_x, (A_i^*)_y\right)$	$r_5 \xleftarrow{\$} Z_q^*$, $A_k \leftarrow r_5 P, h_{19} \leftarrow A_k$	$A_k^* \leftarrow skA_k = \left((A_k^*)_x, (A_k^*)_y\right)$
$h_{15} \leftarrow ID_i^{'} \oplus h\left((A_i^*)_x \| 1\right)$	$A_k^* \leftarrow r_5 PK = \left((A_k^*)_x, (A_k^*)_y\right)$	$ID_k^{'} \leftarrow h_{20} \oplus h\left(\left(A_j^*\right)_x \| 1\right)$
$h_{16} \leftarrow ID_l \oplus h\left((A_i^*)_x \| 2\right)$	$h_{20} \leftarrow ID_k \oplus h\left(\left(A_j^*\right)_x \| 1\right)$	search for $ID_k^{'}$ in L_P
$h_{17} \leftarrow \beta_i^{'} \oplus h\left((A_i^*)_x \| 3\right)$	$h_{21} \leftarrow \beta_k \oplus h\left(\left(A_j^*\right)_x \| 2\right)$	if $ID_k^{'} = ID_k$ and if
$h_{18} \leftarrow h\left(ID_i^{'} \| ID_j \| h_{14} \| h_{15} \| h_{16} \| h_{17} \| T_6\right)$	$h_{22} \leftarrow h\left(ID_k \| h_{18} \| h_{19} \| h_{20} \| h_{21} \| T_7\right)$	$h_{22} = h\left(ID_k \| h_{18} \| h_{19} \| h_{20} \| h_{21} \| T_7\right)$
$M_6 = \{h_{14}, h_{15}, h_{16}, h_{17}, h_{18}, T_6\}$	$M_7 = \{ h_{14}, h_{15}, h_{16}, h_{17}, h_{18}, h_{19}, h_{20}, h_{21}, h_{22}, T_7 \}$	$\beta_k^{'} = h_{21} \oplus h\left((A_k^*)_x \| 2\right)$
$\xrightarrow[ID_i \ 2 \ ID_k]{M_6}$	$\xrightarrow[ID_k \ 2 \ RA]{M_7}$	$Cr_k \leftarrow h\left(ID_k \| r_i \| sk\right)$
		$\beta_k \leftarrow \gamma_k \oplus Cr_k$
	Step4 if $T_9 - T_8 \leq \Delta T$	if $HD\left(\beta_k, \beta_k^{'}\right) \leq \delta$
	$ID_l^{'} \leftarrow h_{23} \oplus h\left((A_k^*)_y \| \alpha_k \| \beta_k^{'} \| 1\right)$	$A_i^* \leftarrow skA_i = \left((A_i^*)_x, (A_i^*)_y\right)$
	$ID_i^{'} \leftarrow h_{24} \oplus h\left((A_k^*)_y \| \alpha_k \| \beta_k^{'} \| 2\right)$	$ID_i^{'} = h_{15} \oplus h\left((A_i^*)_x \| 1\right)$
	$Cr_k \leftarrow \kappa_k \oplus h\left(ID_k \| PW_k \| h_b\left(B_k\right)\right)$	search for $ID_i^{'}$ in L_U
	$R_l \leftarrow \beta_l \oplus Cr_k$, $C_l \leftarrow \gamma_l \oplus Cr_k$	if $ID_i^{'} = ID_i$ and h_{18} is valid
	$h_{29} \leftarrow h\left(ID_l \| C_l \| R_l \| T_9\right)$	$\beta_i^{'} = h_{17} \oplus h\left((A_i^*)_x \| 2\right)$
	sends $\{ C_l, h_{29}, T_9 \}$ to ID_l *if*	$Cr_i \leftarrow h\left(ID_i \| r_i \| sk\right)$
	$T_{10} - T_9 \leq \Delta T$, $R_l^{'} \leftarrow h_b\left(PUF_l\left(C_l\right)\right)$	$\beta_i \leftarrow \gamma_i \oplus Cr_i$
	if $h_{29} = h\left(\left(R_l^{'} \oplus \alpha_l\right) \| C_l \| R_l \| T_9\right)$	if $HD\left(\beta_i, \beta_i^{'}\right) \leq \delta$
	$R_l^* \leftarrow h_b\left(PUF_l\left(h\left(C_l \| T_9\right)\right)\right)$	$ID_l^{'} = h_{16} \oplus h\left((A_i^*)_x \| 2\right)$
	updates $\alpha_l^* \leftarrow R_l^* \oplus R_l^{'} \oplus \alpha_l$	if ID_i in AL_l^k, $\alpha_k \leftarrow \eta_k \oplus Cr_k$
	$h_{30} = h\left(ID_l \| C_l \| R_l \| R_l^* \| ss_{lk} \| T_{10}\right)$	$h_{23} \leftarrow ID_l^{'} \oplus h\left((A_k^*)_y \| \alpha_k \| \beta_k^{'} \| 1\right)$
	sends $\{ R_l^* \oplus R_l^{'}, h_{30}, T_{10} \}$ to ID_k	$h_{24} \leftarrow ID_i^{'} \oplus h\left((A_k^*)_y \| \alpha_k \| \beta_k^{'} \| 2\right)$
Step5	if T_{10} and h_{30} are valid, updates	$r_6 \xleftarrow{\$} Z_q^*$, $\alpha_i \leftarrow \eta_i \oplus Cr_i$
if $T_{12} - T_{11} \leq \Delta T$	$\beta_l^* \leftarrow R_l^* \oplus Cr_k$, $\gamma_l^* \leftarrow C_l^* \oplus Cr_k$	$r_{ik} \leftarrow h\left(ID_i^{'} \| ID_k^{'} \| ID_l^{'} \| \beta_i^{'} \| \beta_k^{'} \| r_6\right)$
$r_{ik}^{'} \leftarrow h_{26} \oplus h\left((A_i^*)_y \| \alpha_i \| \beta_i^{'}\right)$	$r_{ik}^{'} \leftarrow h_{25} \oplus h\left((A_k^*)_y \| \alpha_k \| \beta_k^{'} \| 3\right)$	$h_{25} \leftarrow r_{ik} \oplus h\left((A_k^*)_y \| \alpha_k \| \beta_k^{'} \| 3\right)$
if $h_{28} = h\left(h_{26} \| r_{ik}^{'} \| \beta_i^{'}\right)$	if $h_{27} = h\left(h_{23} \| h_{24} \| h_{25} \| r_{ik} \| \beta_k^{'}\right)$	$h_{26} \leftarrow r_{ik} \oplus h\left((A_i^*)_y \| \alpha_i \| \beta_i^{'}\right)$
$ss_{ik} \leftarrow h\left(ID_i \| r_{ik}^{'} \| r_4 h_{19}\right)$ if	$ss_{ki} \leftarrow h\left(ID_i^{'} \| r_{ik}^{'} \| r_5 h_{14}\right)$	$h_{27} \leftarrow h\left(h_{23} \| h_{24} \| h_{25} \| r_{ik} \| \beta_k^{'}\right)$
$h_{31} = h\left(r_{ik}^{'} \| h_{19} \| h_{26} \| h_{28} \| ss_{ik}\right)$	sets $T_{ikl} = T_{11}$ and writes	$h_{28} \leftarrow h\left(h_{26} \| r_{ik} \| \beta_i^{'}\right)$
sets $T_{ikl} = T_{12}$ and writes $\{A_{ikl}$,	$\{A_{ikl}, ID_i, ID_l, T_{ikl}, r_{ik}^{'}\}$ to cache	$M_8 = \{h_{23}, h_{24}, h_{25}, h_{26}, h_{27}, h_{28}, T_8\}$
$ID_k, ID_l, T_{ikl}, r_{ik}^{'}\}$ to cache	$h_{31} \leftarrow h\left(r_{ik}^{'} \| h_{19} \| h_{26} \| h_{28} \| ss_{ki}\right)$	$\xleftarrow[RA \ 2 \ ID_j]{M_8}$
$h_{32} \leftarrow h\left(r_{ij}^{'} \| ss_{ik} \| T_{12}\right)$	$M_9 = \{h_{19}, h_{26}, h_{28}, h_{31}, T_{11}\}$	
$M_{10} = \{h_{32}, T_{12}\}$	$\xleftarrow[ID_k \ 2 \ ID_i]{M_9}$	
$\xrightarrow[ID_i \ 2 \ ID_k]{M_{10}}$	**Step6** if T_{12} and h_{32} are valid, accepts	

Figure 6

User-Patient Authentication Phase of Our Scheme

$\mathbf{User}(ID_i, PW_i, B_i)$	$\mathbf{RA}(sk)$
inputs $ID_i^{'}, PW_i^{'}, PW_i^{*}$, generates $B_i^{'}$	
$\beta_i \leftarrow h_b\left(B_i^{'}\right) \oplus h\left(ID_i^{'} \| PW_i^{'}\right)$	
$\beta_i^{*} \leftarrow h_b\left(B_i^{'}\right) \oplus h\left(ID_i^{'} \| PW_i^{*}\right)$	
$r_7 \xleftarrow{\$} Z_q^{*}$, $A_i \leftarrow r_7 P, h_{33} \leftarrow A_i$	
$A_i^{*} \leftarrow r_7 PK = \left(\left(A_i^{*}\right)_x, \left(A_i^{*}\right)_y\right)$	
$h_{34} \leftarrow ID_i^{'} \oplus h\left(\left(A_i^{*}\right)_x \| 1\right)$	
$h_{35} \leftarrow \beta_i^{'} \oplus h\left(\left(A_i^{*}\right)_x \| 2\right)$	
$h_{36} \leftarrow \beta_i^{'} \oplus \beta_i^{*}$	
$h_{37} \leftarrow h\left(ID_i^{'} \| h_{33} \| h_{34} \| h_{35} \| h_{36} \| T_{13}\right)$	
sends $\{h_{33}, h_{34}, h_{35}, h_{36}, h_{37}, T_{13}\}$ to RA	if $T_{14} - T_{13} \leq \Delta T$
	$A_i^{*} \leftarrow skh_{33} = \left(\left(A_i^{*}\right)_x, \left(A_i^{*}\right)_y\right)$
	$ID_i^{'} \leftarrow h_{34} \oplus h\left(\left(A_i^{*}\right)_x \| 1\right)$
	search for $ID_i^{'}$ in L_U
	if $ID_i^{'} = ID_i$ and
	$h_{37} = h\left(ID_i \| h_{33} \| h_{34} \| h_{35} \| h_{36} \| T_{13}\right)$
	$\beta_i^{'} \leftarrow h_{35} \oplus h\left(\left(A_i^{*}\right)_x \| 2\right)$
	$Cr_i = h\left(ID_i \| r_i \| sk\right)$
	$\beta_i \leftarrow Cr_i \oplus \gamma_i$
	if $HD\left(\beta_i, \beta_i^{'}\right) \leq \delta$
	$\gamma_i^{*} \leftarrow h_{36} \oplus \beta_i^{'} \oplus Cr_i$
	$\gamma_i \leftarrow \gamma_i^{*}$
	$h_{38} \leftarrow h\left(ID_i \| \left(A_i^{*}\right)_y \| \beta_i^{'} \| T_{14}\right)$
if $T_{15} - T_{14} \leq \Delta T$ and	sends $\{h_{38}, T_{14}\}$ to ID_i
$h_{38} = h\left(ID_i \| \left(A_i^{*}\right)_y \| \beta_i^{'} \| T_{14}\right)$	
accepts update	

Figure 7

Password Update Phase of Our Scheme

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Appendix.pdf