



A Secure and Efficient Certificateless Authenticated Key Agreement Scheme for Smart Healthcare

Yuqian Ma, Yongliu Ma, Yidan Liu, and Qingfeng Cheng^(✉)

Strategic Support Force Information Engineering University,
Zhengzhou 450001, China
qingfengc2008@sina.com

Abstract. Smart healthcare plays a vital role in contemporary society while its security and privacy issues remain critical challenges. With the aim of resolving problems related to the integrity and confidentiality of information transmitted in the smart healthcare, Wang et al. designed a certificateless authenticated key agreement (CL-AKA) scheme recently. However, we analyze their protocol and prove that theirs did not satisfy forward security. Further, this paper proposes an improved authenticated key agreement (AKA) scheme based on the certificateless cryptography. The proposed CL-AKA scheme does not only satisfy the security requirements in smart healthcare networks but also performs more efficient. The performance comparison shows our scheme has comparable efficiency in terms of computation cost.

Keywords: Certificateless authenticated key agreement (CL-AKA) · Scyther · Smart healthcare

1 Introduction

More and more attention has been paid on the medical infrastructure since people ask for higher medical quality and more convenient service. As one of the most promising applications based on the Internet of Things (IoT), smart healthcare system, a self-organizing network realizes the interaction among patients, medical staff, hospitals and medical equipment. However, its communications are conducted through open wireless channels which makes the networks vulnerable to various attacks, such as man-in-the-middle attacks and ephemeral key leakage attacks.

Since users may outsource their sensitive information to servers to alleviate the heavy overheads, secure communications over the public channel are important. Aiming at secure data storage, Chenam and Ali [1] proposed an encryption scheme based on certificateless public key authentication to resist keyword guessing attacks. Besides, to aid security and efficiency, Shiraly et al. [2] first designed a security model facing multi-servers and then proposed a certificateless public key encryption scheme with keyword search proved secure under the

security model they described. To tackle the problem of mutual authentication in the process of data transmission, Turkanović et al. [3] designed a user authentication and key agreement scheme focusing on the wireless sensor networks. However, Farash et al. [4] pointed out that the scheme of Turkanović et al. was susceptible to several shortcomings mainly threatening the identities of users. Further, they [4] proposed an improved protocol tackling and eliminating the security shortcomings of the previous one.

Because of the high bandwidth of mobile communication, lightweight cryptography was proposed to satisfy the urgent requirement of high communication efficiency. In 2016, Gope et al. [5] proposed a realistic lightweight anonymous user authentication protocol in wireless networks. However, in 2019, Adavoudi-Jolfaei et al. [6] showed that in Gope et al.'s scheme the adversary could obtain the session key under the Dolev-Yao model [7]. Further, they designed a lightweight and anonymous three-factor authentication and access control scheme for real-time applications. But one year later, Ryu et al. [8] found the weaknesses of Adavoudi et al.'s protocol including insider attacks, user impersonation attacks, and session key attacks. To address these problems, they proposed a three-factor authentication scheme based on hash function and XOR.

AI-Riyami and Paterson [9] firstly introduced certificateless public key cryptography (CL-PKC) in 2003. Once the concept was proposed, adopted widely has it been to expand authenticated key agreement (AKA) protocols because of the two advantages this scheme possesses. First, CL-PKC is capable of static private key leakage resistance since the full private key is composed of two parts, one generated by key generation center (KGC) and the other generated by the user. Second, few computation resource is needed by CL-PKC which is required urgently in the Internet of Things.

Mandt et al. [10] improved the efficiency of AI-Riyami et al.'s scheme based on the bilinear Diffie-Hellman problem. Wang et al. [11] also pointed out that the efficiency of AI-Riyami et al.'s scheme was low since it at least required a pairing evaluation computed on-line. Thus, Wang et al. proposed a certificateless authenticated key agreement (CL-AKA) protocol for Web client/server setting. Later, Hou and Xu [12] found that the scheme could not resist key compromised impersonation attacks, man-in-the-middle attacks and key replicating attacks.

Because of the advantages of CL-PKC, it has been applied in various environments. Asari et al. [13] utilized CL-PKC in automatic dependent surveillance-broadcast (ADS-B) systems and designed a certificateless authentication protocol resolving the privacy problem. In vehicular ad hoc networks (VANETs), both privacy and efficiency are necessary. A certificateless conditional anonymous authentication scheme was investigated by Samra et al. [14] for softwares in VANETs. Also, patients' diagnosis information plays a vital role in wireless body area network (WBAN) which motivates designers to find resolutions. Cheng et al. [15] designed a CL-AKA for cloud-enabled WBAN based on ECDL assumption.

Recently, considering the drawbacks of existing AKA protocols, Wang et al. [17] designed a computation-transferable AKA scheme without an online

registration center for smart healthcare networks. Nevertheless, in this paper, the shortcomings of Wang et al.'s scheme will be illustrated, proving that theirs could not satisfy the forward security.

The main contributions of this paper are summarized specifically as follows.

- Recently, Wang et al. [17] proposed an AKA protocol, denoted as WHX protocol, for smart healthcare and claimed that it satisfied security and privacy protection requirements. However, an effective attack on WHX protocol is presented, which proves that WHX protocol does not satisfy the forward security.
- To remedy the shortcoming we point out, a secure and efficient CL-AKA scheme is designed which can resist common attacks and achieve mutual authentication as well as key agreement.
- Security analysis claims that the proposed scheme can satisfy security properties required urgently in smart healthcare environment. Performance evaluation and comparison demonstrated in Sect. 6 shows that the design scheme can behave better than other related schemes.

The arrangement of this paper is following. The security model is presented in Sect. 2. In Sect. 3, a brief review of the WHX protocol is presented. Then a specific security analysis of WHX protocol is presented in this section as well. In Sect. 4, the detailed procedures of the proposed scheme are illustrated. Following is the security analysis in Sect. 5. Performance evaluation and comparison are presented in Sect. 6. Finally, Sect. 7 provides some concluding remarks.

2 Security Model

For discussing the security of the proposed scheme, here, we introduce a security model suitable for the CL-AKA setting based on [16]. In particular, let \mathcal{A} and Π_F^φ be a probabilistic polynomial time adversary and φ th instance of a participant Γ , respectively. There exist two types of adversaries, denoted as \mathcal{A}_1 and \mathcal{A}_2 . The main difference between them is that \mathcal{A}_1 does not have the ability of knowing the master key but can replace the public keys of any participant with selected values while \mathcal{A}_2 has the ability of learning the master key but can not replace the public keys of participants.

The security of the proposed scheme is defined based on a game executed between \mathcal{A} and a challenger \mathcal{C} . In the game, the abilities of \mathcal{A} are described by several kinds of queries answered by \mathcal{C} shown in Table 1.

After making a Test-query towards an instance Π_F^φ , \mathcal{A} can also make queries towards Π_F^φ or to the matching session (if it exists) except Reveal-query and Corrupt-query towards the potential partner. Finally, \mathcal{A} should output a guess result c' . If $c' = c$, then \mathcal{A} wins the game.

Definition. A CL-AKA protocol is secure if any session instance Π_F^φ satisfies:

- achieving the same session key with its matching session.
- making sure that the advantage $Advantage_{\mathcal{A}}(\Pi_F^\varphi) = |2P[c' = c] - 1|$ is negligible for any \mathcal{A} .

Table 1. Description of the abilities of adversary

Queries	Description
H_i -query	If \mathcal{C} receives the query with m_i , it verifies if (m_i, H_i) exists in the list L_{H_i} . If so, the challenger returns H_i to \mathcal{A} ; otherwise, \mathcal{C} selects a random number H_i , adds (m_i, H_i) to L_{H_i} , and returns H_i to \mathcal{A}
Create-query	If \mathcal{C} receives the query with a party Γ 's identity ID_Γ , it creates Γ 's private and public key pair
Send-query	If \mathcal{C} receives the query with a session instance Π_Γ^φ and the message m , it returns the corresponding response to \mathcal{A} according to the proposed scheme
Reveal-query	If \mathcal{C} receives the query with a party Γ 's identity ID_Γ , it returns the session key of Π_Γ^φ to \mathcal{A}
Corrupt-query	If \mathcal{C} receives the query with a session instance Π_Γ^φ , it returns Γ 's private key to \mathcal{A}
Ephemeral-query	If \mathcal{C} receives the query with a session instance Π_Γ^φ , it returns Γ 's ephemeral private key to \mathcal{A}
Test-query	If \mathcal{C} receives the query with a session instance Π_Γ^φ , it chooses c randomly in $\{0, 1\}$. If $c = 1$, it returns the session key of Π_Γ^φ to \mathcal{A} ; otherwise, it returns a random string with the same distribution of the session key to \mathcal{A}

3 Review and Cryptanalysis of WHX AKA Protocol

In this section, we review the process of WHX AKA protocol [17] briefly, including initialization, registration, and authentication and key agreement three phases. The notations used in this paper are listed in Table 2.

3.1 Review of WHX AKA Protocol

Let q be a large prime number. The system is initialized by RC. First, it chooses a non-singular elliptic curve $E(F_q)$ and an additive group \mathbb{G} over it. The generator of \mathbb{G} is P whose order is q . RC then chooses s randomly in Z_q^* , computes $P_{pub} = sP$ and selects eight hash functions $H_i : \{0, 1\}^* \rightarrow \{0, 1\}^l$, ($i = 0, 1, \dots, 7$). Finally, it keeps the master key s as a secret and publishes the system parameters $\{q, P, \mathbb{G}, P_{pub}, H_i (i = 0, 1, \dots, 7)\}$.

Before communicating, users and edge servers need to register with RC through a secure channel to get their static private key and corresponding public key. For a comprehensive process, readers can refer to the original paper [17].

After registering successfully with RC, U_i and ES can start to authenticate each other and negotiate about the session key. The detailed steps are as follows:

- U_i selects $a \in Z_q^*$ randomly and computes u, A, η . Then U_i sends the message $M_1 = \{u, A, \eta, T_i\}$ to ES where T_i is the current timestamp.

Table 2. Notations

Notation	Description
RC	The registration center responsible for the initialization and registration phases
ES	The edge server located at the edge of the network and providing service for users
U	Resource-constrained users
P	The generator of the additive group \mathbb{G}
s	The master key of RC
P_{pub}	The public key of RC
H_i	The hash functions, where $i = 0, \dots, 7$
$ID_{U(ES)}$	The real identity of U_i/ES
$(s_{U(ES)}, x_{U(ES)})$	The static private key of U_i/ES
$(R_{U(ES)}, X_{U(ES)})$	The static public key of U_i/ES

- ES checks the freshness of T_i and the validation of η . If holds, ES chooses $b \in E_q^*$ randomly and calculates v, V, K_{ES}, SK_{ES} and ω , where the timestamp is denoted as T_j . Next, ES sends the message $M_2 = \{V, \omega, T_j\}$ to U_i .
- U_i verifies whether T_i is fresh. If successes, U_i computes K_U, SK_U . Further, U_i checks ω . If holds, it calculates λ and sends the message $M_3 = \{\lambda\}$ to ES.
- Finally, ES tests the correctness of λ .

3.2 Cryptanalysis of WHX AKA Protocol

In this subsection, we present that WHX protocol can not satisfy the requirement of forward security. If the private key of user U_i is compromised, the adversary \mathcal{A} will recover the session key easily through the steps below:

Step 1. In the authentication and key agreement phase, \mathcal{A} eavesdrops the message sent from U_i to ES, $M_1 = \{u, A, \eta, T_i\}$.

Step 2. \mathcal{A} eavesdrops the message sent from ES to U_i , $M_2 = \{V, \omega, T_j\}$.

Step 3. After the session is completed, \mathcal{A} launches Reveal-query towards the user U_i to gain its private secret keys (s_U, x_U) .

Step 4. After obtaining the parameters above, \mathcal{A} can easily compute $a = u - x_U$, $PID'_U = A \oplus H_3(u \cdot X_{ES})$. Then, \mathcal{A} can extract K'_U by $K'_U = s_U \cdot (V - X_{ES}) + a \cdot [R_{ES} + H_2(ID_{ES} \| R_{ES}) P_{pub}]$, where X_{ES}, R_{ES}, P_{pub} are the public keys. Finally, \mathcal{A} can compute the session key according to the way generating $SK_U = H_5(K'_U \| ID_{ES} \| PID'_U \| X_U \| X_{ES})$.

Thus, in this way, adversary \mathcal{A} can recover the session key. According to the steps above, we can see that the adversary merely gets the private keys of user, which is accordant with the definition of weak forward security. Besides, although the real identity of the patients is unknown to the public, the PID_U can still be accessed easily, which means that WHX protocol can not resist traceability.

4 The Improved Scheme

We present a detailed description of the improved AKA scheme in this section. There are three phases involved in our scheme, which are the initialization phase, the registration phase, the authentication and key agreement phase, respectively. The details are described as follows.

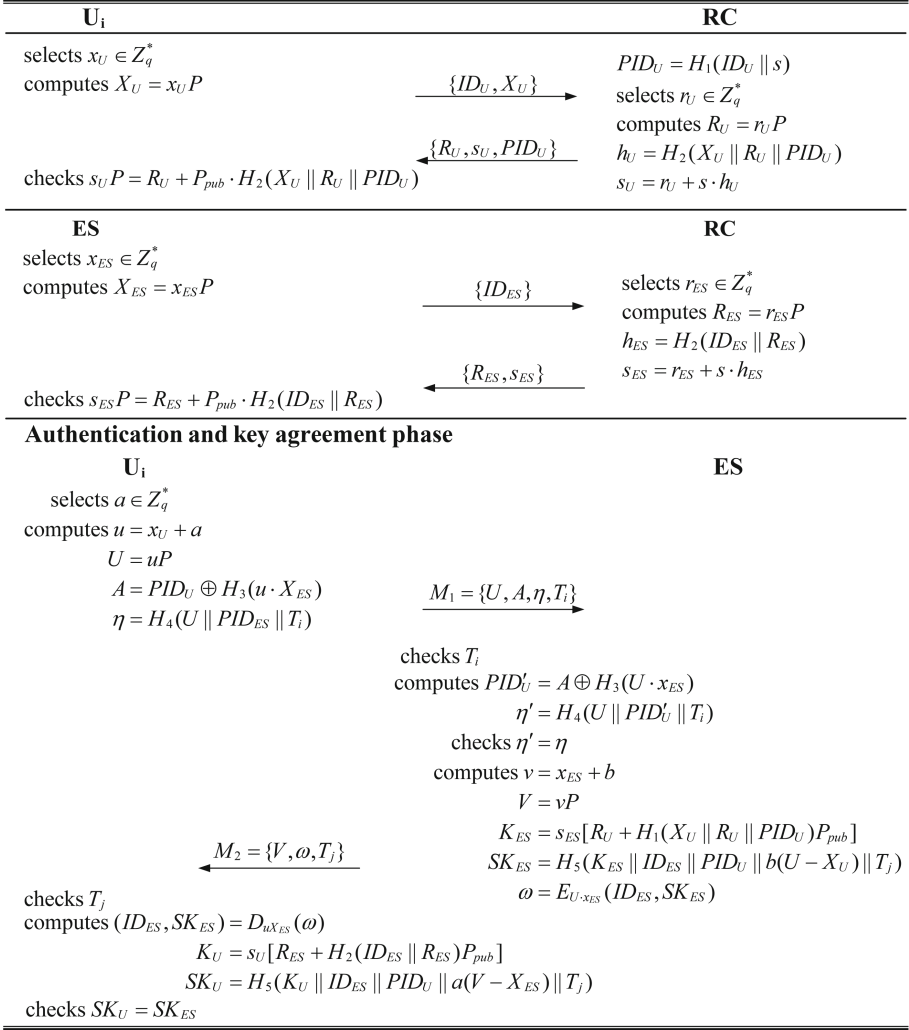


Fig. 1. Description of the improved scheme

4.1 Initialization Phase

Let l represent the length of the session key. RC, responsible for the initialization of the system, acts as the following steps:

- Selects an additive cyclic group \mathbb{G} over a non-singular elliptic curve $E(F_p)$. The order of \mathbb{G} is q , a large prime number, and the generator is P .
- Chooses a random number $s \in Z_q^*$ as its master key and calculates $P_{pub} = sP$.
- Selects five one-way hash functions $H_i (i = 1, 2, \dots, 5)$.
- Keeps the master key s as a secret while publishes the system parameters $\{\mathbb{G}, q, P, P_{pub}, H_i\}$.

4.2 Registration Phase

Before beginning the authentication and key agreement, both the user and the edge server need to register with the RC in the off-line channel. A user U_i with its unique identity ID_U can register with RC according to the steps below:

- Selects $x_U \in Z_q^*$ randomly as the secret key and computes $X_U = x_U P$ and sends $\{ID_U, X_U\}$ to RC through a secure channel.
- On receiving $\{ID_U, X_U\}$, RC extracts $PID_U = H_1(ID_U \parallel s)$. Then it randomly selects $r_U \in Z_q^*$ and computes $R_U = r_U P$, $h_U = H_2(X_U \parallel R_U \parallel PID_U)$, $s_U = r_U + s \cdot h_U$. Then RC sends $\{R_U, s_U, PID_U\}$ to U_i , where s_U is the partial private key of U_i .
- U_i checks if $s_U P = R_U + H_2(X_U \parallel R_U \parallel PID_U) P_{pub}$ is true. If so, U_i securely stores (s_U, x_U) as its full private key and publishes (R_U, X_U) .

Similarly, ES registers with RC, illustrated in Fig. 1.

4.3 Authentication and Key Agreement Phase

User U_i and ES authenticate mutually and agree on a session key for a secure communication. Figure 1 shows the authentication and key agreement phase in detail and the specific process is presented below:

- User U_i selects a random value $a \in Z_q^*$, then computes $u = x_U + a$, $U = u \cdot P$, $A = PID_U \oplus H_3(u \cdot X_{ES})$, and $\eta = H_4(U \parallel PID_U \parallel T_i)$, where T_i is the current timestamp. Then U_i sends $M_1 = \{U, A, \eta, T_i\}$ to ES.
- Upon receiving the message from U_i , ES first checks the validation of timestamp T_i . Then calculates $PID'_U = A \oplus H_3(x_{ES} \cdot U)$, $\eta' = H_4(U \parallel PID'_U \parallel T_i)$. Therefore, ES can validate the user's identity through η' . If the equation holds, ES chooses a random value $b \in Z_q^*$, then calculates $v = x_{ES} + b$, $V = v \cdot P$, $K_{ES} = s_{ES} \cdot [R_U + H_1(X_U \parallel R_U \parallel PID_U) P_{pub}]$, $SK_{ES} = H_5(K_{ES} \parallel ID_{ES} \parallel PID_U \parallel b \cdot (U - X_U) \parallel T_j)$, $\omega = E_{x_{ES}U}(ID_{ES})$. Then ES sends the message $M_2 = \{V, \omega, T_j\}$ to the patient user U_i , where T_j is the current timestamp.

- After receiving M_2 , U_i first checks whether T_j has expired. Then U_i computes $(ID_{ES}) = D_{u_{X_{ES}}}(\omega)$ and checks the identity of server. If it holds, then U_i continues to calculate $K_U = s_U \cdot [R_{ES} + H_2(ID_{ES} \parallel R_{ES})P_{pub}]$, $SK_U = H_5(K_U \parallel ID_{ES} \parallel PID_U \parallel a \cdot (V - X_{ES}) \parallel T_j)$. Consequently, U_i and ES complete the authentication and key agreement phase.

Finally, U_i and ES successfully achieve the same session key since:

$$\begin{aligned}
K_{ES} &= s_{ES} \cdot [R_U + H_1(X_U \parallel R_U \parallel PID_U)P_{pub}] \\
&= s_{ES} \cdot s_U P \\
&= s_U \cdot [R_{ES} + H_2(ID_{ES} \parallel R_{ES})P_{pub}] \\
&= K_U,
\end{aligned}$$

$$\begin{aligned}
SK_{ES} &= H_5(K_{ES} \parallel ID_{ES} \parallel PID_U \parallel b \cdot (U - X_U) \parallel T_j) \\
&= H_5(K_U \parallel ID_{ES} \parallel PID_U \parallel a \cdot (V - X_{ES}) \parallel T_j) \\
&= SK_U.
\end{aligned}$$

Therefore, the proposed scheme is provably correct.

5 Security Analysis of the Proposed Scheme

In this section, we analyze the security of the proposed scheme. First, we prove that the proposed scheme is secure against two types of adversaries. Then, we present the analysis result of Scyther tool claiming that our scheme is secure against common attacks.

Theorem 1. Assume that the Computational Diffie-Hellman (CDH) problem is intractable. Let \mathcal{A}_1 be a probabilistic polynomial time adversary against the proposed scheme Π , the advantage of \mathcal{A}_1 against our scheme is negligible.

Proof. Suppose there exists a probabilistic polynomial time adversary \mathcal{A}_1 who can win the game with a non-negligible advantage in polynomial time t . Then, we can design an algorithm \mathcal{C} to solve the CDH problem using the ability of \mathcal{A}_1 .

Suppose \mathcal{C} is given an instance (aP, bP) of the CDH problem whose subject is to compute $Q = abP$. Suppose \mathcal{A}_1 makes at most q_{H_i} times H_i -query and creates at most q_c participants and q_s be the maximal number of sessions each participant may be involved in.

\mathcal{C} sets P_0 as the system public key P_{pub} , selects the system parameter $params = \{F_p, E/F_p, G, P, P_{pub}, H_i\}$ and sends the public parameters to \mathcal{A}_1 . \mathcal{C} chooses at random $I \in [1, q_{H_2}]$, $J \in [1, q_{H_2}]$, $T \in [1, q_s]$, $s_J, x_J, h_J \in Z_q^*$, then \mathcal{C} computes $R_J = s_J P - h_J P_{pub}$, $X_J = x_J P$. \mathcal{C} answers \mathcal{A}_1 's queries as follows.

- $\text{Create}(ID_j)$: \mathcal{C} keeps an empty list L_C consisting of tuples $(ID_j, (s_j, x_j), (R_j, X_j))$. If $ID_j = ID_J$, \mathcal{C} lets j 's private key and public key be (s_J, x_J) , and

- (R_J, X_J) respectively. \mathcal{C} also lets $H_2(ID_J, R_J) \leftarrow h_J$, where R_J , x_J , and h_J are the variables mentioned above. Otherwise, \mathcal{C} chooses a random $x_j, s_j, h_j \in Z_q^*$ and computes $R_j = s_j P - h_j P_{pub}$ and $X_j = x_j P$. Thus, ID_j 's private key is the tuple (s_j, x_j) and its public key is (R_j, X_j) . At last, \mathcal{C} adds the tuple (ID_j, R_j, h_j) and $(ID_j, (s_j, x_j), (R_j, X_j))$ to the list L_{H_2} and L_C , separately.
- Send($\Pi_{i,j}^n, M$): \mathcal{C} keeps an empty list L_S in the form of a tuple $(\Pi_{i,j}^n, path_{i,j}^n, r_{i,j}^n)$, in which $path_{i,j}^n$ is a record of session message $\Pi_{i,j}^n$ and $r_{i,j}^n$ is defined as below.
 - If $n = T, ID_i = ID_I, ID_j = ID_J$, \mathcal{C} returns aP as U and updates the tuple $r_{i,j}^n = \perp$.
 - Else \mathcal{C} returns the corresponding answer according to the steps.
 - Reveal($\Pi_{i,j}^n$): \mathcal{C} keeps an empty list L_R . If $n = T, ID_i = ID_I, ID_j = ID_J$ or $\Pi_{i,j}^n$ is the matching session of $\Pi_{I,J}^T$, \mathcal{C} aborts this query; otherwise, \mathcal{C} answers as follows:
 - If $ID_i \neq ID_I$, \mathcal{C} searches for the list L_C and L_S for the detailed data and makes an H_5 query to compute the session key $SK_{i,j}^n$.
 - Else \mathcal{C} chooses a random number $SK_{i,j}^n \in \{0, 1\}^l$.
 - Corrupt(ID_i): If $ID_i = ID_I$, then \mathcal{C} aborts this query; otherwise, \mathcal{C} searches for a tuple $\{ID_i, (s_i, x_i), (R_i, X_i)\}$ in L_C indexed by ID_i and returns (s_i, x_i) .
 - Replacement($ID_i, (R'_i, X'_i)$): \mathcal{C} searches for a tuple $\{ID_i, (s_i, x_i), (R_i, X_i)\}$ in L_C which is indexed by ID_i then replaces (R_i, X_i) with (R'_i, X'_i) .
 - H_5 query: \mathcal{C} keeps an empty list L_{H_5} of the tuple $(\{K_i, ID_j, PID_i, \lambda, T_j\}, h_u)$ where λ represents $a(U_j - X_j)$ or $b(U_i - X_i)$ and it answers this query as below:
 - If $(\{K_i, ID_j, PID_i, \lambda, T_j\}, h_u)$ has been in the list L_{H_5} , \mathcal{C} returns h_u .
 - Else \mathcal{C} looks for L_R . If there exists the record then \mathcal{C} returns the correspond session key $SK_{i,j}^n$.
 - Else \mathcal{C} chooses a random number $h_u \in \{0, 1\}^l$ and adds the record in the list L_{H_5} .

The probability is that \mathcal{A}_1 chooses $\Pi_{I,J}^T$ as the *Test* oracle and that $1/q_c^2 q_s$. In this case, \mathcal{A}_1 would not have made Corrupt(ID_I), Corrupt(ID_J) or Reveal($\Pi_{I,J}^T$) queries, and so \mathcal{C} would not have aborted. If \mathcal{A}_1 can win in such a game, then \mathcal{A}_1 must have made the corresponding H_5 query. Therefore, \mathcal{C} can find the corresponding record in the list of L_{H_5} indexed by $\{K_i, ID_j, PID_i, \lambda, T_j\}$ with the probability $1/q_{H_5}$ and output λ as the result of the CDH problem. Therefore, the probability, denoted as α that \mathcal{C} tackles the CDH problem satisfies $\alpha > Adv_{\mathcal{A}_1}/q_c^2 q_s q_{H_5}$, where $Adv_{\mathcal{A}_1}$ is the advantage that \mathcal{A}_1 wins the game.

Theorem 2. Assume that the Computational Diffie-Hellman (CDH) problem is intractable. Let \mathcal{A}_2 be a probabilistic polynomial time adversary against the proposed scheme Π , the advantage of \mathcal{A}_2 against our scheme is negligible.

Proof. Suppose there exists a probabilistic polynomial time adversary \mathcal{A}_2 who can win the game with a non-negligible advantage in polynomial time t . Then, we can design an algorithm \mathcal{C} to solve the CDH problem using the ability of \mathcal{A}_2 .

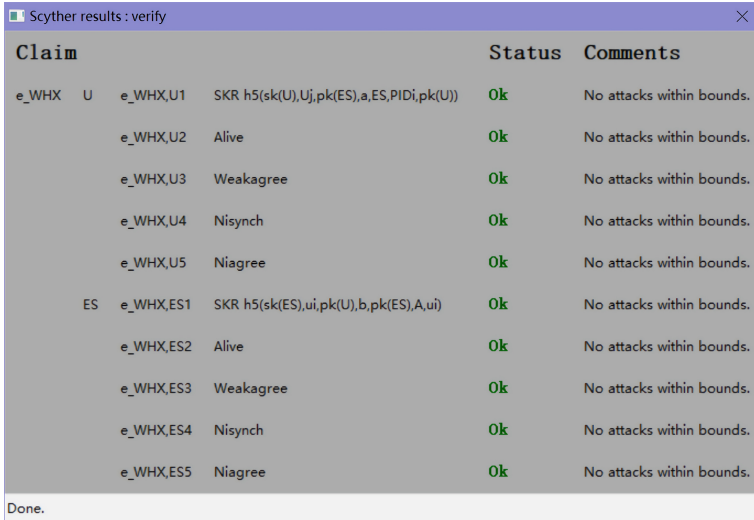
Suppose \mathcal{C} is given an instance (aP, bP) of the CDH problem whose subject is to compute $Q = abP$. Suppose \mathcal{A}_2 makes at most q_{H_i} times H_i -query and creates at most q_c participants and q_s be the maximal number of sessions each participation may be involved in.

\mathcal{C} sets P_0 as the system public key P_{pub} , selects the system parameter $params = \{F_p, E/F_p, G, P, P_{pub}, H_i\}$ and sends the public parameters to \mathcal{A}_2 . \mathcal{C} chooses at random $I \in [1, q_{H_2}]$, $J \in [1, q_{H_2}]$, $T \in [1, q_s]$. \mathcal{C} answers \mathcal{A}_2 's queries as follows.

If \mathcal{A}_2 makes $\text{Create}(ID_i)$ query, \mathcal{C} keeps an empty list L_C consisting of tuples $(ID_i, (s_i, x_i), (R_i, X_i))$. \mathcal{C} randomly selects $s_I, h_I \in Z_q^*$ and computes $R_I = r_I P$, $s_I = r_I + sh_I$ and $X_I = x_I P$. \mathcal{C} can answer other queries as Theorem 1.

The probability is that \mathcal{A}_2 chooses $\Pi_{I,J}^T$ as the *Test* oracle and that $1/q_c^2 q_s$. In this case, \mathcal{A}_2 would not have made $\text{Corrupt}(ID_I)$, $\text{Corrupt}(ID_J)$ or $\text{Reveal}(\Pi_{I,J}^T)$ queries, and so \mathcal{C} would not have aborted. If \mathcal{A}_2 can win in such a game, then \mathcal{A}_2 must have made the corresponding H_5 query. Therefore, \mathcal{C} can find the corresponding record in the list of L_{H_5} indexed by $\{K_i, ID_j, PID_i, \lambda, T_j\}$ with the probability $1/q_{H_5}$ and output λ as the result of the ECDH problem. Therefore, the probability, denoted as α that \mathcal{C} tackles the ECDH problem satisfies $\alpha > Adv_{\mathcal{A}_2}/q_c^2 q_s q_{H_5}$, where $Adv_{\mathcal{A}_2}$ is the advantage that \mathcal{A}_2 wins the game.

From the above two theorems, we can conclude that our scheme is secure against two types of adversaries.



Claim	Status	Comments
e_WHX U SKR h5(sk(U),Uj,pk(ES),a,ES,PIDi,pk(U))	Ok	No attacks within bounds.
e_WHX,U2 Alive	Ok	No attacks within bounds.
e_WHX,U3 Weakagree	Ok	No attacks within bounds.
e_WHX,U4 Nisynch	Ok	No attacks within bounds.
e_WHX,U5 Niagree	Ok	No attacks within bounds.
ES e_WHX,ES1 SKR h5(sk(ES),ui,pk(U),b,pk(ES),A,ui)	Ok	No attacks within bounds.
e_WHX,ES2 Alive	Ok	No attacks within bounds.
e_WHX,ES3 Weakagree	Ok	No attacks within bounds.
e_WHX,ES4 Nisynch	Ok	No attacks within bounds.
e_WHX,ES5 Niagree	Ok	No attacks within bounds.

Done.

Fig. 2. The analysis result by Scyther tool

Besides proving the security of the proposed scheme under the security model, we also use Scyther tool to show the proposed scheme is secure against various attacks. The result of analysis is demonstrated in the Fig. 2. According to the

Fig. 2, we can clearly obtain that under the settings predefined, the scheme can achieve mutual authentication and secure session keys simultaneously.

6 Performance Analysis

This section presents the performance assessment of the proposed scheme on the security features, computation cost and communication cost.

6.1 Security Comparison

In this subsection, we compare the security features of the proposed scheme with other related schemes [17–20], and the result is shown in Table 3. We can see that our proposed scheme can resist various attacks and satisfies the security requirements from Table 3, which means that our scheme is superior to other previous schemes in terms of security features.

Table 3. Comparison of security features

Security features	[17]	[18]	[19]	[20]	Our scheme
Mutual authentication	✓	✓	✓	✓	✓
Key agreement	✓	✓	✓	✓	✓
Forward security	×	✓	-	-	✓
Un-traceability	✓	✓	✓	✓	✓
Computation transferable	✓	×	×	×	✓
No online RC	✓	✓	✓	×	✓
Impersonation attack	✓	✓	×	✓	✓
Man-in-the-middle attack	✓	✓	×	✓	✓
Ephemeral secret attack	✓	×	×	×	✓

6.2 Computation Cost

The computation cost of the proposed scheme is compared with that of previously mentioned schemes. In terms of setting the experimental environment, we choose an additive group with the generator P and the order q , where q is 160 bits. The generator P is a base point on the Koblitz curve secp256k1: $y^2 = x^3 + 7$, denoted as E/F_p and p is 256 bits. In this paper, we mainly consider the execution time of scalar multiplication, hash function and point addition operation on an elliptic curve. Several lightweight operations, such as XOR and addition, are ignored. Table 4 shows the concrete results of these operations [17].

Table 4. The running time of related operations

Symbol	Description	Time(ms)
T_{sm}	Scalar multiplication over \mathbb{G}_1	1.1762
T_a	Point addition over \mathbb{G}_1	0.0084
T_h	Hash function	0.0019
T_{exp}	Exponentiation over \mathbb{G}_2	0.2332
T_{bp}	Bilinear pairing	3.3925
T_{mp}	Map to point in \mathbb{G}_2	3.8426
T_e	Encryption using AES	0.773
T_d	Decryption using AES	0.512

Mainly considering the authentication and key agreement phase, the comparison result is shown in Fig. 3. In our scheme, the computation time needed in user side for authentication and key agreement process is four hash function operations, four scalar multiplication operations, two point additions and one encryption while that of the server side is four hash function operations, five scalar multiplication operations, three point additions and one decryption. Therefore, the total execution time of our proposed scheme is 11.9204 ms. In the scheme of He et al. [18], the computation cost of user side is $T_{mp} + 3T_{sm} + 4T_h + 2T_{exp} = 7.4852$ ms and server side is $2T_{bp} + 5T_h + 2T_a + T_{exp} = 7.2777$ ms. Similarly, the computation overheads of user side and server side in Liu et al.’s scheme [19] are $6T_{sm} + 5T_h + 5T_a = 7.1087$ ms and $6T_{sm} + 5T_h + 5T_a = 7.1887$ ms, respectively.

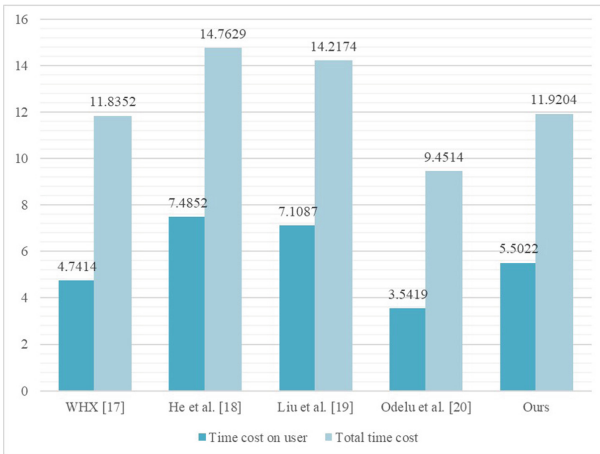


Fig. 3. The comparison result of computation cost

6.3 Communication Cost

In this subsection, the comparison of the communication cost between our proposed scheme with other related schemes is presented. We assume that the length of identity, login request and timestamp is 32 bits, marked as $|ID|$, $|L|$, $|T|$, respectively. The output length of hash function is 160 bits, expressed as $|H|$. A ciphertext block is 128 bits, expressed as $|C|$ and the lengths of p and q are 256 bits and 160 bits, respectively. In this way, a point on elliptic curve $G = (G_x, G_y)$ is 512 bits, denoted as $|G|$. Further, assume a value in Z_q^* be 160 bits, which is denoted as $|Z_q^*|$.

Table 5. Comparison of communication cost

Scheme	User side	Server side	Total
[17]	$3 H + Z_q^* + T $	$ G + H + T $	1376 bits
[18]	$ L + ID + 2 G $	$ G + H $	1760 bits
[19]	$ T + 2 G + H + Z_q^* $	$2 G + ID + Z_q^* $	2592 bits
[20]	$ C + G + 2 H $	$3 C + 2 G + 4 H $	3008 bits
Ours	$ G + 2 H + T $	$ G + C + T $	1536 bits

During the communication between U_i and ES in the proposed scheme, the message M_1 sent by user U_i , requires $|G| + 2|H| + |T| = 864$ bits; and the message M_2 sent by ES, employs the cost of $|G| + |C| + |T| = 672$ bits. Therefore, the addition of all the messages is 1568 bits. In the protocol [19], the communication cost needed by user side is $|T| + 2|G| + |H| + |Z_q^*| = 1376$ bits while that by server require $2|G| + |ID| + |Z_q^*| = 1216$ bits, so the total cost is 2592 bits. The communication cost of the other related schemes can be computed similarly and the final result is shown in Table 5.

From comparison results in Table 5, it can be concluded that the communication cost of our proposed scheme generally has less communication cost than other related schemes. Although the communication cost of our proposed scheme is higher than that of WHX protocol, our scheme can satisfy more secure requirements.

7 Conclusion

In this paper, we point out that there exists forward security problem in WHX protocol. Aiming at remedy such potential risk, we propose an improved scheme based on the former one. The proposed scheme redesigns the generation of the session key without depending too much on the ephemeral keys. To comprehensively prove its security, formal analysis and informal analysis are used by combining theory and tools. Moreover, to evaluate the performance, we give comparisons on computation and communication cost with the former schemes.

The analysis results of security and performance illustrate that our scheme is exactly security-enhanced with the forward security and outperforms WHX protocol from the perspective of computation cost.

Acknowledgment. This work was supported in part by National Natural Science Foundation of China (Grant No. 61872449).

References

1. Chenam, V.B., Ali, S.T.: A designated cloud server-based multi-user certificateless public key authenticated encryption with conjunctive keyword search against IKGA. *Comput. Stand. Interfaces* **81**, 103603 (2022)
2. Shiraly, D., Pakniat, N., Noroozi, M., Eslami, Z.: Paring-free certificateless authenticated encryption with keyword search. *J. Syst. Archit.* **124**, 102390 (2022)
3. Turkanović, M., Brumen, B., Hölbl, M.: A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. *Ad Hoc Netw.* **20**, 96–112 (2014)
4. Farash, M.S., Turkanović, M., Kumari, S., Hölbl, M.: An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Netw.* **36**, 152–176 (2016)
5. Gope, P., Hwang, T.: A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks. *IEEE Trans. Ind. Electron.* **63**(11), 7124–7132 (2016)
6. Adavoudi-Jolfaei, A.H., Ashouri-Talouki, M., Aghili, S.F.: Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks. *Peer Peer Netw. Appl.* **12**(1), 43–59 (2017). <https://doi.org/10.1007/s12083-017-0627-8>
7. Dolev, D., Yao, A.: On the security of public key protocols. *IEEE Trans. Inf. Theory* **29**(2), 198–208 (1983)
8. Ryu, J., Kang, D., Lee, H., Kim, H., Won, D.: A secure and lightweight three-factor-based authentication scheme for smart healthcare systems. *Sensors* **20**(24), 7136 (2020)
9. Al-Riyami, S.S., Paterson, K.G.: Certificateless public key cryptography. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 452–473. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-40061-5_29
10. Mandt, T.K., Tan, C.H.: Certificateless authenticated two-party key agreement protocols. In: Okada, M., Satoh, I. (eds.) ASIAN 2006. LNCS, vol. 4435, pp. 37–44. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77505-8_4
11. Wang, S.B., Cao, Z.F., Wang, L.C.: Efficient certificateless authenticated key agreement protocol from pairings. *Wuhan Univ. J. Nat. Sci.* **11**(5), 1278–1282 (2006)
12. Hou, M.B., Xu, Q.L.: On the security of certificateless authenticated key agreement protocol. In: 2009 IEEE International Symposium on IT in Medicine Education, pp. 974–979. IEEE (2009)
13. Asari, A., Alagheband, M.R., Bayat, M., Asaar, M.R.: A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems. *Comput. Netw.* **185**(11), 107599 (2021)
14. Samra, B., Fouzi, S.: New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET. *Veh. Commun.* **34**, 100414 (2022)

15. Cheng, Q.F., Li, Y.T., Shi, W.B., Li, X.H.: A certificateless authentication and key agreement scheme for secure cloud-assisted wireless body area network. *Mob. Netw. Appl.* **27**, 346–356 (2022)
16. He, D.B., Chen, J.H., Hu, J.: A pairing-free certificateless authenticated key agreement protocol. *Int. J. Commun. Syst.* **25**(2), 221 (2011)
17. Wang, W.M., Huang, H.P., Xiao, F., Li, Q., Xue, L.Y., Jiang, J.S.: Computation-transferable authenticated key agreement protocol for smart healthcare. *J. Syst. Archit.* **118**, 102215 (2021)
18. He, D.B., Kumar, N., Khan, M.K., Wang, L.N., Shen, J.: Efficient privacy-aware authentication scheme for mobile cloud computing services. *IEEE Syst. J.* **12**(2), 1621–1631 (2018)
19. Liu, X., Jin, C., Li, F.: An improved two-layer authentication scheme for wireless body area networks. *J. Med. Syst.* **42**, 143 (2018)
20. Odelu, V., Das, A.K., Goswami, A.: A secure biometrics-based multi-server authentication protocol using smart cards. *IEEE Trans. Inf. Forensics Secur.* **10**(9), 1953–1966 (2015)