An Improved Certificateless Authentication Key Agreement Protocol

Zejie Liu and Haiyan Sun(✉)

College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou 450001, China
sunhaiyan@zzuli.edu.cn

Abstract. Because the information exchange between the Internet of Vehicles (IoV) is mainly through the wireless network, which makes the IoV equipment vulnerable to attack, therefore, in the V2V communication of the IoV, Lei et al. proposed an effective certificate less authenticated key exchange protocol that can resist the transient key disclosure attack, but this protocol cannot resist the temporary key disclosure attack and does not have the eCK security. On this basis, an improved certificate less authenticated key exchange protocol is proposed, and it is proved that the protocol has eCK security under GDH hypothesis and random oracle model. The analysis results show that the protocol only needs 10 elliptic curve point multiplication operations at the completion of key agreement stage, which is more efficient and less costly than the existing protocols, and is suitable for the IoV and the Internet environment.

Keywords: eCK model · certificateless authenticated · key agreement

1 Introduction

In traditional authentication-based key protocols, vehicle keys are mainly generated by a trusted third-party Key Generation Center (KGC), but the key escrow is insecure, which may lead to the theft of users' private information. However, in the certificateless key exchange protocol, KGC generates only part of the private key related to the user's identity information, such as email, certificate number, etc. Users randomly select secret information and combine some private keys to generate a complete private key, which solves key escrow and certificate management problems. Therefore, certificateless authentication key exchange protocol has attracted much attention [1, 2]. Karati et al. [3] proposed a lightweight certificateless signature scheme for the Internet of Things environment, but Zhang et al. [4] pointed out that this scheme has the problem of key leakage, and the security certificate of this scheme is incorrect.

Since certificateless authentication key exchange protocol can better solve the problems of certificate management and key escrow, Li et al. [5] proposed certificateless key agreement protocol, which has been applied in various networks [6–8]. Gong et al. [9] proposed a certificateless authentication protocol without bilinear pairs, which reduced the signature time and improved the protocol efficiency. However, Yeh et al. [10] pointed

V. Gaikar et al. (Eds.): ECIT 2023, AHE 18, pp. 196–205, 2023.
https://doi.org/10.2991/978-94-6463-210-1_25

out that document [9] has low security and is easy to be successfully attacked by adversaries, and then proposed a new certificateless authentication protocol. The authors of [11–14] are trying to improve the efficiency of the protocol to match the computing power of the Internet of vehicles. Nowadays, with the rapid development of the Internet and the exponential growth of data transmission, it is extremely important to ensure the security of key agreement protocol [15, 16].

In view of the shortcomings of the scheme proposed by Lei et al. [17], it is pointed out that the scheme is not secure under eCK model and cannot resist temporary private key attacks, and a certificateless authentication key protocol is proposed to prove security. On this basis, the scheme is improved and proved to be able to achieve eCK security.

2 Propaedeutics

Please refer to Sect. 2.2 literature [18] for complexity assumption. Please refer to Sect. 2.4 literature [18] for the eCK security model.

3 Protocol and Security Analysis of Lei et al. [17]

For the protocol of lei et al., please refer to literature [17], which is not described in detail here.

The following will point out that the scheme of Lei et al.'s [17] does not have eCK security, that is, to prove that there exists an attacker $\mathscr{A}$ who can always win it and simulator $C\mathfrak{H}$ between the game. Assume that the attacker $\mathscr{A}$ want to attack target session $\Pi_{A,B}^{\ell}$, in which the identity of A vehicle for ID_A, the identity of the vehicle B for the ID_B. The game description is as follows:

1. Game initialization: simulator $C\mathfrak{H}$ generates the system master key s and system parameters $(\mu, E/F_p, G, q, P, P_{pub}, H_1, H_2)$, and then send the system parameters to the attacker. Vehicle A randomly selects x_A and computes $X_A = x_A P$, vehicle B randomly selects x_B and computes $X_B = x_B P$, sends X_A, X_B to the simulator $C\mathfrak{H}$, respectively. Simulator $C\mathfrak{H}$ randomly selects r_i, $C\mathfrak{H}$ uses s, r_i and X_i to generate R_A, p_A for vehicle A and R_B, p_B for vehicle B.

2. First stage of the game:

(1) Attacker $\mathscr{A}$ queries *RevealEphemeralKey*$(\Pi_{A,B}^{\ell})$, then the temporary key n_A of vehicle A is obtained.

(2) Attacker $\mathscr{A}$ queries *RevealEphemeralKey*$(\Pi_{B,A}^{\ell})$, then the temporary key n_B of vehicle B is obtained.

(3) Attacker $\mathscr{A}$ queries *RevealSecretValue*(ID_i), then the long-term private key x_B of vehicle B is obtained.

(4) Attacker $\mathscr{A}$ queries *RevealPartialPrivateKey*(ID_i), then the long-term private key p_A of vehicle A is obtained.

3. The second stage of the game:

From fresh definition session $\Pi_{A,B}^{\ell}$ is fresh. Adversary $\mathscr{A}$ to perform the *Test* $(\Pi_{A,B}^{\ell})$. After receiving the Test query, $C\mathfrak{H}$ fairly flips a coin $b \in \{0,1\}$, if $b = 0$, $C\mathfrak{H}$ returns to its specific calculation in accordance with the agreement, the value of the $SK\ell\ A,B$, if b = 1, returns a random value $sk' \in \{0,1\}^k$. The $SK_{AB} = H_2(ID_A||ID_B||\omega'A||\omega'B||T_A||T_B||K_{AB1}||K_{AB2})$, where $K_{AB1} = n_A p_A(R_B + H_1(ID_B||X_B||R_B)P_{pub}) + p_A T_{B1}$, $K_{BA2} = x_B n_B T_{A2}$.

4. Game over: The attacker first computes $p_B P = R_B + H_1(ID_B||X_B||R_B)P_{pub}$, $K_{BA1} = n_B p_B(R_A + H_1(ID_A||X_A||R_A)P_{pub}) + p_B T_{A1} = n_B p_B(R_A + h_A s)P + p_B p_A n_A P = n_B p_A p_B P + p_A p_B n_A P = (n_A + n_A)p_A p_B P$, $K_{BA2} = x_B n_B T_{A2} = x_B n_B x_A n_A P = n_A n_B x_B X_A$. Then give the result of b according to the $SK\ell\ A,B\ ? = SK_{BA}$. If $SK\ell\ A,B = SK_{BA}$, attacker $\mathscr{A}$ guesses b = 0; otherwise, guess b = 1.

Analysis: Because the attacker $\mathscr{A}$ private key known n_A, n_B, x_B, p_A, and ID_A, ID_B, $\omega'A$, $\omega'B$, T_A, T_B are in the open, it is easy to calculate $p_B P$, so $SK\ell\ A,B = SK_{BA}$, therefore, the attacker $\mathscr{A}$ always correctly guesses the value of b, that is, Pr [$\mathscr{A}$ success] = 1. It can be seen that $Adv_{\mathscr{A}}\ (k) = |$ 2Pr [$\mathscr{A}$ success] - 1 $|$ = 1. Therefore, Lei et al.'s protocol doesn't have eCK security. Similarly, knowing n_A, n_B, x_A, p_B, can also break the protocol.

4 New Scheme

To overcome the security flaws in Lei et al.'s [17] scheme, a new protocol is proposed in this paper. The system establishment and user public and private key phases of the proposed scheme are basically consistent with Lei et al.'s protocol, two more hash functions H_3: $\{0, 1\}^*||\{0, 1\}^*||\{0, 1\}^*||\{0, 1\}^*||\{0, 1\}^*||\{0, 1\}^*||G||G||G|| \to \{0, 1\}^\mu$, H_4: $\{0, 1\}^*||\{0, 1\}^*||\{0, 1\}^*||\{0, 1\}^*||\{0, 1\}^*||\{0, 1\}^*||G||G||G||G|| \to \{0, 1\}^\mu$ need to be defined. Assume that vehicle A with a unique ID_A and vehicle B with a unique ID_B perform this phase, and A is the initiator, the authenticated key agreement phase of the new scheme is described as follows:

1. A randomly chooses $n_A \in Z * p$, computes $N_A = n_A P$. Then, A sends N_A, R_A to B.

2. After B receives the message sent by A, B randomly chooses $n_B \in Z * p$, computes $N_B = n_B P$. Then, B sends N_B, R_B to A.

3. A computes.

$f_1 = H_2(ID_A||ID_B||R_A||R_B||N_A||N_B)$,
$f_2 = H_3(ID_A||ID_B||R_A||R_B||N_A||N_B||X_A||X_B)$,
$K_{AB} = (f_1 n_A + f_2 x_A + p_A)(f_1 N_B + f_2 X_B + R_B + H_1(ID_B||X_B||R_B)P_{pub})$,
$SK_{AB} = H_4(ID_A||ID_B||R_A||R_B||N_A||N_B||X_A||X_B\ ||K_{AB})$.

4. B computes.

$f_1 = H_2(ID_A||ID_B||R_A||R_B||N_A||N_B)$,
$f_2 = H_3(ID_A||ID_B||R_A||R_B||N_A||N_B||X_A||X_B)$,
$KBA = (f1nB + f2xB + pB)(f1NA + f2XA + RA + H1(IDA||XA||RA)Ppub)$,
$SK_{BA} = H_4(ID_A||ID_B||R_A||R_B||N_A||N_B||X_A||X_B||K_{BA})$.

The correctness of the verification protocol is as follows: clearly, it is only necessary to verify that $K_{AB} = K_{BA}$, and that is.

$K_{AB} = (f_1 n_A + f_2 x_A + p_A)(f_1 N_B + f_2 X_B + R_B + H_1(ID_B||X_B||R_B)P_{pub})$.
$= (f_1 n_A + f_2 x_A + p_A)(f_1 n_B P + f_2 x_B P + R_B + h_B P_{pub})$.
$= (f_1 n_A + f_2 x_A + p_A)(f_1 n_B P + f_2 x_B P + (r_B + h_B s)P)$.
$= (f_1 n_A + f_2 x_A + p_A)(f_1 n_B + f_2 x_B + p_B)P$.
$= (f_1 n_B + f_2 x_B + p_B)(f_1 n_A\ P + f_2 x_A P + (r_A + h_A s)P)$.

$= (f_1 n_B + f_2 x_B + p_B)(f_1 n_A P + f_2 x_A P + R_A + h_A P_{pub}).$
$= (f_1 n_B + f_2 x_B + p_B)(f_1 N_A + f_2 X_A + R_A + H_1(ID_A \| X_A \| R_A) P_{pub}) = K_{BA},$
so $SK_{AB} = SK_{BA}$.

5 Security Proof

Theorem 1 Under the GDH assumption and with the functions H_1 and H_4 treated as random oracles, the new scheme satisfies the eCK security outlined in Sect. 2.

Proof If the two conditions shown in definition 3 are true, then the protocol satisfies eCK security. The first condition is guaranteed by the correctness shown in Sect. 3. The second condition is proved to be true by the method of contradiction, that is, suppose that an adversary $\mathscr{A}$ successfully breaks the agreement with a probability that cannot be ignored, then we can use $\mathscr{A}$ to construct a simulator $C\mathfrak{H}$ that can solve the GDH problem with a probability that cannot be ignored.

Assuming that k is a security parameter, the PPT adversary $\mathscr{A}$ that attacks the protocol wins the game with a non-negligible advantage $Adv_{\mathscr{A}}(k)$. Assume a game in which each party engages in at most $n_s(k)$ sessions, involves at most $n_p(k)$ different honest parties and performs at most n_0 H_4 queries. Since H_4 is regarded as a random oracle, after launching a Test query (the success probability is 1/2), $\mathscr{A}$ can only guess the attack (guess the correct session key directly); key copy attack (the adversary establishes a session, which does not match the target session, but the session key is the same) and forgery attack (at a certain time, the adversary calculates K_{AB} and then executes $H_4(ID_A, ID_B, R_A, R_B, N_A, N_B, X_A, X_B, K_{AB})$) to win the game (that is, the session key that can successfully distinguish the random string from the target session).

For guessing attacks, because the session key is the output of H_2, the probability of directly guessing the correct session key is $O(1/2^k)$. Obviously, the probability is negligible. For the key replication attack, its probability is $O(n_s(k)^2/2^k)$, which can be ignored.

At present, there are only forgery attacks, which are analyzed by reduction. If adversary $\mathscr{A}$ breaks the protocol through forgery attack with a probability that cannot be ignored, adversary $\mathscr{A}$ can be used to construct a simulator $C\mathfrak{H}$ that can solve the GDH problem with an advantage that cannot be ignored. Here, $C\mathfrak{H}$ and $\mathscr{A}$ execute the game described in the security model together, and $C\mathfrak{H}$ answers all the queries, let $AdvGDH$ $C\mathfrak{H}$ (k) be the advantage of $C\mathfrak{H}$ solving GDH. Given a GDH problem instance ($U = uP$, $V = vP$), where $u, v \in Z^*p$, $P \in G$, $C\mathfrak{H}$'s task is to calculate CDH $(U, V) = uvP$ with the help of DDH. When the game starts, $C\mathfrak{H}$ guesses with probability $1 / n_p(k)^2 n_s(k)$ that the test session selected by the adversary $\mathscr{A}$ is $\Pi^n_{A,B}$, where $a, b \in [1, n_p(k)]$ and $a = b$, $n \in [1, n_s(k)]$. Next, simulator $C\mathfrak{H}$ needs to guess the choice of the adversary. According to Definition 2, it is necessary to consider whether the test session $\Pi^n_{A,B}$ has a matching session or not. If the test session $\Pi^n_{A,B}$ has a matching session $\Pi^l_{B,A}$, then the adversary $\mathscr{A}$ is a passive adversary, and the adversary can only passively forward messages between the two parties, further show that the messages of $\Pi^n_{A,B}$ and $\Pi^l_{B,A}$ as well as the temporary private key are generated by simulator $C\mathfrak{H}$. A matchless session means that adversary $\mathscr{A}$ is an active adversary, that is, ID_A's message and temporary private key are generated by simulator $C\mathfrak{H}$, while ID_B's message and temporary private key are generated by the adversary. Based on the above analysis and freshness definition, simulator $C\mathfrak{H}$ must guess the case selection of the adversary from nine cases such as the following, where, the temporary private key of ID_A refers to the temporary private key of target session $\Pi^n_{A,B}$ held by ID_A, and the temporary private key of ID_B refers to the the temporary private key of matching session $\Pi^l_{B,A}$ held by ID_B.

S1 The passive adversary $\mathscr{A}$ doesn't know the secret value x_A of ID_A and the temporary private key of ID_B.

S2 The passive adversary $\mathscr{A}$ doesn't know the partial private key p_A of ID_A and the temporary private key of ID_B.

S3 The passive adversary $\mathscr{A}$ doesn't know the temporary private key of ID_A and ID_B.

S4 The active or passive adversary $\mathscr{A}$ doesn't know the secret value x_A of ID_A and the secret value x_B of ID_B.

S5 The active or passive adversary $\mathscr{A}$ doesn't know the partial private key p_A of ID_A and the secret value x_B of ID_B.

S6 The active or passive adversary $\mathscr{A}$ doesn't know the temporary private key of ID_A and the secret value x_B of ID_B.

S7 The active or passive adversary $\mathscr{A}$ doesn't know the secret value x_A of ID_A and the partial private key p_B of ID_B.

S8 The active or passive adversary $\mathscr{A}$ doesn't know the partial private key p_A of ID_A and the partial private key p_B of ID_B.

S9 The active or passive adversary $\mathscr{A}$ doesn't know the temporary private key of ID_A and the partial private key p_B of ID_B.

If an adversary $\mathscr{A}$ is able to attack the protocol through forgery attacks with a non-negligible advantage, then at least one of the cases has a non-negligible probability of occurrence.

1 Situation S1.

The game between the $\mathscr{A}$ adversary and simulator $C\mathfrak{H}$ under situation S1 is analyzed as follows.

1) *Setup Phase*: $C\mathfrak{H}$ establishes the public key of the PKG, the partial private key and secret value of all parties. $C\mathfrak{H}$ maintains a list Λ_{Setup} with entries of the form (ID_i, (d_i, R_i), (x_i, X_i)) and initially empty values.

(1) $C\mathfrak{H}$ chooses a random value $P_{pub} \in G$ as the public key of PKG and publishes the parameters param $= \{\mu, q, E/F_p, G, P, P_{pub}, H_1, H_2\ H_3, H_4\}$.

(2) For the participant ID_A, $C\mathfrak{H}$ randomly selects h_A, $r_A \in Z^*q$, calculates $R_A = p_A P - h_A P_{pub}$, lets $H_1(ID_A \| U \| R_A) = h_A, x_A = \perp$, where $U = uP = x_A P$, sets p_A as the partial private key and x_A as the secret value of ID_A. Therefore, the partial long-term public key of ID_A is R_A, and the long-term public key of secret value is U.

(3) For any participant $ID_i(i \neq A)$, $C\mathfrak{H}$ randomly selects x_i, h_i, $r_i \in Z^*q$, calculates $R_i = p_i P - h_i P_{pub}$, lets $H_1(ID_i \| X_i \| R_i) = h_i$, sets p_i as the partial private key and x_i as the secret value of ID_i. Therefore, the partial long-term public key of ID_i is R_i, and the long-term public key of secret value is $X_i = x_i P$.

(4) For any participant ID_i(i $\in [1, n_p(k)]$), $C\mathfrak{H}$ transmits (ID_i, R_i, X_i) to the adversary $\mathscr{A}$ and inserts entries (ID_i, (d_i, R_i), (x_i, X_i)) and (ID_i, R_i, X_i, h_i) in the lists Λ_{Setup} and Λ_{H1}, respectively.

2) *The first stage of the game*: $C\mathfrak{H}$ maintains four lists Λ_{H1}, Λ_{H4}, Λ_{Send} and Λ_{Reveal}, which are used to process random oracle H_1, H_4, *Send* and *RevealSessionKey* queries respectively. For the following questions, $\mathscr{A}$ can ask the number of bounds of polynomials in an unordered manner. $C\mathfrak{H}$ answers $\mathscr{A}$'s question as follows:

(1) $H_1(ID_i, X_i, R_i)$: If there is an entry matching (ID_i, R_i, X_i, h_i) in Λ_{H1}, $C\mathfrak{H}$ responds h_i to $\mathscr{A}$. Otherwise, $C\mathfrak{H}$ selects a random element $h_i \in Z^*\ q$, inserts entries (ID_i, X_i, R_i, h_i) in the list Λ_{H1}, and replies h_i to $\mathscr{A}$.

(2) *RevealSecretValue* (ID_i): If ID_i is ID_A, $C\mathfrak{H}$ aborts; otherwise, $C\mathfrak{H}$ returns the secret value x_i of the ID_i to $\mathscr{A}$.

(3) *RevealPartialPrivateKey*(ID_i): $C\mathfrak{H}$ returns the partial private key p_i of the ID_i to $\mathscr{A}$.

(4) *RevealPKGStaticKey:* $C\mathfrak{H}$ quit the game.

(5) *RevealEphemeralKey*$(\Pi^m_{i,j})$: If $\Pi^m_{i,j}$ are matching sessions $\Pi^l_{A,B}$, $C\mathfrak{H}$ quit the game; otherwise, $C\mathfrak{H}$ returns the temporary private key n_i as the response.

(6) *Send*$(\Pi^m_{i,j}, M)$: The entries in the list Λ_{Send} maintained by $C\mathfrak{H}$ are of the form $(\Pi^m_{i,j}, tran^m_{i,j}, n_i)$ and are initially empty, where $tran^m_{i,j}$ is the set of all messages transmitted and obtained by $\Pi^m_{i,j}$ up to now, and n_i is the temporary private key of session $\Pi^m_{i,j}$ owned by ID_i.

If M is the second message in $tran^m_{i,j}$, $C\mathfrak{H}$ sets the session as accepted; otherwise, if $\Pi^m_{i,j} = \Pi^l_{B,A}$, $C\mathfrak{H}$ lets $n_B = \perp$, gets R_B in the list Λ_{Setup}, response $\{R_B, N_B = V = vP\}$ to $\mathscr{A}$, and modifies the entry of $\Pi^m_{i,j}$ in Λ_{Send}; otherwise, $C\mathfrak{H}$ randomly selects $n_i \in Z^*$ q, gets R_i in the list Λ_{Setup}, response $\{R_i, n_iP\}$ to $\mathscr{A}$, and modifies the entry for $\Pi^m_{i,j}$ in Λ_{Setup}.

(7) *RevealSessionKey*$(\Pi^m_{i,j})$: The entries in the $C\mathfrak{H}$ maintained list Λ_{Reveal} are as follows $(\Pi^m_{i,j}, ID^m_{ini}, ID^m_{resp}, N^m_{ini}, N^m_{resp}, SK^m_{i,j})$ and the initial value is null, where the subscript ini represents the initiator and the subscript resp represents the responder.

If $\Pi^m_{i,j}$ has not yet accepted, $C\mathfrak{H}$ returns $\perp$; otherwise, if $\Pi^m_{i,j}$ is test session $\Pi^n_{A,B}$ or match session $\Pi^l_{B,A}$, $C\mathfrak{H}$ aborts the game; otherwise, if the session key $SK_{i,j}$ of $\Pi^m_{i,j}$ already exists, $C\mathfrak{H}$ returns $SK_{i,j}$; otherwise, obtain $\{R_i, N_i\}$ and $\{R_j, N_j\}$ from the list Λ_{Send}, execute $H_1(ID_i, X_i, R_i)$ query to obtain the result h_i, execute $H_1(ID_j, X_j, R_j)$ query to obtain the result h_j, and then take (ID_i, ID_j, N_i, N_j) (ID_i is the initiator) or (ID_j, ID_i, N_j, N_i) (ID_j is the initiator) as the index, check whether there is a match in the list Λ_{H4} to make $\text{DDH}(f_1N_i + f_2X_i + P_i, f_1N_j + f_2X_j + R_j + H_1(ID_j \| X_j \| R_j)P_{pub}, K_{i,j}) = 1$, where $P_i = R_i + H_1(ID_i \| X_i \| R_i)P_{pub}$. If it exists, obtain h_k from the list Λ_{H4} and sets $h_k = SK^m_{i,j}$; otherwise, selects the random string $SK^m_{i,j} \in \{0, 1\}^k$. Finally, $C\mathfrak{H}$ returns $SK^m_{i,j}$, and inserts an entry in the list $\Lambda_{\text{Reveal}}(\Pi^m_{i,j}, ID^m_{ini}, ID^m_{resp}, X^m_{ini}, X^m_{resp}, SK^m_{i,j})$.

(8) $H_4(ID_i, ID_j, R_i, R_j, N_i, N_j, X_i, X_j, K_{i,j})$: $C\mathfrak{H}$ maintains a list Λ_{H4} with entries of the form $(ID_i, ID_j, R_i, R_j, N_i, N_j, X_i, X_j, K_{i,j}, h_k)$.

If there is a matching entry $(ID_i, ID_j, R_i, R_j, N_i, N_j, X_i, X_j, K_{i,j})$ in the list Λ_{H4}, $C\mathfrak{H}$ returns h_k; otherwise, search in Λ_{Revea}l with $(*, ID_i, ID_j, N_i, N_j, X_i, X_j, *)$ as index. If the matching entry exists, verify whether $\text{DDH}(f_1N_i + f_2X_i + P_i, f_1N_j + f_2X_j + R_j + H_1(ID_j \| X_j \| R_j)P_{pub}, K_{i,j}) = 1$ is true, where $P_i = R_i + H_1(ID_i \| X_i \| R_i)P_{pub}$. If the equation holds, obtain the corresponding *Skm i,j* from Λ_{Reveal} and make them h_k; otherwise (no matching entries), uniformly selects the random string $h_k \in \{0, 1\}^k$. Finally, $C\mathfrak{H}$ returns h_k and updates the list Λ_{H4}.

3) The second stage of the game: $\mathscr{A}$ can only query the following query once.

Test$(\Pi_{i,j}^{m})$: If $\Pi_{i,j}^{m}$ non target session $\Pi_{A,B}^{n}$, $C\mathfrak{H}$ quit the game; otherwise, $C\mathfrak{H}$ uniformly selects random string ξ from $\{0,1\}^{k}$, and return ξ to $\mathscr{A}$.

Analysis: If $\mathscr{A}$ selects *Situation* S1, the target session $\Pi_{A,B}^{n}$ and its matching session $\Pi_{B,A}^{l}$, $C\mathfrak{H}$ will not quit the game. If $\mathscr{A}$ wins the game through forgery attack, then $H_4(ID_A, ID_B, R_A, R_B, N_A, V, U, X_B, K_{AB})$ must be queried, where $K_{AB} = (f_1 n_A + f_2 DLOG(U) + p_A)(f_1 V + f_2 X_B + R_B + H_1(ID_B \| R_B) P_{pub})$. To solve the GDH problem, $C\mathfrak{H}$ obtains entries from Λ_{H4}, then calculates $f_1 = H_2(ID_A \| ID_B \| R_A \| R_B \| N_A \| V)$, $f_2 = H_3(ID_A \| ID_B \| R_A \| R_B \| N_A \| V \|$

$U \| X_B)$, $Z_1 = (f_1 n_A + p_A)(f_2 x_B + p_B)P$, $Z_2 = f_2(f_2 x_B + p_B)uP$, $Z_3 = f_1(f_1 n_A + p_A)vP$ by using the p_A, n_A, x_B and p_B that it knows, and outputs $GDH\ (U, V) = x_A n_B P = (f_1 f_2)^{-1}(K_{AB} - Z_1 - Z_2 - Z_3)$.

The advantages of $C\mathfrak{H}$ in solving the GDH problem are:

$$\mathrm{Adv}_{\mathrm{CH}}^{\mathrm{GDH}}(\mathrm{k}) \geq \frac{\mathrm{Adv}_{\mathrm{A}}(\mathrm{k})}{4\mathrm{n}_0\mathrm{n}_{\mathrm{p}}^2(\mathrm{k})\mathrm{n}_{\mathrm{s}}^2(\mathrm{k})}$$

Therefore, if $Adv_{\mathscr{A}}(k)$ cannot be ignored, then $C\mathfrak{H}$'s advantages cannot be ignored, which contradicts the GDH assumption.

The proof for S2, S3, S4, S5, S6, S7, S8, S9 is similar to S1 and will not be described in detail here.

6 Protocol Comparison

In this section, the improved protocol is compared with other related protocols in terms of computational cost and security. Since most of these protocols are based on dot products, Hash operation, and scalar addition and subtraction operations, only dot products operations with relatively large time complexity are considered in this paper. Let TM represent the time it takes to perform a dot product operation. The security of the scheme is compared in terms of whether it meets the security of eCK. The comparison results are shown in Table 1.

Table 1. Comparison of efficiency and security of different protocols

Computation cost			
Protocol	Key extraction	Key exchange	eCK security
Wu et al. [19]	$6T$M	$14T_{\mathrm{M}}$	No
Sun et al. [20]	$4T$M	$14T_{\mathrm{M}}$	Yes
Deng et al. [21]	$6T$M	$10T_{\mathrm{M}}$	Yes
Li et al. [22]	$6T$M	$12T_{\mathrm{M}}$	Yes
Lei et al. [17]	$4T$M	$14T_{\mathrm{M}}$	No
Our protocol	$\mathbf{4T_{M}}$	$\mathbf{10T_{M}}$	**Yes**

It can be seen from Table 1 that, compared with Deng et al.'s [21] protocol, although the computational cost and security required for key exchange are the same, the computational cost in key extraction stage is higher than that of the improved protocol in this paper. Compared with the protocols of Wu et al. [19] and Lei et al. [17], the improved protocol is more efficient and secure. Compared with the protocols of Sun et al. [20] and Li et al. [22], although the security is the same, the improved protocol in this paper has the highest efficiency.

As can be seen from the above, compared with the existing certificateless authentication key protocol, the improved protocol in this paper has stronger security and higher computational efficiency, so it is more suitable for practical scenarios such as the Internet of vehicles and the Internet.

7 Conclusion

After analyzing the protocol of Lei et al. [17], it is proved that the protocol cannot meet eCK security, and the attack mode is given, and the attack can be successful with different data. Therefore, an enhancement scheme is proposed and its safety is proved by eCK model. The analysis results show that the protocol only needs 4 dot products in the key agreement phase and 10 dot products in the key agreement phase, which greatly improves the computational efficiency and is more suitable for the networking of vehicles scenario.

Acknowledgement. This research is supported by the Science and Technology Project of Henan Province(212102210107).

References

1. Horng S J, Tzeng S F, Huang P H, et al. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. Information Sciences, 2015, 317: 48-66.
2. Gayathri N B, Thumbur G, Reddy P V, et al. Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks[J]. IEEE Access, 2018, 6: 31808-31819.
3. Karati A, Islam S K H, Karuppiah M. Provably secure and lightweight certificateless signature scheme for IIoT environments[J]. IEEE Transactions on Industrial Informatics, 2018, 14(8): 3701-3711.
4. Zhang B, Zhu T, Hu C, et al. Cryptanalysis of a lightweight certificateless signature scheme for IIOT environments[J]. IEEE Access, 2018, 6: 73885-73894.
5. Tao F, Shi T, Li S. Provably secure cross-domain authentication key agreement protocol based on heterogeneous signcryption scheme[C]//2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC). IEEE, 2020, 1: 2261-2266.
6. Liu X, Ma W. CDAKA: A provably-secure heterogeneous cross-domain authenticated key agreement protocol with symptoms-matching in TMIS[J]. Journal of medical systems, 2018, 42: 1-15.

7. Zhou Y, Long X, Chen L, et al. Conditional privacy-preserving authentication and key agreement scheme for roaming services in VANETs[J]. Journal of Information Security and Applications, 2019, 47: 295-301.
8. Luo M, Wu J, Li X. Cross-domain certificateless authenticated group key agreement protocol for 5G network slicings[J]. Telecommunication Systems, 2020, 74: 437-449.
9. Gong P, Li P. Further improvement of a certificateless signature scheme without pairing[J]. International Journal of Communication Systems, 2014, 27(10): 2083-2091.
10. Yeh K H, Su C, Choo K K R, et al. A novel certificateless signature scheme for smart objects in the Internet-of-Things[J]. Sensors, 2017, 17(5): 1001.
11. Azees M, Vijayakumar P, Deboarh L J. EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(9): 2467-2476.
12. Dang L, Xu J, Cao X, et al. Efficient identity-based authenticated key agreement protocol with provable security for vehicular ad hoc networks[J]. International Journal of Distributed Sensor Networks, 2018, 14(4): 1550147718772545.
13. Ma M, He D, Wang H, et al. An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks[J]. IEEE Internet of Things Journal, 2019, 6(5): 8065-8075.
14. Wu L, Sun Q, Wang X, et al. An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network[J]. IEEE Access, 2019, 7: 55050-55063.
15. Chen C M, Fang W, Wang K H, et al. Comments on "an improved secure and efficient password and chaos-based two-party key agreement protocol"[J]. Nonlinear Dynamics, 2017, 87: 2073-2075.
16. Islam S K H, Biswas G P. A pairing-free identity-based two-party authenticated key agreement protocol for secure and efficient communication[J]. Journal of King Saud University-Computer and Information Sciences, 2017, 29(1): 63-73.
17. Meng L, Xu H, Xiong H, et al. An efficient certificateless authenticated key exchange protocol resistant to ephemeral key leakage attack for V2V communication in IoV[J]. IEEE Transactions on Vehicular Technology, 2021, 70(11): 11736-11747.
18. Sun H, Wen Q, Zhang H, et al. A novel pairing-free certificateless authenticated key agreement protocol with provable security[J]. Frontiers of Computer Science, 2013, 7(4): 544-557.
19. Wu T, Jing X. Two-party certificateless authenticated key agreement protocol with enhanced security[J]. Journal of China University Posts and Telecommunications, 2019, 26(1): 12.
20. Sun H, Wen Q, Zhang H, et al. A strongly secure identity-based authenticated key agreement protocol without pairings under the GDH assumption[J]. Security and Communication Networks, 2015, 8(17): 3167-3179.
21. Deng L, Gao R. Certificateless two-party authenticated key agreement scheme for smart grid[J]. Information Sciences, 2021, 543: 143-156.
22. Li Q, Hsu C F, Raymond Choo K K, et al. A provably secure and lightweight identity-based two-party authenticated key agreement protocol for vehicular ad hoc networks[J]. Security and Communication Networks, 2019, 2019: 1-13.