A Secure Mutual Authentication Scheme for Wireless Communication

Jie Song, Xiangyu Pan, and Fagen Li(✉)

School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China
fagenli@uestc.edu.cn

Abstract. With the rapid development of network technology, the number of mobile devices is increasing at a phenomenal speed. However, many wireless communications are established on public wireless networks, which makes it a challenge to ensure the message confidentiality and user privacy. Besides, mobile devices usually have limited resources. It is necessary to design a secure and efficient cryptographic scheme for wireless communication. In this paper, we propose an identity-based mutual authentication scheme for resource-constrained mobile devices. With the help of random oracle model, we show that the scheme is provably secure under extended Canetti-Krawczyk (eCK) security model. Finally, through comparative experiments with six related works, we demonstrate that the proposed scheme is the most suitable for resource-constrained mobile devices in wireless communications.

Keywords: Mutual authentication · Identity-based cryptography · Key exchange · Mobile devices · Wireless communication

1 Introduction

In recent years, 5th generation (5G) network has been gradually popularized with the rapid development of network technology. Meanwhile, a large quantity of emerging applications based on wireless network are integrated into people's daily life. Vehicle ad hoc networks (VANETs) improve the transportation efficiency and driving safety by providing reliable information services for vehicles [32]. Wireless body area networks (WBANs) collect real-time biomedical data through the sensors placed in or around patients' bodies and send it to remote medical personnel for diagnosis [27]. Unmanned aerial vehicle (UAV) technology has been filtering down to ordinary consumers, which can be used for aerial photography, media filming, package delivery, emergency rescue and so forth [33]. Since most applications like the above are established on public wireless networks, the messages transmitted may be intercepted, modified, replayed etc.

Supported by Sichuan Science and Technology Program (Grant No. 2022YFG0172 and 2022ZHCG0037).

H. Yang and R. Lu (Eds.): FCS 2023, CCIS 1992, pp. 114–130, 2024.
https://doi.org/10.1007/978-981-99-9331-4_8

In those cases, users' privacy data can be revealed and the validity of messages cannot be guaranteed. It is crucial to ensure the security of wireless communication, which includes user authentication, data confidentiality, message integrity, privacy preservation and so on. In addition, most mobile devices are considered to have relatively low computation power and small storage space. Therefore, it is necessary to design a cryptographic scheme with high security and efficiency for wireless communication. To reduce the cost of mobile devices, we propose an identity-based mutual authentication scheme for wireless communication. Then, we prove that the proposed scheme is secure under the well-known extended Canetti-Krawczyk (eCK) [12] security model. Through comparison with related works, our scheme is the most suitable for resource-constrained mobile devices in wireless communications.

Related works are discussed in Sect. 2. Section 3 describes preliminaries. Then, we give the concrete construction of the scheme and provide the security analysis in Sect. 4 and 5, respectively. In Sect. 6, we show the comparison results between our scheme with other schemes. Finally, we conclude this paper in Sect. 7.

2 Related Works

Shim [23] introduced an identity-based signature scheme and constructed a conditional privacy-preserving authentication scheme for vehicular sensor networks. The authentication scheme could also support batch verification process. Subsequently, Liu et al. [14] found that [23] was proved only secure against chosen-identity and no-message attack and it had non-negligible error in batch verification. To reduce the computation overhead of message processing in VANET, He et al. [10] designed a pairing-free authentication scheme with conditional privacy protection. To achieve secure communication and driver privacy in a vehicular sensor network, Lo and Tsai [16] developed an identity-based signature scheme and proposed a novel anonymous authentication scheme. To deal with the issue that too many valid identities were held by one user to protect identity privacy, Wang and Yao [26] presented a local identity-based anonymous message authentication protocol based on a hybrid authentication scheme. However, the aforementioned works were designed to support one-way authentication.

In 2008, Yang and Chang [30] put forward an identity-based remote mutual authentication scheme on elliptic curve cryptosystem (ECC). Their scheme also supported a session key agreement between two participants. Later, Yoon and Yoo [31] found out that [30] was not secure against impersonation attack and could not satisfy perfect forward secrecy. They provided an improved scheme which not only solved the security issues in [30] but also reduced computation overhead. In 2012, He et al. [5] came up with a more efficient identity-based remote mutual authentication scheme. It was proved secure under random oracle model (ROM). In the next year, Chou et al. [4] introduced two authentication with key agreement schemes, which included a two-party and three-party identity-based mutual authentication scheme respectively. They claimed that

the two schemes were able to achieve strong notions of security. Unfortunately, Farash and Attari [7] demonstrated that two schemes in [4] were both insecure against impersonation attack. Besides, they presented an improved one to eliminate the security flaws of the first scheme in [4]. Wang and Zhang [27] came up with an anonymous authentication scheme for WBANs and analyzed the security by means of BAN [2] logic. However, Wu et al. [29] demonstrated that [27] was vulnerable to impersonation attack and presented another anonymous authentication scheme under ROM. To provide secure communication in mobile healthcare social networks (MHSNs), He et al. [8] introduced a framework for handshake scheme in MHSNs and proposed a cross-domain handshake scheme which supported symptoms-matching in MHSNs. However, the communication cost in [8] was too expensive. Odelu et al. [20] presented a new provably secure authenticated key agreement scheme for smart grid. They demonstrated that the scheme was secure under Canetti-Krawczyk (CK) [3] model. However, it suffers from denial of service (DoS) attack since the smart meter must send a third message to complete the session. Saeed et al. [22] put forward an authentication key agreement scheme for wireless sensor networks and proved it secure under extended Canetti-Krawczyk (eCK) [12] model. Kumar and Chand [11] designed an identity-based anonymous authentication and key agreement protocol for WBAN, and they showed that the protocol was provably secure under BRP [1] model. Unfortunately, it could not provide perfect forward secrecy because an attacker was able to recover the ephemeral key after a key extraction query, and then calculate the session key.

Besides, Mezrag et al. [18] and Fanian et al. [6] proposed clustering mechanism to extend the wireless sensor networks lifetime. Mezrag et al. [19] presented an identity-based authentication and key agreement scheme, which achieved all desirable security properties of key agreement and prevented specific cyber-attacks on clustered wireless sensor networks. Wang et al. [25], Tao et al. [24] and Liu et al. [15] researched cross-domain authentication key agreement protocol for heterogeneous cryptosystem, where the protocol initiator used PKI and the responder used IBC. However, the communication cost in the above three protocol was too expensive due to too many interaction rounds. Li et al. [13] and He et al. [9] studied on heterogeneous anonymous mutual authentication, where the protocol initiator belonged to IBC while the responder belonged to PKI. Zhang et al. [33] and Wazid et al. [28] worked on lightweight remote authentication protocols for UAV communications.

3 Preliminaries

3.1 Bilinear Pairing

$\mathbb{G}_1$ is an additive group with order q and $\mathbb{G}_2$ is a multiplicative group with order q, where q is a large prime number. $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a bilinear map and it satisfies the following three properties.

– Bilinearity: $\hat{e}(rP, sQ) = \hat{e}(P, Q)^{rs}$ for any $r, s \in \mathbb{Z}_q^*$ and $P, Q \in \mathbb{G}_1$.

– Non-degeneracy: $\hat{e}(P,Q) \neq 1_{\mathbb{G}_2}$ for any $P, Q \in \mathbb{G}_1$, where $1_{\mathbb{G}_2}$ is the identity element of $\mathbb{G}_2$.
– Computability: $\hat{e}(P,Q)$ can be computed efficiently for any $P, Q \in \mathbb{G}_1$.

3.2 Collusion Attack Algorithm with k Traitors (k-CAA) Problem

Given $(h_1, h_2, ..., h_k) \in \mathbb{Z}_q^*$ and $(P, sP, (s+h_1)^{-1}P, (s+h_2)^{-1}P, ..., (s+h_k)^{-1}P) \in \mathbb{G}_1$, it is difficult to compute $(s+h)^{-1}P$ for some $h \in \mathbb{Z}_q^*$.

3.3 q-Strong Diffie-Hellman (q-SDH) Problem

Given a generator $P \in \mathbb{G}_1$ and q elements $(sP, s^2P, ..., s^qP) \in \mathbb{G}_1$, finding a pair $(t, (s+t)^{-1}P)$ is hard.

3.4 Computational Diffie-Hellman (CDH) Problem

Given two randomly selected $rP, sP \in \mathbb{G}_1$, it is difficult to compute rsP.

3.5 System Architecture

The communication system model is depicted in Fig. 1. It is composed of the three participants, namely PKG, User A and User B. All users should register with PKG. It verifies a user's identity and generates a long-term secret key based on the identity. A and B is the initiator and responder of the scheme, respectively. They intend to achieve mutual authentication.

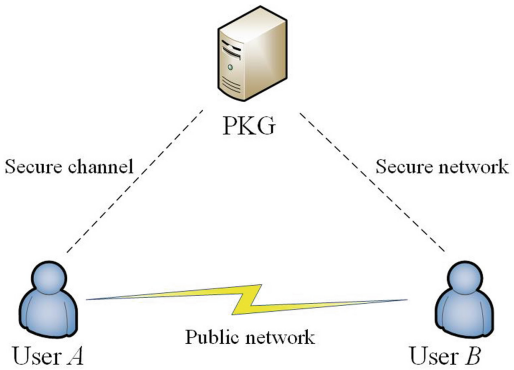

Fig. 1. Communication system model

3.6 Security Model

We adopt the well-known extended Canetti-Krawczyk [12] (eCK) security model. Let $\Gamma^i_{ID_U}$ denote user U's i-th session. We say that $\Gamma^i_{ID_U}$ is accepted if the proposed scheme is finished successfully in the session. Every accepted session has a session key K, a session identification sid. We say that session $\Gamma^i_{ID_U}$ and session $\Gamma^j_{ID_V}$ are partnered if they share a same K and a same sid. The eCK security model can be defined by a game played by an adversary $\mathcal{F}$ and a challenger $\mathcal{C}$ as follows.

$\mathcal{F}$ is allowed to adaptively query the following oracles.

- $H_i(M)$: It takes as input M and returns a random hash value.
- Send$(\Gamma^i_{ID_U}, m)$: It simulates that user U receives message m and replies with the corresponding message according to the proposed scheme.
- Extract(ID_i): It reveals the long-term secret key of ID_i.
- Ephemeral Key Reveal$(\Gamma^i_{ID_U})$: It reveals the ephemeral key chosen by user U in $\Gamma^i_{ID_U}$.
- Reveal$(\Gamma^i_{ID_U})$: It reveals the session key of $\Gamma^i_{ID_U}$.
- Test$(\Gamma^i_{ID_U})$: This query can be issued only once. It randomly chooses a bit $b \in \{0, 1\}$. If $b = 0$, it responds with a random $K \in \mathbb{G}_2$; Otherwise, it responds with the session key of $\Gamma^i_{ID_U}$.

When $\mathcal{F}$ finishes the query phase, it outputs a bit $b' \in \{0, 1\}$ as the guess of b. $\mathcal{F}$ wins the game if $b' = b$ and $\Gamma^i_{ID_U}$ is accepted and clean. Assume that $\Gamma^i_{ID_U}$ and $\Gamma^j_{ID_V}$ are partnered, we say that $\Gamma^i_{ID_U}$ is clean if neither of the following conditions is met.

1. User U or V is an adversary-controlled party. It means that the long-term secret key and ephemeral key are both selected by $\mathcal{F}$.
2. $\mathcal{F}$ reveals both the long-term secret key of user U and ephemeral key chosen by user U in $\Gamma^i_{ID_U}$.
3. $\mathcal{F}$ reveals both the long-term secret key of user V and ephemeral key chosen by user V in $\Gamma^j_{ID_V}$.

4 Our Scheme

We provide the concrete construction of the proposed scheme in this section, which is composed of three phases namely Setup, Registration and Authentication. The symbols involved are shown in Table 1.

4.1 Setup

According to security parameter λ, PKG sets public parameters pp as follows.

1. It selects a large prime number q, a q-order additive group $\mathbb{G}_1$, a q-order multiplicative group $\mathbb{G}_2$, a bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfying the properties in Sect. 3.1. P is a generator of $\mathbb{G}_1$ and $g = \hat{e}(P, P)$ is a generator of $\mathbb{G}_2$.

Table 1. Symbols and descriptions

Symbol	Description
λ	Security parameter
pp	Public parameters
q	A large prime number
$\hat{e}$	A bilinear map from $\mathbb{G}_1$ to $\mathbb{G}_2$
$\mathbb{G}_1$	An additive group with order q
$\mathbb{G}_2$	A multiplicative group with order q
P	A generator in $\mathbb{G}_1$
g	A generator in $\mathbb{G}_2$
H_i	The i-th Hash function
P_{pub}/s	Master public/secret key pair
ID_U	The identity of user U
S_{ID_U}	The long-term secret key of user U

2. It selects five secure one-way hash functions: $H_i : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, where $i = 1$ to 5.
3. It chooses master secret key $s \in \mathbb{Z}_q^*$ and calculates master public key $P_{pub} = sP$.

Finally, PKG publishes public parameters $pp = \{q, \mathbb{G}_1, \mathbb{G}_2, P, g, \hat{e}, H_1, H_2, H_3, H_4, H_5, P_{pub}\}$ and keeps s secret.

4.2 Registration

User A sends its identity ID_A to PKG for registration. PKG takes as input s and ID_A, then calculates a long-term secret key S_{ID_A} for user A.

$$S_{ID_A} = \frac{1}{s + H_1(ID_A)} P$$

PKG transmits S_{ID_A} to user A secretly. After receiving S_{ID_A}, user A computes $s_A = H_2(ID_A, S_{ID_A})$. Similarly, user B registers with PKG for its long-term secret key S_{ID_B} and calculates s_B.

4.3 Authentication

After both users register with PKG, they start a communication session for mutual authentication.

1. In the beginning, user A randomly picks $r_A \in \mathbb{Z}_q^*$ and calculates

$$T_A = (r_A + s_A)(H_1(ID_B)P + P_{pub}),$$

$$K_A = g^{(r_A + s_A)},$$
$$h_1 = H_3(ID_A, T_A, K_A),$$
$$\sigma_A = (r_A + s_A + h_1)S_{ID_A},$$
$$c_A = H_4(K_A, ID_B) \oplus (ID_A, \sigma_A),$$

then delivers message $m_1 = (T_A, c_A)$ to user B through an open public network.

2. Upon receiving message m_1, user B first computes

$$K_A = \hat{e}(S_{ID_B}, T_A),$$

and recovers the sender's identity and the corresponding signature

$$(ID_A, \sigma_A) = c_A \oplus H_4(K_A, ID_B).$$

Then user B calculates

$$h_1 = H_3(ID_A, T_A, K_A),$$

and verifies the validity of the signature

$$\hat{e}(\sigma_A, H_1(ID_A)P + P_{pub}) = g^{h_1} K_A$$

If the above equation does not hold, the verification fails and user B abandons the session. Otherwise, the authentication of user A is completed. Afterwards, user B randomly selects $r_B \in \mathbb{Z}_q^*$ and does the following computations.

$$K_B = g^{r_B + s_B}, K_{BA} = K_A^{r_B + s_B},$$

$$h_2 = H_5(ID_A, ID_B, K_A, K_B, K_{BA}).$$

Then user B accepts K_{BA} as the session key and transmits $m_2 = (K_B, h_2)$ back to user A.

3. After receiving message m_2 from user B, user A computes

$$K_{AB} = K_B^{r_A + s_A},$$

then verifies the following equation.

$$h_2 = H_5(ID_A, ID_B, K_A, K_B, K_{AB})$$

If it holds, the authentication of user B is finished and user A accepts K_{AB} as the session key. Otherwise, user A closes the session.

4.4 Correctness

We prove the correctness of our scheme as below. User B computes

$$\begin{aligned} K_A &= \hat{e}(S_{ID_B}, T_A) \\ &= \hat{e}(\frac{1}{s + H_1(ID_B)}P, (r_A + s_A)(H_1(ID_B)P + P_{pub})) \\ &= \hat{e}(P, P)^{(r_A + s_A)} \\ &= g^{(r_A + s_A)}, \\ h_1 &= H_3(ID_A, T_A, K_A), \end{aligned}$$

then user B verifies the validity of σ_A as follows.

$$\begin{aligned} &\hat{e}(\sigma_A, H_1(ID_A)P + P_{pub}) \\ &= \hat{e}((r_A + s_A + h_1)\frac{1}{s + H_1(ID_A)}P, H_1(ID_A)P + P_{pub}) \\ &= \hat{e}(P, P)^{(r_A + s_A + h_1)} \\ &= K_A g^{h_1} \end{aligned}$$

After that, user B calculates the session key as

$$K_{BA} = K_A^{(r_B + s_B)} = g^{(r_A + s_A)(r_B + s_B)}.$$

In the side of user A, it calculates the session key as

$$K_{AB} = K_B^{(r_A + s_A)} = g^{(r_B + s_B)(r_A + s_A)} = K_{BA}.$$

5 Security Analysis

5.1 Mutual Authentication (MA)

Theorem 1. *If the k-CAA problem is difficult, the proposed scheme can achieve initiator-to-responder authentication.*

Proof. If there is a probabilistic polynomial time (PPT) adversary $\mathcal{F}$ who can forge a valid intialization message, we can construct another PPT algorithm $\mathcal{C}$ using $\mathcal{F}$ as a subroutine to solve the given k-CAA instance $(q_1, q_2, ..., q_k, P, sP, (s+q_1)^{-1}P, (s+q_2)^{-1}P, ..., (s+q_k)^{-1}P)$. $\mathcal{C}$'s task is to find a pair $(q^*, (s+q^*)^{-1}P)$ for some $q^* \in \mathbb{Z}_q^*$. $\mathcal{C}$ sets the challenge initiator identity as ID^*, generates public parameters $pp = \{q, \mathbb{G}_1, \mathbb{G}_2, P, g, P_{pub} = sP\}$ and sends pp to $\mathcal{F}$.

Without loss of generality, we suppose that Send and Extract queries are preceded by an H_1 query, and k is larger than the number of H_1 query. $\mathcal{C}$ generates initially empty lists L_{H_1}, L_{H_2}, L_{H_3}, L_{H_4} and L_{H_5} to store the query results of five hash functions respectively. $\mathcal{C}$ answers $\mathcal{F}$'s queries as follows.

- $H_1(ID_i)$: If $ID_i = ID^*$, $\mathcal{C}$ responds with q^*. Otherwise, $\mathcal{C}$ answers with q_i and adds $(ID_i, q_i, (s+q_i)^{-1}P)$ to L_{H_1}.
- $H_2(m_i)$: $\mathcal{C}$ randomly chooses $s_i \in \mathbb{Z}_q^*$, answers with s_i and adds (m_i, s_i) to L_{H_2}.
- $H_3(m_i)$: $\mathcal{C}$ randomly chooses $h_{1i} \in \mathbb{Z}_q^*$, answers with h_{1i} and adds (m_i, h_{1i}) to L_{H_3}.
- $H_4(m_i)$: $\mathcal{C}$ randomly chooses $k_i \in \mathbb{Z}_q^*$, answers with k_i and adds (m_i, k_i) to L_{H_4}.
- $H_5(m_i)$: $\mathcal{C}$ randomly chooses $h_{2i} \in \mathbb{Z}_q^*$, answers with h_{2i} and adds (m_i, h_{2i}) to L_{H_5}.
- Send($\Gamma^i_{ID_U}, m$): If $ID_U = ID^*$ and $m =$ 'Start', $\mathcal{C}$ randomly selects $r, h \in \mathbb{Z}_q^*$, calculates

$$T = rq^*P + rP_{pub} - hq_VP - hP_{pub},$$

$$K = \hat{e}(\frac{1}{s+q_V}P, T),$$

$$\sigma = \frac{r}{s+q_V}P,$$

$$c = H_4(K, ID_V) \oplus (ID^*, \sigma)$$

  and answers with (T, c), where V is the responder in $\Gamma^i_{ID_U}$. Otherwise, $\mathcal{C}$ answers according to the specification of the proposed scheme. In both cases, (T, c) is a valid initialization message.
- Extract(ID_i): $\mathcal{C}$ finds $(ID_i, q_i, (s+q_i)^{-1}P)$ from L_{H_1} and answers with $(s+q_i)^{-1}P$. Here $\mathcal{F}$ is not allowed to query ID^*.
- Ephemeral-Key-Reveal($\Gamma^i_{ID_U}$): $\mathcal{C}$ answers with the corresponding ephemeral key chosen by user U in $\Gamma^i_{ID_U}$.
- Reveal($\Gamma^i_{ID_U}$): $\mathcal{C}$ answers with the session key of $\Gamma^i_{ID_U}$.
- Test($\Gamma^i_{ID_U}$): $\mathcal{C}$ randomly chooses a bit $b \in \{0, 1\}$. If $b = 0$, $\mathcal{C}$ answers with a random $K \in \mathbb{G}_2$; Otherwise, $\mathcal{C}$ answers with the session key of $\Gamma^i_{ID_U}$.

After query phase, $\mathcal{F}$ forges a valid initialization message (T_A, c_A) from ID^* to ID_V. We replays $\mathcal{C}$ with the same tape but different choices of H_3, as in forking lemma [21], so that $\mathcal{F}$ outputs another valid initialization message (T'_A, c'_A). $\mathcal{C}$ first recovers (K_A, σ_A) and (K'_A, σ'_A) from two messages respectively, then computes h_1 and h'_1 respectively. Finally, $\mathcal{C}$ calculates $S_{ID^*} = (h_1 - h'_1)(\sigma_1 - \sigma_2)$, and outputs S_{ID^*} as the solution of the given k-CAA problem. □

Theorem 2. *If the DL problem and 1-SDH problem are difficult, the proposed scheme can achieve responder-to-initiator authentication.*

Proof. Assume that an adversary $\mathcal{F}$ intercepts an initialization message (T_A, c_A) from user A to user B, $\mathcal{F}$ tries to forges a valid response message from user B to user A. Due to the collision resistance of hash functions, $\mathcal{F}$ has to extract the correct K_A from T_A. There are three cases that $\mathcal{F}$ can recover K_A successfully, which are shown below.

Case 1: $\mathcal{F}$ just guesses the right value of h_2.
Case 2: $\mathcal{F}$ extracts s from $P_{pub} = sP$ so that $\mathcal{F}$ is able to compute user B's long-term secret key $S_{ID_B} = (s + H_1(ID_B))^{-1}P$ and recover K_A.
Case 3: $\mathcal{F}$ calculates $S_{ID_B} = (s + H_1(ID_B))^{-1}P$ and recover K_A.

Apparently the probability of Case 1 is $1/2^{\lambda}$, which is a negligible number. Since DL problem and 1-SDH problem are difficult, Case 2 and 3 can hardly happen. To sum up, forging a valid response message is hard to achieve. □

Based on Theorem 1 and Theorem 2, no adversary can forge a valid initialization message or a valid response message. Therefore, mutual authentication is achieved.

5.2 Key Agreement

From Sect. 4.4, it can be easily seen that user A and user B finally agree on a same session key if the proposed scheme is executed successfully.

5.3 Session Key Security (SKS)

Theorem 3. *If k-CAA, DL, 1-SDH and DBDH problems are difficult to solve, the proposed scheme is able to satisfy SKS under eCK security model.*

Proof. An adversary $\mathcal{F}$ can get advantage in attacking SKS of the proposed scheme in the following two cases:

Case 1: $\mathcal{F}$ intercepts and forges authentication transcripts, which means $\mathcal{F}$ may impersonate a user.
Case 2: $\mathcal{F}$ does not alter any transcripts.

From Sect. 5.1 we can get that, if k-CAA, DL and 1-SDH problems are difficult, the probability of $\mathcal{F}$ forging a valid message is negligible. Therefore, The advantage in Case 1 is negligible too.

Then we discuss Case 2. Given an instance of DBDH problem (aP, bP, cP, X), $\mathcal{C}$ needs to decide if $X = \hat{e}(P, P)^{abc}$. $\mathcal{C}$ selects $s \in \mathbb{Z}_q^*$, generates public parameters $pp = \{q, \mathbb{G}_1, \mathbb{G}_2, P, g, P_{pub} = sP\}$ and sends pp to $\mathcal{F}$. $\mathcal{C}$ guesses α such that $\mathcal{F}$ queries Test with the α-th session.

Without loss of generality, we suppose that Send and Extract queries are preceded by an H_1 query. $\mathcal{C}$ generates initially empty lists L_{H_1}, L_{H_2}, L_{H_3}, L_{H_4} and L_{H_5} to store the query results of five hash functions respectively. $\mathcal{C}$ answers queries as follows.

- $H_1(ID_i)$: $\mathcal{C}$ randomly chooses $q_i \in \mathbb{Z}_q^*$, responds with q_i and adds (ID_i, q_i) to L_{H_1}.
- $H_2(m_i)$: $\mathcal{C}$ randomly chooses $s_i \in \mathbb{Z}_q^*$, answers with s_i and adds (m_i, s_i) to L_{H_2}.
- $H_3(m_i)$: $\mathcal{C}$ randomly chooses $h_{1i} \in \mathbb{Z}_q^*$, answers with h_{1i} and adds (m_i, h_{1i}) to L_{H_3}.

- $H_4(m_i)$: $\mathcal{C}$ randomly chooses $k_i \in \mathbb{Z}_q^*$, answers with k_i and adds (m_i, k_i) to L_{H_4}.
- $H_5(m_i)$: $\mathcal{C}$ randomly chooses $h_{2i} \in \mathbb{Z}_q^*$, answers with h_{2i} and adds (m_i, h_{2i}) to L_{H_5}.
- Send($\Gamma^i_{ID_U}, m$): When $\mathcal{F}$ queries the the α-th session, $\mathcal{C}$ calculates

$$T_U = (s + H_1(ID_V))aP, K_U = \hat{e}(aP, P),$$
$$h_1 = H_3(ID_U, T_U, K_U),$$
$$\sigma_U = \frac{1}{s + H_1(ID_U)}(aP + h_1 P),$$
$$c_U = H_4(K_U, ID_V) \oplus (ID_U, \sigma_U),$$

  and answers (T_U, c_U) as the initialization message. $\mathcal{C}$ then computes

$$K_V = \hat{e}(bP, cP), K_{VU} = X,$$
$$h_2 = H_5(ID_U, ID_V, K_U, K_V, K_{VU}),$$

  and answers (K_V, h_2) as the response message. Otherwise, $\mathcal{C}$ answers according to the specification of the proposed scheme.
- Extract(ID_i): $\mathcal{C}$ finds (ID_i, q_i) from L_{H_1} and answers with $(s + q_i)^{-1}P$.
- Ephemeral-Key-Reveal($\Gamma^i_{ID_U}$): $\mathcal{C}$ answers with the corresponding ephemeral key chosen by user U in $\Gamma^i_{ID_U}$.
- Reveal($\Gamma^i_{ID_U}$): $\mathcal{C}$ answers with the session key of $\Gamma^i_{ID_U}$.
- Test($\Gamma^i_{ID_U}$): If $\mathcal{F}$ queries the α-th session, $\mathcal{C}$ answers with X. Otherwise, $\mathcal{C}$ randomly chooses a bit $b \in \{0, 1\}$. If $b = 0$, $\mathcal{C}$ answers with a random $K \in \mathbb{G}_2$; If $b = 1$, $\mathcal{C}$ answers with the session key of $\Gamma^i_{ID_U}$.

The probability of $\mathcal{F}$ querying Test with the α-th session is at least $1/q_S$, where q_S is the maximum number of Send query. If $\mathcal{F}$ can win the game with a non-negligible advantage ϵ, $\mathcal{C}$ is able to solve the given DBDH problem with an advantage larger than $(1/q_S)\epsilon$. □

5.4 Perfect Forward Secrecy (PFS)

If S_{ID_A} and S_{ID_B} are revealed, the attacker can calculate $s_A = H_1(ID_A, S_{ID_A})$ and $s_B = H_1(ID_B, S_{ID_B})$. It can get $K_B = g^{(r_B + s_B)}$ from transcripts and recover $K_A = g^{(r_A + s_A)}$ from T_A, then compute g^{r_A} and g^{r_B}. However, it is not capable of computing the session key $g^{(r_A + s_A)(r_B + s_B)}$ based on K_A and K_B due to the CDH problem. Only if the attacker gets r_A or r_B, it can calculates the session key. Nevertheless, it is difficult for the attacker to derive r_A or r_B because of the DL problem. Therefore, perfect forward secrecy is achieved.

5.5 Identity Privacy

The transcript of a session consists of two messages, (T_A, c_A) and (K_B, h_2). Only c_A contains the identity information of user A. However, an attacker is not able to extract ID_A from c_A since it cannot extract K_A from T_A without knowing user B's long-term secret key S_{ID_B}. Hence, the identity privacy is preserved.

5.6 Resistance Against Attacks

Since the proposed scheme is proved capable of satisfying mutual authentication, impersonation attack and man-in-the-middle attack will not work.

Owing to the collision resistance of hash functions, the proposed scheme can defend against replay attack if we add two timestamps to H_3 and H_5 respectively.

For the responder B, the session will be immediately abandoned if the verification equation does not hold. If B successfully responds message m_2, the proposed scheme is finished in B's side. For the initiator A, if A does not receive message m_2 from B within a set time interval after A sends message m_1, A closes the session. In other words, the proposed scheme is secure against DoS attack.

Even if an attacker has the access to the ephemeral keys (r_A, r_B), the session key is secure since the attacker does not know two users' long-term secret keys (S_{ID_A}, S_{ID_B}) and is not able to compute s_A or s_B. Therefore, the proposed scheme can resist against ephemeral key compromise attack.

6 Comparison

We compare the proposed scheme with six related works [8,9,11,20,22,29] in terms of security, computation overhead and communication cost. Table 2 shows the security comparison. SP-1, SP-2, SP-3, SP-4, SP-5, SP-6 and SP-7 denote seven security properties respectively, namely MA, SKS, PFS, identity privacy, resistance against replay attack, resistance against DoS attack and resistance against ephemeral key compromise attack. Our scheme can satisfy all security properties even under eCK model while other schemes cannot.

Table 2. Security comparison

Scheme	SP-1	SP-2	SP-3	SP-4	SP-5	SP-6	SP-7	Security model
[29]	Yes	Yes	No	Yes	Yes	Yes	No	BRP
[9]	Yes	Yes	Yes	Yes	Yes	Yes	No	BRP
[8]	Yes	Yes	Yes	Yes	Yes	Yes	No	BRP
[22]	Yes	Yes	Yes	No	Yes	Yes	No	CK
[20]	Yes	Yes	Yes	Yes	Yes	No	No	CK
[11]	Yes	Yes	No	Yes	Yes	Yes	No	BRP
Ours	Yes	Yes	Yes	Yes	Yes	Yes	Yes	eCK

We show the comparison of computation overhead in Table 3. T_{mtp}, T_{bp}, T_{pm} and T_e denote the time of a map-to-point function, a bilinear map, a point multiplication and an exponentiation respectively. In Table 3, we neglect other fast operations such as hash function, point addition, XOR etc.

The comparison of communication cost is shown in Table 4. $|\mathbb{G}_1|$, $|\mathbb{G}_2|$, $|\mathbb{Z}_q^*|$ and $|ID|$ are the length of an element in $\mathbb{G}_1$, an element in $\mathbb{G}_2$, an element in $\mathbb{Z}_q^*$ and an identity respectively.

Table 3. Computation overhead

Scheme	Initiator	Responder
[29]	$3T_{pm} + 2T_e$	$T_{bp} + 3T_{pm} + 2T_e$
[9]	$T_{mtp} + 4T_{pm}$	$T_{mtp} + 2T_{bp} + 4T_{pm}$
[8]	$6T_{pm}$	$6T_{pm}$
[22]	$6T_{pm}$	$6T_{pm}$
[20]	$2T_{pm} + 2T_e$	$2T_{bp} + 2T_{pm} + T_e$
[11]	$4T_{pm}$	$6T_{pm}$
Ours	$3T_{pm} + 2T_e$	$2T_{bp} + T_{pm} + 3T_e$

Table 4. Communication cost

Scheme	Initialization message	Response message	Rounds
[29]	$3\|\mathbb{G}_1\| + \|\mathbb{Z}_q^*\| + \|ID\|$	$\|\mathbb{G}_2\| + \|\mathbb{Z}_q^*\|$	2
[9]	$2\|\mathbb{G}_1\| + \|ID\|$	$\|\mathbb{G}_1\| + \|\mathbb{Z}_q^*\|$	2
[8]	$3\|\mathbb{G}_1\| + 3\|\mathbb{Z}_q^*\| + 2\|ID\|$	$3\|\mathbb{G}_1\| + 3\|\mathbb{Z}_q^*\| + 2\|ID\|$	3
[22]	$2\|\mathbb{G}_1\| + 2\|\mathbb{Z}_q^*\| + \|ID\|$	$2\|\mathbb{G}_1\| + 2\|\mathbb{Z}_q^*\| + \|ID\|$	2
[20]	$2\|\mathbb{G}_1\| + 3\|\mathbb{Z}_q^*\| + \|ID\|$	$\|\mathbb{G}_2\| + \|\mathbb{Z}_q^*\|$	3
[11]	$3\|\mathbb{G}_1\| + \|\mathbb{Z}_q^*\| + \|ID\|$	$\|\mathbb{G}_1\| + \|\mathbb{Z}_q^*\|$	2
Ours	$2\|\mathbb{G}_1\| + \|ID\|$	$\|\mathbb{G}_2\| + \|\mathbb{Z}_q^*\|$	2

We did the experiments on a computer with 3.60 GHz AMD Ryzen 5 3600 CPU, 16.0 GB memory and Windows 10 operating system. We used type-A curve in PBC library [17], which is an elliptic curve $y^2 = x^3 + x$ over $\mathbb{F}_p$ based on a prime order $p \equiv 3 \bmod 4$. Figure 2, 3 and 4 depict the experimental results under 80, 112 and 128 security strength respectively. Under 80 security strength, the total computation overheads of seven schemes are 20.8 ms, 38.5 ms, 30.0 ms, 33.0 ms, 19.3 ms, 26.2 ms and 18.6 ms respectively. Under 112 security strength, the total computation overheads of seven schemes are 75.4 ms, 163.1 ms, 105.8 ms, 110.0 ms, 72.5 ms, 90.9 ms and 73 ms respectively. Under 128 security strength, the total computation overheads of seven schemes are 177 ms, 434 ms, 234 ms, 238 ms, 179 ms, 198 ms and 183 ms respectively.

It can be seen that, our scheme performs better than [8,11,22] in every aspect. The communication cost of [9] is the same as ours, but its computation overhead is higher much than ours and it cannot resist against ephemeral key compromise attack under eCK model. [29] and [20] have similar computation overhead as ours. However, [29] cannot provide PFS and resistance against ephemeral key compromise attack under eCK model. [20] is not able to defend against DoS attack and ephemeral key compromise attack under eCK model. In addition, our scheme has the lowest computation overhead under 80 security strength

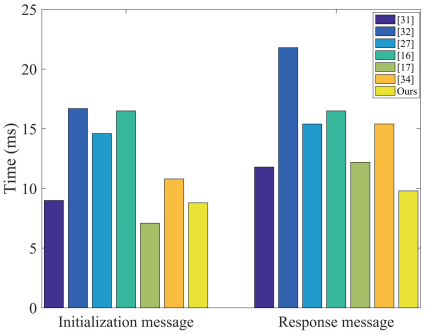

Fig. 2. 80 security strength

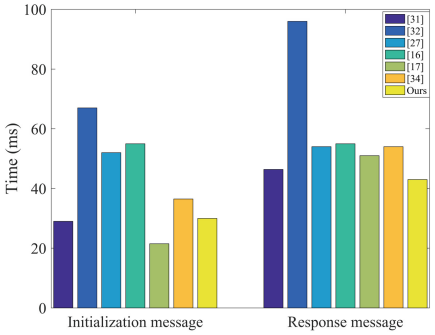

Fig. 3. 112 security strength

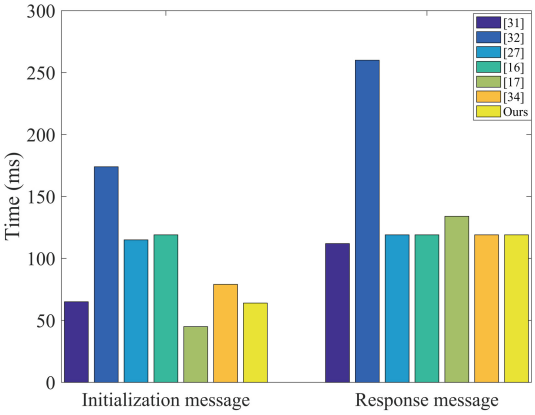

Fig. 4. 128 security strength

while has the highest security and lowest communication cost. It means that our scheme is the most suitable for resource-constrained mobile devices in wireless communications.

7 Conclusion

In this paper, we propose a mutual authentication scheme for wireless communications. We prove that the proposed scheme can achieve mutual authentication, session key security, perfect forward secrecy, identity privacy and resistance against various attacks under eCK model. Besides, through comparative experiments, we demonstrate that the proposed scheme is the most suitable for mobile devices with limited resources.

References

1. Bellare, M., Pointcheval, D., Rogaway, P.: Authenticated key exchange secure against dictionary attacks. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 139–155. Springer, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_11
2. Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. In: Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences, vol. 426, pp. 233–271 (1989)
3. Canetti, R., Krawczyk, H.: Analysis of key-exchange protocols and their use for building secure channels. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 453–474. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44987-6_28
4. Chou, C.H., Tsai, K.Y., Lu, C.F.: Two id-based authenticated schemes with key agreement for mobile environments. J. Supercomput. **66**, 973–988 (2013)
5. Debiao, H., Jianhua, C., Jin, H.: An id-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security. Inf. Fusion **13**, 223–230 (2012)
6. Fania, F., Rafsanjani, M.K.: Cluster-based routing protocols in wireless sensor networks: a survey based on methodology. J. Netw. Comput. Appl. **142**, 111–142 (2019). https://doi.org/10.1016/j.jnca.2019.04.02
7. Farash, M.S., Attari, M.A.: A secure and efficient identity-based authenticated key exchange protocol for mobile client-server networks. J. Supercomput. **69**, 395–411 (2014)
8. He, D., Kumar, N., Wang, H., Wang, L., Choo, K.K.R., Vinel, A.: A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network. IEEE Trans. Dependable Secure Comput. **15**, 33–645 (2018). https://doi.org/10.1109/TDSC.2016.2596286
9. He, D., Zeadally, S., Kumar, N., Lee, J.H.: Anonymous authentication for wireless body area networks with provable security. IEEE Syst. J. **11**, 2590–2601 (2017). https://doi.org/10.1109/JSYST.2016.2544805
10. He, D., Zeadally, S., Xu, B., Huang, X.: An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Trans. Inf. Forensics Secur. **10**, 2681–2691 (2015). https://doi.org/10.1109/TIFS.2015.2473820
11. Kumar, M., Chand, S.: A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network. IEEE Syst. J. **15**, 2779–2786 (2021). https://doi.org/10.1109/JSYST.2020.2990749
12. LaMacchia, B., Lauter, K., Mityagin, A.: Stronger security of authenticated key exchange. In: Susilo, W., Liu, J.K., Mu, Y. (eds.) ProvSec 2007. LNCS, vol. 4784, pp. 1–16. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-75670-5_1
13. Li, F., Wang, J., Zhou, Y., Jin, C.: A heterogeneous user authentication and key establishment for mobile client-server environment. Wireless Netw. **26**, 913–924 (2020)
14. Liu, J.K., Yuen, T.H., Au, M.H., Susilo, W.: Improvements on an authentication scheme for vehicular sensor networks. Expert Syst. Appl. **41**, 2559–2564 (2014). https://doi.org/10.1016/j.eswa.2013.10.003

15. Liu, X., Ma, W.: CDAKA: a provably-secure heterogeneous cross-domain authenticated key agreement protocol with symptoms-matching in TMIS. J. Med. Syst. **42**, 1–15 (2018)
16. Lo, N.W., Tsai, J.L.: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings. IEEE Trans. Intell. Transp. Syst. **17**, 1319–1328 (2016). https://doi.org/10.1109/TITS.2015.2502322
17. Lynn, B., et al.: Pairing-based cryptography library (2013). https://crypto.stanford.edu/pbc/
18. Mezrag, F, Bitam, S., Mellouk, A.: Secure routing in cluster-based wireless sensor networks. In: 2017 IEEE Global Communications Conference, pp. 1–6. GLOBECOM (2017)
19. Mezrag, F., Bitam, S., Mellouk, A.: An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks. J. Netw. Comput. Appl. **200**, 103282 (2022). https://doi.org/10.1016/j.jnca.2021.103282
20. Odelu, V., Das, A.K., Wazid, M., Conti, M.: Provably secure authenticated key agreement scheme for smart grid. IEEE Trans. Smart Grid **9**, 1900–1910 (2016)
21. Pointcheval, D., Stern, J.: Security arguments for digital signatures and blind signatures. J. Cryptol. **13**, 361–396 (2001). https://doi.org/10.1007/s001450010003
22. Saeed, M.E.S., Liu, Q.Y., Tian, G.: AKAIoTs: authenticated key agreement for internet of things. Wireless Netw. **25**, 3081–3101 (2019)
23. Shim, K.A.: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Trans. Veh. Technol. **61**, 1874–1883 (2012). https://doi.org/10.1109/TVT.2012.2186992
24. Tao, F., Shi, T., Li, S.: Provably secure cross-domain authentication key agreement protocol based on heterogeneous signcryption scheme. In: 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), vol. 1, pp. 2261–2266 (2020). https://doi.org/10.1109/ITNEC48623.2020.9084710
25. Wang, C., Liu, C., Niu, S., Wang, X.: An authenticated key agreement protocol for cross-domain based on heterogeneous signcryption scheme. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 723–728 (2017). https://doi.org/10.1109/IWCMC.2017.7986374
26. Wang, S., Yao, N.: LIAP: a local identity-based anonymous message authentication protocol in VANETs. Comput. Commun. **112**, 154–164 (2017)
27. Wang, C., Zhang, Y.: New authentication scheme for wireless body area networks using the bilinear pairing. J. Med. Syst. **39**, 1–8 (2015)
28. Wazid, M., Das, A.K., Kumar, N., Vasilakos, A.V., Rodrigues, J.J.P.C.: Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. IEEE Internet Things J. **6**, 3572–3584 (2019). https://doi.org/10.1109/JIOT.2018.2888821
29. Wu, L., Zhang, Y., Li, L.: Efficient and anonymous authentication scheme for wireless body area networks. J. Med. Syst. **40**, 134 (2016)
30. Yang, J.H., Chang, C.C.: An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem. Comput. Secur. **28**, 138–143 (2009). https://doi.org/10.1016/j.cose.2008.11.008

31. Yoon, E.Y., Yoo, K.Y.: Robust id-based remote mutual authentication with key agreement scheme for mobile devices on ECC. In: 2009 International Conference on Computational Science and Engineering, vol. 2, pp. 633–640 (2009). https://doi.org/10.1109/CSE.2009.363
32. Zhang, C., Lin, X., Lu, R.,Ho, P-H.: RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks. In: 2008 IEEE International Conference on Communications, pp. 451–1457 (2008). https://doi.org/10.1109/ICC.2008.281
33. Zhang, Y., He, D., Li, L., Chen, B.: A lightweight authentication and key agreement scheme for internet of drones. Comput. Commun. **154**, 455–464 (2020). https://doi.org/10.1016/j.comcom.2020.02.067