Journal of *Sensor and Actuator Networks*

MDPI

Article

Efficient Privacy-Preserving and Secure Authentication for Electric-Vehicle-to-Electric-Vehicle-Charging System Based on ECQV

Abdullah M. Almuhaideb [1,*] and Sammar S. Algothami [2]

[1] SAUDI ARAMCO Cybersecurity Chair, Department of Networks and Communications, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia

[2] Department of Computer Science, College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, P.O. Box 1982, Dammam 31441, Saudi Arabia; 2210500095@iau.edu.sa

* Correspondence: amAlmuhaideb@iau.edu.sa

Abstract: The use of Electric Vehicles (EVs) is almost inevitable in the near future for the sake of the environment and our plant's long-term sustainability. The availability of an Electric-Vehicle-Charging Station (EVCS) is the key challenge that owners are worried about. Therefore, we suggest benefiting from individual EVs that have excess energy and are willing to share it with other EVs in order to maximize the availability of EVCSs without the need to rely on the existing charging infrastructure. The Internet of Electric Vehicles (IoEV) is gradually gaining traction, allowing for a more efficient and intelligent transportation system by leveraging these capabilities between EVs. However, the IoEV is considered a trustless environment, with untrustworthy trading partners such as data sellers, buyers, and brokers. Data exchanged between the EV and the Energy AGgregator (EAG) or EV/EV can be used to analyze users' behavior and compromise their privacy. Thus, a Vehicle-to-Vehicle (V2V)-charging system that is both secure and private must be established. Several V2V-charging systems with security and privacy features have been proposed. However, even if the transmitted communications are entirely anonymous, anonymity alone will not prevent the tracking adversary from reconstructing the target vehicle's route. These systems frequently fail to find a balance between privacy concerns (e.g., trade traceability to achieve anonymity, and so on) and security measures. In this paper, we propose an efficient privacy-preserving and secure authentication based on Elliptic Curve Qu–Vanstone (ECQV) for a V2V-charging system that fulfils the essential requirements and re-authentication protocol in order to reduce the overhead of future authentication processes. The proposed scheme utilizes the ECQV implicit-certificate mechanism to create credentials and authenticate EVs. The proposed protocols provide efficient security and privacy to EVs, as well as an 88% reduction in computational time through re-authentication, as compared to earlier efforts.

Keywords: Electric Vehicle (EV); V2V-charging system; authentication; Elliptic Curve Qu–Vanstone (ECQV) implicit certificate; security; privacy-preserving; un-linkability; anonymity; re-authentication

Citation: Almuhaideb, A.M.; Algothami, S.S. Efficient Privacy-Preserving and Secure Authentication for Electric-Vehicle-to-Electric-Vehicle-Charging System Based on ECQV. *J. Sens. Actuator Netw.* **2022**, *11*, 28. https://doi.org/10.3390/jsan11020028

Academic Editor: Jordi Mongay Batalla

Received: 7 April 2022
Accepted: 31 May 2022
Published: 9 June 2022

1. Introduction

Rapid changes in the transportation industry have occurred in recent years, with a conscious effort to combat climate change and cut Greenhouse-Gas emissions (GHG). This industry is responsible for almost 30% of the world's GHG emissions, which in return affects air quality. The electrification of the transportation system is gaining popularity because it has several advantages over vehicles powered by an internal combustion engine (ICE), including the use of sustainable energy, reduction in fossil-fuel dependency

and consumption, and being GHG-emission free. Hence, the Electric Vehicle (EV) is a suitable solution for dealing with the energy crisis and climatic change [1].

Several countries such as Saudi Arabia have announced that at least 30% of cars in the capital city will be electric by 2030. China seeks to have 25% of new cars in the country be electric by 2025. On the other hand, the United Kingdom plans to stop selling new fossil-fuel cars by 2030 [2]. In 2020, over 10 million electric cars were on the roads throughout the world with 1.3 million publicly available chargers, with 30% of them being fast chargers. As one can see, the rate of growth of the Electric-Vehicle-Charging Station (EVCS) is noticeably slower than that of EVs. Therefore, the availability of EVCSs is the most significant hurdle, which is known as "range anxiety", that consumers are concerned about (particularly in the United States and the United Kingdom) according to the climate group's EV100 members [3]. They are anxious that the EV's energy will be consumed before it reaches its destination. This effect is accentuated on highways and in remote regions, which currently have inadequate charging infrastructure and where drivers travel longer distances than in cities [4]. As a result, EV drivers may find themselves abandoned on the street with little to no charge as well as no nearby charging stations, with no other option but to wait for a tow truck. As the demand for electric vehicles evolves, EV-charging stations must be strategically positioned and properly utilized [5].

In fact, deploying charging stations in every location is both impractical and expensive. As a result, auxiliary solutions to alleviate such a worry must be found, and the bidirectional energy-transfer capabilities of EVs, particularly Vehicle-to-Vehicle (V2V) energy transfer, should be seriously studied. Whenever it is hard or impossible for an EV to access an EVCS, V2V charging enables a source EV to travel in order to satisfy another EV-charging request without the need to rely on existing charging infrastructure [6]. AAA (a US corporation) has made this idea a reality by introducing a fleet of EV-charging trucks in different cities such as Portland, Seattle, San Francisco, Los Angeles, Denver, Phoenix, and Orlando. All of their trucks have generators and level-two chargers, and only a few have CHAdeMO fast chargers [7].

With the rapid evolution and advancement in vehicular telecommunications and technologies, EVs can now create numerous forms of data. Modern EVs have been enhanced with communication and data-sharing/trading capabilities with their surroundings (V2V and Vehicle-to-Infrastructure (V2I)). As a result of utilizing these capabilities between EVs, the Internet of Electric Vehicles (IoEV) is progressively emerging, enabling a more efficient and intelligent transportation system. However, the IoEV is seen as a trustless ecosystem, in which trading partners such as data sellers, buyers, and brokers are not trustworthy. Payments and data sharing may be a subject of dispute between the trading parties [8].

To achieve a V2V energy transfer, the suppliers and receivers must first be matched. The best-fit EV supplier (to meet the charging needs of the demander EV) must be identified once the demander EV has made a request from within their neighborhood. This may be accomplished through centralized control and EV automation in order to interact and maintain their engagement through a local Energy AGgregator (EAG). During the search process, an EV seeking charging can request energy trading (amount and price) from its local EAG, which in turn chooses a supplier EV from a list of options and then matches it to the demander EV. EVs can pay for the service via the web app (perhaps with the help of third-party services such as banks or electricity companies). However, after the peers' validation and matching by the EAG, the demander/supplier EV peers must physically meet in order to carry out the actual V2V energy transfer and link their batteries via a specifically designed DC–DC converter or through specified V2V-charging piles. Therefore, these EVs must mutually authenticate each other to ensure that no unauthorized demander/supplier EVs arrive and that the agreed-upon amount of energy can be transferred even though one of the EV's owners is not onsite [9].

While the EV is attached to the charging supplier (EVCS or other EV), it exchanges information with the EAG in a continuous manner. The EV sends sensitive information to

the potentially untrustworthy charging supplier (EVCS or other EV), including the EV's ID, battery status, energy consumed, or geographic location [10]. Adversaries can utilize the submitted data to deduce other sensitive data, such as the EV's identification information, identities of its occupants, and travel patterns [11]. Because the EV and the EAG connect over the Internet and V2V communication occurs over Dedicated Short-Range Communications (DSRC), the information they share is susceptible to a variety of attacks. These attacks can lead to EVCS malfunctions, money theft, payment-transaction mistakes, and battery-charging inconsistencies, among many other issues. Eavesdropping attacks, Denial-of-Service (DoS) attacks, replay attacks, impersonation attacks, and Man-In-The-Middle (MTIM) attacks are some of the significant attacks that could occur in EV-charging systems [10].

1.1. Problem Statement

With the massive increase in EV adoption, one of its key issues has indeed been EV charging. Several methods of wireless charging for electric vehicles have been considered (e.g., charging while parked [8] and wireless dynamic charging on the move [9]). In addition to the EV's transportation service, EVs serve as distributed mobile energy storage and can function as both energy consumer and supplier. Advancement in energy-supply systems, combined with the bidirectional communication of EVs, helps to relieve the issue of the energy demand–supply gap, facilitating the reliable and sustainable fulfilment of ongoing energy needs [7]. The privacy of sensitive data is linked to or includes information about a particular individual. However, fine-grained personal-data collection is frequently required for a specific-use case or to comply with legal obligations. Furthermore, a single data item might not be enough to compromise privacy. However, combining data from multiple actors may enable someone to gain access to extra information and, as a result, compromise an individual's privacy. Unterweger in [12] identified five privacy breaches (e.g., vehicle identification and personal-data sharing). If another entity (other than the client) can utilize the acquired data for an unintended purpose, then a client's privacy is breached.

The legal authority issues the EV credential, which allows vehicles to be identified as well as authenticated. However, because this credential contains the EV's true identification, it provides a method of vehicle tracking. Therefore, the privacy of EVs is threatened during energy-trading processes, as the EV's sensitive and confidential information can be exposed while interacting with an EVCSs or other EVs. Therefore, a solution that balances secure authentication procedures and anonymous communications (privacy) is essential. In previous blockchain approaches, the transactions of energy trading were publicly stored and verified by all network nodes. Moreover, transaction data could be utilized to initiate privacy-related linkage attacks simply by tying it to other publicly available datasets, and there are a variety of data-mining methods and algorithms that could use raw data to conduct attacks.

In Peer-to-Peer (P2P) energy trading between EVs, privacy is still a concern, despite the great benefits of the blockchain in a trustless environment and the transparency of trading. As a result, designing a safe privacy-preserving mechanism for blockchain-based P2P energy trading among EVs is a major challenge. The first concern is to guarantee privacy while maintaining the anonymity of the EV's confidential information. The second challenge is to use an acceptable approach to conceal the data and energy-trading patterns of EVs [8]. Similarly, patterns that reveal behavioral information are rarely discussed in publications, and trustworthy third parties are frequently exploited to hide flaws in privacy-related implementation [12].

To address these concerns, an Elliptic Curve Qu–Vanstone (ECQV)-based EV system might be developed, providing EV users with confidentiality and simple authentication. The ECQV implicit certificate is required for mutual authentication, key establishment, and key exchange between IoT devices. Several V2V-charging systems with security and privacy features have been proposed. However, even if the transmitted communications

are entirely anonymous, anonymity alone will not prevent the tracking adversary from reconstructing the target vehicle's route. These systems frequently fail to find a balance between privacy concerns (e.g., trade traceability to achieve anonymity, and so on) and security measures.

1.2. Motivation and Contribution

With the goal of meeting the previously specified security and privacy standards, this paper contributes the following:

1. Proposes an authentication scheme for an electric-vehicle-to-electric-vehicle-charging system, which provides more secure mutual authentication and efficient privacy preservation based on ECQV.
2. Conducts an informal security analysis to indicate the protocol's security against numerous attacks.
3. Computational costs are compared with other related work, demonstrating that our proposed protocol has a better performance.

1.3. Paper Organization

The remainder of the paper is structured as follows: Preliminaries are covered in Section 2. In Section 3, we present a literature review related to the proposed protocol. Section 4 introduces the proposed system. Section 5 discusses the informal security analysis. We compare the security and functional features, as well as the computational cost, to other related schemes in Section 6. Lastly, in Section 7 is the conclusion.

2. Preliminaries

In this section, we discuss the authentication-solution requirements of EV charging, Elliptic-Curve (EC)-based operations, and present the concepts of the Elliptic Curve Qu–Vanstone (ECQV) implicit certificate.

2.1. Solution Requirements

The sustainability and adoption of electric-vehicle-charging systems (including V2V energy trading) require privacy-preserving authentication. Before a V2V-charging system may be deployed, some critical security standards must be addressed. Nevertheless, the current approaches have limitations that pose various problems concerning V2V-charging systems. Thus, the proposed solution should satisfy the parameters listed below:

1. Mutual authentication: The system must enable participants to authenticate one another and ensure that communication is built on mutual trust. The demander EV authenticates the supplier EV to confirm its identity and its registration with the electricity OPerator (OP). The supplier EV will simultaneously verify the demander EV's registration with the OP, using certificates issued by the OP. As a result, the prospect of a masquerade attack should be eliminated [13,14].
2. Anonymity: It is the ability to stay anonymous among a group of subjects. The real identity of the EV should not be disclosed to other EVs or the EAG during the V2V-charging process [15]. The ability to keep a subject's activities untraceable is known as untraceability. Eavesdroppers are unable to deduce or track the activities of the EV [13,14].
3. Un-linkability: When an attacker cannot detect if two activities are linked, this is known as un-linkability. Different charging sessions of an EV should be un-linkable, and these different charging sessions should be un-linkable to the EV's real identity [14,15].
4. Traceability: This property enables the trustworthy organization (OP) to identify or disclose the malicious EV's true identity if necessary [16].
5. Perfect forward/backward security: If a long-term private key is compromised, the attacker will not be able to access future/old session keys [17].

6. Joint key control: Both the demander and supplier EVs will contribute a random number to generate the session key. Thus, no one other than participating entities receives access to or may obtain any session keys.
7. Effective re-authentication: The process whereby the supplier EV re-authenticates the demander EV, if matched again, causes an overhead. Hence, using information provided by a trusted third party (OP) and the EAG, the supplier EV should be able to verify the demander EV just once in the first encounter. For future access, the supplier EV can re-authenticate the demander EV without relying on the OP or EAG.
8. Revocation method: If the user's registration is terminated, or if the EV's secret key is disclosed, then it is essential to provide the system with a revocation mechanism.
9. Attack resistance: Because the connection between EAG/EV and EV/EV is conducted in an insecure environment, an adversary may initiate an attack during the communications. As a result, the proposed solution must be capable of defeating attacks such as modification attacks, impersonation attacks, replay attacks, MITM, etc.
10. Non-repudiation: Both the demander and supplier EVs provide proof of delivery in order to thwart participation denial. This is required to ensure that any dispute is resolved fairly [14].

2.2. Elliptic-Curve-Based Operations

Elliptic-Curve Cryptography (ECC) can be used to design the most lightweight public-key cryptographic systems. The algebraic form of ECs over finite fields is the foundation for ECC. In the finite field F_p, the curve is characterized by $E_{p(a,b)}$ and is determined using the formula $y^2 = x^3 + ax + b$, in which a and b are both constants $\in$ field F_p and $\Delta = 4a^3 + 27b^2 \neq 0$. The G stands for the base point constructor of the curve ($E_{p(a,b)}$) of prime order q. An additive group is formed by all points on $E_{p(a,b)}$, plus the infinite point. ECC has two main operations: addition and multiplication. The addition operation of two points results in a new EC point R, such that $P1 + P2 = R$. The EC scalar multiplication of $r \in F_p$ with EC point P results in a new EC point R, such that $R = rP = (R_x, R_y)$ where $R_x, R_y \in F_p$ [18].

2.3. ECQV Implicit Certificates

The implicit authentication of the ECQV mechanism offers the advantages of a lightweight certificate, faster computation, and is more suitable for resource-constrained Internet-of-Things (IoT) devices than traditional certificates (such as X.509 certificates) [19]. A traditional certificate demands a signature-verification technique, but an implicit certificate demands a public-key-extraction process, and the latter is significantly faster. The ECQV technique, which is based on Elliptic-Curve Cryptography, is used to create ECQV implicit certificates [20]. The private key can only be derived by the party requesting the security material, therefore not even the Certificate Authority (CA) can access it. Hence, the mechanism is safe from key-escrow attacks. Furthermore, a secure channel is not necessary during the procedure because all variables can be provided via an open channel [21].

3. Literature Review

In this section, we look at some of the most significant security and privacy-preserving V2V-charging solutions. The benefits and drawbacks of various existing security methods, as well as the efforts made in this study to solve the related difficulties, are outlined. The main objective of this work is to develop a secure, privacy-preserving authentication strategy for V2V charging that includes an efficient re-authentication strategy to minimize the authentication-process overhead. Prior work in the fields of security and privacy systems has been investigated to achieve the desired result.

The majority of research [6,22–26] on V2V charging/discharging concentrates on scheduling and coordination algorithms, as well as pricing mechanisms to reduce charging time and expense [27]. An EV-charging model was proposed by Kim et al. (2018) that matches the EV with either an EVCS or another EV in order to charge. They came to the conclusion that collaborating with EVs and CSs is preferable to depending only on EVCSs or V2V [22]. To solve the navigation and matching challenges in cooperative V2V charging, Li et al. (2019) proposed a framework for intelligent V2V navigation [23]. Li et al. (2018) similarly proposed a direct V2V matching for energy trading [24]. The concept of mobile EVCSs (charging trucks) to satisfy EV needs was considered in Kabir et al.'s (2020) routing model [6]. The concern of EV privacy preservation in V2V matching led Yucel et al. (2018) to present a model to address privacy-related issues (mainly location privacy) for a standard stable environment [25] and dynamic environment [26]. Several studies [28,29] used symmetric keys to improve authentication performance but did not guarantee anonymity preservation. Moreover, to preserve the EV's privacy from third-party nodes, Portunes [30] used utility-issued pseudonyms; however, the utility was aware of the linking map between the pseudonyms and real identity.

The basic Diffie–Hellman (DH) key-agreement protocol is a widely known and deployed protocol to thwart eavesdropping [31]. However, it is also known for being vulnerable to active MITM attacks. This has led to the utilization of different versions of DH which add authentication to both entities to mitigate this kind of attack. Roberts et al. (2017) presented a framework for V2V-charging authentication; they used a secure key-exchange (SKE) protocol to eliminate the use and storage of certificates. This authentication technique enables the participating EVs (supplier and demander) to mutually authenticate each other. Furthermore, it protects against several attacks other than MITM. However, one of the main drawbacks of this protocol is not taking into consideration the EV's privacy protection (such as anonymity, un-linkability, and traceability) [32].

Blockchain technology has been used in some previous research [8,27,33–40] to decentralize the complex energy-economy networks and P2P energy trade. Blockchain technologies are now mainly led by industry, giving the domain a slightly distinct perspective than previous academic areas. It faces some confusion in terms of pseudonymity, privacy and anonymity. For example, Bitcoin [41] provides pseudonymous transactions; since it is a distributed global public ledger, pseudonyms can be de-anonymized by analyzing blockchain-usage trends [42]. Blockchain technology offers globally verifiable proof of transactions in a distributed database (DB) depending on the time stamps of its transactions and messages. The trustworthiness of these proofs is provided by the underlying cryptographic techniques of hash functions and digital signatures [43].

To maintain and hide the real identity of an EV, every new session the EV can generate a new pair of addresses (pseudonyms) using the relevant public/private keys. Similarly, Aitzhan and Svetinovic (2016) introduced a distributed V2V energy-trading model that offers anonymity and un-linkability. In their model, EVs with excess energy can sell it to other EVs by sending a broadcast to all network nodes, and EVs who are interested in buying the energy can perform the matching procedure according to the price and amount. This may paralyze EVs by flooding them with unwanted requests from different nodes, especially with large numbers of EVs [33].

Kang et al. (2017) likewise used pseudonyms to ensure EVs' anonymity in a consortium blockchain-based V2V energy-trading system. The elliptic-curve-digital-signature algorithm (ECDSA) is used to initialize the system, and network nodes must register with the TA to obtain their credentials (public/private-key pairs and certificates) [34].

Nevertheless, the distributed system faces several challenges, including high communication overheads throughout the transaction-synchronization process. Due to frequent transactions between P2P nodes, state synchronization becomes inconsistent. A blockchain-based software-defined-network (SDN) framework is being developed by Chaudhary et al. (2019) to overcome these challenges. The underlying SDN architecture reduces network latency and provides real-time service by reducing end-to-end delays.

In the framework, each EV has a wallet that serves as an energy-trading account. The wallet is produced by combining the genuine wallet address with a random pseudonym (salt value) to ensure the transaction's un-linkability. The scheme resists several attacks and provides non-repudiation. However, to be able to trade energy between two EVs, there must be a third EV that works as both an energy broker and a minor node, and the energy trading must happen at a specific location (charging station). These pre-conditions are not convenient after taking into consideration the mobility of EVs; additionally, the specified area may be full, or no other EVs (minor node) may be available. Moreover, the framework does not provide an anonymity feature for participating EVs. In addition, this scheme employs SHA-1 (160 bits), which provides minimal communication costs whilst being vulnerable to collision attacks [35].

Establishing and maintaining a public blockchain among EVs with restricted resources and energy is extremely expensive in the energy market, and the consensus efficiency for all engaged EVs is not encouraging. Furthermore, a private blockchain is managed by a single company, and while it is still a centralized network, it cannot guarantee the accuracy of transaction data. Therefore, Sun et al. (2020) utilized a consortium blockchain to provide security and privacy to a V2V-charging system. ECC and asymmetric algorithms were used to initialize the system. However, the scheme allows energy-node fog (EFN) to generate the EV's public/private-key pair and store it along with other credentials in the account area. Since the EV's real identity and sensitive information are not protected, this could lead to security and privacy breaches if the account area became compromised [27].

In another aspect where the EVs can act as energy sellers or buyers to the local EAG, Yahaya et al. (2020) applied consortium blockchain to provide security and privacy for energy trading between entities. The ECDSA, SHA-256, and Boneh–Boyen short signature were used to initialize the system. The participating entities must register with the trusted authority (TA) to obtain their certificates and public/private-key pairs [36]. Similarly, Li and Hu (2019) proposed a V2V energy-trading system based on a consortium blockchain. The asymmetric encryption algorithm offers security, and a set of anonymous key pairs offers privacy. The scheme verifies the entity's signature to ensure mutual authentication between the EV and EAG, accordingly, and the EAG performs the V2V matching and preselects a charging pile for the matched pair. However, it does not provide a mechanism to mutually authenticate the arriving EVs [37].

One of the privacy-protection schemes is the k-anonymity technique, which depends on k EVs to confuse the adversary. Using this technique, Long et al. (2020) proposed a blockchain-based P2P energy-trading scheme to solve the location-privacy issue. The system entities (EVs and EAGs) must register with the TA to obtain their credentials (public/private-key pairs). The TA's signature on the entity's public key is used to verify its legality. However, both private-key generation and verification mechanisms threaten the system's security [38].

To hide trading patterns in EVs, a blockchain-based privacy-preserving approach was offered by Sadiq et al. (2021). They applied bilinear pairing and pseudonyms to provide security and privacy for the EV in a V2V energy-trading system. The demander EV requests energy trading from the roadside unit (RSU), which in turn authenticates the demander EV and assigns a token to its pseudo-ID. The RSU broadcasts the request to the pool of EVs, and the supplier EV that is willing to trade energy shall respond to it. The RSU plays the role of matcher between demander/supplier EVs and assigns token to them. Whenever they arrive at the scheduled charging pile, they authenticate themselves using these tokens. The scheme resists several attacks and provides privacy features such as anonymity and traceability (as the mapping between the EV's real and pseudo-identity is known by the TA only). However, the TA is responsible for the EV's private-key generation, which is not secure (if the TA is compromised, then it could lead to the compromise of all EVs). Moreover, the tokens used for authentication are generated by the RSU without both EVs' contributions, which allows other entities to gain access to the service [8].

Javed et al. (2021) proposed a V2V energy-trading scheme based on blockchain technology. Their scheme includes both public and private blockchain network characteristics. Therefore, it demands prior permission, making the network more secure and preventing malicious nodes from joining. They rely on the TA to issue the EV's unique identity and public/private-key pairs which could compromise the EV's security. The scheme uses the EV's identity to authenticate to the local EAG. However, this is insufficient as there are chances of identity theft (it is rather an identification mechanism than authentication). Hence, the system lacks initial security and privacy requirements in terms of mutual authentication and anonymity [39].

In the blockchain-enabled Internet of Vehicles (BIoV), Cui et al. (2020) introduced a vehicle-to-vehicle (V2V) energy-trading mechanism based on Bayesian game pricing to guarantee security, trustworthiness, and reliability. The scheme utilizes a certificate authority (CA) for entity registration (EVs and RSUs) and issues their credentials (certificates and public/private-key pairs). Entities prove their authenticity to each other using digital certificates [44].

Among all the security requirements, authentication stands out as the most important, considering it is the first line of defense against malicious attacks. Symmetric-key-based authentication and public-key-based authentication are the two types of authentication protocols. Asymmetric cryptography, commonly referred to as public cryptography, is a mechanism for encryption and decryption that uses a key pair, namely public/private keys [45]. On the other hand, symmetric-key cryptography relies on a single key that may be used for both encryption and decryption [46].

It has been proven that in symmetric-key-based authentication systems, such as in [32], simply using XOR and hash operations can provide mutual authentication to participating EVs. However, privacy preservation fails to ensure the EV's anonymity, traceability, and un-linkability. Moreover, there is no re-authentication mechanism to reduce communication overhead in the authentication process.

Furthermore, according to [47], the group-signature-authentication technique used in [38] has some limitations that need to be assessed during system design, including the distribution mechanism of the private key to the group of EVs, the requirement for the constant changing of the group's public/private-key pairs, and the key-management mechanism.

Anonymity, pseudonymity, and encryption technology are used in many security protection solutions in V2V networks today. Recent studies and protocols such as [8] used traditional procedures such as bilinear pairings to address the issue of anonymity. These solutions need a significant amount of processing power as well as a significant amount of communication overhead, both of which have a huge impact on the performance–security trade-off [48].

To provide security and anonymity, several blockchain-based electric-vehicle-charging solutions have been introduced. Studies [8,27,34,36,38–40] used a certificate to initially register and authenticate, but the EV's public/private-key pair is generated by the TA, which makes these schemes vulnerable to key-escrow attacks. Whilst blockchain is a promising technology for P2P energy trading, there are still several issues that need to be addressed before it can be widely adopted. These issues involve scalability and security as the number of individuals using P2P energy trading grows. There are also issues related to transaction and verification cost: only ten transactions per second can be processed via blockchain while VISA can process 20,000 transactions per second. Moreover, the individual's transaction fees and storage costs will raise the overall expense of the blockchain. Development cost, regularization, and government limitations are other issues that blockchain systems need to solve [49].

While authentication is an unavoidable prerequisite for secure communication on vehicular ad hoc networks (VANETs), privacy preservation is also a critical requirement that must not be overlooked. The ability of a person to selectively reveal information to specific people or organizations is known as privacy. During authentication, the EV's

name, address, location, and other information required to issue the certificate should not be exposed to anyone except the relevant authority, such as the CA/TA. As a result, the authentication mechanism must maintain the EV's privacy and privacy-preserving features such as location tracking, anonymity, un-linkability, and traceability [50].

Due to the resource constraints of IoT devices and the latency-critical nature of VANET applications, Ha et al. (2016) presented an implicit-authentication method based on ECQV. The ECQV implicit certificate is essential for mutual authentication, key generation, and key exchange between IoT devices. Through a computational test, they were able to show that traditional certificates are less suitable for use in resource-constrained IoT devices than ECQV implicit certificates [20]. The impact of authentication overhead in latency-critical apps on EV-driver safety, as well as the extent of this impact, were investigated in Baee et al.'s (2019) study. They also showed that verifying certificates using ECDSA and ECQV over the NIST P-256 curve is a practical solution [51].

Other essential privacy-preserving criteria in VANETs, such as un-linkability and traceability, were overlooked when the prior V2V-charging schemes were designed. Moreover, after observation, we found that the principle of token-based re-authentication for valid EVs in a limited amount of time had been neglected. To our knowledge, no study has used ECQV to authenticate EVs in V2V-charging systems, and we are the first to propose it. As a result, we introduce a lightweight ECQV-based authentication protocol for V2V-charging systems that ensure efficient and secure authentication, re-authentication, and ensure that EV's privacy is not violated.

4. Proposed System

The proposed authentication protocols that meet the solution requirements are presented in this section. The proposed system's focus on authentication as payment is outside the scope of this study. The notations used for this scheme's phases are listed in Table 1. The scheme phases are: (1) initialization, (2) registration, (3) authentication, and (4) charging.

Table 1. Notations.

Notations	Meaning
EV	Electric vehicle
EV_D/EV_S	Demander/Supplier electric vehicle
EAG	Energy aggregator
OP	Electricity operator
E_p	Elliptic curve (EC) over a finite field, where p is a large prime number
G	Base point in E_p with order n
id_{EV}, id_{EAG}	Real identity of EV/EAG
k_x, R_x	EC key pair for entity x
S_x	Private-key-construction data of entity x
$Cert_x$	Certificates of entity x
Sig_x (y)	Signing a message y with entity x's private key
PK_x (y)	Encrypting a message y with entity x's public key
A_x	Authenticator of entity x
AH_x	Hash of authenticator of entity x
T_x	Time stamp generated by x
TL	Time life
e	Hash of certificate
PK_x, PR_x	Public key/Private key for entity x
RK, RK′	Registration key between EV and OP/EAG and OP
Aid_i	i^{th} Anonymous identity of EV issued by OP
Aid_{No}	Counter of Aid_i, incremented by EV

N_x	Nonce generated by x
AT_{EV}^{EAG}	An authorization token, issued by EAG to EV
K_{EV-EAG}	Symmetric master key shared between EV and EAG
IK_{EV-EAG}	Symmetric initial key shared between EV and EAG
TK_{EV-EAG}	Symmetric temporary key shared between EV and EAG
SK_{EV-EAG}	Symmetric session key shared between EV and EAG
$H(.)$	One-way hash function
(y, x)	Concatenation operation

4.1. System Architecture

Our solution constitutes an electricity operator (OP), energy aggregator (EAG), electric vehicles (EVs), and smart meter. The proposed architecture is demonstrated in Figure 1, and the following list states the entities in our scheme:

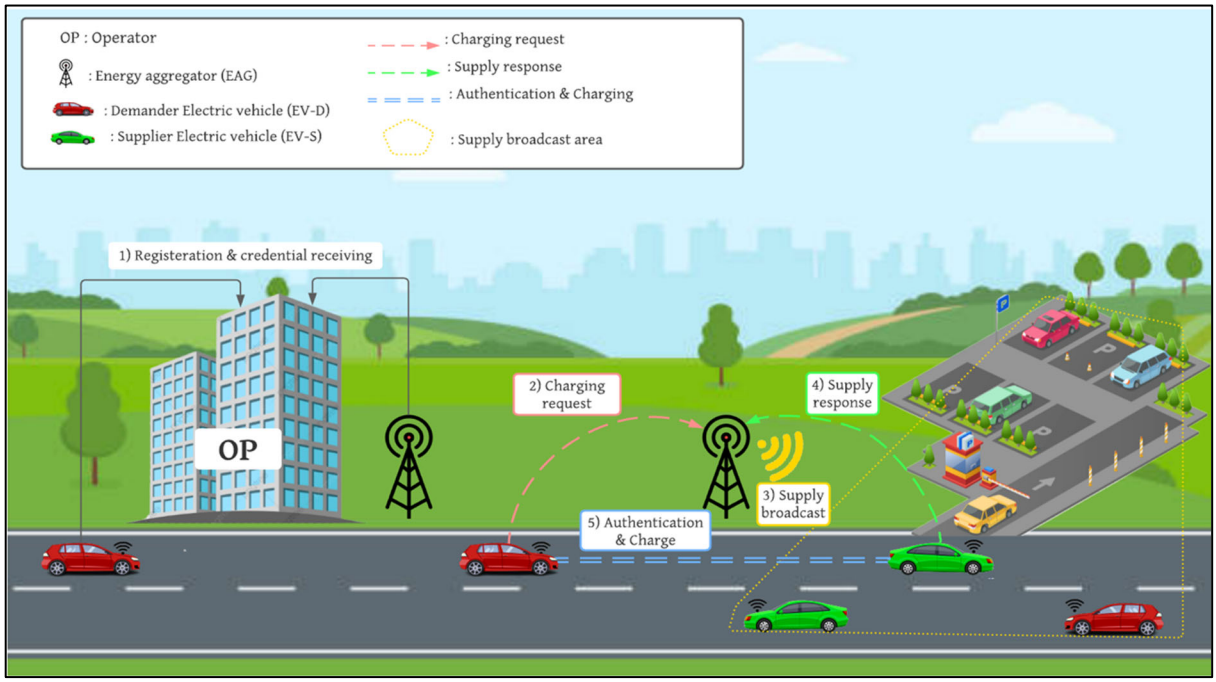

Figure 1. Proposed system architecture.

1. OP: Any entity (EV or EAG) attempting to join the V2V-charging system must register its identifying information via the OP, which is the initializer of the proposed protocol. Since the OP acts as a certificate producer (trusted third party), authorized EVs can acquire access to other EVs' energy-trading services and establish trust between them. Furthermore, the OP has the authority to reveal the identities of malicious or misbehaving entities.
2. EAG: A data aggregator is a smart device or a collection of connected devices that gathers an available EV's energy information during charging. It acts as an energy broker and matcher to handle V2V energy-trading requests. Additionally, it manages energy trading and offers wireless communication to EVs and EVCSs. The EAG has an authentication mechanism in place in order to identify authorized EVs and coordinate V2V charging.
3. EV: Electric vehicles are smart devices that submit charging requests to the EAG and mutually confirm the EV's legitimacy to use its services (charging). Depending on their energy needs, EVs act as either energy supplier (EV_S), demander (EV_D), or idle EV (do not participate in energy trading). EVs can interact with EAGs for energy

trading thanks to the onboard unit's (OBU) communication and computing capabilities. The EV_S offers its excess energy to other electric vehicles in need and receives an incentive in return. Moreover, when the EV_D demands energy, it makes a request to the local EAGs. We assume that the communication takes place in this environment via the dedicated-short-range-communication (DSRC) protocol, and the Internet and EV have a controlled-area-network (CAN) bus linked to the charging port.

4. Smart meter: It is a device that is used to keep track of and compute the amount of energy exchanged between energy nodes. According to smart-meter statistics, energy demanders pay the suppliers the corresponding amount. For the proposed solution, it is considered that each EV has a smart meter installed within the vehicle. We presume that the EV's smart meter has a tamper-resistant seal. We assume that the EAG is responsible for reading the traded energy from each EV's smart meter, and accordingly generates the payment method.

Without the OP's intervention, the EAG first verifies the EVs (EV_D/EV_S) through their A_{EV} signed by the OP and the Aid_i by the EV. Before EV_D/EV_S matching, the EAG authenticates both participants to prevent malicious vehicles from accessing the system. After successful matching and arriving at the scheduled location, the EV_S authenticates EV_D using the Aid_{i-D} token signed by the OP and EV_D. On the other hand, the EV_D authenticates EV_S using the Aid_{i-S} signed by the OP and EV_S in order to thwart impersonation attacks. The proposed approach uses ECQV, symmetry, and PKC to establish mutual authentication between EV_D/EV_S. The proposed solution allows the reuse of AT_D^S for effective re-authentication (similar to [52] and our previous study). The EV_S issues AT_D^S once it has authenticated EV_D. Using AT_D^S shortens the time it takes to verify Aid_{i-D} in a future charge request. The shortage of public EVCSs is the primary issue in the EV-charging infrastructure. EV owners can share (sell) their vehicle's excess energy with other EVs in need. In exchange, EV owners can gain incentives by sharing their energy with other EVs.

4.2. Initialization Phase

To set up the network, the OP performs system initialization, which is outlined below:

Step 1. The OP chooses the base point G on the elliptic curve E_p with order n, with n being a large prime number. It chooses the curve coefficients a and b, q for the field size and h for the cofactor, where hn is the elliptic curve's number of points (these are the domain parameters for an elliptic curve).

Step 2. A hash function that has been approved $H(.)$ is chosen. During the certificate-request/generation operations, the OP and certificate requester pick the random-number generator that will be used to generate the private keys.

Step 3. The elliptic curve domain parameters are coupled with an EC key pair (PR_{OP}, PK_{OP}) that the OP obtains (constructed in step 1).

Step 4. The EV and EAG acquire the EC domain parameters $H(.)$ and PK_{OP} (OP's public key) in an authentic manner.

4.3. Registration Phase

When an entity (EV or EAG) wishes to use the charging system, they must first create their identities and public/private-key pair. Afterwards, from the OP, they obtain the relevant certificate, authenticator, private-key-construction data, and anonymous identity (for EV only).

4.3.1. EV Registration

Figure 2 illustrates the EV-registration process, which is described in detail below:

Step 1: The EV picks its identity id_{EV} and creates an EC key pair (k_{EV}, R_{EV}), with k_{EV} ϵ_R $[1, \ldots, n-1]$ and $R_{EV} = k_{EV}.G$. To maintain integrity, it calculates $I_{EV} =$

$h(R_{EV}, id_{EV}, N_{EV})$, then encrypts $\{id_{EV}, R_{EV}, N_{EV}, I_{EV}\}$ with PK_{OP} (OP's public key) and sends it to the OP.

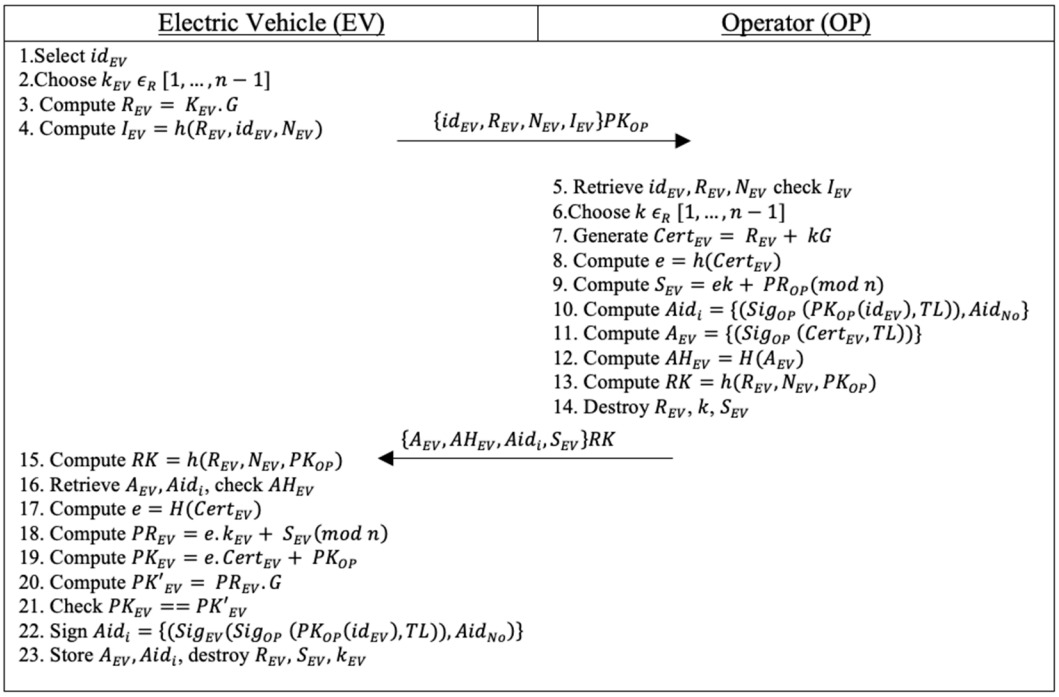

Figure 2. Proposed EV-registration phase.

Step 2: The OP uses its private key PR_{OP} to obtain the message's content and verifies I_{EV}. Then, it selects $k \epsilon_R [1, \dots, n-1]$ and constructs the implicit certificate for the EV ($Cert_{EV} = R_{EV} + kG$). It computes the hash of the certificate $e = h(Cert_{EV})$ and the EV's private-key-construction data $S_{EV} = ek + PR_{OP}(mod\ n)$. To produce the EV's pseudo-identity, the OP uses Formula (1) and signs it with the OP's private key, where the EV's real identity is hidden with PK_{OP} to ensure anonymity, and the pseudo-identity Aid_i is negotiated to be sequentially incremented (Aid_{No}) by the EV itself each time it demands a service. Using Formula (2), the OP computes the EV's authenticator, which contains the issued $Cert_{EV}$, Aid_i, as well as its time life (TL) signed by the OP's private key. To maintain integrity, it calculates $AH_{EV} = H(A_{EV})$. It then calculates a registration key (temporary key) $RK = h(R_{EV}, N_{EV}, PK_{OP})$ that is exclusively shared by the OP and EV. Then, it encrypts $\{A_{EV}, AH_{EV}, Aid_i, S_{EV}\}$ with RK and sends it to the EV. Finally, the OP should destroy R_{EV}, k, and S_{EV} to hinder the adversary from obtaining the EV's secret key.

$$Aid_i = \{\big(Sig_{OP}(PK_{OP}(id_{EV}), TL)\big), Aid_{No}\} \quad (1)$$

$$A_{EV} = \{Sig_{OP}(Cert_{EV}, TL, id_{OP}, PK_{OP}(id_{EV}))\} \quad (2)$$

Step 3: The EV calculates the shared registration key $RK = h(R_{EV}, N_{EV}, PK_{OP})$ to obtain A_{EV}, Aid_i, uses the OP's public key to verify them, and checks AH_{EV}. It computes $e = h(Cert_{EV})$, and uses Formulas (3) and (4) to construct its private/public-key pair PR_{EV}/PK_{EV}.

$$PR_{EV} = e.k_{EV} + S_{EV}(mod\ n) \quad (3)$$

$$PK_{EV} = e.Cert_{EV} + PK_{OP} \quad (4)$$

To confirm that PK_{EV} is valid, it computes $PK'_{EV} = PR_{EV}.G$ and then checks if $PK_{EV} == PK'_{EV}$ as follows:

$$PR_{EV} = e.k_{EV} + S_{EV}(mod\ n)$$

From step 18 of Figure 2

$$= e.k_{EV} + (e.k + PR_{OP}(mod\ n))$$

From step 9 of Figure 2

$$= e.(k_{EV} + k) + PR_{OP}(mod\ n)) \quad (5)$$

$$Cert_{EV} = R_{EV} + kG$$

From step 7 of Figure 2

$$= k_{EV}.G + k.G$$

From step 3 of Figure 2

$$= (k_{EV} + k).G \quad (6)$$

$$PK_{EV} = e.Cert_{EV} + PK_{OP}$$

From step 19 of Figure 2

$$= e.(k_{EV} + k).G + PR_{OP}.G$$

From Formula (6)

$$= e.((k_{EV} + k) + PR_{OP}).G$$

From Formula (5)

$$= PR_{EV}.G \quad (7)$$

Following the confirmation of $PK_{EV} == PK'_{EV}$, the EV signs Aid_i using its own private key. Lastly, the EV encrypts $\{A_{EV}, Aid_i\}$ with PK_{EV} and stores it in the onboard-unit (OBU) memory, and to thwart adversary acquisition of the EV's private key, the EV destroys R_{EV}, k_{EV}, and S_{EV}.

4.3.2. EAG Registration

Figure 3 illustrates the EAG-registration process, which is broken down as follows:

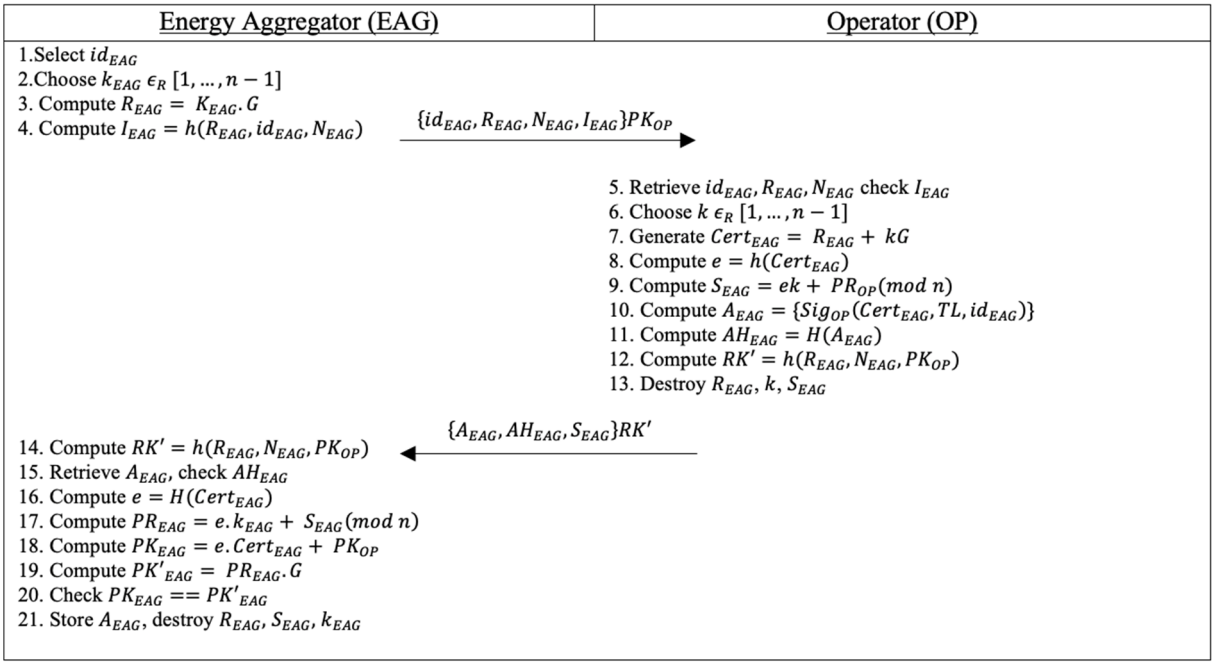

Figure 3. Proposed EAG-registration phase.

Step 1: The EAG picks its identity id_{EAG}, and creates the EC key pair (k_{EAG}, R_{EAG}) with $k_{EAG}\ \epsilon_R\ [1, \dots, n-1]$ and $R_{EAG} = k_{EAG}.G$. To maintain integrity, it calculates $I_{EAG} = h(R_{EAG}, id_{EAG}, N_{EAG})$. Then, it encrypts $\{id_{EAG}, R_{EAG}, N_{EAG}, I_{EAG}\}$ with PK_{OP} and sends it to the OP.

Step 2: The OP uses its private key PR_{OP} to obtain the message's content and verifies I_{EAG}. Then, it selects $k\ \epsilon_R\ [1, \dots, n-1]$ and constructs the implicit certificate for the EAG ($Cert_{EAG} = R_{EAG} + kG$). It computes the hash of the certificate $e = h(Cert_{EAG})$ and the EAG's private-key-construction data $S_{EAG} = ek + PR_{OP}(mod\ n)$. Using Formula (8), the OP computes the EAG's authenticator, which contains the issued $Cert_{EAG}$, id_{EAG}, as well as its time life (TL) signed by the OP's private key. To maintain integrity, it calculates $AH_{EAG} = H(A_{EAG})$. Then, it calculates a registration key (temporary key) $RK' = h(R_{EAG}, N_{EAG}, PK_{OP})$ that is exclusively shared by the OP and EAG. Then, it encrypts $\{A_{EAG}, AH_{EAG}, S_{EAG}\}$ with RK' and sends it to the EAG. Finally, the OP should destroy R_{EAG}, k, and S_{EAG} to hinder an adversary from obtaining the EAG's secret key.

$$A_{EAG} = \{(Sig_{OP}(Cert_{EAG}, TL, id_{EAG})\} \quad (8)$$

Step 3: The EAG calculates the shared registration key $RK' = h(R_{EAG}, N_{EAG}, PK_{OP})$ to obtain A_{EAG}, uses the OP's public key to verify it, and checks AH_{EAG}. It computes $e = h(Cert_{EAG})$ and uses Formulas (9) and (10) to construct its private/public-key pair PR_{EAG}/PK_{EAG}.

$$PR_{EAG} = e.k_{EAG} + S_{EAG}(mod\ n) \quad (9)$$

$$PK_{EAG} = e.Cert_{EAG} + PK_{OP} \quad (10)$$

To confirm that PK_{EAG} is valid, it computes $PK'_{EAG} = PR_{EAG}.G$, then checks if $PK_{EAG} == PK'_{EAG}$ as follows:

$$PR_{EAG} = e.k_{EAG} + S_{EAG}(mod\ n)$$

From step 17 of Figure 3

$$= e.k_{EAG} + (e.k + PR_{OP}(mod\ n))$$

From step 9 of Figure 3

$$= e.(k_{EAG} + k) + PR_{OP}(mod\ n)) \quad (11)$$

$$Cert_{EAG} = R_{EAG} + kG$$

From step 7 of Figure 3

$$= k_{EAG}.G + k.G$$

From step 3 of Figure 3

$$= (k_{EAG} + k).G \quad (12)$$

$$PK_{EAG} = e.Cert_{EAG} + PK_{OP}$$

From step 18 of Figure 3

$$= e.(k_{EAG} + k).G + PR_{OP}.G$$

From Formula (12)

$$= e.((k_{EAG} + k) + PR_{OP}).G$$

From Formula (11)

$$= PR_{EAG}.G \quad (13)$$

Following the confirmation of $PK_{EAG} == PK'_{EAG}$, the EAG encrypts $\{A_{EAG}\}$ with PK_{EAG} and stores it in memory, and to thwart adversary acquisition of the EAG's private key, the EAG destroys R_{EAG}, k_{EAG}, and S_{EAG}.

4.4. Authentication Phase

Whenever an EV wants to use the V2V-charging system, the EV_D and EV_S must authenticate each other and establish a session key. The authentication process can be divided into two categories: First is the mutual authentication, for which the EV_D and EV_S have not yet built trust between them. As a result, they rely on information provided by a third source that they can trust (OP). Second is lightweight re-authentication, in which the EV_D and EV_S authenticate each other without the involvement of a third party (OP).

4.4.1. Mutual-Authentication Protocol

The mutual-authentication process is initially conducted once, whereby the EV_S depends on the OP's information to authenticate the EV_D, unless Aid_{i-D} is expired. The procedure is illustrated in Figure 4, and is as follows:

Step 1: The EV_D generates the charging request $CH_{EV} = Sig_{EV-D}(amount_D, price_D, distance_D, TL)$, a random number N_{EV-D}, and a time stamp T_{EV-D}, where "$amount_D$" states the amount of power needed, "$price_D$" states the price EV_D is willing to pay for the traded energy, and "$distance_D$" states EV_D's distance from the local EAG in order to maintain its current location privacy. To obtain a unique anonymous identity for the session, the EV_D sequentially increments the Aid_{i-D} counter (adds 1 to the previous EV_D's pseudo-ID) and hashes it. The EV_D signs CH_{EV} using its private key, encrypts $\{CH_{EV-D}, A_{EV-D}, Aid_{i-D}, N_{EV-D}, T_{EV-D}\}$ with PK_{EAG}, and sends it to the local EAG.

Step 2: The EAG decrypts the message using its own private key PR_{EAG} to retrieve the content. It uses the OP's signature to verify A_{EV-D} and checks T_{EV-D} to ensure it is not a replayed message. Then, it computes $e_{EV-D} = h(Cert_{EV-D})$ to extract the EV_D's public key $PK_{EV-D} = e_{EV-D}.Cert_{EV-D} + PK_{OP}$. It verifies Aid_{i-D} by EV_D's signature along with the OP's signature. After verification, the EAG generates a supply request $SB_{EV} = Sig_{EAG}(amount_D, price_D, TL)$ and broadcasts it to nearby EVs.

Step 3: Nearby EVs that receive the SB_{EV} verify the supply request through the EAG's signature, and EVs with excess energy that are interested in selling it to other EVs generate a random number N_{EV-S}, a time stamp T_{EV-S}, and $RSP_{EV-S} = Sig_{EV-S}(amount_S, price_S, TL)$, where "$amount_S$" is the amount of energy EV_S is offering to sell, and "$price_S$" states the price that EV_S is demanding for the traded energy. The EV_S signs RSP_{EV-S} using its private key and encrypts $\{A_{EV-S}, Aid_{i-S}, N_{EV-S}, T_{EV-S}, RSP_{EV-S}\}$ with PK_{EAG}, then sends it to the local EAG.

Step 4: The EAG decrypts the message using its own private key PR_{EAG} to retrieve the content. Then, it uses the OP's signature to verify A_{EV-S} and checks T_{EV-S} to ensure it is not a replayed message. It computes $e_{EV-S} = h(Cert_{EV-S})$ to extract the EV_S's public key $PK_{EV-S} = e_{EV-S}.Cert_{EV-S} + PK_{OP}$. It verifies Aid_{i-S} by the EV_S's signature along with OP's signature. The EAG matches EV_D to the best-fit EV_S and schedules a V2V-charging location (Loc_{D-S}) for them. After matching, the EAG computes X_{EV} and temporary keys TK_{EV-EAG} for both sides. For EV_D, the EAG computes $X_{EV-D} = h(PK_{EV-S}, N_{EV-S}, T_{EV-S})$ to be further used in the EV_D/EV_S mutual authentication, and computes $TK_{EV-D-EAG} = h(id_{EAG}, N_{EV-D}, T_{EV-D})$ to protect the transmission of $\{PK_{EV-S}, X_{EV-D}, Aid_{i-S}, Loc_{D-S}\}$ to EV_D. For EV_S, the EAG compute $X_{EV-S} = h(PK_{EV-D}, N_{EV-D}, T_{EV-D})$ to be further used in EV_D/EV_S mutual authentication, and computes $TK_{EV-S-EAG} = h(id_{EAG}, N_{EV-S}, T_{EV-S})$ to protect the transmission of $\{PK_{EV-D}, X_{EV-S}, Aid_{i-D}, Loc_{D-S}\}$ to EV_S.

Step 5: Both EV_S/EV_D generate their corresponding temporary keys TK_{EV-EAG} to retrieve the content of the message. EV_D retrieves the matched EV_S's public key and verifies its Aid_{i-S} by the EV_S's signature and PK_{EV-S} that is included in it along with the OP's signature. When both EV_S and EV_D arrive at the specified location (Loc_{D-S}), EV_D generates a new random number N'_{EV-D} and time stamp T'_{EV-D}. It then generates the shared master key K_{EV-D_S} and the first initial key IK_{EV-D-S} using Formulas (14) and (15), respectively. Then, it encrypts $\{Aid_{i-D}, N'_{EV-D}, T'_{EV-D}\}$ with IK_{EV-D-S} and sends it to EV_S over DSRC.

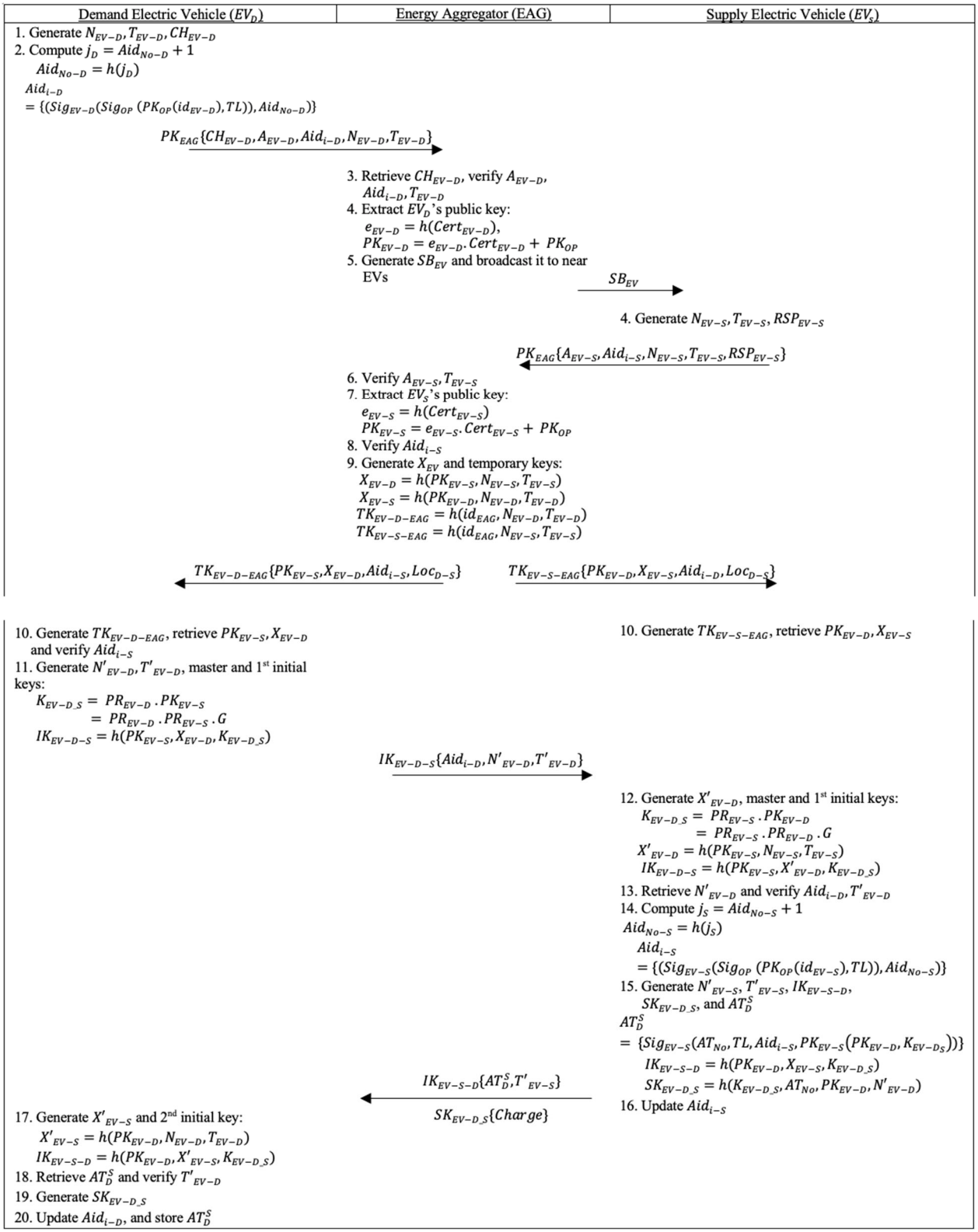

Figure 4. Proposed V2V mutual-authentication protocol.

$$K_{EV-D\_S} = PR_{EV-D}.PK_{EV-S} = PR_{EV-D}.PR_{EV-S}.G \quad (14)$$

$$IK_{EV-D-S} = h(PK_{EV-S}, X_{EV-D}, K_{EV-D\_S}) \quad (15)$$

Step 6: EV_S generates $X'_{EV-D} = h(PK_{EV-S}, N_{EV-S}, T_{EV-S})$, the master key K_{EV-D_S} and the first initial key IK_{EV-D-S} using Formulas (14) and (15), respectively. It retrieves N'_{EV-D} and verifies Aid_{i-D} by EV_D's signature along with the OP's signature, and checks the validity of T'_{EV-D} to ensure it is not a replayed message. To obtain a unique anonymous identity for this session, EV_S sequentially increments the Aid_{i-S} counter (adds 1 to the previous EV_S's pseudo-ID) and hashes it. After verification, EV_S generates a new random number N'_{EV-S}, a time stamp T'_{EV-S}, and the second initial key IK_{EV-S-D} using Formula (16). EV_S generates AT_D^S, which is the authorization token for EV_D, and the session key SK_{EV-D_S} using Formulas (17) and (18), respectively. Then, it sends it to EV_D $\{AT_D^S, T'_{EV-S}\}$ encrypted by IK_{EV-S-D}, and begins the V2V-charging service for EV_D, which is protected by SK_{EV-D_S}. Lastly, it updates the Aid_{i-S} in the memory.

$$IK_{EV-S-D} = h(PK_{EV-D}, X_{EV-S}, K_{EV-D\_S}) \quad (16)$$

$$AT_D^S = \{Sig_{EV-S}(AT_{No}, TL, Aid_{i-S}, PK_{EV-S}(PK_{EV-D}, K_{EV-D_S}))\} \quad (17)$$

$$SK_{EV-D\_S} = h(K_{EV-D\_S}, AT_{No}, PK_{EV-D}, N'_{EV-D}) \quad (18)$$

Step 7: EV_D generates $X'_{EV-S} = h(PK_{EV-D}, N_{EV-D}, T_{EV-D})$ and the second initial key IK_{EV-S-D} using Formula (16) to retrieve AT_D^S, and checks the validity of T'_{EV-S}. Then, using Formula (18), it generates the session key to be used during the charging session. Lastly, it stores the AT_D^S issued by EV_S and updates the Aid_{i-S} in the memory. By the completion of this procedure, EV_S and EV_D will have a trust relationship established and will no longer need to rely on the OP for future session authentication.

4.4.2. Lightweight Mutual-Re-Authentication Protocol

As previously stated, at this point, EV_S and EV_D should have built a relationship of trust. They can now immediately authenticate each other in future V2V-charging services. This phase (re-authentication phase) can only be used when the EV_D has a valid AT_D^S and has been scheduled for the same EV_S within the last 12 h. Moreover, recalculating all the parameters for a new session key when the user is already trusted is wasteful and time- and energy-consuming. Due to EV mobility, EV_D utilizes its local EAG to match its V2V request. If the previous EV_S is available and within the EAG's area, EV_S and EV_D shall be matched. The following is a full description of the process of effective re-authentication as shown in Figure 5:

Step 1: EV_D generates the charging request $CH_{EV} = Sig_{EV-D}(amount_D, price_D, distance_D, TL, Aid_{i-S})$, a random number N_{EV-D}, and a time stamp T_{EV-D}, where "$amount_D$" states the amount of power needed, "$price_D$" states the price EV_D is willing to pay for the traded energy, and "$distance_D$" states EV_D's distance from the local EAG in order to maintain its current location privacy. To obtain a unique anonymous identity for this session, EV_D sequentially increments the Aid_{i-D} counter (adds 1 to the previous EV_D's pseudo-ID) and hashes it. However, since EV_D has a valid authorization token AT_D^S, this time it includes the Aid_{i-S} of the corresponding EV_S in the request. EV_D signs CH_{EV} using its private key and encrypts $\{CH_{EV-D}, A_{EV-D}, Aid_{i-D}, N_{EV-D}, T_{EV-D}\}$ with PK_{EAG}, then sends it to the local EAG.

Step 2: The EAG decrypts the message using its own private key PR_{EAG} to retrieve the content. Then, it uses the OP's signature to verify A_{EV-D}, and checks T_{EV-D} to ensure it is not a replayed message. It computes $e_{EV-D} = h(Cert_{EV-D})$ to extract EV_D's pub-

lic key $PK_{EV-D} = e_{EV-D}.Cert_{EV-D} + PK_{OP}$. Next, it verifies Aid_{i-D} by EV_D's signature along with the OP's signature. The EAG checks if the specified EV_S is available within its area. After verification, the EAG generates a supply request $SB_{EV} = Sig_{EAG}(amount_D, price_D, TL)$ and sends it to that EV_S.

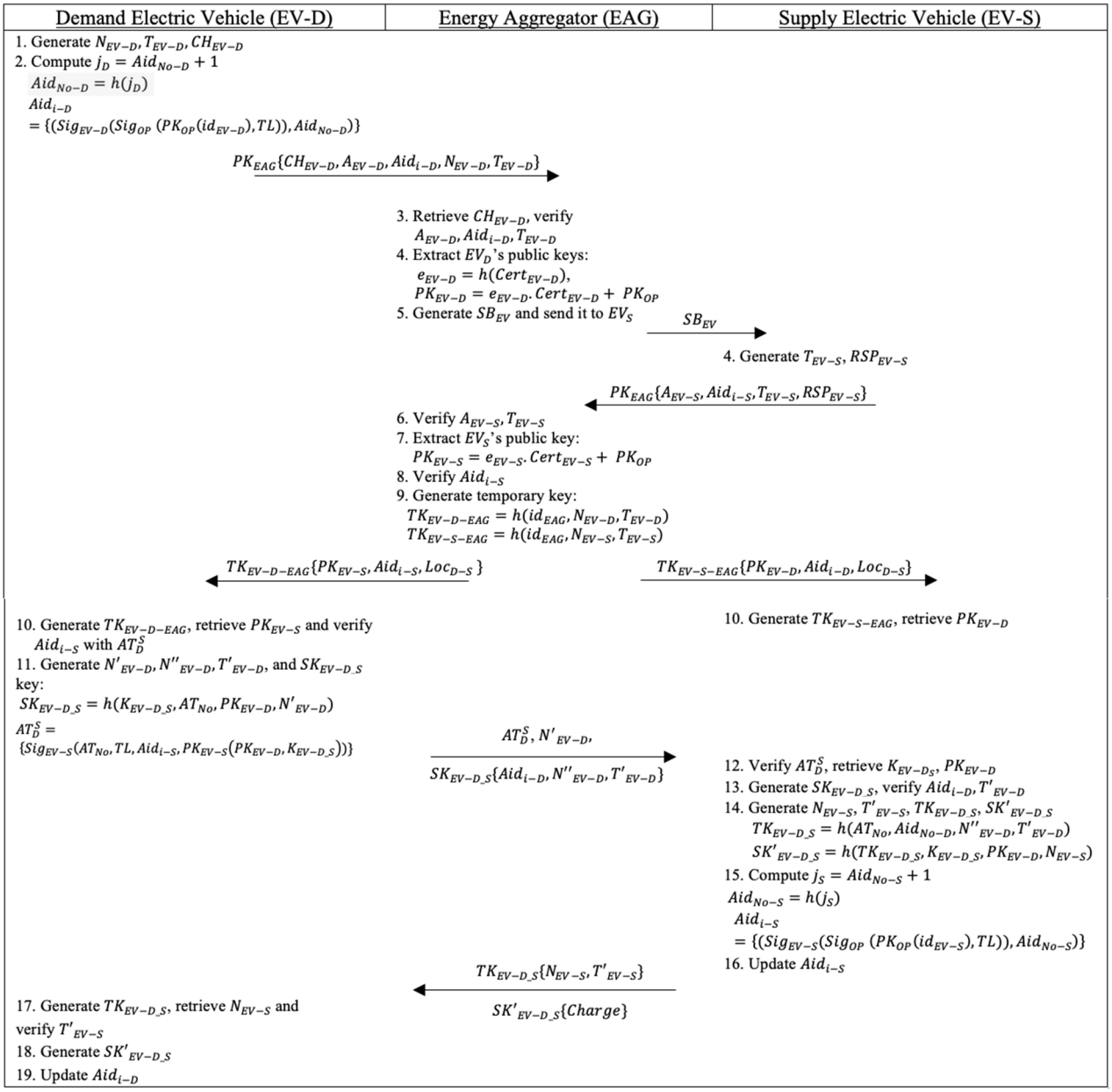

Figure 5. Proposed V2V mutual-re-authentication protocol.

Step 3: The EV_S that received the SB_{EV} verifies the supply request through the EAG's signature, and if the EV_S has excess energy and is interested in selling it to the other EV_D, then it generates a time stamp T_{EV-S} and $RSP_{EV-S} = Sig_{EV-S}(amount_S, price_S, TL)$, where "$amount_S$" is the amount of energy EV_S is offering to sell, and "$price_S$" states the price EV_S is demanding for the traded energy. EV_S signs RSP_{EV-S} using its private key and encrypts $\{A_{EV-S}, Aid_{i-S}, T_{EV-S}, RSP_{EV-S}\}$ with PK_{EAG}, then sends it to the local EAG.

Step 4: The EAG decrypts the message using its own private key PR_{EAG} to retrieve the content. Then, it uses the OP's signature to verify A_{EV-S}, and checks T_{EV-S} to ensure it is not a replayed message. It computes $e_{EV-S} = h(Cert_{EV-S})$ to extract EV_S's public

key $PK_{EV-S} = e_{EV-S}.Cert_{EV-S} + PK_{OP}$. Next, it verifies Aid_{i-S} by EV_S's signature along with the OP's signature. The EAG matches EV_D to EV_S and schedules a V2V-charging location (Loc_{D-S}) for them. After matching, the EAG computes temporary keys TK_{EV-EAG} for both sides. For EV_D, the EAG computes $TK_{EV-D-EAG} = h(id_{EAG}, N_{EV-D}, T_{EV-D})$ to protect the transmission of $\{PK_{EV-S}, Aid_{i-S}, Loc_{D-S}\}$ to EV_D. For EV_S, the EAG compute $TK_{EV-S-EAG} = h(id_{EAG}, N_{EV-S}, T_{EV-S})$ to protect the transmission of $\{PK_{EV-D}, Aid_{i-D}, Loc_{D-S}\}$ to EV_S.

Step 5: Both EV_S/EV_D generate their corresponding temporary keys TK_{EV-EAG} to retrieve the content of the message. EV_D retrieves the matched EV_S's public key and verifies its Aid_{i-S} with the one included within AT_D^S. When both EV_S and EV_D arrive at the specified location (Loc_{D-S}), EV_D generates new random numbers, N'_{EV-D} and N''_{EV-D}, and computes the previous session key using Formula (18), to be used in $Aid_{i-D}, N''_{EV-D}, T'_{EV-D}$ encryption, and sends AT_D^S, N'_{EV-D}, and $SK_{EV-D\_S}\{Aid_{i-D}, N''_{EV-D}, T'_{EV-D}\}$ to EV_S over DSRC.

Step 6: EV_S verifies the validity of AT_D^S through the signature Sig_{EV-S} using PK_{EV-S} and TL. It decrypts the AT_D^S using PR_{EV-S} to retrieve PK_{EV-D}, K_{EV-D_S}. EV_S needs to compute SK_{EV-D_S} to obtain $Aid_{i-D}, N''_{EV-D}, T'_{EV-D}$, and to ensure that the AT_D^S was sent by the authorized EV_D. To obtain a unique anonymous identity for this session, EV_S sequentially increments the Aid_{i-S} counter (adds 1 to the previous EV_S's pseudo-ID) and hashes it. Then, it uses $AT_{No}, Aid_{No-D}, N''_{EV-D}, T'_{EV-D}$ to generate the temporary key TK_{EV-D_S} using Formula (19). It then generates N_{EV-S}, T'_{EV-S}, and a new session key SK'_{EV-D_S} such as in Formula (20). EV_S then sends $\{N_{EV-S}, T'_{EV-S}\}$ encrypted by TK_{EV-D_S} to EV_D and begins the V2V-charging service for EV_D, which is protected by SK'_{EV-D_S}. Lastly, it updates the Aid_{i-S} in the memory.

$$TK_{EV-D\_S} = h(AT_{No}, Aid_{No-D}, N''_{EV-D}, T'_{EV-D}) \quad (19)$$

$$SK'_{EV-D\_S} = h(TK_{EV-D\_S}, K_{EV-D\_S}, PK_{EV-D}, N_{EV-S}) \quad (20)$$

Step 7: EV_D generates the TK_{EV-D_S} to retrieve N_{EV-S} and verifies T'_{EV-S}. Then, it generates SK'_{EV-D_S} using Formula (20), to be used during the charging session, and updates Aid_{i-D}.

4.5. V2V-Charging Phase

After successful authentication, EV_D connects with the OBU through the CAN bus to unlock the vehicle's charging port. EV_S now plugs its vehicle to EV_D and begins charging it. The CHAdeMO protocol, which is utilized by Nissan, Toyota, and others, is an example of how to conduct V2V charging after authentication [53]. The EV_S can use CHAdeMO to initiate and control the charging energy-transfer process by interacting with the EV_D over the CAN bus. EV_D acts as if it is linked to a fast-charging station when it is using this protocol. When the EV_D stops charging, the operation is finished. Our proposed scheme focuses on providing a secure authentication mechanism for V2V-charging systems. Hence, we assume that payment might be handled by other schemes since it is beyond our scope.

4.6. Revocation Protocol

The proposed scheme includes a revocation technique to protect entities from impersonation and MITM attacks, as well as to notify them that a parameter is no longer trustworthy, even before its validity period expires. Due to EV mobility and the short lifetime of AT_D^S (12 h and can only be used once), it is hard to revoke it. However, the Aid_i token is revoked if the EV suspects it was stolen by an adversary. The procedure for revocation of Aid_i is as follows:

Step 1: The EV creates the revocation request for Aid_i 's, $Rev_{EV-id} = \{PK_{OP}(Sig_{EV}, Aid_i, RevAid, T_{EV})\}$, uses the OP's public key PK_{OP} to encrypt it, and forwards it to the OP.

Step 2: The OP uses its private key PR_{OP} to decrypt the revocation request, then verifies Sig_{EV} using PK_{EV} and Sig_{OP}, which is within Aid_i. The OP should also check whether T_{EV} is valid in order to avoid a replay attack. Finally, the OP changes the status of Aid_i to revoked. Because the EV's signature is required, the adversary cannot create a fake revocation request.

5. Security Analysis

In this section, we discuss the security analysis of the proposed protocol and carry out informal analysis.

5.1. Informal Security Analysis

The proposed protocol is examined to prove that it meets the design solution requirements.

5.1.1. Mutual Authentication

In the authentication phase, the EV_D can ensure that it interacts with the legitimately matched EV_S through the validation of the OP's and EV_S signatures on the Aid_{i-S}, which is forwarded by the EAG after verification, and through the second initial key IK_{EV-S-D}, which is constructed by EV_D's parameter (N_{EV-D}, T_{EV-D}) and submitted to the EAG for a charging request. The EV_S can also validate EV_D by the OP's and EV_D signatures on the Aid_{i-D}, which is forwarded by the EAG after verification, and by the first initial key IK_{EV-D-S}, which is constructed by EV_S's parameter (N_{EV-S}, T_{EV-S}) and submitted to the EAG for a trading response. Unlike [37], where they either settled for EV and EAG mutual authentication and did not allow authentication between arriving EVs, or [39], where they used the EV's identity for authentication purposes (it is rather an identification mechanism than authentication), our proposed protocol ensures mutual authentication for both EV/EAG and EV/EV interactions.

5.1.2. Anonymity

Both the EV_D/EV_S real identities id_{EV} are concealed and encrypted by the OP's public key $PK_{OP}(id_{EV})$ within the Aid_i, which is created during the registration stage; only the OP has authority to access it in the case of necessity. Hence, id_{EV} cannot be disclosed by either the EAG or any other party (EVs), unlike in [32,39], where they used the EV's real identity for V2V authentication .

5.1.3. Un-Linkability

Both EV_D/EV_S will have an automatically updated anonymous identity Aid_i for each charging session. As the Aid_i is issued by the OP, each V2V-charging request from EV_D sequentially increments the previous Aid_i (adds 1), unlike [8,32], where they either used the EV's real identity or the same pseudo-ID for every new charging request. These strategies allow the adversary to track and compromise the privacy of the targeted EV. However, the proposed protocol sessions cannot be linked to each other as they hold different identities. However, as the proposed protocol utilizes different identities for each session, it thwarts the linkage attacks (cannot be linked together).

5.1.4. Traceability

Even though the real identity of the EV is concealed through encryption $PK_{OP}(id_{EV})$, the OP is the only entity in the scheme that can reveal id_{EV}, so as to maintain the order in the system. In the case of a malicious or misbehaving EV, there is a necessity for id_{EV} disclosure. To secure the system and to function as required by all parties, anonymity

should not be absolute, unlike in [38], where they utilized the k-anonymity technique to solve location-privacy issues. However, this technique prevents the TA from knowing the identity of malicious EVs. Our proposed protocol ensures the EV's anonymity, but at the same time gives the OP the ability to trace it if necessary.

5.1.5. Forward/Backward Security

In the event that an adversary obtains any SK_{EV-D_S}, the confidentiality of future/old session keys (SK_{EV-D_S}) should not be compromised. For the authentication phase, dynamic session keys are created, which comprise a unique random number N'_{EV-D}. A symmetric initial key (IK_{EV-D-S}) protect the transmission of N'_{EV-D}. For the re-authentication phase, SK'_{EV-D_S} contains a unique random number N_{EV-S}. A symmetric temporary key (TK_{EV-D_S}) protects the N_{EV-S}, which dynamically updates with a new unique random number N''_{EV-D} in every new session. Moreover, since the shared master key $K_{EV-\mathrm{D\_S}}$ is a long-lasting key (generated from the participant's PK_{EV} and PR_{EV}), it is eliminated from the encryption of any transmitted message between EV_D/EV_S. Each session generates a unique session key; if an adversary can deduce a session key, that key is only legitimate for the current communication. As a result, the proposed protocol ensures both forward and backward security, unlike other schemes such as in [36,44], where they obtained their public/private-key pair from the TA, which threatens the secrecy of their long-term keys and the security of their sessions.

5.1.6. Joint Key Control

The session key SK_{EV-D_S} of the authentication phase and the new session key SK'_{EV-D_S} for re-authentication, including random numbers N, are created by both parties (EV_D/EV_S) without the assistance of other parties, even the OP. Moreover, the shared master key $K_{EV-\mathrm{D\_S}}$ is created from the combination of both parties' (EV_D/EV_S) private and public keys, therefore only these two parties can obtain the master key. Thus, the proposed protocol allows for cooperative key control, unlike [8,39], where the session key is issued by the RSU or TA.

5.1.7. Non-Repudiation

The demand and supply requests (CH_{EV-D}, SB_{EV}, RSP_{EV-S}) are signed by the sender. As the sender's signature is needed, participating entities cannot deny the delivery of these requests. Moreover, an adversary cannot generate fake requests as a signature is required.

5.1.8. Effective Re-Authentication

To reduce the required amount of time spent and to minimize the cost each time EV_S re-authenticates EV_D, it issues an authorization token (AT_D^S) with a lifetime of 48 h and a single usage. For initial authentication, EV_S depends on the information provided by the OP (trusted third party) to authenticate EV_D once at the first encounter. After that, EV_S can directly authenticate EV_D without reliance on the OP's information, as long as it holds a valid AT_D^S (valid for one use only), unlike the previous schemes [8,27,32–40]. Hence, the proposed protocol allows both parties to establish full trust between them (EV_D/EV_S).

5.1.9. Revocation Functionality

To prevent an adversary from misusing stolen token Aid_i, or if the EV suspects its Aid_i has been stolen, it can use the revocation protocol to notify OP. Additionally, the token will be regarded as revoked if the EV reports to the OP to revoke its Aid_i. The pseudonyms supplied by the service provider were not revocable in related works.

5.1.10. Resist MITM/Replay Attack

In case an adversary acquires A_{EV-D}, the EV_D private key is needed to produce the shared master key (K_{EV-D_S}) for EV_S authentication to be successful. On the other hand, if the adversary acquires AT_D^S, the possibility to retrieve the master key (K_{EV-D_S}) is zero, as it is included within AT_D^S and encrypted using the EV_S public key. As a result, without K_{EV-D_S}, the adversary will be unable to produce the session key necessary for an MITM attack. Furthermore, in each communication between the parties, random time stamps and numbers are transmitted to ensure that previous sessions cannot be replayed. Therefore, the proposed protocol protects against replay attacks.

5.1.11. Resist Impersonation Attack

The solution tokens A_{EV}, Aid_i or AT_D^S cannot be generated by an adversary with the EV or OP name since they require the issuer's signature. Since the issuer's signature needs to be verified, the A_{EV}, Aid_i and AT_D^S counterfeit is doubtful. Therefore, the proposed protocol prevents an adversary from launching impersonation attacks.

6. Comparison with Related Schemes

In this section, the proposed scheme is compared to similar systems in terms of security and functionality, as well as computational cost. These are recent V2V-charging-system schemes that emphasize secure EV-to-EV communication.

6.1. Security and Functional-Feature Comparison

Table 2 summarizes the evaluation of the proposed system's security and functional aspects as well as those of related systems. The solutions in [8,27,34,38–40] are vulnerable to well-known attacks. Additionally, the solutions in [8,27,32,36–40] are inappropriate for V2V charging because they lack critical security and privacy features such as forward security, un-linkability, traceability, and effective re-authentication. In [32,35], more messages are required, which raises the communication channel's overhead. In comparison to previous studies, our proposed scheme meets all the solution requirements.

Table 2. Security feature comparison of proposed protocols and other related works.

Feature/Approach	**Sadiq et al. [8]**	**Sun et al. [27]**	**Roberts et al. [32]**	**Aitzhan and Svetinovic [33]**	**Kang et al. [34]**	**Chaudhary et al. [35]**	**Yahaya et al. [36]**	**Li and Hu [37]**	**Long et al. [38]**	**Javed et al. [39]**	**Cui et al. [44]**	**Proposed**
	2021	2020	2017	2016	2017	2019	2020	2019	2020	2021	2020	2022
Mutual Authentication	✓	✓	✓	✓	✓	✓	✓	×	✓	×	✓	✓
Forward security	×	×	✓	✓	×	×	×	×	×	×	×	✓
Anonymity	✓	×	×	✓	✓	×	×	✓	✓	×	✓	✓
Resist replay attack	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓
Resist impersonation attack	✓	×	✓	✓	✓	✓	✓	✓	×	✓	✓	✓
Resist MITM attack	×	×	✓	✓	×	✓	✓	✓	✓	×	×	✓
Un-linkability	×	×	×	✓	✓	✓	✓	✓	×	×	×	✓
Traceability	✓	✓	×	✓	✓	✓	✓	✓	×	✓	×	✓
Effective Re-authentication	×	×	×	×	×	×	×	×	×	×	×	✓
Revocation method	×	×	×	×	×	×	×	×	×	×	×	✓
Joint key control	×	×	×	×	×	×	×	×	×	×	×	✓
Non-Repudation	✓	✓	×	✓	×	✓	✓	✓	✓	✓	✓	✓
Number of Messages (EV)	2	1	5	2	2	3	1	1	1	2	1	2

6.2. Computational Cost Comparison

This section calculates the authentication protocols' computing overhead based on all the operations provided by the protocols. The EAG has sufficient capabilities to conduct all needed processes due to its high degree of performance. Contrary to the EAG, the EV's memory and computational resources are limited. Therefore, we must concentrate on the cost of EV computation. The time calculations are based on [54,55], as they stated that a one-way hash function (T_h) takes $\approx$ 0.0023 milliseconds (ms), the elliptic-curve encryption ($T_{enc-ecc}$) takes $\approx$ 0.43 ms, the symmetric encryption (T_{sym}) takes $\approx$ 0.0046 ms, the scalar multiplication (T_{sm}) takes $\approx$ 2.226 ms, and modular exponentiation (T_{me}) takes $\approx$ 3.85 ms. Table 3 presents a summary of the timing operations. The computational costs of the proposed protocol and related works are compared in Table 4 and Figure 6.

Table 3. Operation's Timing [54,55].

Notation/ Operation	$T_{enc-ecc}$/ Elliptic-Curve Encryption	T_h/hash	T_{sym}/ Symmetric	T_{sm}/ Scalar Multiplication	T_{me}/Modular Exponentiation
Time (ms)	0.43	0.0023	0.0046	2.226	3.85

Table 4. Computational-cost comparison.

Approach/Efficiency Feature	Computational Cost of EV	
	Authentication Phase	Re-Authentication Phase
Roberts et al. 's scheme [32]	$T_{me} + 3T_h \approx 3.8569\ ms$	$T_{me} + 3T_h \approx 3.8569\ ms$
Proposed scheme	$T_{enc-ecc} + 5T_h + 4T_{sym} + 2T_{sm} \approx 1.3439\ ms$	$T_{enc-ecc} + 4T_h + 4T_{sym} \approx 0.4576\ ms$

In Roberts et al.'s scheme [32], the authentication phase of the EVs takes $\approx$ 3.8569 ms ($T_{me} + 3T_h$). The proposed protocol requires $\approx$ 1.3439 ms ($T_{enc-ecc} + 5T_h + 4T_{sym} + 2T_{sm}$), and it provides better security and privacy preservation for the EV as well as a 65% improvement in computational cost. For the re-authentication process of the EV, the proposed protocol requires $\approx$ 0.4576 ms ($T_{enc-ecc} + 4T_h + 4T_{sym}$), while Roberts et al.'s scheme [32] requires $\approx$ 3.8569 ms ($T_{me} + 3T_h$). Hence, the proposed re-authentication protocol's computational cost is roughly 88% lower than the earlier protocol. Given the capabilities of the EV, it is evident that the proposed protocol outperforms the previous protocol.

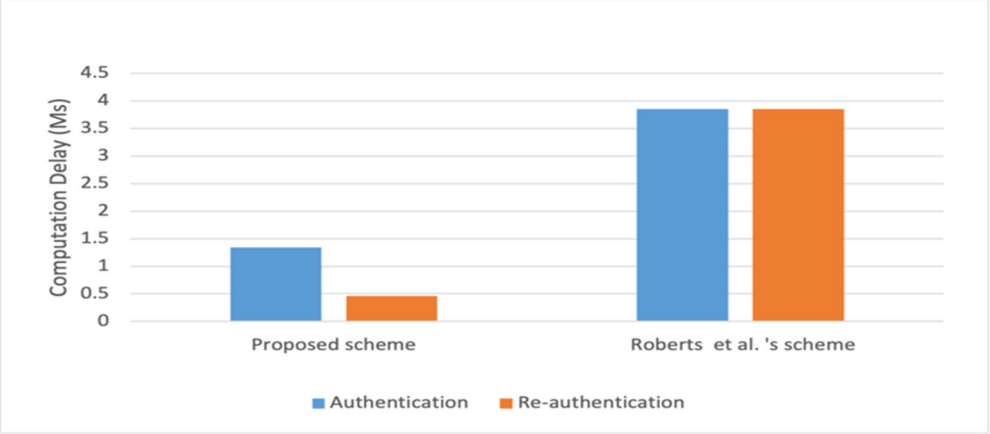

Figure 6. EV's authentication computational comparison among different protocols.

6.3. Limitations

This section highlights the shortcomings of the proposed solution. This study is limited to the centralized authentication methods of communicating entities for EV-charging systems, hence any other model is not included. Furthermore, we are developing the EV-charging-authentication protocol, which focuses on secure key exchange and privacy protection. As a result, our protocol may not be suitable for all VANET architectures that require more advanced algorithms and are capable of managing systems with higher computational complexity. Additionally, our method attempts to preserve the privacy requirements (anonymity, un-linkability, and traceability) of the EVs involved in the communication, as well as secure key exchange and mutual authentication between entities. The scope of this study does not include EV-charging-service scheduling, routing, coordination, actual energy trading, or payment methods. The following are the study's limitations:

- The proposed scheme does not consider any parameter that is sent (between entities) and is not relevant to the authentication process in terms of shared key, identity, or security parameters.
- The proposed scheme is limited to the proposed EV-charging architecture, and any IoV architecture that can outperform EV-charging systems in terms of performance is not considered.
- The proposed scheme is a centralized authentication protocol; other authentication models, such as distributed and hybrid, were not investigated.
- The proposed scheme combines asymmetric and symmetric key structures, so any authentication technique based solely on the symmetric-key structure was not considered.

7. Conclusions

In this paper, we propose a privacy-preserving and secure authentication scheme for V2V-charging systems. The scheme fulfils the fundamental requirements as well as a re-authentication protocol to reduce future authentication-process overhead. The ECQV mechanism's implicit authentication has been utilized to obtain the benefit of a small certificate and faster computation, which is better suited to resource-constrained Internet-of-Things (IoT) devices than a traditional certificate. Informal security analysis was used to show that the proposed protocols can accomplish mutual authentication and meet the solution requirements. The comparison with related work shows that the proposed scheme achieves approximately 65% efficiency in terms of authentication computational cost, and it provides better security and privacy preservation for the EV. Moreover, the proposed re-authentication protocol outperforms Roberts et al.'s scheme [32], with a nearly 88% reduction. For future work, we consider working on an authentication protocol for vehicles selling excess energy to the grid, since it will help EV-charging infrastructure maximize the energy offered during peak hours. In addition, we consider exploring emerging techniques (such as blockchain), how these emerging techniques can comply with ECQV algorithm, and hybrid models in EV-charging authentication.

Author Contributions: Conceptualization, A.M.A. and S.S.A.; methodology, A.M.A. and S.S.A.; validation, A.M.A. and S.S.A.; writing–original draft preparation, S.S.A.; writing–review and editing, A.M.A.; supervision, A.M.A.; funding acquisition, A.M.A. All authors have read and agreed to the published version of the manuscript.

Funding: This work was funded by SAUDI ARAMCO Cybersecurity Chair at Imam Abdulrahman Bin Faisal University, Saudi Arabia.

Informed Consent Statement: Not applicable.

Acknowledgments: We would like to thank Imam Abdulrahman Bin Faisal University for facilitating access to the resources used in this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ahmadi, P. Environmental Impacts and Behavioral Drivers of Deep Decarbonization for Transportation through Electric Vehicles. *J. Clean. Prod.* **2019**, *225*, 1209–1219. https://doi.org/10.1016/j.jclepro.2019.03.334.
2. Nereim, V. *Saudi Arabia to Start Electric-Vehicle Push in Capital Riyadh*; Bloomberg: New York, NY, USA, 2021.
3. Global EV Outlook 2021—Analysis. IEA. Available online: https://www.iea.org/reports/global-ev-outlook-2021 (accessed on 2 November 2021).
4. Kester, J.; Sovacool, B.K.; Noel, L.; Zarazua de Rubens, G. Rethinking the Spatiality of Nordic Electric Vehicles and Their Popularity in Urban Environments: Moving beyond the City? *J. Transp. Geogr.* **2020**, *82*, 102557. https://doi.org/10.1016/j.jtrangeo.2019.102557.
5. Fu, Z.; Dong, P.; Ju, Y. An Intelligent Electric Vehicle Charging System for New Energy Companies Based on Consortium Blockchain. *J. Clean. Prod.* **2020**, *261*, 121219. https://doi.org/10.1016/j.jclepro.2020.121219.
6. Kabir, M.E.; Sorkhoh, I.; Moussa, B.; Assi, C. Routing and Scheduling of Mobile EV Chargers for Vehicle to Vehicle (V2V) Energy Transfer. In Proceedings of the 2020 IEEE Power Energy Society General Meeting (PESGM), Montreal, QC, Canada, 2–6 August 2020; pp. 1–5. https://doi.org/10.1109/PESGM41954.2020.9281674.
7. AAA Says That Its Emergency Electric Vehicle Charging Trucks Served "Thousands" of EVs without Power-Electrek. Available online: https://electrek.co/2016/09/06/aaa-ev-emergency-charging-truck/ (accessed on 28 March 2022).
8. Sadiq, A.; Javed, M.U.; Khalid, R.; Almogren, A.; Shafiq, M.; Javaid, N. Blockchain Based Data and Energy Trading in Internet of Electric Vehicles. *IEEE Access* **2021**, *9*, 7000–7020. https://doi.org/10.1109/ACCESS.2020.3048169.
9. Liu, H.; Zhang, Y.; Yang, T. Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. *IEEE Netw.* **2018**, *32*, 78–83. https://doi.org/10.1109/MNET.2018.1700344.
10. Nedyalkov, I.; Arnaudov, D. Attacks and Security Measures of the Exchanged Information in the Charging Infrastructure for Electromobiles. In Proceedings of the 2019 IEEE XXVIII International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 12–14 September 2019; pp 1–4. https://doi.org/10.1109/ET.2019.8878500.
11. Kilari, V.T.; Yu, R.; Misra, S.; Xue, G. Robust Revocable Anonymous Authentication for Vehicle to Grid Communications. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 4845–4857. https://doi.org/10.1109/TITS.2019.2948803.
12. Unterweger, A.; Knirsch, F.; Engel, D.; Musikhina, D.; Alyousef, A.; de Meer, H. An Analysis of Privacy Preservation in Electric Vehicle Charging. *Energy Inform.* **2022**, *5*, 3. https://doi.org/10.1186/s42162-022-00190-y.
13. Saxena, N.; Grijalva, S.; Chukwuka, V.; Vasilakos, A.V. Network Security and Privacy Challenges in Smart Vehicle-to-Grid. *IEEE Wirel. Commun.* **2017**, *24*, 88–98. https://doi.org/10.1109/MWC.2016.1600039WC.
14. Mustafa, M.A.; Zhang, N.; Kalogridis, G.; Fan, Z. Smart Electric Vehicle Charging: Security Analysis. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6. https://doi.org/10.1109/ISGT.2013.6497830.
15. Hansen, M.; Jensen, M.; Rost, M. Protection Goals for Privacy Engineering. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 21–22 May 2015; pp. 159–166. https://doi.org/10.1109/SPW.2015.13.
16. Mundhe, P.; Verma, S.; Venkatesan, S. A Comprehensive Survey on Authentication and Privacy-Preserving Schemes in VANETs. *Comput. Sci. Rev.* **2021**, *41*, 100411. https://doi.org/10.1016/j.cosrev.2021.100411.
17. Zhang, J.; Cui, J.; Zhong, H.; Chen, Z.; Liu, L. PA-CRT: Chinese Remainder Theorem Based Conditional Privacy-Preserving Authentication Scheme in Vehicular Ad-Hoc Networks. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 722–735. https://doi.org/10.1109/TDSC.2019.2904274.
18. Koblitz, N.; Menezes, A.; Vanstone, S. The State of Elliptic Curve Cryptography. *Des. Codes Cryptogr.* **2000**, *19*, 173–193. https://doi.org/10.1023/A:1008354106356.
19. Brown, D.R.L.; Gallant, R.; Vanstone, S.A. Provably Secure Implicit Certificate Schemes. In *Financial Cryptography*; Syverson, P., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2002; pp. 156–165. https://doi.org/10.1007/3-540-46088-8_15.
20. Ha, D.A.; Nguyen, K.T.; Zao, J.K. Efficient Authentication of Resource-Constrained IoT Devices Based on ECQV Implicit Certificates and Datagram Transport Layer Security Protocol. In *Seventh Symposium on Information and Communication Technology*; SoICT '16; Association for Computing Machinery: New York, NY, USA, 2016; pp. 173–179. https://doi.org/10.1145/3011077.3011108.
21. Campagna, M. Sec 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (Ecqv). *Stand. Effic. Cryptogr. Version* **2013**, *1*, 5-11.
22. Kim, O.T.T.; Tran, N.H.; Nguyen, V.; Kang, S.M.; Hong, C.S. Cooperative between V2C and V2V Charging: Less Range Anxiety and More Charged EVs. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 679–683. https://doi.org/10.1109/ICOIN.2018.8343205.
23. Li, G.; Sun, Q.; Boukhatem, L.; Wu, J.; Yang, J. Intelligent Vehicle-to-Vehicle Charging Navigation for Mobile Electric Vehicles via VANET-Based Communication. *IEEE Access* **2019**, *7*, 170888–170906. https://doi.org/10.1109/ACCESS.2019.2955927.
24. Li, G.; Boukhatem, L.; Zhao, L.; Wu, J. Direct Vehicle-to-Vehicle Charging Strategy in Vehicular Ad-Hoc Networks. In Proceedings of the 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5. https://doi.org/10.1109/NTMS.2018.8328689.
25. Yucel, F.; Bulut, E.; Akkaya, K. Privacy Preserving Distributed Stable Matching of Electric Vehicles and Charge Suppliers. In Proceedings of the 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), Chicago, IL, USA, 27–30 August 2018; pp. 1–6. https://doi.org/10.1109/VTCFall.2018.8690603.

26. Yucel, F.; Akkaya, K.; Bulut, E. Efficient and Privacy Preserving Supplier Matching for Electric Vehicle Charging. *Ad Hoc Netw.* **2019**, *90*, 101730. https://doi.org/10.1016/j.adhoc.2018.07.029.
27. Sun, G.; Dai, M.; Zhang, F.; Yu, H.; Du, X.; Guizani, M. Blockchain-Enhanced High-Confidence Energy Sharing in Internet of Electric Vehicles. *IEEE Internet Things J.* **2020**, *7*, 7868–7882. https://doi.org/10.1109/JIOT.2020.2992994.
28. Li, H.; Dán, G.; Nahrstedt, K. FADEC: Fast Authentication for Dynamic Electric Vehicle Charging. In Proceedings of the 2013 IEEE Conference on Communications and Network Security (CNS), National Harbor, MD, USA, 14–16 October 2013; pp. 369–370. https://doi.org/10.1109/CNS.2013.6682732.
29. Huang, X.; Xu, C.; Wang, P.; Liu, H. LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem. *IEEE Access* **2018**, *6*, 13565–13574. https://doi.org/10.1109/ACCESS.2018.2812176.
30. Li, H.; Dán, G.; Nahrstedt, K. Portunes+: Privacy-Preserving Fast Authentication for Dynamic Electric Vehicle Charging. *IEEE Trans. Smart Grid* **2017**, *8*, 2305–2313. https://doi.org/10.1109/TSG.2016.2522379.
31. Diffie, W.; Hellman, M. New Directions in Cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. https://doi.org/10.1109/TIT.1976.1055638.
32. Roberts, B.; Akkaya, K.; Bulut, E.; Kisacikoglu, M. An Authentication Framework for Electric Vehicle-to-Electric Vehicle Charging Applications. In Proceedings of the 2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), Orlando, FL, USA, 22–25 October 2017; pp. 565–569. https://doi.org/10.1109/MASS.2017.93.
33. Aitzhan, N.Z.; Svetinovic, D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 840–852. https://doi.org/10.1109/TDSC.2016.2616861.
34. Kang, J.; Yu, R.; Huang, X.; Maharjan, S.; Zhang, Y.; Hossain, E. Enabling Localized Peer-to-Peer Electricity Trading Among Plug-in Hybrid Electric Vehicles Using Consortium Blockchains. *IEEE Trans. Ind. Inform.* **2017**, *13*, 3154–3164. https://doi.org/10.1109/TII.2017.2709784.
35. Chaudhary, R.; Jindal, A.; Aujla, G.S.; Aggarwal, S.; Kumar, N.; Choo, K.-K. R. BEST: Blockchain-Based Secure Energy Trading in SDN-Enabled Intelligent Transportation System. *Comput. Secur.* **2019**, *85*, 288–299. https://doi.org/10.1016/j.cose.2019.05.006.
36. Yahaya, A.S.; Javaid, N.; Javed, M.U.; Shafiq, M.; Khan, W.Z.; Aalsalem, M.Y. Blockchain-Based Energy Trading and Load Balancing Using Contract Theory and Reputation in a Smart Community. *IEEE Access* **2020**, *8*, 222168–222186. https://doi.org/10.1109/ACCESS.2020.3041931.
37. Li, Y.; Hu, B. An Iterative Two-Layer Optimization Charging and Discharging Trading Scheme for Electric Vehicle Using Consortium Blockchain. *IEEE Trans. Smart Grid* **2020**, *11*, 2627–2637. https://doi.org/10.1109/TSG.2019.2958971.
38. Long, Y.; Chen, Y.; Ren, W.; Dou, H.; Xiong, N.N. DePET: A Decentralized Privacy-Preserving Energy Trading Scheme for Vehicular Energy Network via Blockchain and K-Anonymity. *IEEE Access* **2020**, *8*, 192587–192596. https://doi.org/10.1109/ACCESS.2020.3030241.
39. Javed, M.U.; Javaid, N.; Malik, M.W.; Akbar, M.; Samuel, O.; Yahaya, A.S.; Othman, J.B. Blockchain Based Secure, Efficient and Coordinated Energy Trading and Data Sharing between Electric Vehicles. *Clust. Comput.* **2021**, *25*, 1839–1867. https://doi.org/10.1007/s10586-021-03435-9.
40. Cui, Z.; XUE, F.; Zhang, S.; Cai, X.; Cao, Y.; Zhang, W.; Chen, J. A Hybrid BlockChain-Based Identity Authentication Scheme for Multi-WSN. *IEEE Trans. Serv. Comput.* **2020**, *13*, 241–251. https://doi.org/10.1109/TSC.2020.2964537.
41. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized Bus. Rev.* **2008**, *4*, 21260.
42. Halpin, H.; Piekarska, M. Introduction to Security and Privacy on the Blockchain. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), Paris, France, 26–28 April 2017; pp. 1–3. https://doi.org/10.1109/EuroSPW.2017.43.
43. Piao, Y.; Ye, K.; Cui, X. A Data Sharing Scheme for GDPR-Compliance Based on Consortium Blockchain. *Future Internet* **2021**, *13*, 217. https://doi.org/10.3390/fi13080217.
44. Xia, S.; Lin, F.; Chen, Z.; Tang, C.; Ma, Y.; Yu, X. A Bayesian Game Based Vehicle-to-Vehicle Electricity Trading Scheme for Blockchain-Enabled Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6856–6868. https://doi.org/10.1109/TVT.2020.2990443.
45. Khan, A.G.; Basharat, S.; Riaz, M.U. Analysis of Asymmetric Cryptography in Information Security Based on Computational Study to Ensure Confidentiality during Information Exchange. *Int. J. Sci. Eng. Res.* **2018**, *9*, 992–999.
46. Bokhari, M.U.; Shallal, Q.M. A Review on Symmetric Key Encryption Techniques in Cryptography. *Int. J. Comput. Appl.* **2016**, *147*, 43-48.
47. Al-Shareeda, M.A.; Anbar, M.; Hasbullah, I.H.; Manickam, S. Survey of Authentication and Privacy Schemes in Vehicular Ad Hoc Networks. *IEEE Sens. J.* **2021**, *21*, 2422–2433. https://doi.org/10.1109/JSEN.2020.3021731.
48. Braeken, A.; Touhafi, A. AAA—Autonomous Anonymous User Authentication and Its Application in V2G. *Concurr. Comput. Pract. Exp.* **2018**, *30*, e4303. https://doi.org/10.1002/cpe.4303.
49. Ali, F.S.; Aloqaily, M.; Alfandi, O.; Ozkasap, O. Cyberphysical Blockchain-Enabled Peer-to-Peer Energy Trading. *Computer* **2020**, *53*, 56–65. https://doi.org/10.1109/MC.2020.2991453.
50. Azam, F.; Yadav, S.K.; Priyadarshi, N.; Padmanaban, S.; Bansal, R.C. A Comprehensive Review of Authentication Schemes in Vehicular Ad-Hoc Network. *IEEE Access* **2021**, *9*, 31309–31321. https://doi.org/10.1109/ACCESS.2021.3060046.
51. Baee, M.A.R.; Simpson, L.; Foo, E.; Pieprzyk, J. Broadcast Authentication in Latency-Critical Applications: On the Efficiency of IEEE 1609.2. *IEEE Trans. Veh. Technol.* **2019**, *68*, 11577–11587. https://doi.org/10.1109/TVT.2019.2945339.

52. Almuhaideb, A.M. Re-AuTh: Lightweight Re-Authentication with Practical Key Management for Wireless Body Area Networks. *Arab. J. Sci. Eng.* **2021**, *46*, 8189–8202. https://doi.org/10.1007/s13369-021-05442-9.
53. CHAdeMO. Available online: https://www.chademo.com/ (accessed on 2 April 2022).
54. Kumar, G.; Saha, R.; Rai, M.K.; Buchanan, W.J.; Thomas, R.; Geetha, G.; Hoon-Kim, T.; Rodrigues, J.J.P.C. A Privacy-Preserving Secure Framework for Electric Vehicles in IoT Using Matching Market and Signcryption. *IEEE Trans. Veh. Technol.* **2020**, *69*, 7707–7722. https://doi.org/10.1109/TVT.2020.2989817.
55. Kilinc, H.H.; Yanik, T. A Survey of SIP Authentication and Key Agreement Schemes. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1005–1023. https://doi.org/10.1109/SURV.2013.091513.00050.