Wireless Networks (2023) 29:1421–1438
https://doi.org/10.1007/s11276-022-03205-4

ORIGINAL PAPER

Provably secure certificateless protocol for wireless body area network

Susmita Mandal[1]

Accepted: 1 December 2022 / Published online: 15 December 2022

Abstract

Wireless body area networks are gaining popularity due to their innovative applications such as timely analysis, remote monitoring of patients' health, and high patient care quality. However, these healthcare systems that carry patient's physiological data need special attention for the security and privacy of information. Due to the openness of transmitted data, the healthcare system gets prone to several adverse attacks. In this paper, a provably secure remote healthcare system is proposed based on the elliptic curve cryptosystem. The goal is to enable confidentiality and privacy of sensitive information by designing a certificateless authenticated key agreement protocol with low computational cost and higher security. The proposed scheme achieves anonymity, resistance to key escrow problems, mutual authentication between the sensor nodes attached to patients and the application provider. Furthermore, the protocol undergoes formal security analysis using the random oracle model, and the soundness of the proposed scheme is validated using ProVerif. Finally, the performance analysis depicts that the proposed scheme is efficient compared to existing methods.

Keywords Authentication · Certificateless · Elliptic-curve cryptography · ProVerif · Wireless body area network (WBAN)

1 Introduction

The rapid advancement in the Internet of Things (IoT) has brought significant improvements in human life. IoT enables a connection between interrelated computing devices with the Internet that gathers information over the network without any person-to-person or person-to-computer interaction. It has a broader application, like wireless sensor networks, smart homes, smart transportation, intelligent healthcare systems, etc. Among these, the wireless body area network (WBAN) has become an essential application in the healthcare ecosystem. WBANs are useful in short distance communication that consists of wearable sensor nodes responsible for monitoring the patient's health-related sensitive information such as heartbeat rate, body temperature, blood pressure, blood sugar, oxygen level, etc. This technology provides a high quality of convenient and reliable service using IoT devices. These networks are beneficial to elderlies with permanent care at home. The biosensors are placed in or around the patient connected through a star or multi-hop topology. These sensors are responsible for sending the patient's sensed data to the medical doctor to provide a real-time diagnosis with the right decisions. The shared information traverses several resource constraints devices, making it challenging to secure the transmitted data confidentiality. As if the patient's physiological data is tampered with during the transmission process, it will mislead the physician, which will result in a false diagnosis of the patient's health condition. Another crucial challenge concerns the resource-constrained devices connected to the patient; therefore, they must be exposed to lower complex computations for efficiency. Therefore, the patient's medical record's security and privacy are the primary concern in the healthcare industry. The data transmitted over the public network must be accessible by only authorized entities [1]. However, strong authentication and the key establishment must be achieved for securing the communication of WBAN. The first WBAN work was proposed by Zimmerman using a wireless personal area network (WPAN) technology [2]. In 2001, Van et al. introduced the concept of body area networks as a step towards a wearable future [3]. The traditional public-key cryptosystem uses trusted Certificate Authority (CA) to bind the user identity to the public key

✉ Susmita Mandal
susmitamandal.nitrkl@gmail.com

[1] Institute for Development and Research in Banking Technology, Hyderabad, India

that causes heavy management overhead. Identity-based cryptosystem eliminates the need for explicit certificates by assigning public keys to its user identity; however, it suffers from the key-escrow problem. Over the decade, several WBAN models have been proposed. Still, the privacy and security of a patient stand as a big challenge for researchers. Authentication in WBAN is a relatively new research paradigm; however, few articles have recently discussed this research topic. Most of the existing schemes are based on traditional public key infrastructure (PKI) [4–6] and identity-based cryptosystem (IBC) [7–9].

1.1 Related work

In the recent COVID-19 pandemic, the need for a remote health monitoring system shows promising solutions where a physician can remotely observe critical patients' health status. However, patients' physiological data need to be secured during transmission such that unauthorized entities can not access it. Therefore, it is necessary to enhance the security, which protects data from unauthorized manipulation and confidentiality to prevent data leakage. It is achieved from authenticated key agreement mechanism, which plays a vital role in dealing with the security requirements. Several schemes have recently been proposed for authenticating clients with the application provider remotely in a WBAN environment. However, these authentication schemes are based on traditional public-key cryptography (PKC) and identity-based cryptosystem (IBC) with complex computations. The difficulties in managing the certificates in public key infrastructure for the PKC make it unsuitable for WBAN. Whereas the IBC overcomes the certificate issuing and management problems, however, suffers from the key escrow problem. Al-Riyami and Paterson proposed a certificateless public key cryptography (CL-PKC) to overcome the issues mentioned earlier. However, the scheme increases the overall computation cost due to the usage of complex bilinear pairing operations [10]. In 2012, Drira et al. [11] has proposed an ID-based hybrid authentication and key establishment scheme based on a symmetric key cryptosystem. However, Kompara et al. [12] states that the protocol lacks data confidentiality, integrity, forward and backward secrecy. Also, it is susceptible to key escrow and impersonation attacks. In 2013, Liu et al. [13] proposed a lightweight certificateless authentication protocol based on a short certificateless signature method. However, the scheme fails to achieve session key security. Later Liu et al. [14] tried to resolve the issues mentioned in his above protocol by designing two certificateless remote anonymous authentication schemes for WBANs, namely, preliminary scheme and enhanced secure scheme. In contrast, Hu Xiong et al. [15] proves that the two protocols suffer from public key replacement attack. Zhao [16] pointed out that the preliminary version can not provide anonymity and the security-enhanced version suffers from stolen verifiertable attacks. In 2014, Zhao [16] proposed an efficient anonymous authentication scheme for wireless body area networks using ECC. Later, Wang et al. [17] demonstrated that [16] scheme lacks user anonymity and unable to provide unlikability features and proposed a new anonymous authentication scheme using bilinear pairing. In 2016, Wu et al. [18] found that [17] scheme is susceptible to impersonation attack. Recently, He et al. [19] proved that Liu et al. [13] also suffers from impersonation attack. Therefore, it may not suit the e-healthcare based privacy-preserving applications. Further, they have proposed a provably secure anonymous authentication scheme for WBANs. Several other schemes were proposed based on certificateless cryptosystem to overcome the traditional challenges, like Hu Xiong et al. [20] presented an anonymous certificateless authentication scheme for remote WBANs. Although the scheme withstands key escrow problems due to bilinear pairing usage, the scheme suffers from heavy computation overhead. Liu et al. [21] presented an anonymous 1-round authentication protocol for WBAN based on ECC and claims to achieve essential security features. However, Li et al. [22] prove that the scheme fails to provide key-compromise impersonation attack, stolen-verifier attack, and denial-of-service attack, and proposes an enhanced 1-round authentication protocol based on ECC. Later, Khan et al. [23] designed an improvement over Li et al. [22] by enabling a privacy-preserving key agreement for WBANs to achieve forward secrecy and unlinkability issues. Recently, Hassan et al. [24] proposed an ID-based authenticated key agreement protocol using a pairing-based cryptosystem. The protocol applies a ring signature to authenticate users within the multi-server environment anonymously. However, Kumar et al. [25] show that the scheme suffers from impersonation attack, man-in-the-middle attack, and significantly has higher computation cost. Shen et al. [26] proposed an anonymous certificateless authentication scheme. The protocol enables secure communication between hand-held PDA and application provider. However, the protocol lacks user anonymity and also suffers from collusion attack [27]. In 2020, Kasyoka et al. [28] proposed a pairing-free authentication scheme for healthcare management and proves that the protocol can thwart stolen verifier attacks. However, the scheme lacks rigorous formal security analysis. Recently, Sowjanya et al. [29] proved that [22] scheme lacks perfect forward secrecy, which is essential session key secrecy and has proposed a new end-to-end authenticated scheme for wearable monitoring devices. In the same year, Shuai et al. [30] introduced a privacy-preserving authentication scheme for WBANs using ECC suitable for multi-server architecture. Lately, Kumar et al. [31] proposed an identity-based anonymous authentication and key agreement scheme for WBAN.

In 2021, Azees et al. [32] proposed an efficient anonymous affine cipher-based encryption technique for WBANs. The work focuses on enhancing data confidentiality and authenticity, however the proposed model uses complex bilinear operations which increases the computational overhead. Therefore, the scheme may not be adequate for resource-constrained environment. Later, Lara et al. [33] proposed a two-party authentication scheme using self-certified public keys based on ECC for healthcare application. The scheme focus to establish communication between the patient's portable personal terminal and an application provider (AP) with a Two-party scheme. The scheme has lowered the computational cost but lacks consideration of honest but curious network manager during registration as the secret values are accepted without verification by end nodes. To address the high computation cost Soni et al. [34] proposes an authentication and key agreement mechanism using low-cost functions (one-way hash, bit-wise XOR, and concatenation) for data exchanges in WBAN. The patient wearing a smart wearable device will collect real-time health information and share with healthcare providers. The protocol lacks discussion on prevention from hash collusion attack and is also vulnerable to offline password-guessing attacks. Peng et al. [35] proposes an efficient certificateless online/offline signature scheme which is designed in a lightweight manner for WBANs. The scheme focuses on ensuring both security and efficiency of the online/offline signature for the real-world deployment. The scheme tries to reduce the computational cost by addressing the offline mode of verification. In order to achieve data confidentiality and fine-grained access control simultaneously on transmitted data Liu et al. [36] proposed an attribute-based online/offline encryption and Identity-based ring signature scheme to achieve an outsourced online/offline hybrid signcryption mechanism applied for WBAN. The scheme allow patients to share fine-grained data without leaking any extra information. Despite its promising solution, the scheme may lead to the heavy computational cost on resource-constrained devices. Later, Cheng et al. [37] proposed an improvement on Kumar et al. [31] scheme on lightweight cloud-assisted identity-based AKA scheme for WBAN. They claimed that the scheme lacks perfect forward secrecy and proposed a protocol a new anonymous identity-based AKA scheme. The proposed scheme claimed to be a certificateless AKA scheme, however the key shared by the network manager to cloud server and leaf node are not partial private keys but private keys. An approach of annonymization using identity-based authenticated encryption scheme without bilinear pairing, known as IB-AAE is proposed by Li et al. [38]. The scheme combines the functionality of being anonymous and identity-based encryption, to achieve forward security. However, the generation of private keys are completely dependent on the trusted key generator. Recently, Hasan et al. [39] proposed an architectural framework that incorporates blockchain with Software-Defined Wireless Body Area Networks (SDWBANs) to facilitate secure data sharing. The proposed framework of WBAN is modified by adding SDN enabled switches to communicate with sensors and forwarding the information through an interface between to Blockchain for just access validation. This solution may increase the overhead of data management and communication across the WBAN layers.

So far, from the literature study, it is clear that using identity based cryptosystem may create a key escrow problem. As a malicious PKG could perform a man-in-the-middle (MITM) attack using the private keys. Therefore, desiging a certificateless authenticated key agreement protocol with backward and forward secrecy is suitable for resource constraint wireless body area networks. As the patient's health information is very sensitive data, it must be accessed only by the authorized medical staff, including doctors and technicians. Therefore it is crucial to obtain data security to wireless body area networks such that confidential information may not be altered or abused by misusers. A remote WBAN based authenticated key agreement protocol must withhold the following properties: user authentication, data integrity, session key security, replay attack, impersonation attack, backward and forward secrecy. This paper proposes a provably secure certificateless authenticated key agreement protocol to meet the security requirements mentioned above and the challenges. The main contributions of this paper are summarized as follows:

1. Design of a pairing-free secure authentication protocol that overcomes the traditional certificate issuing and management problem of public-key cryptosystem and achieves immunity against key escrow problem faced by IBC.
2. The proposed scheme enables the network manager to generate partial private keys for each registered entity which can be validated publicly, thus preventing impersonating legitimate users.
3. The security is based on the hardness assumption of Elliptic Curve Diffie–Hellman assumption and Computational Diffie–Hellman (CDH) problem. The scheme undergoes rigorous formal analysis and informal analysis using automated protocol analyzer ProVerif, and formal analysis using Real-Or-Random (ROR) model.

4. The comparative analysis of the scheme is performed concerning computation, communication, and security features with existing schemes.

1.2 Paper organization

The rest of the paper is organized as follows. Section 2 deals with the mathematical background, network model, system model, and security model. The proposed scheme is depicted in Sect. 3. In Sect. 4, the formal informal security analysis along with protocol validation using ProVerif is presented. The performance analysis concerning security features, computation, and communication costs is shown in Sect. 5. Finally, we conclude in Sect. 6.

2 Preliminaries

This section provides brief introduction of cryptographic techniques used in this paper, network model, system model, and security model.

2.1 Elliptic curve cryptography

The security of Elliptic curve cryptography (ECC) is based upon the difficulty of solving Ellipic curve discrete logarithmic problem (ECDLP). Let E/F_q be a set of elliptic curve points over a finite field F_q, defined by an equation

$$y^2 = x^3 + ax + b, \quad a, b \in F_q \tag{1}$$

where $(4a^3 + 27b^2) \neq 0$. The additive elliptic curve group defined as $G_q = \{(x, y) : x, y \in F_q, (x, y) \in E/F_q\} \cup \{O\}$, where the point *"O"* is known as *"point at infinity"* or *"zero point"*. The definitions about the elliptic curve group as follows.

- *Point addition* Let P, Q be two points on the curve shown in Eq. (2), such that P+Q=R, where the line joining P and Q intersects the curve at negative R, and the reflection towards *x-axis* is R.
- *Scalar point multiplication* It is defined on a cyclic group G_q as $rP = P + P + \cdots + P(rtimes)$, where $r \in Z_q^*$ is scalar.

2.2 Computational problem

Definition 1 (Elliptic curve discrete logarithm problem (ECDLP)) Given $P, R \in G_q$, where R=xP and $x \in Z_q^*$. It is difficult to compute x from R.

Definition 2 (Computational Diffie–Hellman problem (ECDH)) Given (P,xP,yP) $\in$ G_q for $x, y \in Z_q^*$, where computation of xyP is hard from the group G_q.

2.3 Network model

The WBAN ecosystem consists of in-body, on-body, and off-body sensors which communicate and share data across three layers. The description is depicted in Fig. 1.

- *Layer 1* In this layer, the sensor nodes placed over and within the body communicate with the aggregator (i.e., mobile device). This layer is also known as Intra-BAN, i.e., an internal network.
- *Layer 2* In this layer, the aggregator passes the collected data to the access points. This layer is also known as Inter-BAN.
- *Layer 3* This layer depicts whole network of the server where communication happens beyond the BAN, therefore known as Beyond-BAN. The transmission occurs over a TCP/IP connection between the access points and the medical server.

2.4 System model

The proposed model consists of three entities, namely, the Patient's Mobile device (MD), Application Provider (AP), and Network Manager (NM). The model is depicted in Fig. 2.

- *Patient's mobile device (MD)* The patient implies to the person who avails the medical facilities remotely. With sensors placed in or on the body to collect physiological information. These pieces of information are sent to an intermediate node known as an aggregator, such as PDA and hand-held mobile device. The sensors and mobile device should be registered with the Network Manager before it accesses the Application Provider's services.
- *Network manager (NM)* It acts as a Key Generation Center (KGC) responsible for registering the sensor nodes, aggregator device, and application providers to legally access and avail the services. After the registration process, the NM generates partial private keys for every node and distributes them through a secure channel (i.e, TLS protocol). It is more likely a trusted third party that manages the whole network and participants.
- *Application provider (AP)* This represents the hospitals that the network manager authorizes to provide services to patients suffering from any critical ailment.

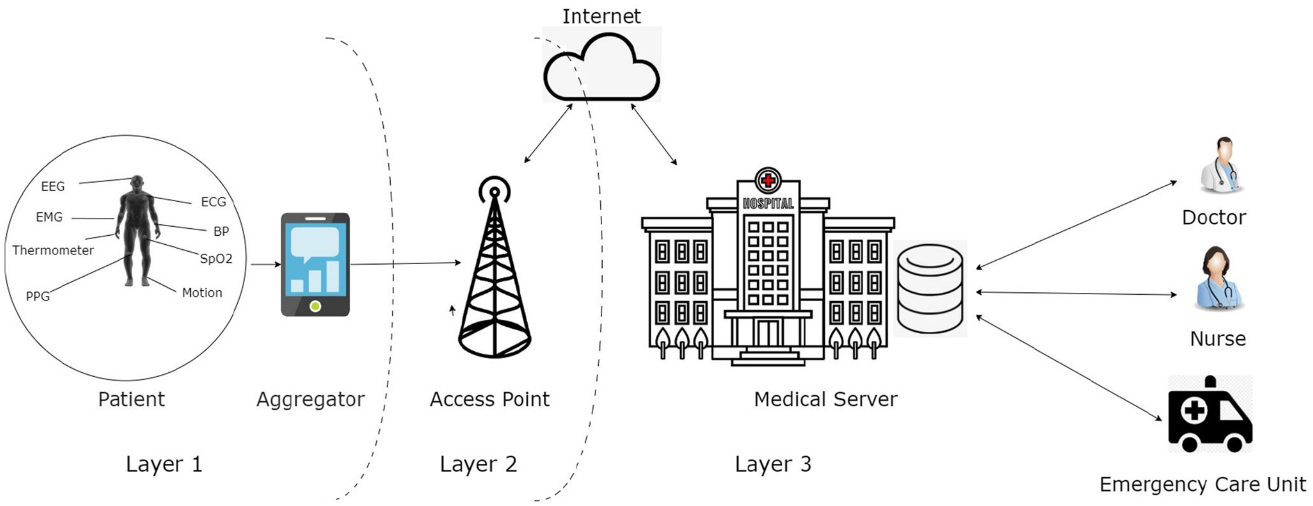


Fig. 1 Architecture of a WBAN

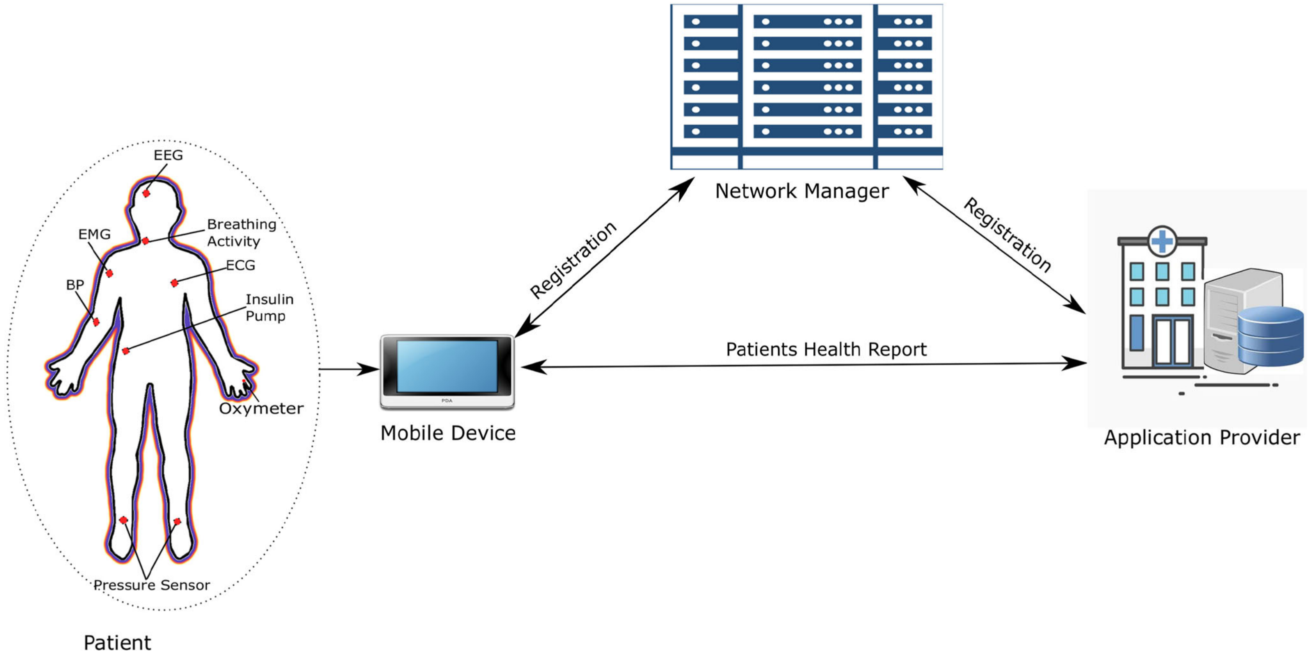


Fig. 2 System model of a WBAN

2.5 Security model

This section outlines the widely accepted Dolev-Yao threat model [40] pursued in the paper using the following assumptions:

- The Network Manager (NM) is assumed to be a trusted server that generates a partial private key for every registered user. Therefore, even if a passive/active adversary compromises the partial private key, he/she will not be able to forge the session key. The full private key is generated using the secret value and partial private key of each participating entity.
- The messages exchanged at the authentication phase between two entities are communicated over an insecure channel. An adversary can eavesdrop on all the messages transmitted and intercept, inject, modify, and resend any previously sent message. However, the adversary can not access messages in a secure channel.
- The application provider is assumed to be trustworthy; however, an adversary can compromise the database for malicious purposes.

- A privileged insider can act as an adversary by intercepting the registered request parameters.

3 Proposed work

In this section, the proposed certificateless authenticated key agreement protocol is discussed, which involves three phases: (1) Initialization, (2) Registration, and (3) Authentication. The registration occurs in a secure channel, with all the participating entities registering themselves with the network manager. A secure channel can be defined as a bidirectional communication medium that ensures the confidentiality, integrity, and freshness of data transferred through the channel. This can be achieved either by exchanging data through a trusted person in offline mode or through a strong Transport Layer Security (TLS) connection, defined in RFC 8446 [34, 41]. Typically the registration process is a one-time matter. Thus, an adversary cannot tamper the partial private keys sent by the entities during the registration process. In contrast, the authentication and key agreement phase between the aggregator and the application provider occur through an open/insecure channel, which means that an adversary (based on the Dolev-Yao model) can intercept, modify, delete the message tuple [42]. The notations used throughout the paper are mentioned in Table 1.

3.1 Initialization phase

Network manager chooses a security parameter 1^k as input and generates a group G with prime order q and determines a point P as generator in group G. The NM then selects a random integer $s_{nm} \in Z_q^*$ as a master key and computes a public key $P_{nm} = (s_{nm} \cdot P)$. Then six different hash functions are computed based on SHA-256 algorithm taking following three types of input sets: (a) $\{0,1\}^*$ is the set of binary bit-strings of arbitrary size, (b) Z_q^* is a set of positive integers where q is prime number, and (c) G is a cyclic multiplicative group of prime q, to obtain different hash values. The hash functions are depicted as follows: $H_0 : \{0,1\}^* \times Z_q^* \rightarrow Z_q^*$, where hash function H_0 takes a set of binary bit-strings of arbitrary length concatenated with a set of integers and result is the integer coded in set Z_q^*. Similarly, $H_1 : Z_q^* \times Z_q^* \rightarrow Z_q^*$, $H_2 : Z_q^* \times G \rightarrow Z_q^*$, $H_3 : \{0,1\}^* \times G \times G \rightarrow Z_q^*$, $H_4 : G \times Z_q^* \times G \times Z_q^* \rightarrow Z_q^*$, $H_5 : \{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times G \times G \rightarrow Z_q^*$. Later, NM publishes the public parameters $params = \{G, q, P, P_{nm}, H_0, H_1, H_2, H_3, H_4, H_5\}$ while keeping the master key (s_{nm}) secret.

Table 1 Notations

Notation	Description
s_{nm}	Master secret key of network manager
P_{nm}	Public key of network manager
ID_u	Identity of patient
x_u	Private key of patient
P_u	Public key of patient
x_{ap}	Private key of application provider
P_{ap}	Public key of application provider
t_i/t_u	Timestamp
P	Generator of the elliptic curve
$\|\|$	Concatenation function
$\oplus$	XOR operation
SK	Session key between patient and application provider
H_i	Cryptographic hash function $\forall i \in \{0,1,2,3,4,5\}$
$A \overset{?}{=} B$	Verifies whether A is equal to B

3.2 Registration phase

In this phase, the patients must register the mobile device with network manager. Similarly, the application provider must register with required details to the network manager. Where NM is a trusted authority. In real-time, the role of NM can be hosted by a central e-healthcare institution or any distributed authorized center. Patients willing to avail remote healthcare facilities from the application provider (i.e., medical institutions) must register their mobile devices assigned as an aggregator to receives details from the sensor nodes. The NM generates partial private keys to all the noted entities. The registration process is described below and also depicted in Fig. 3.

3.2.1 Sensor nodes registration

Step 1 The Application provider (AP) deploys the sensor nodes (SN) to each patient upon registration with NM. The AP generates $ID_{SNi} \in \{0,1\}^*$ and a random secret $s_{ri} \in Z_q^*$ where $\forall i \in \{1,2,3,\ldots,n\}$. Then computes $N_i = H_0(s_{ri}||ID_{SNi})$ and sends the message tuple $\langle ID_{ap}, N_i \rangle$ to NM. Once received, NM stores it in its database. Similarly, AP sends $\langle ID_{SNi}, N_i \rangle$ to sensor nodes later stores in its memory.

Step 2 Upon receiving the message tuple NM generates a random number $r_{SNi} \in Z_q^*$, a fresh nonce N_c and computes $Y_i = N_i \oplus H_1(s_{nm}||r_{SNi})$, $SK_{sn} = H_1(s_{nm}||r_{SNi}) \oplus (ID_{nm}||N_c)$. Later after the registration of MD, network manager computes $K_i = N_i \oplus H_2(Q_{md}||R_{md})$ and sends a message tuple $\langle Y_i, SK_{sn}, N_c, K_i, ID_{nm} \rangle$ to sensor nodes.

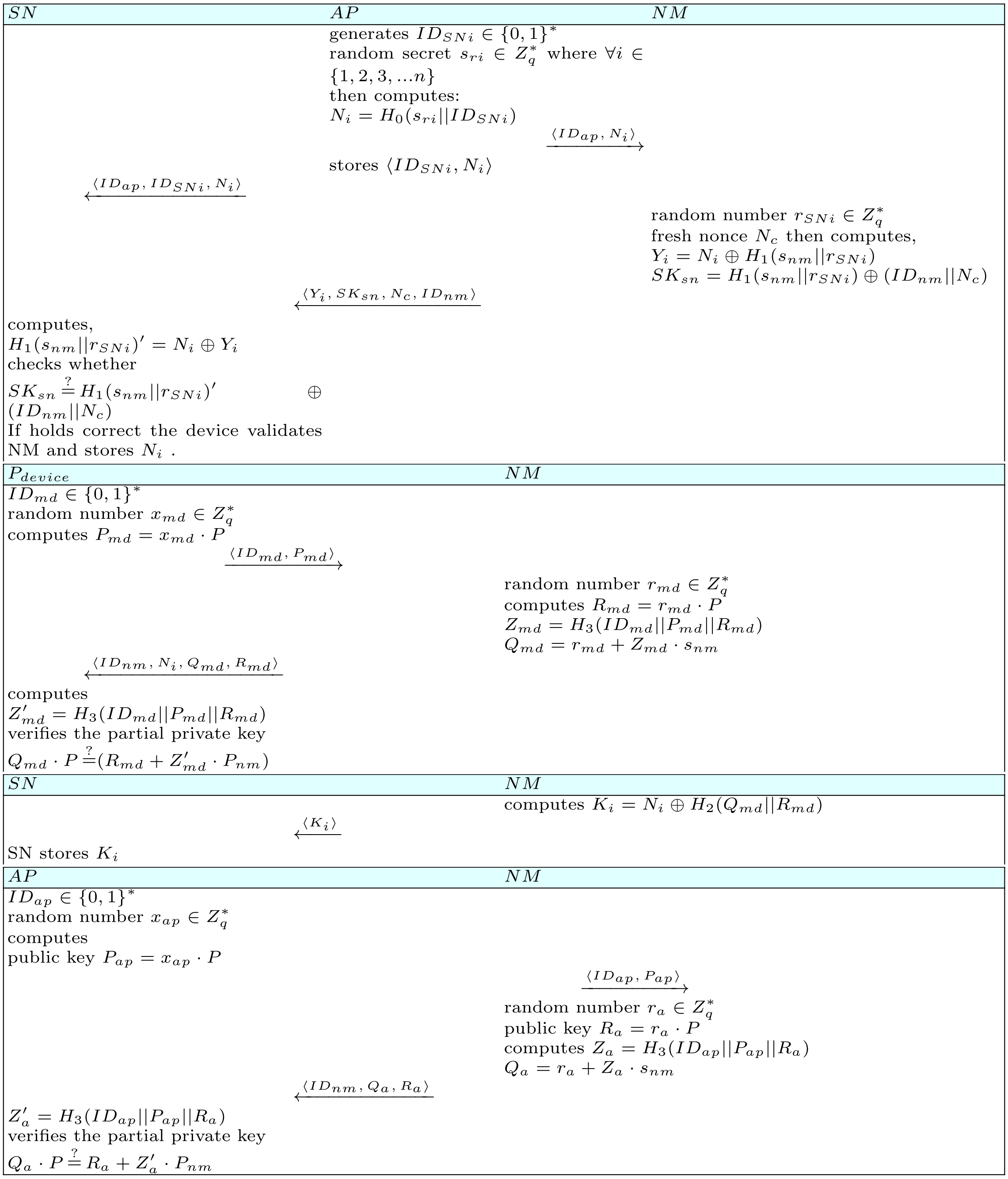

SN
AP
NM
generates $ID_{SNi} \in \{0,1\}^*$
random secret $s_{ri} \in Z_q^*$ where $\forall i \in \{1,2,3,...n\}$
then computes:
$N_i = H_0(s_{ri}||ID_{SNi})$
$\xrightarrow{\langle ID_{ap}, N_i \rangle}$
stores $\langle ID_{SNi}, N_i \rangle$
$\xleftarrow{\langle ID_{ap}, ID_{SNi}, N_i \rangle}$
random number $r_{SNi} \in Z_q^*$
fresh nonce N_c then computes,
$Y_i = N_i \oplus H_1(s_{nm}||r_{SNi})$
$SK_{sn} = H_1(s_{nm}||r_{SNi}) \oplus (ID_{nm}||N_c)$
$\xleftarrow{\langle Y_i, SK_{sn}, N_c, ID_{nm} \rangle}$
computes,
$H_1(s_{nm}||r_{SNi})' = N_i \oplus Y_i$
checks whether
$SK_{sn} \overset{?}{=} H_1(s_{nm}||r_{SNi})' \oplus (ID_{nm}||N_c)$
If holds correct the device validates NM and stores N_i .
P_{device}
NM
$ID_{md} \in \{0,1\}^*$
random number $x_{md} \in Z_q^*$
computes $P_{md} = x_{md} \cdot P$
$\xrightarrow{\langle ID_{md}, P_{md} \rangle}$
random number $r_{md} \in Z_q^*$
computes $R_{md} = r_{md} \cdot P$
$Z_{md} = H_3(ID_{md}||P_{md}||R_{md})$
$Q_{md} = r_{md} + Z_{md} \cdot s_{nm}$
$\xleftarrow{\langle ID_{nm}, N_i, Q_{md}, R_{md} \rangle}$
computes
$Z'_{md} = H_3(ID_{md}||P_{md}||R_{md})$
verifies the partial private key
$Q_{md} \cdot P \overset{?}{=} (R_{md} + Z'_{md} \cdot P_{nm})$
SN
NM
computes $K_i = N_i \oplus H_2(Q_{md}||R_{md})$
$\xleftarrow{\langle K_i \rangle}$
SN stores K_i
AP
NM
$ID_{ap} \in \{0,1\}^*$
random number $x_{ap} \in Z_q^*$
computes
public key $P_{ap} = x_{ap} \cdot P$
$\xrightarrow{\langle ID_{ap}, P_{ap} \rangle}$
random number $r_a \in Z_q^*$
public key $R_a = r_a \cdot P$
computes $Z_a = H_3(ID_{ap}||P_{ap}||R_a)$
$Q_a = r_a + Z_a \cdot s_{nm}$
$\xleftarrow{\langle ID_{nm}, Q_a, R_a \rangle}$
$Z'_a = H_3(ID_{ap}||P_{ap}||R_a)$
verifies the partial private key
$Q_a \cdot P \overset{?}{=} R_a + Z'_a \cdot P_{nm}$

Fig. 3 Registration phase

Step 3 Once SN receives the message, each sensor node computes $H_1(s_{nm}||r_{SNi})' = N_i \oplus Y_i$. Then every node checks whether $SK_{sn} \overset{?}{=} H_1(s_{nm}||r_{SNi})' \oplus (ID_{nm}||N_c)$. If it matches then the sensor nodes successfully validates that NM has shared the correct parameter N_i for future communication else reply with an $\perp$ message. Later, SN stores (K_i) in its database.

3.2.2 Patients registration

Step 1 Initially, the patient desiring to register for home care facility provides his/her identity, address proof along with device identification as $ID_{md} \in \{0,1\}^*$. Then generates a random number $x_{md} \in Z_q^*$ and computes its respective public key $P_{md} = x_{md} \cdot P$. Then the patient's device sends a message tuple $\langle ID_{md}, P_{md} \rangle$ to NM.

Step 2 Once received, NM first chooses a random number $r_{md} \in Z_q^*$ then computes $R_{md} = r_{md} \cdot P$, $Z_{md} = H_3(ID_{md}||P_{md}||R_{md})$, $Q_{md} = (r_{md} + Z_{md} \cdot s_{nm})$ as partial private key. Then responds back with message $\langle ID_{nm}, N_i, Q_{md}, R_{md} \rangle$ to patient's device.

Step 3 Upon receiving the response, patient's device computes $Z'_{md} = H_3(ID_{md}||P_{md}||R_{md})$ and verifies the partial private key as $Q_{md} \cdot P \overset{?}{=} (R_{md} + Z'_{md} \cdot P_{nm})$. Therefore, patient's mobile device holds the private keys $U_{priv} = (x_{md}, Q_{md})$ and public keys $U_{pub} = (P_{md}, Q_{md} \cdot P)$.

3.2.3 Application provider registration

Step 1 Like MD, the application provider sends his/her identity $ID_{ap} \in \{0,1\}^*$ then generates a random number $x_{ap} \in Z_q^*$ and computes the public key $P_{ap} = x_{ap} \cdot P$. Then sends the message tuple $\langle ID_{ap}, P_{ap} \rangle$ to NM.

Step 2 Once received, NM first chooses a random number $r_a \in Z_q^*$ and a public key $R_a = r_a \cdot P$. Then computes $Z_a = H_3(ID_{ap}||P_{ap}||R_a)$, $Q_a = (r_a + Z_a \cdot s_{nm})$ as the partial private key. Then responds back with message $\langle ID_{nm}, Q_a, R_a \rangle$ to AP.

Step 3 Upon receiving the message, the application provider then verifies the partial private keys as $Z'_a = H_3(ID_{ap}||P_{ap}||R_a)$ then check if $Q_a \cdot P \overset{?}{=} R_a + Z'_a \cdot P_{nm}$. Therefore, AP holds private keys $A_{pri} = (x_{ap}, Q_a)$ and public keys $A_{pub} = (P_{ap}, Q_a \cdot P)$ respectively.

3.3 Authentication phase

Upon completing the registration process with the network manager, now each sensor node attached to the patient body, senses the health vitals and share it with the mobile device. The patient's device is capable of communicating all the gathered information to the application provider for suitable diagnosis and treatment from concerned doctors. The process is described in following steps and depicted in Fig. 4.

Step 1 To begin the communication, each sensor node collect the information related to blood glucose, temperature, oxygen levels, pulse, blood pressure etc. Then send the aggregated data along with a timestamp t_i, parameter K_i stored in SN to the mobile device. The patient's device first checks if $|t_i - t_c| \leq \triangle T$ to validate whether the received timestamp t_i falls within the tolerable time delay $\triangle T$ else abort the message. Now MD computes $N'_i = K_i \oplus H_2(Q_{md}||P_{md})$ then check if $N'_i \overset{?}{=} N_i$ from database. If matches, then aggregates the health vitals from all the nodes and generate a fresh nonce n_u, timestamp t_u, and an ephemeral key $y_{md} \in Z_q^*$. Then computes, $C_1 = H_1(y_{md}||n_u)$, $F = x_{md} \cdot P_{ap}$, $C_2 = (P_{nm}||F||ID_{ap}||ID_{md}) \oplus C_1$, $C_3 = x_{md} + H_4(P_{ap}||t_u||P_{nm}||N'_i) \cdot C_1$. Later sends $\langle t_u, C_2, C_3 \rangle$ to the application provider.

Step 2 Once received, AP first checks whether the time stamp t_u is fresh as $t_u - t_n \leq \triangle T$. Then computes $F' = P_{md} \cdot x_{ap}$, $C'_1 = C_2 \oplus (P_{nm}||F'||ID_{ap}||ID_{md})$. AP checks whether $C_3 \cdot P \overset{?}{=} P_{md} + H_4(P_{ap}||t_u||P_{nm}||N_i) \cdot C'_1 \cdot P$ if matches, then AP further generates a random number n_a and a time-stamp t_a. Then computes, $D_1 = (y_{ap} + n_a)$, $K_z = C'_1 \cdot P_{ap}$, $D_2 = D_1 \oplus (K_z||ID_{md}||ID_{ap}||C_2)$, $D_3 = x_{ap} + H_4(C_3||P_{ap}||P_{md}||t_a) \cdot D_1$. Finally, computes the session key $SK = H_5(C'_1 \cdot D_1 \cdot P||K_z||ID_{md}||ID_{ap}||ID_{nm})$. Later, sends a message tuple $\langle t_a, D_2, D_3 \rangle$.

Step 3 Upon receiving the message tuple the patient's device checks the freshness of the timestamp as $t_a - t_n \leq \triangle T$. Then computes, $K'_z = C_1 \cdot P_{ap}$, $D'_1 = D_2 \oplus (K'_z||ID_{md}||ID_{ap}||C_2)$. Patient's device now checks whether $D_3 \cdot P \overset{?}{=} P_{ap} + H_4(C_3||P_{ap}||P_{md}||t_a) \cdot D'_1 \cdot P$ if matches then patient computes the session key $SK = H_5(C_1 \cdot D'_1 \cdot P||K'_z||ID_{md}||ID_{ap}||ID_{nm})$ for future communication.

4 Security analysis

In this section, a formal and informal (non-mathematical) security analysis of proposed scheme is performed. Furthermore, the protocol is verified using the widespread automated tool ProVerif.

4.1 Formal proof using ROR model

In this section, the formal security analysis using the probabilistic Real- Or-Random (ROR) model [43] is used to prove the session key security of the proposed scheme. The model states that an adversary $\mathcal{A}$ has complete control over all the transmitted messages between the entities such that, $\mathcal{A}$ can intercept, replay, or modify the messages. Though $\mathcal{A}$ does not have direct access to the private keys and session keys, however, it can perform the following queries to capture the leaked information.

In this scheme, there are three participants P_{device}, *Network Manager*, and *Application Provider*. For convenience we denote P_{device} as P_i and *Application Provider* AP_j such that P_i and AP_j represents the i^{th} and j^{th} instances of P_{device} and AP in the authentication phase. Each instance is considered to be an oracle which has three states *Accept*,

P_{device}	AP
Initially, P_{device} receives K_i from SN then computes, $N_i' = K_i \oplus H_2(Q_{md} \| \| P_{md})$ check if $N_i' \overset{?}{=} N_i$ If matches then generates a fresh nonce n_u, timestamp t_u, ephemeral key $y_{md} \in Z_q^*$ computes, $C_1 = H_1(y_{md} \| \| n_u)$, $F = x_{md} \cdot P_{ap}$, $C_2 = (P_{nm} \| \| F \| \| ID_{ap} \| \| ID_{md}) \oplus C_1$, $C_3 = x_{md} + H_4(P_{ap} \| \| t_u \| \| P_{nm} \| \| N_i') \cdot C_1$	
$\xrightarrow{\langle t_u, C_2, C_3 \rangle}$	
	Check if, $t_u - t_n \leq \triangle T$ computes, $F' = P_{md} \cdot x_{ap}$, $C_1' = C_2 \oplus (P_{nm} \| \| F' \| \| ID_{ap} \| \| ID_{md})$ Checks if, $C_3 \cdot P \overset{?}{=} P_{md} + H_4(P_{ap} \| \| t_u \| \| P_{nm} \| \| N_i) \cdot C_1' \cdot P$ if holds then generates a random nonce n_a and a time-stamp t_a Computes, $D_1 = (y_{ap} + n_a)$ $K_z = C_1' \cdot P_{ap}$ $D_2 = D_1 \oplus (K_z \| \| ID_{md} \| \| ID_{ap} \| \| C_2)$ $D_3 = x_{ap} + H_4(C_3 \| \| P_{ap} \| \| P_{md} \| \| t_a) \cdot D_1$ $SK = H_5(C_1' \cdot D_1 \cdot P \| \| K_z \| \| ID_{md} \| \| ID_{ap} \| \| ID_{nm})$
$\xleftarrow{\langle t_a, D_2, D_3 \rangle}$	
Check if $t_a - t_n \leq \triangle T$ Computes, $K_z' = C_1 \cdot P_{ap}$ $D_1' = D_2 \oplus (K_z' \| \| ID_{md} \| \| ID_{ap} \| \| C_2)$ & checks whether $D_3 \cdot P \overset{?}{=} P_{ap} + H_4(C_3 \| \| P_{ap} \| \| P_{md} \| \| t_a) \cdot D_1' \cdot P$ If holds correct then compute the session $SK = H_5(C_1 \cdot D_1' \cdot P \| \| K_z' \| \| ID_{md} \| \| ID_{ap} \| \| ID_{nm})$	

Fig. 4 Authentication phase

Reject, and $\perp$, where *Accept* means oracle receives correct message else sends a *Reject* message otherwise send a $\perp$ symbol means not able to produce a response. $\mathcal{A}$ can simulate following oracle queries:

- *Execute*(P_i, AP_j) It simulates passive attack and allow $\mathcal{A}$ to learn the messages exchanges between honest instances P_i and AP_j.
- *Send*$(P_i/AP_j, m)$ It simulates active attack where $\mathcal{A}$ can generate any message m and send it to P_i/AP_j. As a result, the corresponding operation is performed according to the protocol description.
- *SSReveal*(P_i/AP_j) It allows $\mathcal{A}$ to obtain session-specific information.
- *SKReveal*(P_i/AP_j) It allows $\mathcal{A}$ to obtain the session key held by P_i/AP_j, if it has been negotiated.
- *Corrupt*(P_i/AP_j) This query is used to capture the perfect forward secrecy, in which $\mathcal{A}$ is allowed to obtain the long-term private key.
- *Test*(P_i/AP_j) This query returns a session key or a random value else sends back a null value. $\mathcal{A}$ is allowed to send a single *Test* query. In response a coin $b \in \{0, 1\}$ is flipped. If $b = 1$ the session key is returned or a random value with same bit length is returned if $b = 0$.

Partnering The instances P_i and AP_j are partners if they authenticate each other and share the same session key.

Freshness As instances, P_i and AP_j are fresh, if the session key is not revealed *SKReveal*. The adversary $\mathcal{A}$'s goal is to identify the difference between a fresh session key from a random value.

Semantic security An adversary $\mathcal{A}$ can execute several *Test* queries to either P_i or AP_j. In this query, the oracle flips the coin b, if a bit b' is returned at the end of the experiment. $\mathcal{A}$ can win the game if $b' = b$. The advantage of $\mathcal{A}$ breaking the semantic security of the proposed certificateless authenticated key aggrement (CL-AKA) referred as W becomes $Adv_W^{CL-AKA}(\mathcal{A})$= $2Pr[b' = b] - 1$ where b' is the bit $\mathcal{A}$ guesses.

One-way hash function This query simulates the hash function. When P_i/AP_j receives the message m from $\mathcal{A}$, the hash value of m is calculated and returned to $\mathcal{A}$.

Lemma 1 (*Difference Lemma*): *Let* R_1,R_2 *and* R_3 *denote the events defined in some probability distribution. If* $R_1 \wedge \neg R_3 \Leftrightarrow R_2 \wedge \neg R_3$, *we have* $|Pr[R_1] - Pr[R_2]| \leq Pr[R_3]$ [44].

Theorem 1 *Assume* $\mathcal{A}$ *is a probabilistic polynomial time adversary against the semantic security who can issue at most* q_s *times Send query*, q_e *time Execute query*, *and* q_h *times hash query. The advantage of* $\mathcal{A}$ *is given as*

$$Adv_W^{CL-AKA}(\mathcal{A}) \leq (q_h^2/2^{(l+1)}) + (q_s + q_e)^2/2p + (q_s/2^l) + q_h Adv_{CL-AKA}^{ECDHP}(\mathcal{A}).$$

Proof In order to prove the semantic security of the proposed scheme, a sequence of gamer G_{m0} to G_{m4} is presented where G_{m0} represents the real attack. Let $Succ_i$ is the event where the adversary $(\mathcal{A})$ correctly guesses the bit b after the *Test* query.

Game G_{m0} This games simulation is the real attack situation against the protocol in the random oracle model. Thus, we have

$$Adv_W^{CL-AKA}(\mathcal{A}) = |2Pr[Succ_0] - 1| \qquad (2)$$

Game G_{m1} In this game, all the oracle queries and responses are stored in following list:

L_W stores all messages in the whole process.

L_H stores answers of all random hash oracles $H_0, H_1, H_2, H_3, H_4, H_5$.

L_T stores the transcript of all the messages. The answer to hash queries are generated in the form of (x, y, f) such that on a hash query $f(x)$ where $f \in \{H_0, H_1, H_2, H_3, H_4, H_5\}$, if the record x, y, f is found in the list L_H then return y directly, else a random string y with the same bit length will be produced as the returned value and then add x, y, f into the list L_H. It is observed that the transcript distribution of games G_{m0} and G_{m1} are indistinguishable. Therefore,

$$Pr[Succ_0] = Pr[Succ_1] \qquad (3)$$

Game G_{m2} In this game, all the oracle queries are simulated as same as in the game G_{m1}, however collision occurred at transcript and collision occur at hash queries are aimed to be avoided. According to the birthday paradox,

(a) $x_{md}, x_{ap} \in Z_q^*$, the probability of collision in the transcripts is at most $\frac{(q_s+q_e)^2}{2p}$.

(b) The probability of hash collision is at most $\frac{qh^2}{2^{l+1}}$ where l is the length of hash output string.

Therefore, we have $|Pr[Succ_2] - Pr[Succ_1]| \leq \frac{qh^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2p}$.

Game G_{m3} In this game, if adversary $(\mathcal{A})$ can guess the C_3 and D_3 without asking the random oracle queries H_4, then the scheme is aborted. Such situation appears in the send queries, which means G_{m3} and G_{m2} are indistinguishable unless this case occurs. Thus,

$$|Pr[Succ_3] - Pr[Succ_2]| \leq \frac{q_s}{2^l} \qquad (4)$$

Game G_{m4} In this game, the session key security is considered. The notion of this security feature is that $\mathcal{A}$ must not be able to obtain the past session keys even if some information among $\{y_{md}, n_u, y_{ap}, n_a, x_{ap}\}$ is revealed. The adversary $\mathcal{A}$ knows the session transcripts (t_u, C_2, C_3) and (t_a, D_2, D_3). The adversary must ask H_5 query to win the game. The goal of $\mathcal{A}$ is to compute the session key in the following four cases and by asking $Execute(P_i, AP_j)$ and hash queries.

(*Case 1*) $Corrupt(P_i)$ and $Corrupt(AP_j)$ are queried from which adversary $\mathcal{A}$ obtain the long-term private keys x_{md}, x_{ap} of P_i and AP_j respectively. However, to derive the session key $SK = H_1((y_{md} + n_u) \cdot (y_{ap} + n_a) \cdot P||((y_{md} + n_u) \cdot x_{ap} \cdot P)||ID_{md}||ID_{ap}||ID_{nm})$ either of the random nonces n_u, n_a and the ephemeral key y_{md} of P_i and y_{ap} of AP_j are also required.

(*Case 2*) $SSReveal(P_i)$ and $Corrupt(AP_j)$ are queried from which adversary $\mathcal{A}$ obtains the nonce n_u, ephemeral keys y_{md} of P_i and long-term private key x_{ap} of AP_j.

(*Case 3*) $Corrupt(P_i$ and $SSReveal(AP_j)$ are queried from which adversary $\mathcal{A}$ obtains the long-term secret key x_{md} of P_i and ephemeral key y_{ap} and nonce n_a.

(*Case 4*) $SSReveal(P_i)$ and $SSReveal(AP_j)$ are queried from which adversary $\mathcal{A}$ obtains the ephemeral key of both but not the private key. However, in all the above four cases, the information available to adversary are insufficient to break the ECDHP assumption. As a result the difference between G_{m3} and G_{m4} is negligible as long as the ECDHP assumption holds.

$$|Pr[Succ_4] - Pr[Succ_3]| \leq q_h Adv_{CL-AKA}^{ECDHP}\mathcal{A} \qquad (5)$$

In G_{m4}, all the random oracles are simulated. $\mathcal{A}$ is only left to guess the winning bit b after querying the *Test* query. Therefore, we have,

$$Pr[Succ_4] = \frac{1}{2} \qquad (6)$$

From Eq. 2, we have

$$\frac{1}{2}Adv_{W}^{CL-AKA}\mathcal{A} = |Pr[Succ_0] - \frac{1}{2}| \tag{7}$$

From Eqs. 3 and 4, we have

$$\frac{1}{2}Adv_{W}^{CL-AKA}\mathcal{A} = |Pr[Succ_1] - \frac{1}{2}| \tag{8}$$

Applying triangular inequality, we obtain,

$$\begin{aligned}|Pr[Succ_4] - Pr[Succ_1]| &\leq |Pr[Succ_4] - Pr[Succ_3]| \\ &+ |Pr[Succ_3] - Pr[Succ_1]| \\ &\leq |Pr[Succ_4] - Pr[Succ_3]| \\ &+ |Pr[Succ_3] - Pr[Succ_2]| \\ &+ |Pr[Succ_2] - Pr[Succ_1]| \\ &\leq \frac{q_h^2}{2^{l+1}} + \frac{(q_s+q_e)^2}{2p} + \frac{q_s}{2^l} + q_h Adv_{CL-AKA}^{ECDHP}(\mathcal{A})\end{aligned}$$

From the games G_{m0} to G_{m4} and using the Lemma 1, Theorem 1 is proven.

4.2 Informal security analysis

4.2.1 Mutual authentication

In the proposed scheme, at the authenticated phase the application provider verifies the authenticity of the patient communicating with his registered device as $C_3 \cdot P \overset{?}{=} P_{md} + H_4(P_{ap}||t_u||P_{nm}||N_i) \cdot C_1' \cdot P$. Similarly, the patients device also verifies whether the response is obtained from legitimate application provider by checking if $D_3 \cdot P \overset{?}{=} P_{ap} + H_4(C_3||P_{ap}||P_{md}||t_a) \cdot D_1' \cdot P$. Else the session is terminated. Therefore, the proposed scheme could provide mutual authentication successfully.

4.2.2 Resistance against sensor node impersonation attack

Suppose an adversary $\mathcal{A}$ intercepts the sensor node's message $\langle t_i, K_i \rangle$ claiming to be a legitimate sensor node to access the network for malicious gain. In the proposed scheme, an adversary fails to deduce the parameter K_i as the temporary identity N_i is computed using a random secret generated by the application provider and the identities of each sensor node. Then the one-way hash function is applied on N_i. Therefore, even if an adversary tries to compromise a sensor node the random secret cannot be disclosed.

4.2.3 Perfect forward secrecy

Suppose an adversary $\mathcal{A}$ had compromised the session key SK. The PFS holds when even after compromising long-term keys of the current session, it must not affect any past or future sessions. For instance, despite an adversary obtains P_{device} and AP's private keys to compute the session key SK, an adversary $\mathcal{A}$ still requires the ephemeral keys and random nonces which are different and fresh at every session. Therefore, the proposed scheme achieves perfect forward secrecy.

4.2.4 Resistance against application provider impersonation attack

Suppose an adversary $\mathcal{A}$ intercepts the application provider message $\langle t_a, D_2, D_3 \rangle$ to forge its identity to the Patient's device. However, in the proposed scheme, an adversary fails to deduce the parameter D_1 as it includes a random ephemeral key y_{ap} and nonce n_a. Thus, it is difficult for $\mathcal{A}$ to obtain two secret parameters to forge successfully.

4.2.5 Replay attack

In the proposed scheme, the timestamp t_u, t_a is used between P_{device} and AP to prevent the replay attack. Even if an adversary tries to intervene the tolerable time delay will exceed and the session will be aborted. Therefore, it is infeasible to replay a message from any previous session into a new session.

4.2.6 Resistance against patient impersonation attack

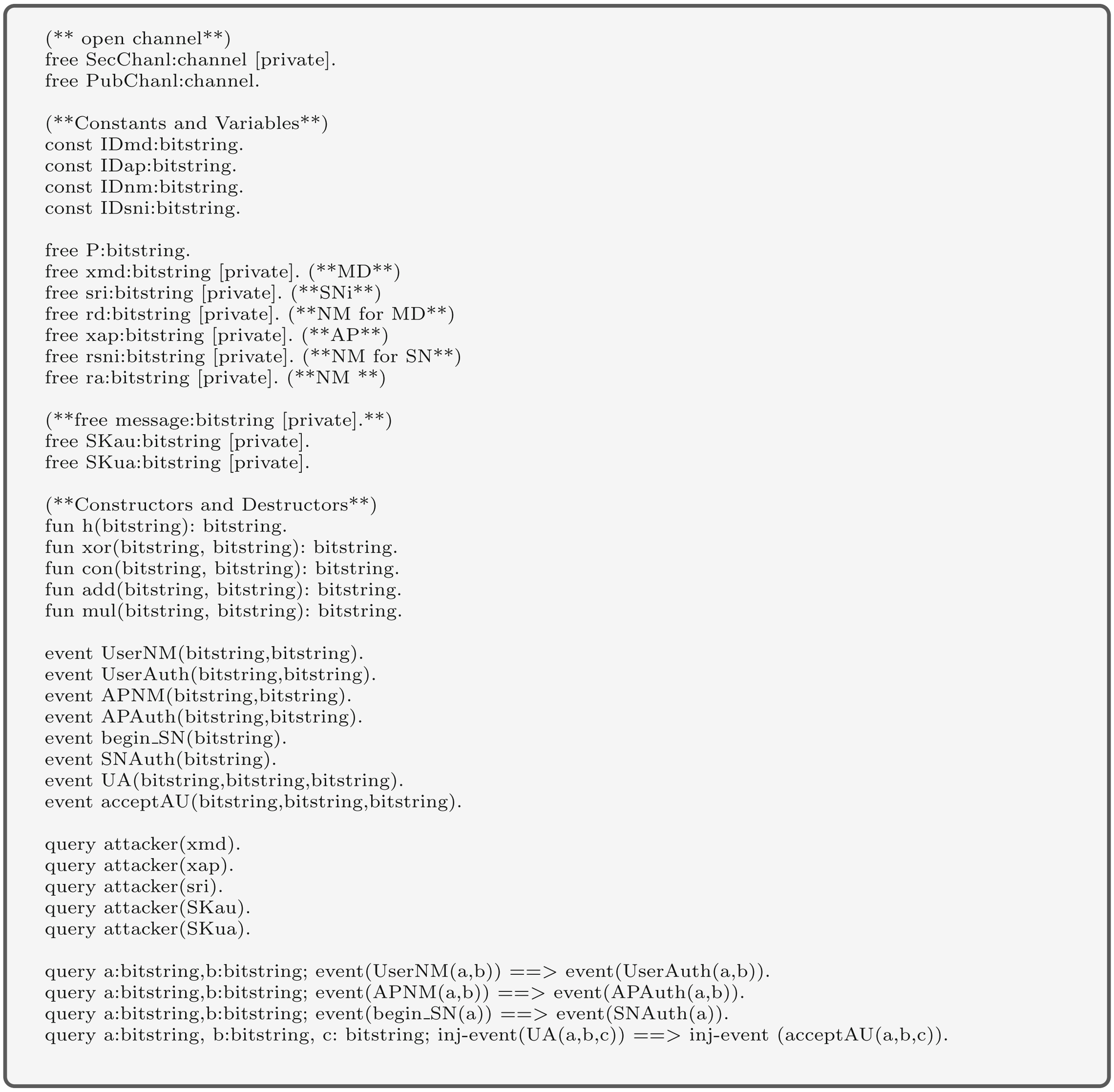
Suppose an adversary $\mathcal{A}$ intercepts the message send by the Patient's device $\langle t_u, C_2, C_3 \rangle$ to forge its identity to the application provider. However, in the proposed scheme, an adversary fails to deduce the parameter C_1 as it includes a random ephemeral key y_{md} and nonce n_u. Thus, it is difficult for $\mathcal{A}$ to obtain two secret parameters to forge successfully.

4.2.7 Known session key secrecy

In this scheme, the application provider, and patient's mobile device chooses a secret ephemeral key $y_{ap}/y_{md} \in Zp$, random nonces n_a/n_u which are generated freshly each time the protocol is run. In the protocol, the session key SK is generated using the combination of nonces, long-term secret key, and ephemeral keys. Therefore, an adversary will fail to re-create the session key with partial information due to the difficulty of solving the ECDLP assumption.

4.3 ProVerif security analysis

In this section, we aim to analyze the proposed CL-AKA protocol using the widely accepted ProVerif tool [45]



```
(** open channel**)
free SecChanl:channel [private].
free PubChanl:channel.

(**Constants and Variables**)
const IDmd:bitstring.
const IDap:bitstring.
const IDnm:bitstring.
const IDsni:bitstring.

free P:bitstring.
free xmd:bitstring [private]. (**MD**)
free sri:bitstring [private]. (**SNi**)
free rd:bitstring [private]. (**NM for MD**)
free xap:bitstring [private]. (**AP**)
free rsni:bitstring [private]. (**NM for SN**)
free ra:bitstring [private]. (**NM **)

(**free message:bitstring [private].**)
free SKau:bitstring [private].
free SKua:bitstring [private].

(**Constructors and Destructors**)
fun h(bitstring): bitstring.
fun xor(bitstring, bitstring): bitstring.
fun con(bitstring, bitstring): bitstring.
fun add(bitstring, bitstring): bitstring.
fun mul(bitstring, bitstring): bitstring.

event UserNM(bitstring,bitstring).
event UserAuth(bitstring,bitstring).
event APNM(bitstring,bitstring).
event APAuth(bitstring,bitstring).
event begin_SN(bitstring).
event SNAuth(bitstring).
event UA(bitstring,bitstring,bitstring).
event acceptAU(bitstring,bitstring,bitstring).

query attacker(xmd).
query attacker(xap).
query attacker(sri).
query attacker(SKau).
query attacker(SKua).

query a:bitstring,b:bitstring; event(UserNM(a,b)) ==> event(UserAuth(a,b)).
query a:bitstring,b:bitstring; event(APNM(a,b)) ==> event(APAuth(a,b)).
query a:bitstring,b:bitstring; event(begin_SN(a)) ==> event(SNAuth(a)).
query a:bitstring, b:bitstring, c: bitstring; inj-event(UA(a,b,c)) ==> inj-event (acceptAU(a,b,c)).
```

Fig. 5 Definition of the code

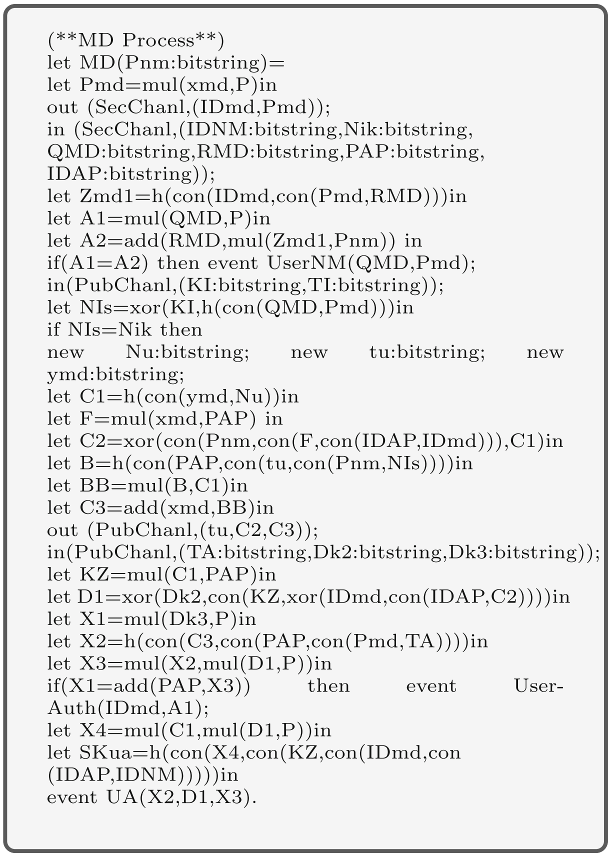
which is used to verify the security of cryptographic protocols automatically. The tool used pi-calculus language for describing and analyzing protocols. ProVerif supports several cryptographic properties such as encryption/decryption (symmetric and asymmetric), hash functions, and digital signatures. This tool enables session simulation and message space to determines whether the correctness of the protocol can be proved. The adversary is assumed to be able to eavesdrop, insert, and delete the messages. Upon the verification of cryptographic protocol based on required security properties, one of the following may occur:

- If the proof is true, it states that the attacker is unreachable. This makes ProVerif suitable for proving the secrecy of terms in a protocol.
- Otherwise, if the proof is false, it states that ProVerif is able to provide an attack trace.

Further, it proves security properties like perfect secrecy, mutual authentication, based on which our proposed protocol is verified.

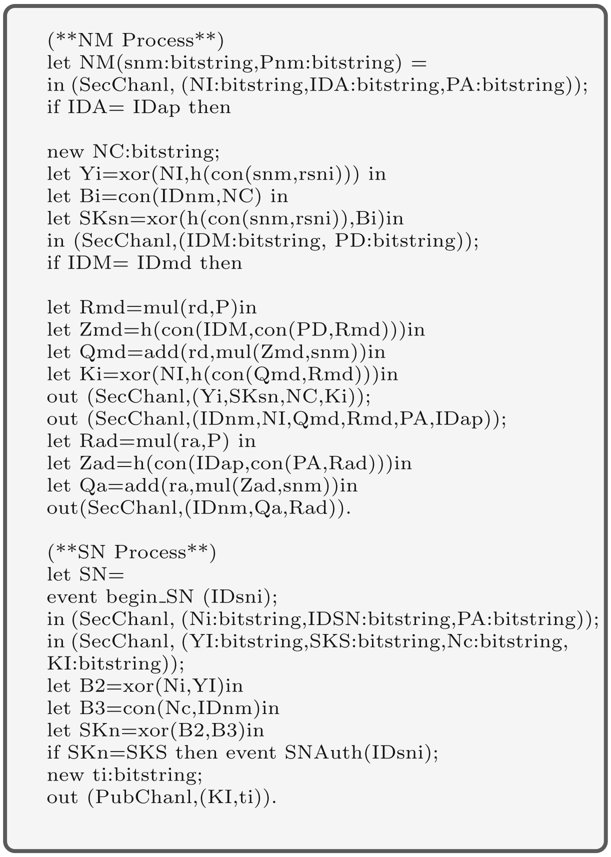
4.3.1 Definitions

Open channels *SecChanl*, *PubChanl* are defined for registration and authentication. The code has few constants like identities $IDmd, IDap, IDnm, IDsni$ and variables $(P, xmd, sri,\ rd, xap, rsni, ra)$. The operations are string concatenation, XOR operation, hash function, addition, and multiplication. Followed by events that are applied to check correspondence relation in the mutual authentication phase of the proposed scheme. The queries about session keys are to check the secrecy of the key. The definitions are depicted in Fig. 5.



```
(**MD Process**)
let MD(Pnm:bitstring)=
let Pmd=mul(xmd,P)in
out (SecChanl,(IDmd,Pmd));
in (SecChanl,(IDNM:bitstring,Nik:bitstring,
QMD:bitstring,RMD:bitstring,PAP:bitstring,
IDAP:bitstring));
let Zmd1=h(con(IDmd,con(Pmd,RMD)))in
let A1=mul(QMD,P)in
let A2=add(RMD,mul(Zmd1,Pnm)) in
if(A1=A2) then event UserNM(QMD,Pmd);
in(PubChanl,(KI:bitstring,TI:bitstring));
let NIs=xor(KI,h(con(QMD,Pmd)))in
if NIs=Nik then
new Nu:bitstring; new tu:bitstring; new
ymd:bitstring;
let C1=h(con(ymd,Nu))in
let F=mul(xmd,PAP) in
let C2=xor(con(Pnm,con(F,con(IDAP,IDmd))),C1)in
let B=h(con(PAP,con(tu,con(Pnm,NIs))))in
let BB=mul(B,C1)in
let C3=add(xmd,BB)in
out (PubChanl,(tu,C2,C3));
in(PubChanl,(TA:bitstring,Dk2:bitstring,Dk3:bitstring));
let KZ=mul(C1,PAP)in
let D1=xor(Dk2,con(KZ,xor(IDmd,con(IDAP,C2))))in
let X1=mul(Dk3,P)in
let X2=h(con(C3,con(PAP,con(Pmd,TA))))in
let X3=mul(X2,mul(D1,P))in
if(X1=add(PAP,X3)) then event User-
Auth(IDmd,A1);
let X4=mul(C1,mul(D1,P))in
let SKua=h(con(X4,con(KZ,con(IDmd,con
(IDAP,IDNM)))))in
event UA(X2,D1,X3).
```

Fig. 6 Process for patient's device



```
(**NM Process**)
let NM(snm:bitstring,Pnm:bitstring) =
in (SecChanl, (NI:bitstring,IDA:bitstring,PA:bitstring));
if IDA= IDap then

new NC:bitstring;
let Yi=xor(NI,h(con(snm,rsni))) in
let Bi=con(IDnm,NC) in
let SKsn=xor(h(con(snm,rsni)),Bi)in
in (SecChanl,(IDM:bitstring, PD:bitstring));
if IDM= IDmd then

let Rmd=mul(rd,P)in
let Zmd=h(con(IDM,con(PD,Rmd)))in
let Qmd=add(rd,mul(Zmd,snm))in
let Ki=xor(NI,h(con(Qmd,Rmd)))in
out (SecChanl,(Yi,SKsn,NC,Ki));
out (SecChanl,(IDnm,NI,Qmd,Rmd,PA,IDap));
let Rad=mul(ra,P) in
let Zad=h(con(IDap,con(PA,Rad)))in
let Qa=add(ra,mul(Zad,snm))in
out(SecChanl,(IDnm,Qa,Rad)).

(**SN Process**)
let SN=
event begin_SN (IDsni);
in (SecChanl, (Ni:bitstring,IDSN:bitstring,PA:bitstring));
in (SecChanl, (YI:bitstring,SKS:bitstring,Nc:bitstring,
KI:bitstring));
let B2=xor(Ni,YI)in
let B3=con(Nc,IDnm)in
let SKn=xor(B2,B3)in
if SKn=SKS then event SNAuth(IDsni);
new ti:bitstring;
out (PubChanl,(KI,ti)).
```

Fig. 7 Process for NM

4.3.2 Process

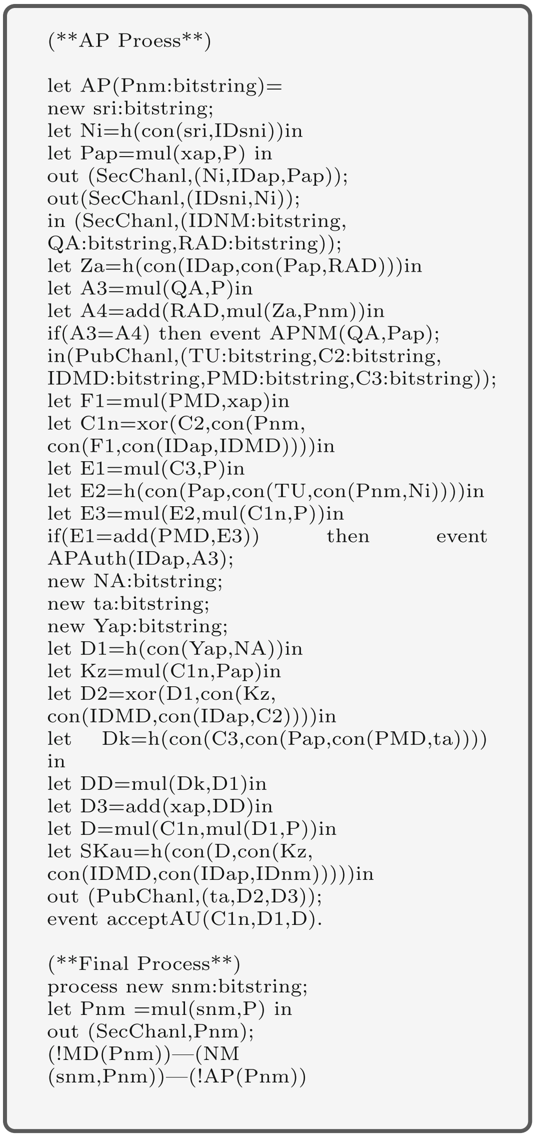
The code is written for four entities namely, Patient's device (MD), AP (Application provider), sensor nodes (SN) and NM (Network manager). The MD, SN and NM processes are depicted in Figs. 6 and 7. It consist of the registration phase of Patient through mobile device, sensor nodes with NM. Whereas, Fig. 8 represents the registration phase of AP with NM and the authentication phase details of exchange of session between AP and Patient's device for mutual authentication and secure exhange. The detail process of NM's key generation and work process is also depicted in it.

4.3.3 Result

The results for the eight queries are demonstrated in Fig. 9. The result of relation query shows that the $event(UserNM(a,b))$ is correctly executed after the $event(UserAuth(a,b))$. Similarly, $event(APNM(a\_17,b\_18))$ is correctly executed after the $event(APAuth(a\_17,b\_18))$, $event(begin\_SN(a\_19))$ is correctly executed after the $event(SNAuth(a\_19))$ and $inj-event(UA(a\_21,b\_22,c))$ is correctly executed after the $inj-event(acceptAU(a\_21,b\_22,c))$. The events are executed in the simulation process $RESULT\ not\ attacker(xmd[])\ is\ true$, $RESULT\ not\ attacker(xap[])\ is\ true$, and $RESULT\ not\ attacker(sri[])\ is\ true$. This shows that the private keys are secured. Also the $RESULT\ not\ attacker(SKua[])\ is\ true$ states that the session keys are secured against various attacks. Thus, the scheme is verified under ProVerif.

5 Performance analysis

In this section, the performance analysis of the proposed CL-AKA scheme is discussed in comparison with existing competent schemes namely, [13, 17–19, 29– 31, 33], and [37]. This section demonstrates the comparision of the proposed scheme with respect to security features, computation cost, and communication cost with above mentioned seven related protocols.



```
(**AP Process**)

let AP(Pnm:bitstring)=
new sri:bitstring;
let Ni=h(con(sri,IDsni))in
let Pap=mul(xap,P) in
out (SecChanl,(Ni,IDap,Pap));
out(SecChanl,(IDsni,Ni));
in (SecChanl,(IDNM:bitstring,
QA:bitstring,RAD:bitstring));
let Za=h(con(IDap,con(Pap,RAD)))in
let A3=mul(QA,P)in
let A4=add(RAD,mul(Za,Pnm))in
if(A3=A4) then event APNM(QA,Pap);
in(PubChanl,(TU:bitstring,C2:bitstring,
IDMD:bitstring,PMD:bitstring,C3:bitstring));
let F1=mul(PMD,xap)in
let C1n=xor(C2,con(Pnm,
con(F1,con(IDap,IDMD))))in
let E1=mul(C3,P)in
let E2=h(con(Pap,con(TU,con(Pnm,Ni))))in
let E3=mul(E2,mul(C1n,P))in
if(E1=add(PMD,E3))        then        event
APAuth(IDap,A3);
new NA:bitstring;
new ta:bitstring;
new Yap:bitstring;
let D1=h(con(Yap,NA))in
let Kz=mul(C1n,Pap)in
let D2=xor(D1,con(Kz,
con(IDMD,con(IDap,C2))))in
let    Dk=h(con(C3,con(Pap,con(PMD,ta))))
in
let DD=mul(Dk,D1)in
let D3=add(xap,DD)in
let D=mul(C1n,mul(D1,P))in
let SKau=h(con(D,con(Kz,
con(IDMD,con(IDap,IDnm)))))in
out (PubChanl,(ta,D2,D3));
event acceptAU(C1n,D1,D).

(**Final Process**)
process new snm:bitstring;
let Pnm =mul(snm,P) in
out (SecChanl,Pnm);
(!MD(Pnm))—(NM
(snm,Pnm))—(!AP(Pnm))
```

Fig. 8 Process for AP

5.1 Comparison of computation cost

The evaluation environment is a laptop running Windows 10 and 64-bit Intel(R) Core(TM) i7-10750 H CPU @2.60GHz, 16.00GB RAM. If we consider the schemes based on bilinear pairing, then the Tate pairing $e : G_1 \times G_1 \rightarrow G_T$ defined on a super-singular curve $E_1 : y^2 = x^3 - x + 1 \bmod p$ where p denotes 160-bit prime number and the size of elements taken for computation in G_1 is 320 bits. The state-of-the-art of computing the Tate bilinear pairing is eta pairing, introduced by Barreto et al. [46] is used for implementation. This achieves the security level of the RSA algorithm with a 1024-bit key length.

To attain same security level, in the proposed scheme the Koblitz curve secp256k1 defined in Standards for Efficient Cryptography (SEC) [47] is utilized. The curve $E_2 : y^2 = x^3 + ax + b \bmod p$ where p is 160-bit prime number for $a, b \in Z_q^*$ where $q = 160$ bits and size of elements in G is 320 bits. Table 2, shows the notations for different cryptographic operations along with their execution time in seconds. The computation cost of proposed CL-AKA scheme is compared with existing competent schemes in Table 3.

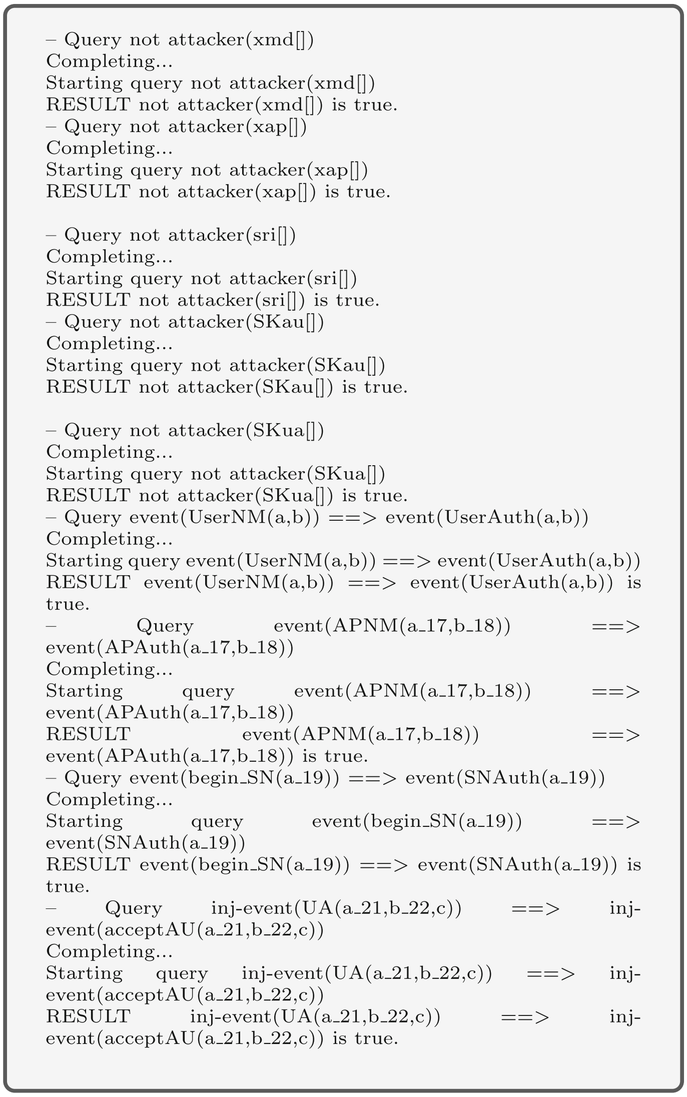
5.2 Comparison of communication cost

In order to compare the communication cost of the proposed CL-AKA scheme with existing ones, let us assume that the length of the identity as $|ID|$ is 32 bits, timestamp $|T|$ is 32 bits, the size of random number $|Z_q|$ is 160 bits, the scalar point multiplication as $|G|$ is 320 bits, pairing-based scalar multiplication as $|G_1|$ is 320 bits, hash function as $|H|$ is 256 bits, and symmetric enc/dec function ED is 256 bits, respectively. In the proposed scheme the message transferred between Patient to AP contains $\langle t_u, C_2, C_3 \rangle$ which needs (32 + 160 + 160) = 352 bits and response message from AP contains $\langle t_a, D_2, D_3 \rangle$ which needs (32 + 160 + 160) = 352 bits. Therefore, the total communication cost of the proposed CL-AKA scheme is 704 bits. The communication costs of competent existing schemes are depicted in Table 4.

5.3 Comparison of security and functional features

In this subsection, we analyze the security and functional features of the proposed CL-AKA scheme with the existing competent schemes. Table 5 emphasizes on the security features which includes, mutual authentication, impersonation attack, user anonymity, untraceability, session key agreement, perfect forward secrecy, and formal security proof. In this table ’Y’ indicates the security feature is addressed whereas ’N’ indicates the absence of that feature.

Fig. 9 Result



```
– Query not attacker(xmd[])
Completing...
Starting query not attacker(xmd[])
RESULT not attacker(xmd[]) is true.
– Query not attacker(xap[])
Completing...
Starting query not attacker(xap[])
RESULT not attacker(xap[]) is true.

– Query not attacker(sri[])
Completing...
Starting query not attacker(sri[])
RESULT not attacker(sri[]) is true.
– Query not attacker(SKau[])
Completing...
Starting query not attacker(SKau[])
RESULT not attacker(SKau[]) is true.

– Query not attacker(SKua[])
Completing...
Starting query not attacker(SKua[])
RESULT not attacker(SKua[]) is true.
– Query event(UserNM(a,b)) ==> event(UserAuth(a,b))
Completing...
Starting query event(UserNM(a,b)) ==> event(UserAuth(a,b))
RESULT event(UserNM(a,b)) ==> event(UserAuth(a,b)) is
true.
– Query event(APNM(a_17,b_18)) ==>
event(APAuth(a_17,b_18))
Completing...
Starting query event(APNM(a_17,b_18)) ==>
event(APAuth(a_17,b_18))
RESULT event(APNM(a_17,b_18)) ==>
event(APAuth(a_17,b_18)) is true.
– Query event(begin_SN(a_19)) ==> event(SNAuth(a_19))
Completing...
Starting query event(begin_SN(a_19)) ==>
event(SNAuth(a_19))
RESULT event(begin_SN(a_19)) ==> event(SNAuth(a_19)) is
true.
– Query inj-event(UA(a_21,b_22,c)) ==> inj-
event(acceptAU(a_21,b_22,c))
Completing...
Starting query inj-event(UA(a_21,b_22,c)) ==> inj-
event(acceptAU(a_21,b_22,c))
RESULT inj-event(UA(a_21,b_22,c)) ==> inj-
event(acceptAU(a_21,b_22,c)) is true.
```

Table 2 Execution time of various operations

Notation	Execution time (seconds)
T_{mul}	Time complexity for executing the modular multiplication is 0.343 s
T_{exp}	Time complexity for executing the modular exponentiation is 0.140 s
T_{sm}	Time complexity for executing the elliptic curve scalar point multiplication is 0.031 s
$T_{enc/dec}$	Time complexity for executing AES-256 encryption and decryption is 0.937 s
T_{bp}	Time complexity for executing the bilinear pairing operation is 4.06 s
T_h	Time complexity for executing the hash function is 0.001 s

Table 3 Computation cost

Schemes	Patients	AP	Total
Liu et al. [13]	$4T_{sm} + T_{exp}$	$T_{sm} + T_{exp} + T_{bp}$	$5T_{sm}+2T_{exp} + T_{bp} \approx 4.495$
Wang et al. [17]	$3T_{sm} + T_{bp}$	$2T_{sm} + T_{bp}$	$5T_{sm} + 2T_{bp} \approx 8.275$
Wu et al. [18]	$3T_{sm} + 4T_h + 2T_{exp}$	$3T_{sm} + 4T_h + 2T_{exp} + T_{bp}$	$6T_{sm} + 8T_h + 4T_{exp} + T_{bp} \approx 4.814$
He et al. [19]	$4T_{sm} + 4T_h$	$4T_{sm} + 2T_{bp}$	$8T_{sm} + 4T_h + 2T_{bp} \approx 8.372$
Sowjanya et al. [29]	$3T_{sm} + T_h + T_{mul}$	$6T_{sm} + 3T_h + T_{mul}$	$9T_{sm} + 4T_h + 2T_{mul} \approx 0.969$
Shuai et al. [30]	$4T_{sm} + 4T_h + T_{mul}$	$4T_{sm} + 4T_h + T_{mul}$	$8T_{sm} + 8T_h + 2T_{mul} \approx 0.942$
Kumar et al. [31]	$3T_{sm} + 4T_h + 2T_{mul}$	$6T_{sm} + 4T_h$	$9T_{sm} + 8T_h + 2T_{mul} \approx 0.973$
Lara et al. [33]	$3T_{sm} + 4T_h + T_{enc}$	$3T_{sm} + 4T_h + T_{dec}$	$6T_{sm} + 8T_h + 2T_{enc/dec} \approx 2.069$
Cheng et al. [37]	$3T_{sm} + 5T_h + 2T_{mul}$	$5T_{sm} + 3T_h + 2T_{mul}$	$8T_{sm} + 8T_h + 4T_{mul} \approx 1.628$
Proposed CL-AKA	$4T_{sm} + 3T_h + T_{mul}$	$4T_{sm} + 4T_h + T_{mul}$	$8T_{sm} + 7T_h + 2T_{mul} \approx 0.941$

Table 4 Communication cost

Scheme	Communication cost	Length (in bits)
Liu et al. [13]	$\lvert T\rvert + 2\lvert Z_q\rvert + \lvert G_1\rvert + 2\lvert H\rvert$	1184
Wang et al. [17]	$2\lvert T\rvert + 2\lvert G_1\rvert + \lvert ED\rvert + \lvert H\rvert$	1216
Wu et al. [18]	$2\lvert T\rvert + \lvert Z_q\rvert + \lvert ED\rvert + \lvert G_1\rvert$	800
He et al. [19]	$\lvert T\rvert + \lvert ED\rvert + 2\lvert G_1\rvert + \lvert H\rvert$	1184
Sowjanya et al. [29]	$\lvert ED\rvert + 2\lvert G\rvert + \lvert H\rvert$	1152
Shuai et al. [30]	$2\lvert T\rvert + 2\lvert G\rvert + 3\lvert Z_q\rvert$	1184
Kumar et al. [31]	$\lvert T\rvert + 2\lvert G\rvert + \lvert Z_q\rvert + \lvert H\rvert$	1088
Lara et al. [33]	$\lvert T\rvert + 2\lvert G\rvert + \lvert Z_q\rvert$	832
Cheng et al. [37]	$3\lvert T\rvert + 2\lvert G\rvert + \lvert ED\rvert + 3\lvert H\rvert$	1760
Proposed CL-AKA	$2\lvert T\rvert + 4\lvert Z_q\rvert$	704

6 Conclusion

This paper proposes a certificateless authenticated key agreement protocol for remotely monitoring patients health using WBAN. The proposed scheme provides perfect forward secrecy, resistance against sensor/application provider & patient's device impersonation attack, mutual authentication, and known session key secrecy. The formal security analysis shows that the proposed scheme is able to provide session key security in the widely accepted ROR model. The validation of the proposed CL-AKA scheme using the widely accepted ProVerif tool states that the protocol is safe. In addition, the performance analysis shows that the proposed scheme has low computation and communication cost compared with existing competent

Table 5 Security features

Scheme	[13]	[17]	[18]	[19]	[29]	[30]	[31]	[33]	[37]	Proposed CL-AKA
Mutual authentication	N	Y	N	Y	Y	Y	Y	Y	Y	Y
Resistance against sensor impersonation attack	N	N	N	Y	Y	Y	Y	Y	Y	Y
Resistance against AP impersonation attack	N	N	N	Y	Y	Y	Y	Y	Y	Y
Replay attack	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Resistance against patient impersonation attack	N	Y	Y	Y	Y	Y	Y	Y	Y	Y
Known session key secrecy	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Perfect forward secrecy	N	Y	Y	Y	Y	Y	N	Y	Y	Y
Formal security proof	N	N	Y	Y	Y	Y	Y	Y	N	Y

schemes. Therefore, the proposed scheme can be applied to e-healthcare applications.

Data availibility Not applicable

References

1. Thotahewa, K. M. S., Redouté, J. M., & Yuce, M. R. (2014). *Ultra wideband wireless body area networks*. Cham: Springer International Publishing.
2. Zimmerman, T. G. (1996). Personal area networks: Near-field intrabody communication. *IBM Systems Journal, 35*(3.4), 609–617.
3. Van Dam, K., Pitchers, S., & Barnard, M. (2001). Body area networks: Towards a wearable future. In *Proc. WWRF kick off meeting*. (pp. 6–7).
4. Sangari, A. S., Manickam, J. M. L. (2014). Public key cryptosystem based security in wireless body area network. In *Circuit, power and computing technologies (ICCPCT), 2014 international conference on*. (pp. 1609–1612). IEEE.
5. Li, J., Chen, X., Li, M., Li, J., Lee, P. P. C., & Lou, Wenjing. (2014). Secure deduplication with efficient and reliable convergent key management. *IEEE Transactions on Parallel and Distributed Systems, 25*(6), 1615–1625.
6. Shen, J., Zheng, W.-Y., Wang, J., Zheng, Y.-H., Sun, X.-M., & Lee, S.-Y. (2013). An efficient verifiably encrypted signature from weil pairing. *Journal of Internet Technology, 14*(6), 947–952.
7. Tan, C. C., Wang, H., Zhong, S., & Li, Q. (2009). Ibe-lite: A lightweight identity-based cryptography for body sensor networks. *IEEE Transactions on Information Technology in Biomedicine, 13*(6), 926–932.
8. Li, J., Li, J., Chen, X., Jia, C., & Lou, W. (2015). Identity-based encryption with outsourced revocation in cloud computing. *IEEE Transactions on Computers, 64*(2), 425–437.
9. Li, X., Niu, J., Liao, J., & Liang, Wei. (2015). Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update. *International Journal of Communication Systems, 28*(2), 374–382.
10. Al-Riyami, S. S. & Paterson, K. G. (2003). Certificateless public key cryptography. In *International conference on the theory and application of cryptology and information security* (pp. 452–473). Springer.
11. Drira, W., Renault, É. & Zeghlache, D. (2012) A hybrid authentication and key establishment scheme for wban. In *2012 IEEE 11th international conference on trust, security and privacy in computing and communications* (pp. 78–83). IEEE.
12. Kompara, M., & Hölbl, M. (2018). Survey on security in intra-body area network communication. *Ad Hoc Networks, 70*, 23–43.
13. Liu, J., Zhang, Z., Chen, X., & Kwak, K. S. (2013). Certificateless remote anonymous authentication schemes for wirelessbody area networks. *IEEE Transactions on Parallel and Distributed Systems, 25*(2), 332–342.
14. Liu, J., Zhang, Z., Chen, X., & Kwak, K. S. (2014). Certificateless remote anonymous authentication schemes for wirelessbody area networks. *IEEE Transactions on Parallel and Distributed Systems, 25*(2), 332–342.
15. Xiong, H. (2014). Cost-effective scalable and anonymous certificateless remote authentication protocol. *IEEE Transactions on Information Forensics and Security, 9*(12), 2327–2339.
16. Zhao, Z. (2014). An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *Journal of Medical Systems, 38*(2), 13.
17. Wang, C., & Zhang, Y. (2015). New authentication scheme for wireless body area networks using the bilinear pairing. *Journal of Medical Systems, 39*(11), 136.
18. Wu, L., Zhang, Y., Li, L., & Shen, J. (2016). Efficient and anonymous authentication scheme for wireless body area networks. *Journal of Medical Systems, 40*(6), 134.
19. He, D., Zeadally, S., Kumar, N., & Lee, J. H. (2016). Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal, 11*(4), 2590–2601.
20. Xiong, H., & Qin, Z. (2015). Revocable and scalable certificateless remote authentication protocol with anonymity for wireless body area networks. *IEEE Transactions on Information Forensics and Security, 10*(7), 1442–1455.
21. Liu, J., Zhang, L., & Sun, R. (2016). 1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks. *Sensors, 16*(5), 728.
22. Li, X., Peng, J., Kumari, S., Wu, F., Karuppiah, M., & Choo, K. K. R. (2017). An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. *Computers & Electrical Engineering, 61*, 238–249.
23. Khan, H., Dowling, B. & Martin, K.M. (2018). Highly efficient privacy-preserving key agreement for wireless body area Networks. In *2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE)* (pp. 1064-1069). IEEE.
24. Hassan, A., Omala, A. A., Ali, M., Jin, C., & Li, F. (2019). Identity-based user authenticated key agreement protocol for multi-server environment with anonymity. *Mobile Networks and Applications, 24*(3), 890–902.
25. Kumar, P., & Liyanage, M. (2020). Efficient and anonymous mutual authentication protocol in multi-access edge computing (MEC) environments (pp. 119–131). IoT Security: Advances in Authentication.
26. Shen, J., Gui, Z., Ji, S., Shen, J., Tan, H., & Tang, Y. (2018). Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. *Journal of Network and Computer Applications, 106*, 117–123.
27. Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., & Hayajneh, T. (2018). Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet of Things Journal, 6*(1), 410–420.
28. Kasyoka, P., Kimwele, M., & Mbandu Angolo, S. (2020). Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. *Journal of Medical Engineering & Technology, 44*(1), 12–19.
29. Sowjanya, K., Dasgupta, M., & Ray, S. (2020). An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. *International Journal of Information Security, 19*(1), 129–146.
30. Shuai, M., Liu, B., Yu, N., Xiong, L., & Wang, C. (2020). Efficient and privacy-preserving authentication scheme for wireless body area networks. *Journal of Information Security and Applications, 52*, 102499.
31. Kumar, M., & Chand, S. (2020). A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network. *IEEE Systems Journal, 15*(2), 2779–2786.
32. Azees, M., Vijayakumar, P., Karuppiah, M., & Nayyar, A. (2021). An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks. *Wireless Networks, 27*(3), 2119–2130.

33. Lara, E., Aguilar, L., & García, J. A. (2021). Lightweight authentication protocol using self-certified public keys for wireless body area networks in health-care applications. *IEEE Access, 9*, 79196–79213.
34. Soni, M. & Singh, D.K. (2021). LAKA: Lightweight authentication and key agreement protocol for internet of things based wireless body area network. *Wireless Personal Communications*, 1–18.
35. Peng, C., Luo, M., Li, L., Choo, K. K. R., & He, D. (2021). Efficient certificateless online/offline signature scheme for wireless body area networks. *IEEE Internet of Things Journal, 8*(18), 14287–14298.
36. Liu, S., Chen, L., Wang, H., Fu, S. & Shi, L. (2022). O3HSC: Outsourced online/offline hybrid signcryption for wireless body area networks. *IEEE Transactions on Network and Service Management*.
37. Cheng, Q., Li, Y., Shi, W., & Li, X. (2022). A certificateless authentication and key agreement scheme for secure cloud-assisted wireless body area network. *Mobile Networks and Applications, 27*(1), 346–356.
38. Li, C., & Xu, C. (2022). Efficient anonymous authentication for wireless body area networks. *IEEE Access, 10*, 80015–80026.
39. Hasan, K., Chowdhury, M. J. M., Biswas, K., Ahmed, K., Islam, M. S., & Usman, M. (2022). A blockchain-based secure data-sharing framework for software defined wireless body area networks. *Computer Networks, 211*, 109004.
40. Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on information theory, 29*(2), 198–208.
41. The Transport Layer Security (TLS) Protocol Version 1.3. Retrieved Aug 2022 from, https://www.rfc-editor.org/rfc/rfc8446.html.
42. Insecure Communication. Retrieved Aug 2022 from, https://owasp.org/www-project-mobile-top-10/2016-risks/m3-insecure-communication.
43. Bellare, M., & Rogaway, p. (1993). Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the 1st ACM conference on computer and communications security* pp. 62–73.
44. Shoup, V. (2004). Sequences of games: A tool for taming complexity in security proofs. *IACR Cryptology ePrint Archive, 2004*, 332.
45. Blanchet, B., Smyth, B., Cheval, V. & Sylvestre, M. (2018). ProVerif 2.00: Automatic cryptographic protocol verifier, user manual and tutorial. Version from, pp. 05-16.
46. Barreto, P. S., Galbraith, S. D., & hÉigeartaigh, C. Ó. (2007). Efficient pairing computation on supersingular abelian varieties. *Designs, Codes and Cryptography, 42*(3), 239–271.
47. Brown, D. R. (2010). Sec 2: Recommended elliptic curve domain parameters. *Standars for Efficient Cryptography*.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Dr. Susmita Mandal received her Ph.D. in computer science and engineering from National Institute of Technology Rourkela, India. She is currently an Assistant Professor associated with the Center for Distributed Ledger Technology and Innovation at Institute for Development and Research in Banking Technology, (Established by RBI), India. She is currently leading three Government sponsored Projects as Principle Investigator in the area of Cryptographic applications to Blockchain and secure communication using Internet of Things. She is the Managing Editor for the Journal of Banking and Financial Technology, Springer. Her current research interest are in Applied Cryptography, Security and Privacy aspects in Blockchain, Secure Low-cost communication solution, Authentication, and Privacy preserving mechanisms.