



## OPEN ACCESS

## EDITED BY

Francisco Wellington Lima,  
Federal University of Piauí, Brazil

## REVIEWED BY

Devishree Naidu,  
Shri Ramdeobaba College of Engineering and  
Management, India  
Tommaso Bianchi,  
University of Padua, Italy

## \*CORRESPONDENCE

Yan Wang,  
✉ Wangyan1016@mails.ccnu.edu.cn

RECEIVED 07 March 2025

ACCEPTED 31 July 2025

PUBLISHED 26 August 2025

## CITATION

Sun Z and Wang Y (2025) An anonymous  
authentication protocol for vehicle to grid  
based on elliptic curve cryptography.  
*Front. Phys.* 13:1589195.  
doi: 10.3389/fphy.2025.1589195

## COPYRIGHT

© 2025 Sun and Wang. This is an open-access  
article distributed under the terms of the  
[Creative Commons Attribution License \(CC  
BY\)](#). The use, distribution or reproduction in  
other forums is permitted, provided the  
original author(s) and the copyright owner(s)  
are credited and that the original publication  
in this journal is cited, in accordance with  
accepted academic practice. No use,  
distribution or reproduction is permitted  
which does not comply with these terms.

# An anonymous authentication protocol for vehicle to grid based on elliptic curve cryptography

Zeyu Sun<sup>1</sup> and Yan Wang<sup>2\*</sup>

<sup>1</sup>Department of Information Engineering, Ningxia Communications Technical College, Yinchuan, China, <sup>2</sup>School of Computer, Central China Normal University, Wuhan, China

As an important component of the smart grid, Vehicle-to-Grid (V2G) can achieve bidirectional exchange of data and power flow between electric vehicles and smart grid, and is an effective promoter for grid storage and decarbonization. However, when electric vehicles are connected to the grid, the V2G network involves a large amount of privacy data exchange and sensitive charging and discharging transactions. Once these data are leaked, the privacy and security of users will be threatened. The existing authentication protocols in V2G network lack sufficient protection for vehicle user identity privacy and cannot provide user identity anonymity. Therefore, this article proposes an anonymous and privacy-preserving authentication protocol tailored for V2G environments, aiming to protect user identity privacy. The protocol integrates Elliptic Curve Cryptography (ECC) and Physical Unclonable Function (PUF) to achieve mutual authentication between EVs and the grid. It ensures the anonymity of participants through the use of temporary identity values and secures the session key. The security and efficiency of the protocol are verified through Scyther simulation and heuristic analysis. Compared with other protocols, the protocol proposed in this article not only meets the security requirements in smart grid environment, but also reduces costs, demonstrating significant security and overhead advantages. This work contributes to building a more trustworthy, scalable and privacy-conscious V2G network, thereby supporting sustainable energy development and smart grid security.

## KEYWORDS

vehicle to grid, elliptic curve cryptography, anonymous, security, Scyther

## 1 Introduction

As human society continues to advance rapidly, the significance of energy and environmental challenges has grown increasingly pronounced. To address these issues, the smart grid has emerged as a focal point of global research. This new generation of power grid aims to establish an energy system that is green, low-carbon, safe, and reliable, thereby mitigating the impact of energy consumption on the environment [1–3]. Unlike traditional power grids, smart grid has advantages such as safety, flexibility and cleanliness. They can achieve bidirectional communication of power flow and information flow between the grid and users, improve the traditional one-way power service mode, and provide people with better quality services. At the same time, smart grid has fully implemented an intelligent and lean power grid operation and maintenance mode. This greatly enhances the ability of the power grid to respond to sudden events and emergency

failures and optimizes resource allocation capabilities. In addition, the combination of smart grid and emerging energy storage technologies enables the grid connected operation of renewable energy, making renewable energy a more suitable energy supply mode for human social development [4–7]. However, the integration of renewable energy into power generation can introduce instability and volatility, potentially affecting grid reliability [8]. To mitigate these fluctuations, auxiliary systems are necessary. Electric vehicle (EV), serving as capable energy storage units, offer a solution to stabilize the incorporation of clean energy into the grid. To facilitate mutual benefits between EV and the grid, energy exchange and communication must occur through a dedicated network. Consequently, the concept of the Vehicle-to-Grid (V2G) network has been proposed [9–11].

V2G integrates EV as mobile energy storage devices with smart grid to achieve a more sustainable, efficient and safe energy system. The significance of V2G technology lies in its ability to achieve bidirectional flow and management of energy. On the one hand, when the load on the power grid is low, the grid can use the excess electricity to charge the batteries of electric vehicles, avoiding resource waste. On the other hand, when the load on the power grid is high, electric vehicles transfer the energy stored in the battery to the grid, helping to alleviate the load pressure on the grid and improve its flexibility and stability [12]. Meanwhile, users can use electric vehicles as reliable energy storage devices through V2G technology to generate revenue. This new source of income can encourage more people to purchase electric vehicles, thereby promoting the popularization of EV. Therefore, V2G presents enormous practical efficiency and has broad application prospects.

V2G plays a crucial role in the development of smart grid by facilitating data and power exchange. However, bidirectional communication and power flow in V2G environments involve a large amount of private data, which is vulnerable to malicious attacks and can cause property damage [13]. And due to the high-speed mobility of EV, privacy breaches in V2G are more severe than in other parts of smart grid. Overall, the following security threats still exist in V2G environments [14]. Firstly, unauthorized adversaries may attempt to disguise themselves as the vehicle owner in order to gain access to the vehicle and engage in charging/discharging activities without the owner's knowledge, resulting in wastage of resources. Secondly, the V2G environment involves the exchange of user personal information and vehicle data, such as energy transmission, driving routes, charging/discharging habits, etc. When adversaries steal this information, they will make guesses about users' consumption levels, company locations, home addresses, lifestyle habits, and other private information, posing a great threat to users. In addition, in V2G environments, users frequently perform charging/discharging transactions, so it is necessary to ensure the data integrity. Finally, due to the V2G environment being exposed to public environments, the entire communication process will also be subjected to more and more complex attacks, such as replay attacks, physical attacks, etc. Identity authentication is a security mechanism used to confirm the legitimacy and authenticity of an entity's identity [15–17]. In the V2G environment, the importance of identity authentication

is particularly prominent. Through identity authentication, unauthorized access and tampering can be prevented, ensuring the security of information and systems. Existing V2G authentication protocols continue to suffer from notable limitations, particularly in terms of privacy and security. Many lack robust mechanisms to ensure user identity anonymity, leaving vehicles vulnerable to tracking through identifiable information or communication behavior. Additionally, inadequate privacy protection measures expose users to the risk of having their locations and movement patterns analyzed by adversaries. Moreover, these protocols often fail to provide comprehensive defenses against a range of security threats, such as replay attacks, man-in-the-middle attacks, and identity forgery, reflecting an incomplete set of security guarantees. To address these issues, this paper proposes a lightweight anonymous authentication protocol that combines Elliptic Curve Cryptography (ECC) and Physically Unclonable Functions (PUFs). The proposed scheme not only enables mutual authentication and session key agreement between electric vehicles and charging stations, but also significantly enhances both security properties and performance. By leveraging PUF technology, storage and computational costs are reduced, and the use of ECC decreases key length and computational complexity, thereby greatly minimizing communication and computational overhead—making the scheme suitable for resource-constrained V2G devices. The main contributions of this article are as follows:

- (1) Based on elliptic curve cryptography and physically unclonable function technology, this paper designs an anonymous authentication protocol. This protocol enables electric vehicles and charging stations to verify their identities and successfully establish session keys for future communication. The protocol ensures the security of session keys by combining temporary secret values with long-term secret values. In order to protect the anonymity of participants, entities send temporary identity values for transmission to prevent attackers from locating them.
- (2) This article uses two security analysis methods to analyze the design protocol. By using Scyther tool to simulate the protocol process, it has been proven that the protocol can achieve bidirectional authentication and ensure the security of session keys. The heuristic analysis results indicate that the protocol can have good forward security and anonymity, and is not easily susceptible to replay attacks, etc.
- (3) Compared with other protocols, the security comparison results show that the protocol can meet all security requirements in smart grid environments, while other protocols have security vulnerabilities. The performance analysis results indicate that the protocol reduces costs while achieving the same level of security. From this, it can be concluded that the protocol has advantages in terms of security and overhead.

The organization of this paper is as follows: In [Section 2](#), we review pertinent literature. [Section 3](#) presents the models. [Section 4](#) provides detailed information on the design. [Section 5](#) conducts a security analysis. [Section 6](#) reports the performance and [Section 7](#) concludes the paper.

## 2 Related work

V2G refers to the technology of bidirectional interaction, allowing electric vehicles to not only serve as terminal devices for consuming electrical energy, but also as energy storage and injection devices, providing support for the power grid. However, V2G security and privacy issues have also attracted widespread attention from scholars [13,14]. In order to ensure the reliability and security of V2G, effective security and privacy protection measures need to be taken. In the communication process, authentication protocols are a key component to ensure secure communication.

[18] used an anonymous mechanism to protect the privacy. In this protocol, the central aggregator issues licenses to vehicles using partially blind signatures, establishes communication sessions with the local aggregator using licenses and pseudo-random identities, and regularly sends status reports. The privacy of electric vehicles is guaranteed, but if any car cheats, the central aggregator will disclose its true identity. [19] designed an efficient Privacy Aware Authentication (PAA) scheme and demonstrated its ability to resist various attacks. [20] pointed out that [19] cannot resist forgery attacks from service providers. They proposed a novel PAA scheme based on [19], which uses identity-based signature technology to resist server forgery attacks and protect user identity privacy. [21] designed a lightweight V2G scheme that is secure and protects user privacy. Meanwhile, the protocol generates static pseudonyms through private credentials for electric vehicles, suitable for vehicles with limited resources. However, as the protocol does not provide a password update phase, it cannot achieve perfect forward security and resist asynchronous attacks. [22] proposed a privacy protected blockchain power auction scheme. This protocol uses smart contracts to automatically auction protocols to facilitate transactions, utilizes group signatures to protect the privacy of electric vehicles and charging stations, and trusted institutions can query real identity information in emergency situations. However, due to the use of bilinear pairing to construct random signatures, it imposes an additional computational burden on vehicles. [23] proposed a lightweight authentication framework for V2G (Vehicle-to-Grid) networks. The framework uses PUF responses to establish authentication among electric vehicles, charging stations, and the grid server. However, electric vehicles and charging stations share their real identities over insecure channels, making it impossible for them to remain anonymous within the network. [24] proposed another authentication and key generation protocol for V2G networks using Elliptic Curve Cryptography (ECC), XoR operations, and one-way hash functions. However, the scheme fails to ensure the security of the session key and does not provide user anonymity for electric vehicles and charging stations. [25] designed a lightweight authentication. [26] designed a secure communication protocol. This protocol considers the traceability of EV, but does not take into account forward security. [27] pointed out that the security issues need to be considered when EV play different roles, and proposed an authentication scheme to achieve secure communication. However, this scheme ignores issues such as tracking, revoking, and forward security for malicious EV. [25] introduced a privacy-preserving authentication protocol for V2G networks that employs elliptic curve cryptography and one-way hash functions to achieve mutual authentication among participants. Despite its strengths, the scheme

lacks non-traceability and is vulnerable to user impersonation attacks. [13] presented a session key generation and authentication mechanism for a cloud-based V2G environment, utilizing ECC, one-way hashing, and XoR operations. However, their approach falls short in securing the session key when faced with ephemeral secret leakage attacks. [28] proposed an authentication mechanism b, which also requires assigning pseudonyms to EV. [29] proposed a protocol for V2G. Although this scheme can resist various security attacks, EV in this scheme also requires TA to generate pseudonyms for it. [30] designed a new license generation scheme. But the security assumption for LAG is too high. [23] proposed a secure user key exchange identity authentication protocol from the perspective of physical security. During the authentication process, there is no need to store any secret information in the EV and aggregator, but the security assumption for physical devices in the scheme is too high. [31] designed a key negotiation scheme based on elliptic curve cryptography technology. The scheme realizes secure communication between multiple layers of architecture in the smart grid environment. However, this scheme lacks a comprehensive security model and formal security analysis. [27] considered that electric vehicles may interact with the grid as different roles in V2G environments, and designed a scheme based on this requirement. [32] proposed a privacy protection protocol for V2G, which achieves mutual authentication without exposing the user's true identity, and achieves self-synchronization by updating pseudonyms in the session. [33] pointed out that [32] cannot resist simulated attacks and offline password guessing attacks, and cannot achieve session key security. [34] proposed a privacy protection authentication scheme for V2G communication based on Energy Internet (EI). A new communication model based on EI enables electric vehicles to seamlessly charge or discharge batteries at different charging stations. [35] pointed out that [34] may suffer from desynchronization attacks during the user login phase, and adversaries can select legitimate information on open channels to conduct replay attacks on vehicles. Therefore, they combined fuzzy extractor technology to propose a lightweight security model based on EI communication architecture, allowing vehicles to communicate or charge/discharge at desired service stations and resist various attacks. [36] introduced fog servers to achieve parallel management based on V2G network environment. However, the entire protocol incurs significant computational overhead. Some representative works are shown in Table 1.

## 3 Preliminaries

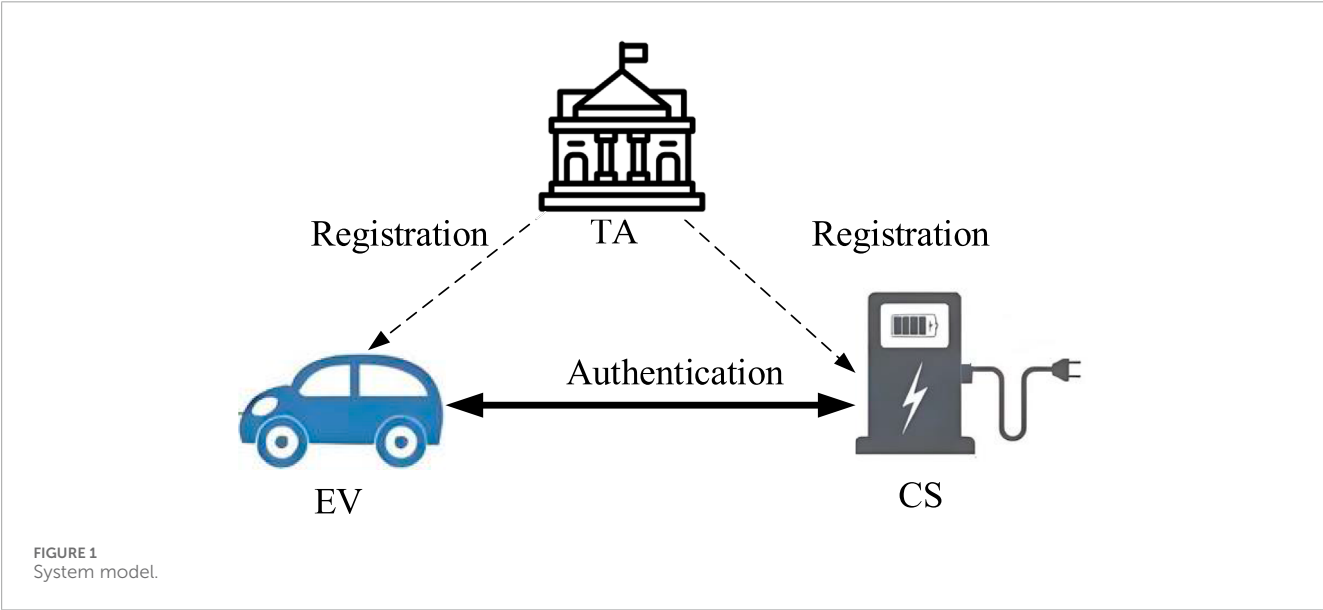
### 3.1 System model

This protocol mainly considers the privacy, security, and anonymity issues of the interaction layer between vehicles and smart grids in V2G networks [13,20–32]. As shown in Figure 1, the system model mainly consists of three components, namely, trusted authority (TA), electric vehicle (EV) and charging station (CS). The specific descriptions of each part are as follows:

- (1) Trusted Authority (TA): TA plays a crucial role as a trusted third-party organization, typically analogous to official entities such as power regulatory agencies. Its core responsibilities

TABLE 1 Comparison of representative V2G authentication protocols.

Reference	Method/Technology	Advantages	Limitations
[18]	Partially blind signatures	Privacy protection, identity traceability	Risk of identity exposure
[21]	Lightweight authentication	Suitable for resource-limited vehicles	No forward security; vulnerable to asynchronous attacks
[22]	Blockchain, group signatures	Automated transactions, privacy protection	High computational overhead
[27]	Role-based authentication	Role-specific security consideration	Ignores tracking, revocation, and forward security
[31]	Elliptic curve cryptography	Secure communication in multi-layered architecture	No formal security analysis



- include the comprehensive initialization of the V2G network system, ensuring the legal registration of all participating entities, and being responsible for publishing and maintaining the security parameter system of the entire system. This step is crucial for building a safe and reliable V2G interaction environment.
- (2) Electric Vehicle (EV): Each EV is equipped with a Tamper Resistant Device (TRD) specifically designed to securely store sensitive information and secret keys of the vehicle. During the initialization phase of V2G, EV must register through TA, which verifies their identity information and hardware integrity. EV that has not been registered with TA will be denied access by the system and will not be able to enjoy the various services provided by the V2G, effectively preventing unauthorized access and potential security risks.
  - (3) Charging Station (CS): As a key component of the smart grid, CS not only undertakes the task of providing electrical energy supply to EVs, but also is responsible for efficient and safe two-way exchange of information and electrical energy with EV. To ensure the legality and security of interactions between entities, CS also needs to complete the registration process with TA during the initialization phase.

3.2 Threat model

The threat model is used to identify potential threats in proposed protocols in order to reduce the security risks of the protocol [13,25–36]. The protocol in this article will be able to achieve the claimed security under the Dolev Yao model. In this model, the capabilities possessed by attackers are defined as follows:

- (1) Attackers can eavesdrop on messages in V2G public channels;
- (2) Attackers are able to maintain existing states, record communication information, and store commonly used values in communication message processes.
- (3) Attackers can forge and send tampered messages after hijacking them;
- (4) Attackers can impersonate legitimate users to participate in the operation of the protocol.

3.3 Security requirement

In this article, a secure and efficient authentication key protocol is designed [13,20–36,41]. This protocol can meet the following design objectives:



- (1) Privacy protection: In V2G environment, CS and EV will achieve mutual authentication and exchange important information. However, users' privacy information may be obtained by adversaries, who will analyze this sensitive data and infer users' lifestyle habits and social activities. Therefore, the design of the protocol needs to implement privacy protection and ensure the anonymity of users during the authentication process.
- (2) Session key security: Session keys are mainly used for encrypting and decrypting communication content, so it is necessary to ensure the security of session keys. In V2G environment, after completing authentication, the vehicle will share a session key with the aggregator for subsequent transmission of confidential data. If this key is stolen by an adversary, the entire communication process will no longer be secure. Therefore, the designed protocol needs to ensure the security of session keys.
- (3) Resist impersonation attacks: Adversaries may disguise themselves as EVs or CSs and illegally access authorized data and privacy information. This may lead to the leakage of user identity privacy and data privacy. Therefore, the protocol needs to be able to resist impersonation attacks.
- (4) Resist physical attacks: EVs are usually parked in easily accessible areas for adversaries and left unattended. This means that adversaries can easily capture devices on vehicles and launch various attacks on the keys stored in the device's memory to steal sensitive data. Therefore, it is very important for the protocol to ensure that V2G entities are protected from physical attacks.
- (5) Resist replay attacks: In this type of attack, the adversary will impersonate a legitimate entity by sending information from the previous session or a message from the current session. The entities in the entire communication session should be able to detect the freshness of messages and reject stale messages.

### 3.4 Elliptical curve cryptography

Elliptical Curve Cryptography (ECC) is a public key cryptography system constructed based on the characteristics of elliptic curves over finite fields [37].

For the additive cyclic subgroup  $G$  of elliptic curves with order  $q$ , we have:

1. Given  $P, Q \in G$ ,  $Q = nP$ , Solving  $n$  is difficult in polynomial time, also known as the Elliptic Curve Discrete Logarithm Problem (ECDLP).
2. Given  $P, Q, R \in G$ ,  $Q = nP$ ,  $R = mP$ , solving  $n, m$  is difficult in polynomial time, also known as the Elliptic Curve Computational Diffie Hellman Problem (ECCDHP).

### 3.5 Physical unclonable function

Physical unclonable function (PUF) is a random function that extracts the unique randomness of each integrated circuit from the changes in its physical and electrical characteristics, mapping

TABLE 2 Notations.

Notations	Definitions
$TA$	Trusted authority
$EV$	Electric vehicle
$CS$	Charging Station
$ID$	Identity
$F$	Finite field
$H$	Hash function
$PID$	Pseudonym identity
$s$	Master key
$SK$	Session key
$PUF$	Physical unclonable function
$T$	Timestamp

the basic properties of hardware entities into a stream of bit information [38]. This mode is called challenge response pair (CRP). The PUF with challenge  $C$  as input and response  $R$  as output can be represented as:  $R = PUF(C)$ . A secure PUF needs to meet the following properties: 1) No two challenges can produce the same response; 2) PUF should satisfy uniqueness, that is, it is not allowed for two PUF devices to be the same, because in the manufacturing process of PUF devices, some processing is required to maintain the uniqueness of PUF; 3) PUF should also meet unpredictability; 4) PUF should also meet reliability characteristics.

Due to the above characteristics of PUFs, even if attackers can capture nodes equipped with PUF and detect the internal circuit structure of non-volatile memory (NVM) in the chip, attempting to modify the internal organization to obtain key secret data stored therein, these operations will affect the internal structure of PUF and their response to challenges, rendering them useless. Therefore, using PUF can ensure the security of keys without occupying storage space, reduce the computational overhead of encryption algorithms, and alleviate hardware costs. This makes PUF more suitable for resource constrained IoT environments.

## 4 Protocol

Table 2 shows the definitions of notation.

### 4.1 Generation of system parameters

In the V2G network system, trusted authority  $TA$  is responsible for the establishment and initialization of the entire system, as well as selecting safety parameters for the system.

Step 1: Let  $E$  be an elliptic curve defined on the finite field  $F$ , and TA select a group  $G$  of order  $q$  with a large prime number on  $E$ .

Step 2: TA randomly selects  $s \in \mathbb{Z}_q^*$  as the master key of the system and calculates  $P_{pub} = sP$ , where  $P$  is a generator in group  $G$ .

Step 3: TA selects a secure hash function  $H$ . In addition,  $EV$  and  $CS$  are equipped with their own physically unclonable functions  $PUF_i$  and  $PUF_j$ . Therefore, the security parameters of the system are  $parm = \{q, G, P, P_{pub}, H\}$ .

## 4.2 Registration

### 4.2.1 $CS_j$ registration

$CS_j$  sends the identity value  $ID_j$  to TA through a secure channel. TA randomly selects  $c_j$  and calculates  $e_j = H(ID_j, c_j, s)$ ,  $E_i = e_j \cdot P$ . Then TA sends  $\{e_j, E_i\}$  to  $CS_j$ . After receiving the information,  $CS_j$  stores  $\{e_j, E_i\}$  and exposes the  $E_i$ .

### 4.2.2 $EV_i$ registration

R1:  $EV_i$  sends the identity information  $\{ID_i\}$  to TA for registration. TA generates a challenge  $C_i$ , a secret parameter  $k_i$ , and a pseudo-random identity  $PID_i = H(ID_i, k_i, s)$ . Then TA sends  $\{C_i, PID_i, k_i\}$  to  $EV_i$  and sends  $\{PID_i, k_i\}$  to  $CS_j$  through a secure channel.

R2:  $TA \Rightarrow EV_i: \{C_i, PID_i, k_i\}$

R3:  $EV_i$  inputs  $C_i$  into the PUF to get the response  $K_i = PUF_i(C_i)$ . Then  $EV_i$  calculates  $ED_i = H(ID_i, C_i, K_i) \oplus k_i$ ,  $EA_i = H(PID_i, k_i, ED_i) \bmod n$ . Finally,  $EV_i$  stores  $\{C_i, PID_i, ED_i, EA_i\}$  in the memory.

R4:  $TA \Rightarrow CS_j: \{PID_i, k_i\}$

R5:  $CS_j$  calculates  $K_j = PUF_j(e_j)$ ,  $DA_i = H(ID_j, PID_i, e_j, K_j) \oplus k_i$ . Finally,  $CS_j$  stores  $\{PID_i, DA_i\}$  in the database.

## 4.3 Authentication phase

The specific process is shown in Figure 2.

The specific steps are as follows:

A1.  $EV_i$  extracts the challenge  $C_i$  from memory and obtains the response  $K_i = PUF_i(C_i)$ .  $EV_i$  calculates  $k_i = H(ID_i, C_i, K_i) \oplus ED_i$ ,  $EA_i^* = H(PID_i, k_i, ED_i) \bmod n$ , and compares  $EA_i^*$  with  $EA_i$ . If they are equal, it means that the stored data has not been tampered with and continues with the subsequent calculations; Otherwise, the protocol terminates the session.  $EV_i$  randomly selects  $r_i$  and the current timestamp  $T_i$ , then calculates  $EB_i = H(K_i, r_i)P$ ,  $ES_i = H(K_i, r_i)E_i$ ,  $ECV_i = H(PID_i, ES_i, k_i, T_i)$ .

A2.  $EV_i \rightarrow CS_j: M_1 = (PID_i, EB_i, ECV_i, T_i)$

A3.  $CS_j$  checks whether the  $T_i$  is fresh and whether  $PID_i$  can be found in the database. If it cannot be found, the protocol terminates the session. Otherwise,  $CS_j$  continues and calculates  $K_j = PUF_j(e_j)$ ,  $k_i = H(ID_j, PID_i, e_j, K_j) \oplus DA_i$ ,  $ES_i' = e_j EB_i$ ,  $ECV_i' = H(PID_i, ES_i', k_i, T_i)$ .

A4. If  $ECV_i'$  and  $ECV_i$  are not equal, the protocol terminates the session; Otherwise,  $CS_j$  randomly selects  $n_i$ , a new pseudo-random identity  $PID_i^{new} = H(PID_i, n_i)$ , and  $T_j$ . Then, to calculate the session key,  $CS_j$  calculates  $N_j = PUF_j(n_i)$ ,  $NP_j = N_j EB_i$ ,  $DC_j = H(NP_j, k_i, T_j) \oplus PID_i^{new}$ ,  $SK_j = H(NP_j, k_i, ES_i', PID_i, ID_j)$ ,  $DA_i^{new} = H(PID_i^{new}, e_j, K_j) \oplus$

$k_i$ ,  $VM_j = H(SK_j, DC_j, PID_i^{new}, T_j)$ . Finally,  $CS_j$  completed mutual authentication with  $EV_i$  and saved it in the established session key  $SK$ . Finally,  $CS_j$  replaces  $\{PID_i, DA_i\}$  in the database with  $\{PID_i^{new}, DA_i^{new}\}$ .

A5.  $CS_j \rightarrow EV_i: M_2 = (N_j, DC_j, VM_j, T_j)$

A6.  $EV_i$  determines whether  $T_j$  is fresh. If it is fresh, it then calculates  $NP_j' = H(K_i, r_i)N_j$ ,  $PID_i^{new} = H(NP_j', k_i, T_j) \oplus DC_j$ ,  $SK_i = H(NP_j', k_i, ES_i, PID_i, ID_j)$ ,  $VM_j^* = H(SK_i, DC_j, PID_i^{new}, T_j)$ .

A7. If  $VM_j^*$  and  $VM_j$  are not equal, the protocol terminates the session. Otherwise,  $EV_i$  continues to calculate  $A_i^{new} = H(PID_i^{new}, k_i, ED_i) \bmod n$ . Finally,  $EV_i$  completes mutual authentication with  $CS_j$  and saves it in the established session key  $SK_i$ .  $EV_i$  replaces  $\{PID_i, A_i\}$  in the database with  $\{PID_i^{new}, A_i^{new}\}$ .

## 5 Security analysis of the protocol

### 5.1 Simulation security analysis based on Scyther

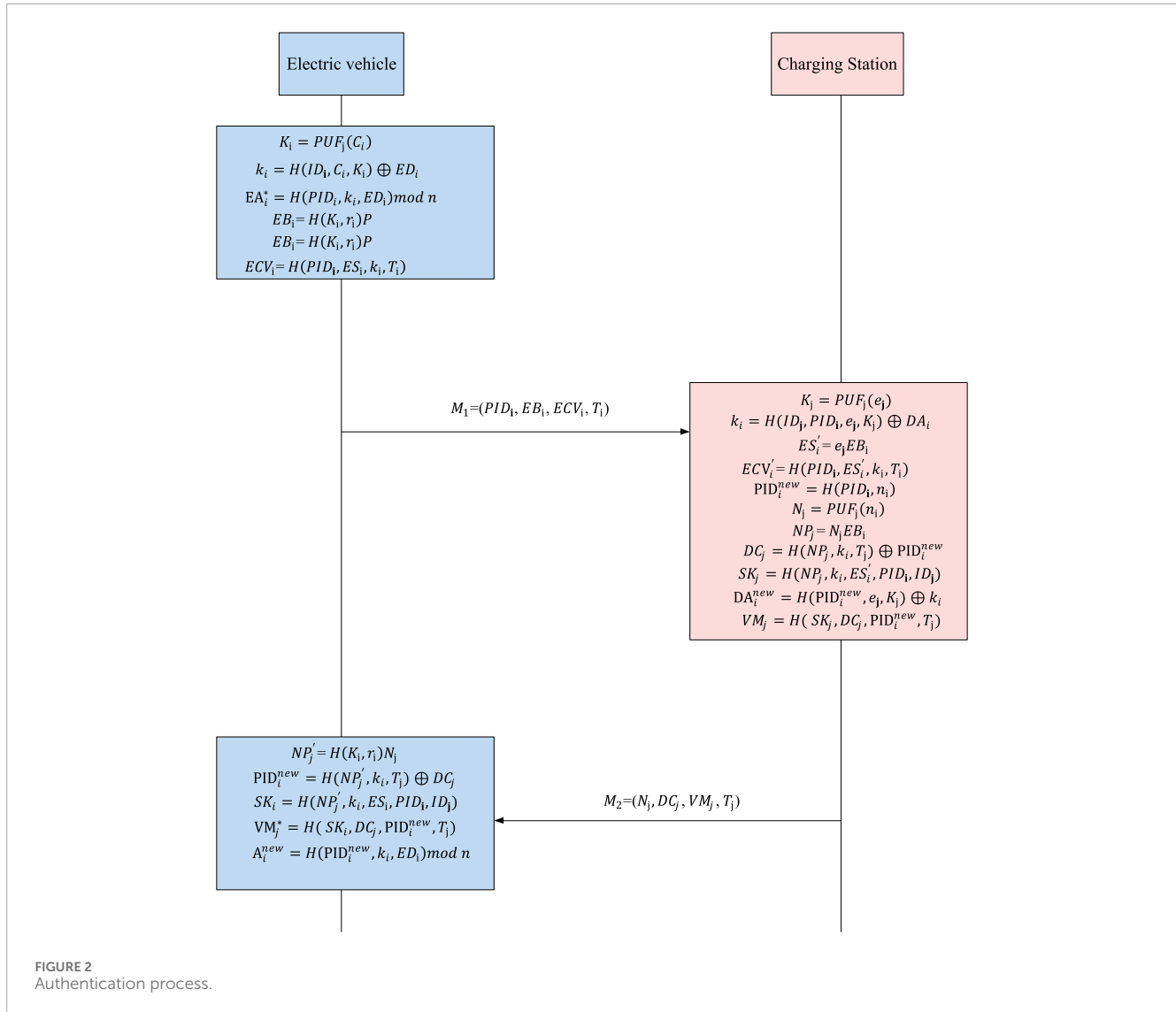
Scyther is a tool for formal analysis of protocol security, widely used to verify the security of protocols [38]. Scyther uses Secure Protocol Description Language (SPDL) for protocol description. SPDL simulates the message transmission process based on the participating roles, verifying the security of messages in the protocol from a formal security perspective, and whether they can resist security issues such as message tampering and forgery, replay attacks, and desynchronization attacks. If there is an attack, Scyther can present a graphical interface related to the attack for users to analyze. In Scyther, in addition to the Dolev Yao model, various types of adversarial models are also provided to verify the protocol's resistance to newly introduced attacks.

This article uses Scyther security tool to simulate and analyze this protocol. In the proposed protocol, there are two roles:  $EV$  and  $CS$ . This article uses SPDL to model the proposed protocol roles and conducts security analysis of the protocol through security declarations. The Secret declaration can test the confidentiality of keys or other secret parameters. To describe different levels of security attributes, this article also uses the following statements: Alive and Weakage statements can test the protocol's ability to resist man in the middle attacks. Niagree declares that it can control modules to confirm that they have received instructions from the controller, while Nisynch declares that it can synchronize operations between multiple modules in an attack.

The running results of Scyther security tool simulation analysis are shown in Figure 3. According to the analysis results, this protocol can meet the security requirements mentioned. The session key of this agreement is secure and cannot be cracked temporarily within a limited state space. Overall, the protocol proposed in this article is provably secure.

### 5.2 Security analysis using ROM

In this section, the tool employed for protocol security verification is the random oracle model. The security model, query model, and detailed security proofs used in the security analysis are described as follows.



**Security Model:** In this protocol, the primary participants are denoted as  $EV_i$  and  $CS_j$ . Under this security model, an adversary  $\mathcal{A}$  is permitted to eavesdrop, intercept, or even modify all messages transmitted over the public channel within probabilistic polynomial time. We use  $U_i^j$  to denote an instance.

**Query Model:** The adversary  $\mathcal{A}$ 's capabilities are modeled by the following five query types:

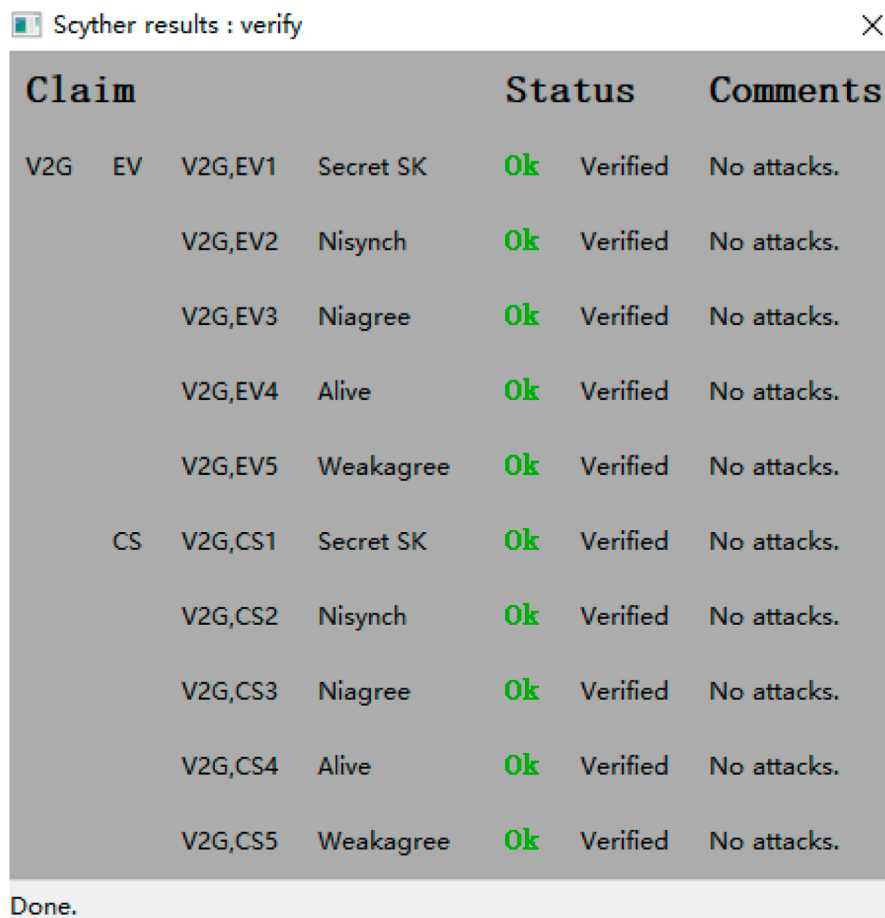
- **Execute ( $EV_i^j, CS_j^k$ ):** This query simulates passive attacks by the adversary  $\mathcal{A}$ , who captures all messages transmitted between parties on the public channel.
- **Send ( $U_i^j, m$ ):** This query simulates active attacks by adversary  $\mathcal{A}$ . Specifically,  $\mathcal{A}$  can intercept messages on the public channel, modify them, and then send the altered messages to instance  $U_i^j$ . After  $U_i^j$  receives the modified message, adversary  $\mathcal{A}$  can also intercept any response message generated by participant  $U_i^j$ .
- **Reveal ( $U_i^j$ ):** This query simulates the scenario in which instance  $U_i^j$  has generated the session key (SK). Through this query, adversary  $\mathcal{A}$  can obtain the session key SK if it has been

established. If SK has not yet been generated by instance  $U_i^j$ , adversary  $\mathcal{A}$  can only obtain an invalid identifier.

- **Corrupt ( $U_i^j$ ):** This query simulates the scenario in which a participant is compromised. Adversary  $\mathcal{A}$  can obtain secret credentials of the participant through this query. Specifically, in this protocol, adversary  $\mathcal{A}$  can obtain the information stored by  $EV_i$ .
- **Test ( $U_i^j$ ):** This query is employed to verify the security of the session key SK held by instance  $U_i^j$ . After this query, the simulator executes a "coin toss". If the result is 1, the real SK is returned to adversary  $\mathcal{A}$ ; if the result is 0, a random string is returned with the same length as the real session key. Therefore, adversary  $\mathcal{A}$  must distinguish whether the returned value is the real SK or a random string.

**Theorem 1:** The advantage of adversary  $\mathcal{A}$  breaking the semantic security of scheme  $P$  is bounded by:

$$Adv(\mathcal{A}) \leq \frac{q_h^2}{2^l} + \frac{(q_s + q_e)^2}{p} + \frac{2q_p^2}{|PUF|} + 2Adv_P^{ECDHHP}(\mathcal{A})$$



Scyther results : verify						
Claim				Status	Comments	
V2G	EV	V2G, EV1	Secret SK	Ok	Verified	No attacks.
		V2G, EV2	Nisynch	Ok	Verified	No attacks.
		V2G, EV3	Niagree	Ok	Verified	No attacks.
		V2G, EV4	Alive	Ok	Verified	No attacks.
		V2G, EV5	Weakagree	Ok	Verified	No attacks.
	CS	V2G, CS1	Secret SK	Ok	Verified	No attacks.
		V2G, CS2	Nisynch	Ok	Verified	No attacks.
		V2G, CS3	Niagree	Ok	Verified	No attacks.
		V2G, CS4	Alive	Ok	Verified	No attacks.
		V2G, CS5	Weakagree	Ok	Verified	No attacks.

Done.

FIGURE 3  
Scyther results.

Where  $q_h$ ,  $q_p$ , and  $q_s$  represent the numbers of Hash, PUF, and Send queries, respectively. Parameters  $l$  and  $|PUF|$  represent the output space of the hash function  $h(\cdot)$  and the PUF function  $PUF(\cdot)$ .  $Adv_p^{ECDHHP}(\mathcal{A})$  indicates the adversary's advantage in solving the Elliptic Curve Diffie-Hellman Hard Problem.

**Proof:** We prove this theorem by defining a sequence of games  $GM_i$ . Each game is described below: Game 0: Adversary  $\mathcal{A}$  can execute a real attack on the proposed protocol in this game, and we obtain:

$$Adv(\mathcal{A}) = |2Pr[Succ_0] - 1|$$

**Game 1:** In this game, adversary  $\mathcal{A}$  adds Execute queries. Passive eavesdropping through Game 1 does not increase the adversary's advantage. Hence, the adversary's advantage in Game 0 and Game 1 are equal, thus:

$$Pr[Succ_0] = Pr[Succ_1]$$

**Game 2:** Based on the birthday paradox principle, the collision probability of the hash function output is bounded by  $\frac{q_h^2}{2^{l+1}}$ , and the collision probability of random numbers is at most  $\frac{(q_s + q_e)^2}{2p}$ .

Thus, we have:

$$Pr[Succ_2] - Pr[Succ_1] \leq \frac{q_h^2}{2^{l+1}} + \frac{(q_s + q_e)^2}{2p}$$

**Game 3:** Adversary  $\mathcal{A}$  executes Send and PUF queries. Due to the security properties of  $PUF()$ , we have:

$$Pr[Succ_3] - Pr[Succ_2] \leq \frac{q_p^2}{|PUF|}$$

**Game 4:** In Game 4, adversary  $\mathcal{A}$  intercepts messages transmitted during communication. After intercepting these messages, the primary objective of  $\mathcal{A}$  is to construct the session key SK. To achieve this,  $\mathcal{A}$  must solve the ECCDHP problem within polynomial time. Thus, we obtain:

$$|Pr[Succ_4] - Pr[Succ_3]| \leq Adv^{ECDHHP}(t)$$

All random oracles are simulated, and adversary  $\mathcal{A}$  does not gain any advantage during guessing:

$$Pr[Succ_4] = \frac{1}{2}$$

Finally, we obtain:

$$Adv(\mathcal{A}) \leq \frac{q_h^2}{2^l} + \frac{(q_s + q_e)^2}{p} + \frac{2q_p^2}{|PUF|} + 2Adv_P^{ECDHHP}(\mathcal{A})$$

Through the above analysis, we can prove the security of the scheme under the ROM model.

## 5.3 Informal security analysis

### 5.3.1 Forward security

The session keys for  $EV_i$  and  $CS_j$  are  $SK_j = H(NP_j, k_i, ES'_i, PID_i, ID_i)$ . This key is related to  $ID_i$ ,  $k_i$ ,  $H(K_i, r_i)$  and  $N_j$ . Assuming that attacker A possesses the long-term key of the protocol participating entity, but needs to solve the ECCDHP difficulty problem in order to obtain the secret values  $H(K_i, r_i)$  and  $N_j$ , and cannot obtain the  $K_i$  calculated through PUF, thus unable to calculate the session key. Even if the previous session key is captured, the previous or subsequent session keys are still secure because the random numbers in each session key are different. Therefore, the proposed protocol satisfies forward security.

### 5.3.2 User anonymity and untraceability

During the registration phase,  $EV_i$  sends the identity identifier  $ID_i$  to TA. TA calculates a pseudo-random identity  $PID_i = H(ID_i, k_i, s)$ , and then sends the anonymous identity identifier  $PID_i$  to  $EV_i$  through a secure channel. Moreover, the identity identifier  $ID_i$  of  $EV_i$  is not stored in  $CS_j$ , so there is no possibility for attacker to crack the data stored in  $CS_j$  and obtain the user's identity identifier  $ID_i$ . Secondly, during the authentication and key negotiation phase, if the identity identifier  $ID_i$  of EV is not transmitted over the public channel, attacker A cannot obtain it. Therefore, it can ensure user anonymity during the registration phase and authentication and key negotiation phase. And after each successful authentication,  $EV_i$  and  $CS_j$  will update the anonymous identity  $PID_i$  synchronously. Therefore, attacker is unable to track specific users, ensuring their untraceability.

### 5.3.3 Man in the middle attack

Assuming that attackers can eavesdrop on the messages transmitted during the authentication process through public channels. However, the attacker cannot obtain the identity identifier  $ID_i$  of  $EV_i$  and the response value  $K_i = PUF_j(C_i)$ . Therefore, even if attacker disguises as an  $EV_i$  and sends a false message  $M_1 = (PID_i, EB_i, EV_i, T_i)$ , it cannot pass  $CS_j$  authentication. Similarly, attacker does not know the response value  $K_j = PUF_j(e_j)$  of  $CS_j$ , so it cannot tamper with the  $M_2 = (N_j, DC_j, VM_j, T_j)$  transmitted on the common channel. It is also unable to pass  $EV_i$  authentication. Therefore, this agreement can resist man in the middle attacks.

### 5.3.4 User forgery attack

Attackers cannot forge  $EV_i$ 's identity authentication information to obtain  $CS_j$  authentication. On the one hand, attackers cannot know  $ID_i$  and response value  $K_i = PUF_j(C_i)$ , and cannot calculate  $k_i = H(ID_i, C_i, K_i) \oplus ED_i$ . Therefore, attackers cannot forge  $EA_i^*$  and cannot continue authentication. On the other hand, even if the attacker intercepts the anonymous identity  $PID_i$  of  $EV_i$ , they cannot

forge  $EB_i = H(K_i, r_i)P$ ,  $ES_i = H(K_i, r_i)E_i$ ,  $EV_i = H(PID_i, ES_i, k_i, T_i)$ , because the attacker cannot calculate  $K_i$  and  $r_i$ , so the attacker cannot forge  $M_1 = (PID_i, EB_i, EV_i, T_i)$ . In summary, attackers cannot forge  $EV_i$  to launch attack.

### 5.3.5 Mutual authentication

In this protocol,  $EV_i$  and  $CS_j$  implement authentication and key negotiation. In the mutual authentication process,  $EV_i$  and  $CS_j$  verify the identity of  $CS_j$  by verifying whether the parameters  $ECV'_i$  and  $EVV_i$  are equal, and  $CS_j$  and  $EV_i$  verify the identity of  $EV_i$  by verifying whether the parameters  $VM_j^*$  and  $VM_j$  are equal. Therefore, this protocol can achieve mutual authentication.

### 5.3.6 Replay attack

The protocol in this article uses timestamps and random numbers in its design, both of which can resist replay attacks. Firstly, using timestamps  $T_i$  and  $T_j$  to avoid replay attacks can ensure the freshness of information. Specifically, the identity authentication message of the  $EV_i$  contains a timestamp  $T_i$ . By comparing timestamps, attackers can avoid replay attacks. Secondly, using random numbers to further avoid replay attacks, both parties involved in mutual authentication can avoid replay attacks by determining whether the random number contained in the reply message is the same as the initial value.

### 5.3.7 Session key security

In the authentication protocol,  $EV_i$  and  $CS_j$  negotiate to generate a session key  $SK_i = H(NP'_j, k_i, ES_i, PID_i, ID_i)$  for subsequent secure communication. Among them, the calculation of session key SK requires the secret value  $H(K_i, r_i)$  generated by  $EV_i$  and the secret value  $N_j$  generated by  $CS_j$ , both of which are updated during protocol execution. Therefore, if a session key is compromised, it does not help to recover past or future session keys. Therefore, authentication protocol can ensure the security of session keys.

### 5.3.8 Brief secret leakage attack

In the proposed protocol,  $EV_i$  and  $CS_j$  establish a common session key  $SK_i = H(NP'_j, k_i, ES_i, PID_i, ID_i)$ . Assuming that the adversary has obtained brief secret values  $r_i$  and  $n_i$ , but  $NP'_j$  in the session key is generated through its corresponding PUF value, which the adversary cannot calculate. Therefore, the protocol resisted brief secret leak attacks.

## 5.4 Security attribute

This article compares the security properties implemented by the protocol with those of other authentication protocols such as Tsai [19], Lwamo [39], Zhao [40] and Wang [41]. Tsai [19] and Lwamo [39] have implemented many security attributes, but there are still some attributes that have not been fully satisfied. In addition, although Zhao [40] achieves various security attributes well, it didn't analyze the session key security and secret leakage. At the same time, this protocol implements all security attributes, as shown in Table 3. Therefore, compared with the comparison protocol, this protocol implements all security attributes.



TABLE 3 Comparison of security.

Attribute	[19]	[39]	[40]	[41]	Our
Forward security	√	×	√	√	√
User anonymity	√	√	√	×	√
Unlinkability	√	×	√	√	√
Replay attack	√	√	√	√	√
Forgery attack	√	√	√	√	√
Man-in-the-middle attack	√	√	√	√	√
Session key security	√	√	×	√	√
Secret leakage	×	×	×	√	√

TABLE 4 Comparison of computational overhead.

Protocol	Total computation overhead	Total time
[19]	$2T_{bp} + 2T_{mul} + 2T_{pa} + 2T_{mep} + 4T_h$	33.802
[39]	$9T_h + 6T_{enc/dec}$	7.047
[40]	$8T_{mul} + T_{fe} + 22T_h$	26.346
[41]	$8T_{mul} + 16T_h + T_{puf}$	23.538
Our	$5T_{mul} + 3T_{puf} + 13T_h$	15.029

## 6 Performance analysis

### 6.1 Computational overhead

Here, we compare the computational cost of this protocol with Tsai [19], Lwamo [39] and Zhao [40]. In the experiment, this protocol used the JPBC library for experimental simulation. The hardware of the PC used is Intel Core i5 3.10 GHz CPU, 16GB RAM, programming language is Java, and the experimental code is executed on MyEclipse integrated development environment. By calculation, the time for hash operation, multiplication operation, pairing operation, PUF operation, fuzzy extractor and point addition operation are  $T_h = 0.003$  ms,  $T_{mul} = 2.92$  ms,  $T_{bp} = 13.81$  ms,  $T_{puf} = 0.13$  ms,  $T_{fe} = 2.92$  ms and  $T_{pa} = 0.035$  ms. The time for modular operation, encryption operation, and decryption operation is  $T_{mep} = T_{enc/dec} = 1.17$  ms. In addition, due to the small execution time of XOR operation, it was not taken into account. In the authentication phase, the computational cost of Tsai [19] is  $2T_{bp} + 2T_{mul} + 2T_{pa} + 2T_{mep} + 4T_h$ . The computational cost of Lwamo [39] is  $9T_h + 6T_{enc/dec}$ , while the computational cost of Zhao [40] is  $8T_{mul} + T_{fe} + 22T_h$ . The computational cost of the protocol in this article is  $5T_{mul} + 3T_{puf} + 13T_h$ . The response results are shown in Table 4.

As shown in Figure 4, compare the overall computational cost of this protocol with [19], [39] and [40]. In the authentication scenario,

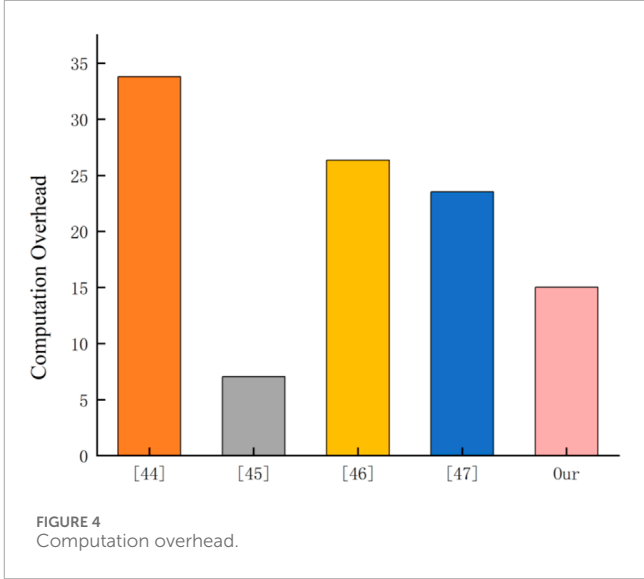


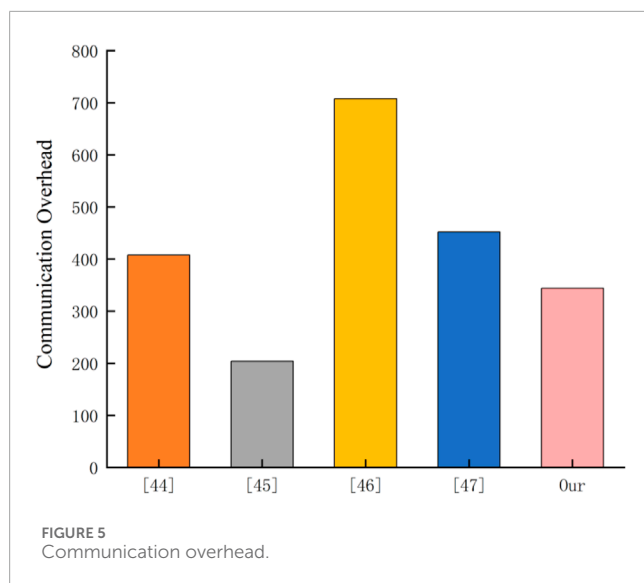
TABLE 5 Comparison of the communication overhead.

Protocol	Communication overhead
[19]	408
[39]	204
[40]	708
[41]	452
Our	344

the computational costs of [19], [39] and [40] are 35.882 ms, 7.047 ms and 26.346 ms, respectively. The computational cost of this protocol is only 15.029 ms, which is the shortest compared to other protocols such as [19] and [40]. The cost of this protocol is higher than that of Lwamo [39]. But [39] did not allow for forward security, unlinkability and secret leakage. Therefore, compared to other protocols, this protocol achieves better computational overhead on a more comprehensive security basis.

### 6.2 Communication overhead

In this article, we will compare the communication overhead of our protocol with [19], [39] and [40]. In the comparison of communication overhead, the relevant group elements and variables are described as follows:  $|G_1|$  represents the size of an element in group  $G_1$ , which is 128 bytes. In addition, the length of the hash value is 20 bytes, the length of the response message or identifier is set to 4 bytes, and the size of the timestamp is 4 bytes. In Table 5, this article compares the communication overhead of this protocol with [19], [39] and [40]. In the identity authentication stage, the data involved in the protocol communication overhead in this article consists of  $M_1 = (PID_i, EB_i, ECV_i, T_i)$  and  $M_2 = (N_j, DC_j, VM_j, T_j)$ . The communication overhead of  $M_1 = (PID_i, EB_i, ECV_i, T_i)$  is 172



bytes, and the communication overhead of  $M_2 = (N_j, DC_j, VM_j, T_j)$  is 172 bytes. So, the overall communication overhead of this protocol is 344 bytes. In contrast, [19] has a communication overhead of 408 bytes. The communication overhead of [40] is 708 bytes. Similarly, The communication overhead of [40] is 204 bytes.

In Figure 5, further comparison of communication overhead among various protocols is shown. It can be seen that although the overall communication overhead of this protocol is slightly higher than [39], it is still lower than [19] and [40]. It should be explained that compared to [39], the communication overhead in this protocol is relatively high. In order to improve the security of the protocol, this paper sacrifices a small amount of communication overhead to achieve lower computational complexity and stronger security properties. Overall, in terms of communication overhead, this protocol is slightly weaker than [39], but better than [19] and [40]. However, in other aspects, compared to [19], [39] and Zhao [40], this protocol has more advantages.

## 7 Conclusion

This article focuses on the security challenges of V2G networks in smart grids and proposes an efficient and secure anonymous authentication protocol aimed at protecting user privacy and ensuring communication security. Through studying security threats in V2G environments, we have found that unauthorized access, user privacy breaches, and issues with transaction data integrity, as well as various forms of attacks during public communication, pose serious threats to the stable operation of V2G networks. In response to these challenges, we have designed an authentication protocol based on elliptic curve cryptography and physically unclonable function technology. This protocol not only achieves bidirectional authentication, ensuring the security of session keys, but also effectively protects the anonymity of participants by sending temporary identity values. Through simulation analysis and heuristic analysis using Scyther tool, we have verified the excellent performance of the protocol in terms of

bidirectional authentication, session key security, forward security, and anonymity. At the same time, we have demonstrated that the protocol can resist various security threats. In addition, the performance comparison with other protocols shows that the proposed solution in this paper reduces costs while meeting the security requirements in the smart grid environment, demonstrating significant advantages in terms of security and overhead. In summary, the anonymity and privacy protection authentication protocol proposed in this article provides strong guarantees for the secure operation of V2G networks in smart grids. At the same time, the protocol is of great significance in promoting the popularization of electric vehicles, facilitating the two-way flow and management of energy and improving the flexibility and stability of the power grid.

## Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

## Author contributions

ZS: Conceptualization, Data curation, Methodology, Supervision, Writing – original draft. YW: Formal Analysis, Methodology, Project administration, Supervision, Validation, Visualization, Writing – review and editing.

## Funding

The author(s) declare that no financial support was received for the research and/or publication of this article.

## Conflict of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

## Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

## References

- Khalid M. Smart grids and renewable energy systems: perspectives and grid integration challenges. *Energy Strategy Rev* (2024) 51:101299. doi:10.1016/j.esr.2024.101299
- Zhang Y, Chen L, Battino M, Farag MA, Xiao J, Simal-Gandara J, et al. Blockchain: an emerging novel technology to upgrade the current fresh fruit supply chain. *Trends Food Sci and Technology* (2022) 124:1–12. doi:10.1016/j.tifs.2022.03.030
- Faheem M, Kuusniemi H, Eltahawy B, Bhutta MS, Raza B. A lightweight smart contracts framework for blockchain-based secure communication in smart grid applications. *IET Generation, Transm and Distribution* (2024) 18(3):625–38. doi:10.1049/gtd2.13103
- Zhang Z, Liu M, Sun M, Deng R, Cheng P, Niyato D, et al. Vulnerability of machine learning approaches applied in iot-based smart grid: a review. *IEEE Internet Things J* (2024) 11(11):18951–75. doi:10.1109/jiot.2024.3349381
- Bai Z, Miao H, Miao J, Xiao N, Sun X. Artificial intelligence-driven cybersecurity applications and challenges. *Innovative Appl AI* (2025) 2(2):26–33. doi:10.70695/aa1202502a09
- Jin Y, Liu J, Xu Z, Yuan S, Li P, Wang J. Development status and trend of agricultural robot technology. *Int J Agric Biol Eng* (2021) 14(4):1–19. doi:10.25165/j.ijabe.20211404.6821
- Lu Y, Xu W, Leng J, Liu X, Xu H, Ding H, et al. Review and research prospects on additive manufacturing technology for agricultural manufacturing. *Agriculture* (2024) 14(8):1207. doi:10.3390/agriculture14081207
- Udo WS, Kwakye JM, Ekechukwu DE, Ogundipe OB. Smart grid innovation: machine learning for real-time energy management and load balancing. *Int J Smart Grid Appl* (2024) 22(4):405–23. doi:10.51594/estj.v4i6.1395
- İnci M, Savrun MM, Çelik Ö. Integrating electric vehicles as virtual power plants: a comprehensive review on vehicle-to-grid (V2G) concepts, interface topologies, marketing and future prospects. *J Energy Storage* (2022) 55:105579. doi:10.1016/j.est.2022.105579
- Li J, Wu Z, Li M, Shang Z. Dynamic measurement method for steering Wheel Angle of Autonomous agricultural vehicles. *Agric Basel* (2024) 14(9):1602. doi:10.3390/agriculture14091602
- Escoto M, Guerrero A, Ghorbani E, Juan AA. Optimization challenges in vehicle-to-grid (V2G) systems and artificial intelligence solving methods. *Appl Sci* (2024) 14(12):5211. doi:10.3390/app14125211
- Naik N, Vyjayanthi C. Optimization of vehicle-to-grid (V2G) services for development of smart electric grid: a review[C]//2021 International Conference on smart generation computing, communication and networking (SMART GENCON). IEEE (2021). p. 1–6.
- Sureshkumar V, Mugunthan S, Amin R. An enhanced mutually authenticated security protocol with key establishment for cloud enabled smart vehicle to grid network. *Peer-to-Peer Networking Appl* (2022) 15(5):2347–63. doi:10.1007/s12083-022-01350-3
- Liang Y, Liu Y, Zhang X, Liu G. Physically secure and privacy-preserving charging authentication framework with data aggregation in vehicle-to-grid networks. *IEEE Trans Intell Transportation Syst* (2024) 25:18831–46. doi:10.1109/tits.2024.3443171
- Prateek K, Maity S, Saxena N. Qska: a quantum secured privacy-preserving mutual authentication scheme for energy internet-based vehicle-to-grid communication. *IEEE Trans Netw Serv Management* (2024) 21:6810–26. doi:10.1109/tnsm.2024.3445972
- Wei H, Miao J, Lv J, Chen CM, Kumari S, Amoon M. Secure and Trustworthy data management mechanism for Dance-Consumer Electronics in AIoT. *IEEE Trans Consumer Electronics* (2024) 71:1970–9. doi:10.1109/tce.2024.3471573
- Miao J, Wang Z, Wang M, Feng X, Xiao N, Sun X. Security authentication protocol for massive machine type communication in 5G networks. *Wireless Commun Mobile Comput* (2023) 2023(1):1–10. doi:10.1155/2023/6086686
- Yang Z, Yu S, Lou W, Liu C. P<sup>2</sup>: privacy-preserving communication and Precise Reward architecture for V2G networks in smart grid. *IEEE Trans Smart Grid* (2011) 2(4):697–706. doi:10.1109/tsg.2011.2140343
- Tsai JL, Lo NW. A privacy-aware authentication scheme for distributed mobile cloud computing services. *IEEE Syst J* (2015) 9(3):805–15. doi:10.1109/jsyst.2014.2322973
- He D, Kumar N, Khan MK, Wang L, Shen J. Efficient privacy-aware authentication scheme for mobile cloud computing services. *IEEE Syst J* (2016) 12(2):1621–31. doi:10.1109/jsyst.2016.2633809
- Abdallah A, Shen XS. Lightweight authentication and privacy-preserving scheme for V2GConnections. *IEEE Trans Vehicular Technology* (2016) 66(3):2615–29. doi:10.1109/tvt.2016.2577018
- Zhang W, Yang W, Chen C, Li N, Bao Z, Luo M. Toward privacy-preserving blockchain-based electricity auction for V2G networks in the smart grid. *Security Commun Networks* (2022) 2022:1–12. doi:10.1155/2022/6911463
- Bansal G, Naren N, Chamola V, Sikdar B, Kumar N, Guizani M. Lightweight mutual authentication protocol for V2G using physical unclonable function. *IEEE Trans On Vehicular Technology* (2020) 69:7234–46. doi:10.1109/tvt.2020.2976960
- Khan A, Kumar V, Ahmad M, Jangirala S. A secure and energy efficient key agreement framework for vehicle-grid system. *J Of Inf Security And Appl* (2022) 68:103231. doi:10.1016/j.jisa.2022.103231
- Su Y, Shen G, Zhang M. A novel privacy-preserving authentication scheme for V2G networks. *IEEE Syst J* (2019) 1–9. doi:10.1109/JSYST.2019.2932127
- Mahmoud HE, Qi S, Angelos KM. Efficient, secure, and privacy-preserving PMIPv6 protocol for V2G networks. *IEEE Trans Vehicular Technology* (2019) 68(1):1–12. doi:10.1109/TVT.2018.2880834
- Liu H, Ning H, Zhang Y, Xiong Q, Yang LT. Role-dependent privacy preservation for secure V2G networks in the smart grid. *IEEE Trans Inf Forensics Security* (2014) 9(2):208–20. doi:10.1109/tifs.2013.2295032
- Saxena N, Choi BJ, Cho S. Lightweight privacy-preserving authentication scheme for V2G networks in the smart grid. In: IEEE Trustcom. IEEE (2015). p. 20–2.
- Kaur K, Garg S, Kaddoum G, Gagnon F, Ahmad SH, Guizani M. A secure, lightweight, and privacy-preserving authentication scheme for V2G connections in smart grid. In: IEEE INFOCOM 2019 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE (2019). p. 541–6. doi:10.1109/INFOCOMW.2019.8845140
- Wang H, Qin B, Wu Q, Xu L, Domingo-Ferrer J. TPP: Traceable privacy-preserving communication and Precise Reward for vehicle-to-grid networks in smart grids. *IEEE Trans Inf Forensics and Security* (2015) 10(11):2340–51. doi:10.1109/tifs.2015.2455513
- Nicanfar H, Leung VC. Multilayer Consensus ECC-based password authenticated key-exchange(MCEPAK) protocol for smart grid system. *IEEE Trans Smart Grid* (2013) 4(1):253–64. doi:10.1109/tsg.2012.2226252
- Shen J, Zhou T, Wei F, Sun X, Xiang Y. Privacy-preserving and lightweight key agreement protocol for V2G in the social internet of things. *IEEE Internet things J* (2017) 5(4):2526–36. doi:10.1109/jiot.2017.2775248
- Park K, Park Y, Das AK, Yu S, Lee J, Park Y. A dynamic privacy-preserving key management protocol for V2G in social internet of things. *IEEE Access* (2019) 7:76812–32. doi:10.1109/access.2019.2921399
- Gope P, Sikdar B. An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication. *IEEE Trans Smart Grid* (2019) 10(6):6607–18. doi:10.1109/tsg.2019.2908698
- Irshad A, Usman M, Chaudhry SA, Naqvi H, Shafiq M. A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework. *IEEE Trans Industry Appl* (2020) 56(4):4425–35. doi:10.1109/TIA.2020.2966160
- Sureshkumar V, Chinnaraj P, Saravanan P, Amin R, Rodrigues JJ. Authenticated key agreement protocol for secure communication establishment in vehicle-to-grid environment with FPGA Implementation. *IEEE Trans Vehicular Technology* (2022) 71(4):3470–9. doi:10.1109/tvt.2022.3146409
- Miao J, Wang Z, Wang M, Garg S, Hossain MS, Rodrigues JJ. Secure and efficient communication approaches for industry 5.0 in edge computing. *Computer Networks* (2024) 242:110244. doi:10.1016/j.comnet.2024.110244
- Nyangaresi VO, AlRababah AA, Yenurkar GK, Chinthaginjala R, Yasir M. Anonymous authentication scheme based on physically unclonable function and Biometrics for smart Cities. *Eng Rep* (2025) 7(1):e13079. doi:10.1002/eng2.13079
- Lwamo NMR, Zhu L, Xu C, Sharif K, Liu X, Zhang C, et al. SUAA: a secure user authentication scheme with anonymity for the single and multi-server environments. *Inf Sci* (2019) 477:369–85. doi:10.1016/j.ins.2018.10.037
- Zhao X, Li D, Li H. Practical three-factor authentication protocol based on elliptic curve cryp-tography for industrial internet of things. *Sensors* (2022) 22(19):7510. doi:10.3390/s22197510
- Wang J, Wang S, Wen K, Weng B, Zhou X, Chen K. An ecc-based authentication protocol for dynamic charging system of electric vehicles. *Electronics* (2024) 13(6):1109. doi:10.3390/electronics13061109