electronics

MDPI

Article

A Lightweight Authentication Scheme for V2G Communications: A PUF-Based Approach Ensuring Cyber/Physical Security and Identity/Location Privacy

Masoud Kaveh [1], Diego Martín [1,*] and Mohammad Reza Mosavi [2]

[1] ETSI de Telecomunicación, Universidad Politécnica de Madrid, Av. Complutense 30, 28040 Madrid, Spain; m_kaveh@elec.iust.ac.ir

[2] Department of Electrical Engineering, Iran University of Science and Technology, Tehran 13114-16846, Iran; m_mosavi@iust.ac.ir

* Correspondence: diego.martin.de.andres@upm.es

Received: 17 August 2020; Accepted: 4 September 2020; Published: 9 September 2020

Abstract: Vehicle-to-grid (V2G) technology has become a promising concept for the near future smart grid eco-system. V2G improves smart grid resiliency by enabling two-way communication and electricity flows while reducing the greenhouse gases emission. V2G practicality and stability is strongly based on the exchanged data between electrical vehicles (EVs) and the grid server (GS). However, using communication protocols to exchange vital information leads grid to being vulnerable against various types of attack. To prevent the well-known attacks in V2G network, this paper proposes a privacy-aware authentication scheme that ensures data integrity, confidentiality, users' identity and location privacy, mutual authentication, and physical security based on physical unclonable function (PUF). Furthermore, the performance analysis shows that the proposed scheme outperforms the state-of-the-art, since EVs only use lightweight cryptographic primitives for every protocol execution.

Keywords: vehicle-to-grid communications; privacy-friendly authentication; physical unclonable function; physical security; lightweight design

1. Introduction

The smart grid has been introduced as a promising concept to improve the traditional power grid in recent years. By enabling two-way communications along with two-way electrical flows using the information and communication technology (ICT), smart grid increases the efficiency, reliability, and better monitoring of the power grid and reduces the emission of greenhouse gases [1–3]. However, one of the most important parts of the smart grid to address these goals is vehicle-to-grid (V2G) technology, which has received a significant attention in recent years.

The concept of V2G was initially introduced by Kempton and Tomic in 2005 [4]. More precisely, V2G technology mainly consists of entities that enhance the bi-directional electrical flow between the vehicles and grid. The electrical energy can flow from the grid to the vehicle to charge the vehicle's battery (when the battery is low), or inversely flow from the vehicle to the grid during the peak power demand situations. This bi-directional charging property makes the electric vehicle (EV) as an important component in the V2G eco-system and provides a significant level of resiliency for the smart grid. In a V2G eco-system, an EV needs to charge its battery by drawing electrical power from the grid. For that purpose, EV sends a request to its nearest charge station (CS). After confirming the request by the grid server (GS), EV can charge its battery and pay the price to the selling company. EVs can also deliver power to the grid through a CS in the same way, and get rewards according to

their deliverance. Therefore, the use of V2G technology brings two important advantages for the smart grid: one is that it delivers power to the grid in times of peak power consumption, and the second is that, during times of lowest consumption, it prevents wastage of generated electricity by charging its own battery. Furthermore, the other advantage for the EV owners is that they can buy the power with the lower price and sell it when the price is high [5–9].

Although employing ICT provides the mentioned bold advantages for the smart grid, it introduces some important challenges in the security issues [10–13]. This is because using insecure channels for establishing communications between EV and CS and communications between CS and GS can create a vulnerable environment containing malicious attacks. These well-informed adversarial attacks may target the EVs' identity (ID), EVs' location, or the privacy of all entities' vital data. Furthermore, the physical attacks may lead to disclose the stored secrets in their devices' memory. Hence, this paper aims to propose an efficient authentication protocol for securing communications in V2G environment.

1.1. Related Works

There are a lot of security protocols that have been proposed in recent years for V2G communications [14–32]. Most of mentioned schemes could not provide one or more important features in both terms of security and efficiency. For example, although the authentication schemes proposed in [14–22] have insured the privacy of EVs (owners), the location privacy of EVs has not been considered. Furthermore, the use of heavyweight cryptographic primitives like sign-encryption and group signature based on public key infrastructures is another disadvantage of the mentioned schemes. Although Shen et al. [23] have proposed a very lightweight authentication protocol in 2017, it has a lack of location privacy and session key integrity. Some other proposed schemes in the literature [24–27] suffer not only from the aforementioned drawbacks, but are also vulnerable against some well-known security attacks. For example, the proposed scheme in [27] is not secure against replay and masquerade attacks [28].

Efforts to propose a secure and efficient protocol have continued. Recently, in 2019, Gope and Sikdar [29] proposed a lightweight privacy-preserving authentication protocol for V2G communications. Their proposed scheme could resist against well-known cyber-attacks and provide location privacy and low computational cost, especially at the EV side. However, it lacks physical security. A little after in 2019, Su et al. [30] proposed a novel privacy-preserving authentication protocol for V2G communications based on a nonsupersingular elliptic curve, in order to improve the efficiency of nonsupersingular elliptic curve-based authentication protocols. However, their proposed scheme not only has the disadvantage of Gope's scheme in [29], but also uses heavyweight cryptographic primitives. Quite recently in 2020, Abbasinezhad-Mood et al. [31] have presented a key agreement protocol for V2G connections based on escrow-less Chebyshev chaotic map. Despite providing good security features, their scheme endures of lacking location privacy, physical security, and heavyweight design. A little after, in 2020, Bansal et al. [32] proposed a mutual authentication scheme for V2G using physical unclonable functions (PUFs). As far as the knowledge of the authors in this paper, the proposed scheme in [32] is the only scheme that could resist physical attack. However, their scheme does not provide location privacy, or the EVs' privacy against CS (the selling company). Furthermore, their scheme suffers inefficient design in terms of computational costs at the EV side.

1.2. Paper Contributions

As mentioned earlier, the former authentication schemes for V2G suffer from some security and efficiency-related drawbacks. Some of them, such as the proposed schemes in [23,27], have security issues and are vulnerable to some well-known attacks [28,31]. Furthermore, most of them use computational inefficient cryptographic primitives, do not provide location privacy, and do not consider physical attacks. Therefore, based on these motivations, the contribution of this paper is as follows:

- The proposed scheme ensures a good range of privacy. The privacy here consists of data and identity privacy against the external adversary, the location privacy of the EVs, and privacy against internal entities. For example, except for a trusted party like GS, any other internal entities like EVs and CSs have not to know each other's secrets and private data.
- Proposing an efficient and secure protocol that performs the key agreement and data transmission phases simultaneously.
- Proposing a PUF-based authentication scheme which not only resists against all well-known attacks, such as replay, impersonation, data analysis, data integrity, etc., but is also secure against physical threats.
- The proposed scheme consumes the lowest computational and communication resources in comparison with the state-of-the-art.

The layout of this paper is organized as follows. Section 2 presents some backgrounds of PUF and explains the system and threat model. Section 3 elaborates the proposed scheme. Sections 4 and 5 analyze the proposed protocol in security and performance terms, respectively. Finally, Section 6 concludes this paper.

2. Preliminary Backgrounds and Assumptions

In this section, we briefly explain about PUF and its important metrics, and then describe the V2G system model and the correspondence adversary model.

2.1. Background of PUF

A PUF can be defined as a unique and unclonable physical feature of an integrated circuit (IC). In recent years, it has become known as the digital fingerprint; as unique as the fingerprints of the human [33]. In general, the most important features of PUF are first: being non-reproducible by the cryptographic primitives; and second: too hard, or impossible, to be cloned physically. This unique property of PUF introduces it as a promising technology in key generation, identification, and authentication problems [34–36]. A PUF is particularly considered as a one-way physical function that maps a set of inputs as its challenges to a set of responses as its response. This mapping is mainly based on the complex physical structure of its used circuit. Figure 1 depicts a ring oscillator PUF (ROPUF), which is built with N frequency oscillators, two 2 to 1 multiplexers, two frequency counters, and one comparator [36].

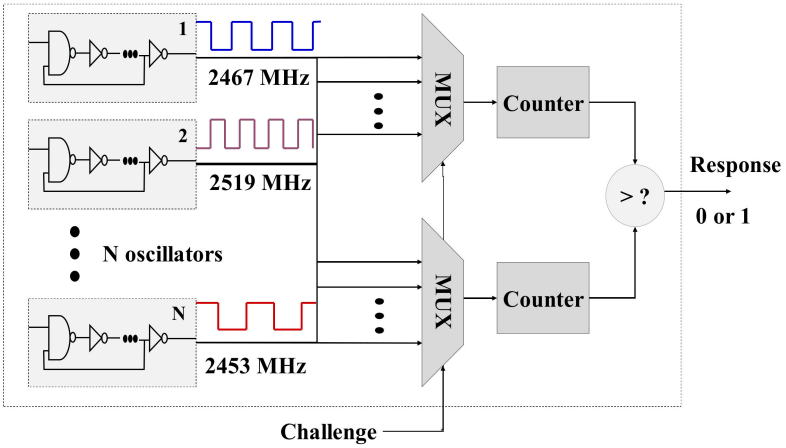

Figure 1. A typical ring oscillator physical unclonable function (ROPUF).

Each of the two counters start counting the number of received cycles from the selected oscillators by the multiplexers during a predefined time interval. After, the values of the frequency counters are compared by the comparator. Based on the comparison result, a random bit will be produced.

The unpredictable and uncontrollable effect of IC manufacturing process results a good range of randomness in PUF responses. If we assume a PUF with challenge C and response R, the most important unique characteristics of this PUF is as follows:

- If we input different challenges $C_1, C_2, \ldots, C_n$ to the same PUF, we will obtain different responses $R_1, R_2, \ldots, R_n$ with great distances. The concept of distance here can be considered as an appropriate distance metric while the responses are always considered as bit vectors.
- If we input same challenge, C, to the same PUF in different situations (n times), we will obtain identical responses $R_1 = R_2 = \ldots = R_n$ with great possibility.
- If we input same challenge, C, to different PUF instances $PUF_1, PUF_2, \ldots, PUF_n$, we will obtain different responses $R_1, R_2, \ldots, R_n$ with great distances.

The first, second, and third properties are named as diffuseness, reliability, and uniqueness, respectively. These three properties alongside the randomness are the most important features of PUF. However, since there are always some errors in different PUF evaluations, the reliability of PUF is usually less than 100%. On the other hand, error correcting methods like fuzzy extractors as a combating tool facing this problem, will cost in considerable overheads for PUF-based authentication schemes [37–39]. Nonetheless, several PUFs have been proposed in recent years, with 100% reliability over different situations of temperature and supply voltage [40–44]. Although using these kinds of ideal PUFs usually leads to increasing expenses, using them in countable numbers by a prosperous company (like CS investors) will be reasonable. As a result, by considering ideal PUFs for V2G communications, a stable and promising key generation approach will be achieved.

2.2. V2G System Model

Figure 2 indicates a typical V2G network model. A V2G network mainly consists of three entities in a specific area: (many) EVs, (several) CSs, and (one) GS. EVs are personal electrical vehicles that may want to charge/discharge their batteries through a CS very often. They have limited computational and storage capacities, and, as might be expected, have adequate hardware protection [31]. On the other hand, CSs are electrical charge stations belongs to some private or public companies, which are located in the open without considerable hardware protection. Each CS is equipped with a PUF that is embedded with its communication board. The communication between a CS and its PUF is assumed to be secure and tamper-proof. Although the CSs may have limited computational resources, they have slightly more computational capacity than EVs. GS is a grid server with a high computational and storage capacities. It has large database including different information of all legal entities, i.e., the registered EVs and CSs. GS is considered as trusted party in the grid that has access to all private information and makes the final decisions about the electricity and information flows.

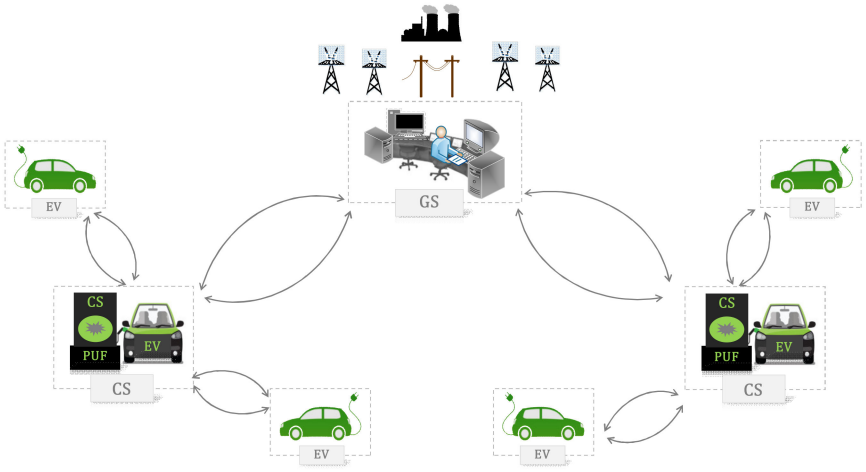

Figure 2. Vehicle-to-grid (V2G) network.

2.3. Threats Facing V2G System

Although all the steps of registering the EVs and CSs by the GS is done through a secure channel, all the packets have to transmitted through an insecure channel during the authentication phase. Therefore, it makes the communication protocols between all entities vulnerable to different kinds of attack. There are some kinds of attacks have been introduced in recent years. For example, Dolev-Yao proposed a threat model (DY model) for V2G [45], in which a malicious adversary is able to eavesdrop on, modify, or remove the transmitted packets in the insecure communication link. However, to the best of our knowledge, the greatest number of attacks and threats facing a V2G system is considered in this paper. For example, an adversary may impersonate her/himself to any entity in the grid and then tries to abuse the situation. In addition, she/he may replay the older packets to an entity or disrupt the network by performing the denial-of-service (DoS) attack. She/he may also intentionally alter the packets or tries to discover a confidential data. The privacy of the EVs are another important concern that has to be considered with caution. In the V2G network, not only an adversary may want to breach of privacy of EVs, but other legal entities may also want to access each other's private data. These malicious legal entities may be some EVs who want to charge their batteries for free, or sell their energy for higher price. Furthermore, a malicious legal entity can be a CS who wants to obtain private information about EVs and sell it to someone concerned about this information. Last but not least, an adversary may get physically access to a device's memory and try to obtain the important stored secrets. This paper proposes a privacy-preserving authentication protocol to protect the all V2G entities' information, identity, and location privacy in all mentioned aspects.

3. Methodology

The proposed PUF-based authentication scheme is elaborated in this section. We divide the proposed protocol into two main phases: installation phase and authentication phase. The following subsections present each phase in detail. Furthermore, all the notations in this paper are shown in Table 1 with their meanings.

Table 1. Notations and their meanings.

Notation	Description	Notation	Description
EV_j	j-th Electrical Vehicle	Loc_j^i	location of EV_j in i-th authentication
CS_n	n-th Charge Station	TS	Timestamp
GS	Grid Server	$h(X)$	Hash of X
ID_j^i	Identity of EV_j in i-th Authentication	$\bigoplus$	Logical XOR
ID_n	Identity of CS_n	$\|\|$	Concatenation operation
B	Byte	S	Second

3.1. Installation Phase

In this phase, every vehicle (e.g., j-th vehicle is considered as EV_j) and charge station (CS_n) has to be registered by GS. First, for EVs' registrations, EV_j sends a given value as its identity (ID_j^0) to GS. After receiving ID_j^0, GS generates a random number r_j^0 and then calculates $K_j^1 = h\left(r_j^0 \,\|\, ID_j^0\right)$ as a secret key for EV_j, where h is a collision-resistant one-way hash function. Furthermore, GS computes another hash value $ID_j^1 = h\left(K_j^1 \,\|\, ID_j^0\right)$ as EV_j's new identity, and sends K_j^1 and ID_j^1 to EV_j. Finally, GS stores K_j^1 and ID_j^1 in EV_j's corresponding row in its database. On the other side, EV_j stores K_j^1 and ID_j^1 in its non-volatile memory (NVM) after receiving them.

For CSs' registrations, CS_n first generates a given value as its identity (ID_n) and sends it to GS. Afterward, GS generates a challenge C_n^1 and sends it to CS_n. Then, CS_n produces a response R_n^1 by inputting the received challenge (C_n^1) to its PUF and sends its location, LOC_n, and its response, R_n^1, to GS. Meanwhile, CS_n removes the CRP from its NVM. As mentioned before, since CS is located in the open without (enough) hardware protection, it is necessary for CS to not store any secret or vital

data in its memory, to prevent physical attacks. Finally, GS stores CRP_n^1, LOC_n, and ID_n in a row of database that belongs to CS_n.

3.2. Authentication Phase

At the very beginning of starting i-th authentication (after the registration phase) for drawing power from the grid or deliver power back to it, EV_j encrypts its current location and private data (such as battery status, type of service, and payment records) using its shared key K_j^i, as $E_j^{i1} = \left(LOC_j^i \parallel D_j^i\right) \bigoplus K_j^i$ and generates a hash value $V_j^{i1} = h\left(LOC_j^i \parallel D_j^i \parallel K_j^i \parallel ID_j^i \parallel TS\right)$ for verification, where ID_j^i is EV_j's agreed identity for the i-th authentication and TS is a fresh timestamp. Afterward, EV_j sends $\left\{E_j^{i1},\ V_j^{i1},\ ID_j^i,\ TS\right\}$ to CS_n (its nearest charge station). At this step, CS_n only checks if TS is fresh and then sends the received packet with its ID, i.e., $\left\{E_j^{i1},\ V_j^{i1},\ ID_j^i,\ TS\right\}\&\{ID_n\}$ to the GS. GS first checks if ID_n is a valid ID and TS is a fresh timestamp. If so, it then finds the corresponding location and CRP, i.e., LOC_n, C_n^i, and R_n^i within its database. Furthermore, GS locates ID_j^i in its database and finds K_j^i to verify $V_j^{i1} = h\left(LOC_j^i \parallel D_j^i \parallel K_j^i \parallel ID_j^i \parallel TS\right)$ and decrypt $LOC_j^i \parallel D_j^i = E_j^{i1} \bigoplus K_j^i$. If V_j^{i1} passes the verification and GS finds CS_n as a proper charge station for EV_j by comparing LOC_j^i and LOC_n, it generates a hash value $V_n^{i2} = h\left(C_n^i \parallel R_n^i \parallel TS\right)$ and sends $\left\{V_n^{i2},\ C_n^i,\ TS\right\}$ to CS_n. CS_n first uses its PUF and C_n^i to generate R_n^i, and then verifies $V_n^{i2} = h\left(C_n^i \parallel R_n^i \parallel TS\right)$. If the verification is passed, it computes a new challenge and response, $C_n^{i+1} = h\left(C_n^i \parallel R_n^i\right)$ and $R_n^{i+1} = PUF\left(C_n^{i+1}\right)$, for future authentication. Furthermore, it computes $E_n^{i2} = R_n^{i+1} \bigoplus R_n^i$ and $V_n^{i3} = h\left(C_n^{i+1} \parallel R_n^{i+1} \parallel ID_n \parallel TS\right)$ for encrypting R_n^{i+1} and for being verified by GS, respectively. Finally, CS_n sends $\left\{V_n^{i3},\ E_n^{i2},\ TS\right\}$ to the GS. After receiving this packet and checking the freshness of the timestamp, GS acts as follows:

- Decrypts R_n^{i+1} using R_n^i and E_n^{i2} i.e., $R_n^{i+1} = E_n^{i2} \bigoplus R_n^i$. Now, GS has the new key (R_n^{i+1}) to communicates with CS_n in the future authentication phase.
- Computes the new challenge as the same of CS_n, i.e., $C_n^{i+1} = h\left(C_n^i \parallel R_n^i\right)$.
- Verifies V_n^{i3} by computing $V_n^{i3} = h\left(C_n^{i+1} \parallel R_n^{i+1} \parallel ID_n \parallel TS\right)$. GS goes to the next step only if the verification is passed.
- Generates two pseudo-random number r_{GS}^{i1} and r_{GS}^{i2}.
- Computes the new key for EV_j as $K_j^{i+1} = h\left(r_{GS}^{i1} \parallel K_j^i\right)$. GS and EV_j will use it for future authentication.
- Generates a pseudo-random number as new ID for EV_j named ID_j^{i+1}.
- Encrypts the message for CS_n using R_j^i and r_{GS}^{i2} as $E_n^{i3} = \left(\left(m_n^i \bigoplus r_{GS}^{i2}\right) \parallel r_{GS}^{i2}\right) \bigoplus R_n^i$.
- Encrypts the message for EV_j using K_j^i and r_{GS}^{i1} as $E_j^{i4} = \left(\left(\left(m_j^i \parallel ID_j^{i+1}\right) \bigoplus r_{GS}^{i1}\right) \parallel r_{GS}^{i1}\right) \bigoplus K_j^i$.
- Computes hash values for CS_n's and EV_j's side verification as $V_n^{i4} = h\left(m_n^i \parallel r_{GS}^{i2} \parallel R_n^i \parallel TS\right)$ and $V_j^{i5} = h\left(m_j^i \parallel ID_j^{i+1} \parallel r_{GS}^{i1} \parallel K_j^i \parallel TS\right)$, respectively.
- Replaces new parameters i.e. C_n^{i+1}, R_n^{i+1}, K_j^{i+1}, and ID_j^{i+1} with the previous ones.
- Sends the packet $\left\{E_n^{i3},\ V_n^{i4}, E_j^{i4},\ V_j^{i5},\ TS\right\}$ to CS_n.

CS_n first checks the freshness of the timestamp and then decrypts its message (m_n^i) and r_{GS}^{i2} as $\left(m_n^i \bigoplus r_{GS}^{i2}\right) \parallel r_{GS}^{i2} = E_n^{i3} \bigoplus R_n^i$. It is worth mentioning that only CS_n can decrypt the plaintext m_n^i and r_{GS}^{i2}, because no one except CS_n and GS gets access to R_n^i. Now, by decrypting m_n^i and r_{GS}^{i2}, CS_n verifies V_n^{i4} by computing $V_n^{i4} = h\left(m_n^i \parallel r_{GS}^{i2} \parallel R_n^i \parallel TS\right)$. If the verification is passed, it removes all the

old and new CRPs and secrets from its memory and sends $\left\{E_j^{i4},\ V_j^{i5},\ TS\right\}$ to EV_j. After verifying the freshness of the received packet, EV_j decrypts the message from GS using its secret key, K_j^i as $\left(\left(m_j^i \parallel ID_j^{i+1}\right) \bigoplus r_{GS}^{i1}\right) \parallel r_{GS}^{i1} = E_j^{i4} \bigoplus K_j^i$. After that, it verifies the authority of the sender by checking if $V_j^{i5} = h\left(m_j^i \parallel ID_j^{i+1} \parallel r_{GS}^{i1} \parallel K_j^i \parallel TS\right)$ holds or not. If the verification is passed, EV_j accepts the message otherwise, it discards it. Furthermore, EV_j computes its new key $K_j^{i+1} = h\left(r_{GS}^{i1} \parallel K_j^i\right)$, and its new ID $ID_j^{i+1} = h\left(ID_j^i \parallel K_j^{i+1}\right)$, for future authentication. Finally, EV_j stores K_j^{i+1} and ID_j^{i+1}, and removes K_j^i and ID_j^i from its memory. Figure 3 demonstrates a general schema of the proposed protocol.

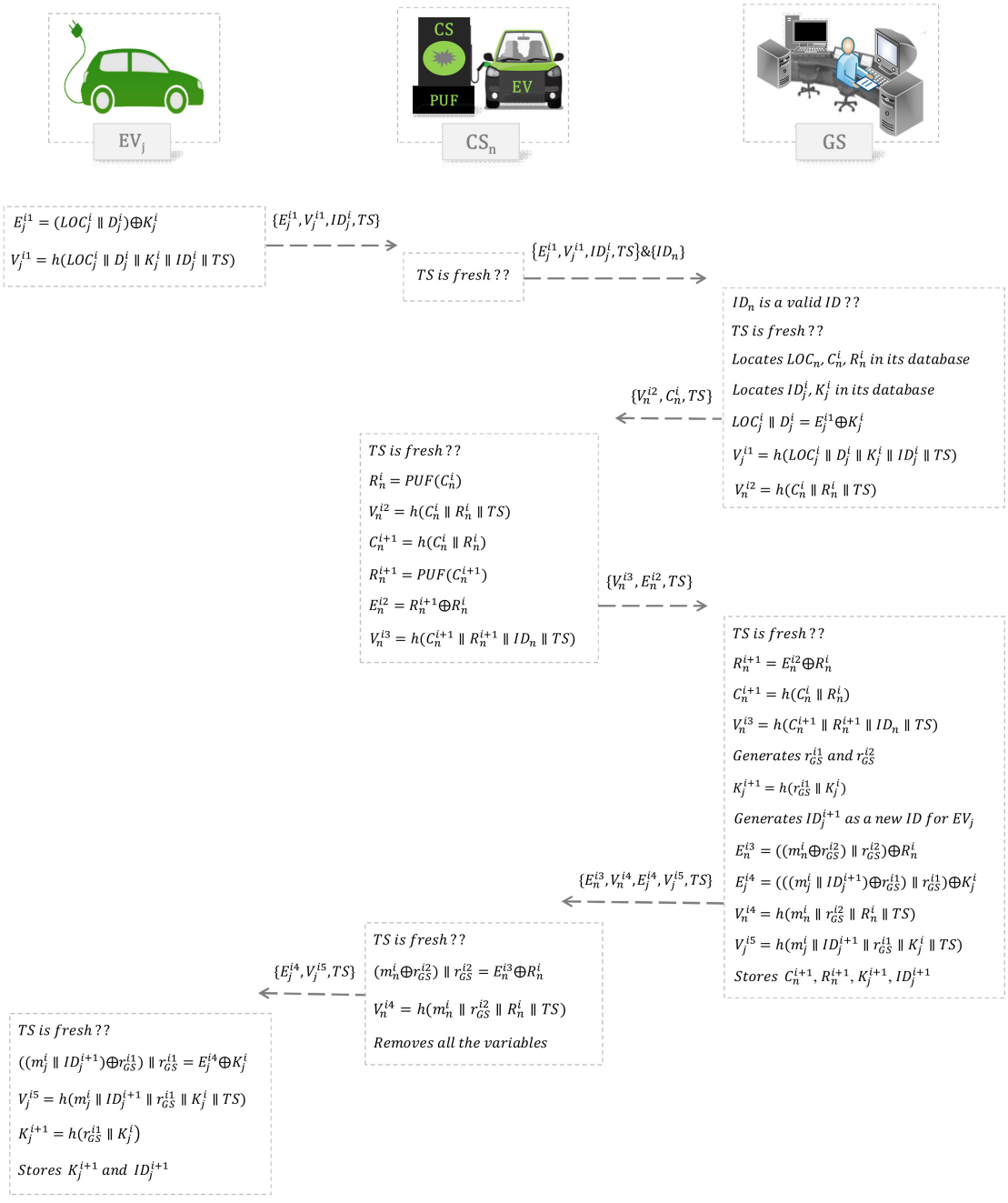

Figure 3. The proposed protocol.

It is worth mentioning that if the output length of the used hash function (SHA-256) is 256 bits, the length size of TS is considered 32 bits, m_j^i, ID_j^i, m_n^i, ID_n^i, r_{GS}^{i2} is considered 64 bits, LOC_j^i, D_j^i, R_n^i, r_{GS}^{i1} is considered 128 bits, K_j^i, E_j^i, V_j^i, E_n^i, V_n^i is considered 256 bits, and C_n^i is considered 530 bits. Therefore, all operands of the Exclusive OR (XOR) operations have same size.

As a brief conclusion, a mutual authentication between GS and CS, and GS and EV is established, and their future keys are agreed in one execution of the proposed protocol. Furthermore, because only EV_j and GS has access to K_j^i, any CS (nor external adversary) cannot get access EV_j's confidential message, current location, and new identity. Therefore, our proposed protocol can provide a good range of privacy for the users in the grid. Last but not least, using PUF leads to ensuring the physical security of the charge stations. More details of the security and performance analysis of the proposed scheme is presented in the following sections.

4. Security Analysis

In this section, we discuss how the proposed protocol in this paper can resist against different kinds of attack.

4.1. Resistance to Eavesdropping and Message Analysis Attack

This kind of attack targets the confidentiality of the vital data, where an adversary may eavesdrop on the communication link and attempt to obtain the transmitted information between EV_j and CS_n, or CS_n and GS. There are no security problems concerning the hashed values or non-encrypted data i.e., V_j^{i1}, ID_j^i, TS, ID_n, V_n^{i2}, C_n^i, V_n^{i3}, V_n^{i4}, and V_j^{i5}. However, she/he may try to decrypt the encrypted packets, i.e., E_j^{i1}, E_n^{i2}, E_n^{i3}, and E_j^{i4} to get access to private data or secret parameters. While the E_j^{i1}, E_n^{i2}, E_n^{i3}, and E_j^{i4} are encrypted by K_j^i and R_n^i, the adversary has to know them to obtain the plaintext. Since K_j^i is one-time pad secret key known by only EV_j and GS, and R_n^i is a PUF response; a true random and unpredictable key known by only CS_n and GS, the adversary will have no chance to discover the encrypted packets. Furthermore, the cryptographic keys (K_j^i and R_n^i) in this paper are updated for every protocol execution that significantly mitigates the vulnerability of the protocol against the brute-force attack. As a result, the proposed scheme is secure against message analysis attack and provides a good level confidentiality.

4.2. Resistance to Message Altering Attack

In this kind of attack, an adversary may modify a message, and then send it to one of the entities in the network. For example, if she/he tries to alter E_j^{i1} to E_j^{i1**}, or more specific, LOC_j^i and D_j^i to LOC_j^{i**} and D_j^{i**}, she/he has to compute a hash value $V_j^{i1**} = h\Big(LOC_j^{i**} \parallel D_j^{i**} \parallel K_j^i \parallel ID_j^i \parallel TS\Big)$ to pass the verification. Since the used one-way cryptographic hash function is collision-resistant and the adversary has no access to K_j^i, her/his chance will be negligible to compute a hash for passing the verification. Therefore, the receiving entity (GS in this case) finds out if the message is altered and discards the received packet. The same is true for E_n^{i2}, E_n^{i3}, and E_j^{i4}, when the adversary tries to alter the corresponding messages. Furthermore, the proposed protocol is secure against a message altering attack, and can provide a good level of message integrity.

4.3. Resistance to Impersonation and Message Injection Attack

In this kind of attack, the adversary attempts to impersonate her/himself as a legal entity and then injects her/his forged message. For that, she/he has to compute a hash value to pass the verification as an authorized source of the message. For instance, if she/he tries to impersonate EV_j, she/he has to compute a hash value V_j^{i1**} to pass the verification at the GS side, i.e., $V_j^{i1**} = h\Big(LOC_j^i \parallel D_j^i \parallel K_j^i \parallel ID_j^i \parallel TS\Big)$. Since she/he has no access to K_j^i, and because of the collision-resistant property of one-way cryptographic hash function, the chance for her/his success will be negligible. Furthermore, if she/he tries to

impersonate CS_n and inject a forged message to GS, she/he should get access R_n^i or collide a proper hash value to pass the verification. However, both of them are very hard or impossible for a probabilistic polynomial time (PPT) adversary. By the same analysis, it will be too hard or impossible for PPT adversary to impersonate GS in the proposed protocol. Therefore, our proposed scheme is secure against impersonation and message injection attack.

4.4. Resistance to Replay Attack

In the proposed scheme, each EV, EV_j, sends its packet $\left\{E_j^{i1},\ V_j^{i1},\ ID_j^i,\ TS\right\}$ to CS and GS, where TS is a fresh time stamp, ID_j^i securely varies for each run of protocol, and V_j^{i1} is equal to $h\left(LOC_j^i \parallel D_j^i \parallel K_j^i \parallel ID_j^i \parallel TS\right)$. Here, when an adversary tries to replay the old messages, her/his replayed message will be detected by GS during the verification of V_j^{i1}. Similarly, when she/he tries to replay a packet between CS and GS, her/his attempt will be detected because of hashing the fresh time timestamp and updated secret values. Therefore, the proposed protocol can resist replay attack.

4.5. Resistance to DoS Attack

In this kind of attack, an adversary may overload the network by sending waste and false packets to the all entities of the protocol. She/he may force the targeted party to spend unnecessary or a lot of computations or store vain messages and consequently prevent them from receiving the authentic messages. In our proposed scheme, every entity immediately verifies the received packets by bogus packet in i-th authentication phase, it can easily discards it by executing one hash operation to compute $V_j^{i1} = h\left(LOC_j^i \parallel D_j^i \parallel K_j^i \parallel ID_j^i \parallel TS\right)$. Similarly, CS needs to run one PUF and one hash operation, and EV needs to run on hash operation to discard the bogus messages. Here, the computation cost of logical XOR or locating at database has been ignored. As a result, the proposed protocol has shown a good resistance against DoS attack where an adversary who tries to perform this attack, cannot overload the V2G network.

4.6. Resistance to Physical Attack

In this kind of attack, an adversary may attempt to get physically access to a device including the encryption system and then try to obtain the stored secrets on that device's memory. When the adversary successes to perform physical attack, she/he can easily perform various kinds of attacks. It is a reasonable assumption that GS and EVs may have enough hardware protection to prevent the adversaries getting easily access to their devices' memory [32]. However, the CSs are usually located in the open, an adversary can easily capture its memory and obtain the important stored secrets. To prevent this kind of attack, we have used PUF for every CS in the network which causes the CSs remove all the secret parameters after each protocol execution. Therefore, the adversary will obtain nothing after getting access to CS's memory, which makes the proposed protocol secure against the physical attack.

4.7. User Privacy Protection

In our proposed protocol, GS generates a new ID for EV_j at each authentication phase and sends it securely to EV_j ($E_j^{i4} = \left(\left(\left(m_j^i \parallel ID_j^{i+1}\right) \bigoplus r_{GS}^{i1}\right) \parallel r_{GS}^{i1}\right) \bigoplus K_j^i$). Therefore, EV_j uses its ID only once, which it receives securely at the authentication phase. As a result, EV_j will have a level of good privacy not only against the external adversaries, but also against corresponding CS and other vehicles within the grid. In other words, only GS is aware of EVs' activities in our protocol. Furthermore, in each EV_j's request to charge/discharge its battery, LOC_j^i is encrypted by K_j^i ($E_j^{i1} = \left(LOC_j^i \parallel D_j^i\right) \bigoplus K_j^i$). Since K_j^i is only owned by EV_j and GS, no other entity will be aware of EV_j's location. As a result, the proposed protocol ensures the ID and location privacy for users.

5. Performance Evaluation and Comparison

In this section, we evaluate the performance of the proposed protocols and compare them with the closely-related and the most recent and outperforming authentication schemes presented in [29–32], in terms of communication overhead and computational cost. Furthermore, we provide a feature-based comparison where the security and functionality characterizations of our proposed protocol is compared with other schemes proposed in [29–32].

5.1. Communication Overhead

The total communication overhead of our proposed scheme consists of four parts: the transmitted packets from EV_j to CS_n, CS_n to GS, GS to CS_n, and CS_n to EV_j. The communication overhead for EV_j to CS_n data transmission is $\left|E_j^{i1}\right| + \left|V_j^{i1}\right| + \left|ID_j^i\right| + |TS| = 76\ B$, where $|X|$ indicates the bit-length of message X. The communication overhead for CS_n to GS data transmission is $\max\left\{\left[\left|E_j^{i1}\right| + \left|V_j^{i1}\right| + \left|ID_j^i\right| + |TS| + |ID_n|\right],\ \left[\left|E_n^{i2}\right| + \left|V_n^{i3}\right| + |TS|\right]\right\} = 84\ B$. The communication overhead for GS to CS_n data transmission is $\max\left\{\left[\left|E_n^{i3}\right| + \left|V_n^{i4}\right| + \left|E_j^{i4}\right| + \left|V_j^{i5}\right| + |TS|\right], \left[\left|C_n^i\right| + \left|V_n^{i2}\right| + |TS|\right]\right\} = 132\ B$. The communication overhead for CS_n to EV_j data transmission is $\left|E_j^{i4}\right| + \left|V_j^{i5}\right| + |TS| = 68\ B$. Therefore, the total communication overhead of our proposed scheme in each protocol execution is 360 B. Figure 4 demonstrates the communication cost of our scheme in comparison with the proposed ones in [29–32]. According to this Figure 4, our protocol could outperform the proposed schemes in [29,31,32]. The communication cost of proposed scheme in [30] is less than ours, however, the authors of [30] did not consider the communications between CS and GS. Furthermore, our scheme is the only protocol among the proposed ones in [29–32], which transmits confidential data packets along each the authentication process, which leads to increasing the communication overhead. For having more comprehensive comparison with the scheme proposed in [30], if we only consider the communications between EV and CS, and ignore the confidential data packets in the communication link, then the overall communication of our scheme is 80 B (<<212 B). As a result, and in a nutshell, we can say that the proposed protocol in this paper has good performance in communication overhead.

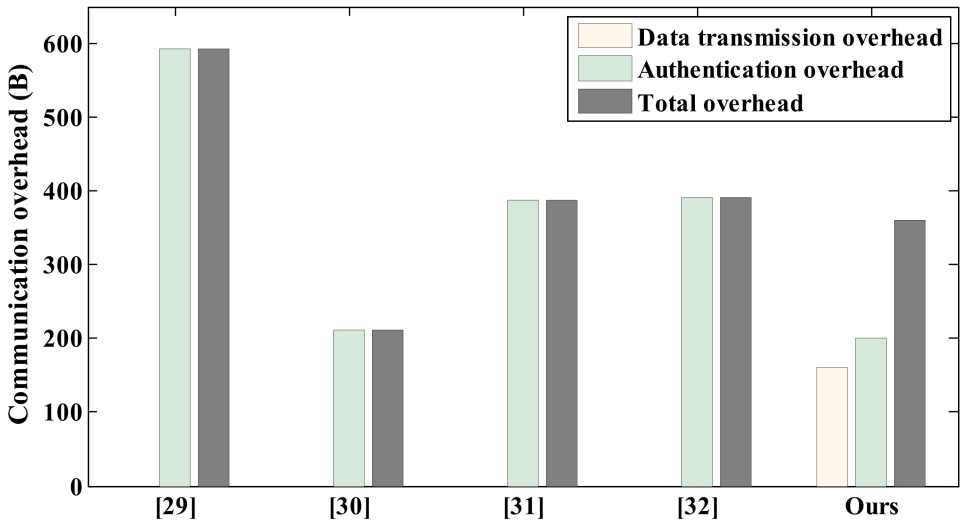

Figure 4. Comparative communication overheads for each protocol execution.

5.2. Computational Cost

In this section, we calculate the computational cost of our protocol and compare it with the schemes presented in [29–32]. Since GS is assumed to be a server with high computing power, we only consider computational costs for EV and CS sides. For calculating the execution time of each cryptographic

operator, the advantage of ArduinoLibs cryptographic library [46] has been taken. For simulating the cryptographic operators on an EV, an ARM Cortex-M3 microcontroller board named AT91SAM3 × 8E has been used, which is equipped with 512 kB flash memory and 96 kB SRAM, and has a clock speed of 84 MHz. To compute the execution times for a CS, the cryptographic operations have been conducted on a 64-bit operating system with processor Intel® Core™ i7-3612QM CPU @2.10 GHz and 6 GB (5.86 GB usable) RAM. The computed execution time of each cryptographic operation for EV and CS is demonstrated in Table 2. In addition, to compute the execution time of a PUF, we have considered the execution time of 128-bit Arbiter PUF on [47] AT91SAM3X8E. Since the execution time of a Chebyshev polynomial operation is one third of a point multiplication of the elliptic curve [48,49], we computed this value by dividing elliptic curve point multiplication run-time by three, without losing of any generality. In Table 2, T_h, T_{rng}, T_{PUF}, T_{mul}, T_{add}, T_{Chev}, T_{MAC}, T_m, T_{enc}, T_{dec}, , T_{Pol}, and T_{Fst} represent the execution time of SHA-256 hash function, a pseudo-random number generation, 128-bit Arbiter PUF key generation, an elliptic curve point multiplication, an elliptic curve point addition, the Chebyshev polynomial computation, one MAC operation, a multiplication, AES encryption, AES decryption, and Feistel structure-based encryption, respectively.

Table 2. Execution time of each cryptographic operation conducted on AT91SAM3X8E and Intel® Core™ i7 for electric vehicles (EV) and charge stations (CS), respectively.

	T_h	T_{rng}	T_{PUF}	T_{mul}	T_{add}	T_{Cehv}	T_{MAC}	T_m	T_{enc}	T_{dec}	T_{Fst}
EV	39.2 µs	82.3 µs	160.7 µs	37.9 ms	0.79 ms	12.6 ms	119.3 µs	0.67 ms	199.6 µs	309.7 µs	191.1 µs
CS	11.1 µs	31.5 µs		14.9 ms	216.1 µs	4.96 ms	33.8 µs	201.4 µs	41.8 µs	64.5 µs	39.1 µs

By discarding the computation complexity of logical XOR, our proposed protocol only executes three one-way hash functions in EV side. This ultra-lightweight design of protocol makes it very proper for EV side communication because of its constrained processing resources. Furthermore, our proposed protocol burdens CS only four one-way hash functions and two PUF operations, which takes a little time for CS (a fraction of one millisecond). Note that CS is usually considered an entity that has slightly more computational power than EV. Tables 3 and 4 demonstrate the number of cryptographic operators used in each protocol run-time for the EV and CS, respectively. According to Table 3, the proposed protocol has the lowest computational cost in the EV side. According to Table 4, although the proposed scheme is the second superior scheme in CS computational cost, it is still far better than the other schemes. Figure 5 depicts the EV side, CS side, and total computational cost of our proposed protocol, in comparison with the ones presented in [29–32]. As a result, it can be concluded that our scheme has an excellent performance in term of computational cost, especially (best) in the EV side.

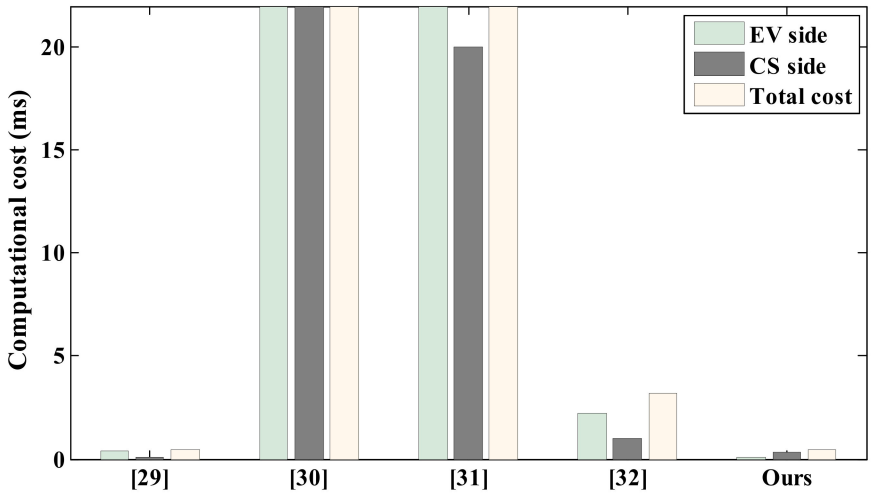

Figure 5. Comparative computational cost for each protocol execution.

Table 3. Number of each cryptographic operation used in one execution of each protocol and the computational cost for EV.

	T_h	T_{rng}	T_{PUF}	T_{mul}	T_{add}	T_{Cehv}	T_{MAC}	T_m	T_{enc}	T_{dec}	T_{Fst}	**Total Cost**
[29]	8	1	✘	✘	✘	✘	✘	✘	✘	✘	✘	0.396 ms
[30]	2	1	✘	5	3	✘	✘	✘	✘	✘	✘	192.03 ms
[31]	7	✘	✘	✘	✘	4	✘	2	✘	1	✘	52.32 ms
[32]	✘	2	2	✘	✘	✘	2	✘	1	1	5	2.19 ms
Ours	3	✘	✘	✘	✘	✘	✘	✘	✘	✘	✘	0.117 ms

Table 4. Number of each cryptographic operation used in one execution of each protocol and the computational cost for CS.

	T_h	T_{rng}	T_{PUF}	T_{mul}	T_{add}	T_{Cehv}	T_{MAC}	T_m	T_{enc}	T_{dec}	T_{Fst}	**Total Cost**
[29]	3	1	✘	✘	✘	✘	✘	✘	✘	✘	✘	0.065 ms
[30]	2	1	✘	4	2	✘	✘	✘	✘	✘	✘	60.08 ms
[31]	7	✘	✘	✘	✘	4	✘	2	✘	1	✘	20.36 ms
[32]	✘	3	2	✘	✘	✘	4	✘	1	1	10	1.04 ms
Ours	4	✘	2	✘	✘	✘	✘	✘	✘	✘	✘	0.365 ms

5.3. Characteristics Comparison

In this section, we present some important security and functional features of our protocol and compare them with the proposed schemes in [29–32] as demonstrated in Table 5. In this paper F_1 represents data confidentiality, F_2 represents data integrity, F_3 represents replay attack resistance, F_4 represents DoS attack resistance, F_5 represents physical attack resistance, F_6 represents enabling two-way communication, F_7 represents providing identity privacy against external adversary, F_8 represents providing location privacy against external adversary, F_9 represents ensuring privacy of the users against other legal entities in the network, F_{10} represents ultra-lightweight design, and F_{11} represents providing mutual authentication. Furthermore, the symbols ✔, ✘, and NA specified for each feature in Table 5 indicate ensuring corresponding feature, not ensuring corresponding feature, and that feature has not been investigated, respectively. According to Table 5, the proposed protocol in this paper provides all mentioned important features of the V2G network.

Table 5. Feature-based characterization of our proposed protocol in comparison with other schemes.

	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}
[29]	NA	NA	✔	✔	✘	✘	✔	✔	✔	✔	✔
[30]	NA	NA	✔	NA	✘	✘	✔	✘	✘	✘	✔
[31]	NA	NA	✔	NA	✘	✘	✔	✘	✘	✘	✔
[32]	NA	✔	✔	NA	✔	✘	✔	✘	✘	✘	✔
Ours	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

6. Conclusions

In this paper, we proposed a PUF-based secure authenticated protocol for V2G communications. We modeled a V2G network with three main entities, i.e., EVs, CSs, and GS, and a PPT adversary that can perform different kinds of attacks. The security analysis showed that our scheme may resist all possible known attacks, including eavesdropping and message analysis attack, message altering attack, impersonation and message injection attack, replay attack, DoS attack, physical attack, and different kinds of attack against identity and location privacy. Furthermore, the performance evaluations showed that our protocol has a good performance in communication overhead and excellent performance in computational cost. Especially seeing as each EV only needs to execute only three one-way hash function in our protocol. In addition, we saw, in the feature-based comparison section, that the proposed scheme ensured all important features related to V2G network. As a result, our scheme

could create a good trade-off between security and efficiency and propose a real-time and secure authenticated protocol for V2G communications.

Author Contributions: Conceptualization, M.K., D.M., and M.R.M.; Funding acquisition, D.M.; Investigation, M.K.; Methodology, M.K.; Supervision, M.R.M. and D.M.; Validations, M.K.; Original draft writing, M.K.; Review and editing, M.R.M. and D.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: This work is supported by the Ministry of Science, Innovation, and Universities through the COGNOS project.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Li, F.; Qiao, W.; Sun, H.; Wan, H.; Wang, J.; Xia, Y.; Xu, Z.; Zhang, P. Smart transmission grid: Vision and framework. *Renew. Sustain. Energy Rev.* **2010**, *1*, 168–177. [CrossRef]
2. Challa, S.; Das, A.K.; Gope, P.; Kumar, N.; Wu, F. Design and analysis of authenticated key agreement scheme in cloud-assisted cyber/Physical systems. *Future Gener. Comput. Syst.* **2020**, *108*, 1267–1286. [CrossRef]
3. Vasudev, H.; Das, D.; Vasilakos, A.V. Secure message propagation protocols for IoVs communication components. *Comput. Electr. Eng.* **2020**, *82*, 106555. [CrossRef]
4. Kempton, W.; Tomi'c, J. Vehicle-to-grid power fundamentals: Calculating capacity and net revenue. *J. Power Sources* **2005**, *144*, 268–279. [CrossRef]
5. Park, J.; Kim, H.; Choi, J. Improving TCP performance in vehicle-to-grid (V2G) communication. *Electronics* **2019**, *8*, 1206. [CrossRef]
6. Shen, Y.; Fang, W.; Ye, F.; Kadoch, M. EV charging behavior analysis using hybrid intelligence for 5G smart grid. *Electronics* **2020**, *9*, 80. [CrossRef]
7. Khan, P.; Byun, Y. Smart contract centric inference engine for intelligent electric vehicle transportation system. *Sensors* **2020**, *20*, 4252. [CrossRef]
8. Fazeli, S.S.; Venkatachalam, S.; Chinnam, R.B.; Murat, A. Two-stage stochastic choice modeling approach for electric vehicle charging station network design in urban communities. *IEEE Trans. Intell. Transp. Syst.* **2020**, 1–16. [CrossRef]
9. Abronzini, U.; Attaianese, C.; D'Arpino, M.; Monaco, M.D.; Tomasso, G. Cost minimization energy control including battery aging for multi-source EV charging station. *Electronics* **2019**, *8*, 31. [CrossRef]
10. Wazid, M.; Das, A.K.; Kumar, N.; Vasilakos, A.V. Design of secure key management and user authentication scheme for fog computing services. *Future Gener. Comput. Syst.* **2019**, *91*, 475–492. [CrossRef]
11. Kaveh, M.; Mosavi, M.R. A lightweight mutual authentication for smart grid neighborhood area network communications based on physically unclonable function. *IEEE Syst. J.* **2020**, *14*, 4535–4544. [CrossRef]
12. Wazid, M.; Das, A.K.; Bhat, V.; Vasilakos, A.V. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. *J. Netw. Comput. Appl.* **2020**, *150*, 102496. [CrossRef]
13. Aghapour, S.; Kaveh, M.; Martín, D.; Mosavi, M.R. An ultra-lightweight and provably secure broadcast authentication protocol for smart grid communications. *IEEE Access* **2020**, *8*, 125477–125487. [CrossRef]
14. Mustafa, M.; Zhang, N.; Fan, Z. Smart electric vehicle charging: Security analysis. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference, Washington, DC, USA, 24–27 February 2013; pp. 1–6.
15. Guo, H.; Wu, Y.; Ma, M. UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications. *IEEE Trans. Smart Grid* **2011**, *2*, 707–714. [CrossRef]
16. Liu, H.; Ning, H.; Yang, L. Role-dependent privacy preservation for secure V2G networks in the smart grid. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 208–220. [CrossRef]
17. Yang, Z.; Yu, S.; Liu, C. P2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid. *IEEE Trans. Smart Grid* **2011**, *2*, 697–706. [CrossRef]
18. Liu, H.; Ning, H.; Zhang, Y.; Yang, L.T. Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid. *IEEE Trans. Smart Grid* **2012**, *66*, 1722–1733. [CrossRef]

19. Abdallah, A.; Shen, X. Lightweight authentication and privacy-preserving scheme for V2G connections. *IEEE Trans. Veh. Technol.* **2017**, *3*, 2615–2629. [CrossRef]
20. Saxena, N.; Choi, B.J. Authentication scheme for flexible charging and discharging of mobile vehicles in the V2G networks. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1438–1452. [CrossRef]
21. He, D.; Chan, S.; Guizani, M. A privacy-friendly and efficient secure communication framework for V2G networks. *IET Commun.* **2018**, *12*, 304–309. [CrossRef]
22. Zhang, Y.; Gjessing, S.; Liu, H.; Ning, H.; Yang, L.T.; Guizani, M. Securing vehicle-to-grid communications in the smart grid. *IEEE Wirel. Commun.* **2018**, *20*, 66–73. [CrossRef]
23. 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*, 2526–2536. [CrossRef]
24. He, D.; Zeadally, S.; Xu, B.; Huang, X. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. *IEEE Trans. Inf. Forensics Secur.* **2015**, *10*, 2681–2691. [CrossRef]
25. Liu, Y.; Wang, Y.; Chang, G. Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749. [CrossRef]
26. 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 Secur.* **2015**, *10*, 2340–2351. [CrossRef]
27. Vijayakumar, P.; Azees, M.; Kannan, A.; Deborah, L.J. Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 1015–1028. [CrossRef]
28. Tan, H.; Choi, D.; Kim, P.; Pan, S.; Chung, I. Comments on Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2149–2151. [CrossRef]
29. Gope, P.; Sikdar, B. An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication. *IEEE Trans. Smart Grid* **2019**, *10*, 6607–6618. [CrossRef]
30. Su, Y.; Shen, G.; Zhang, M. A novel privacy-preserving authentication scheme for V2G networks. *IEEE Syst. J.* **2019**, *14*, 1963–1971. [CrossRef]
31. Abbasinezhad-Mood, D.; Ostad-Sharif, A.; Mazinani, S.M.; Nikooghadam, M. Provably-secure escrow-less Chebyshev chaotic map-based key agreement protocol for vehicle to grid connections with privacy protection. *IEEE Trans. Ind. Inform.* **2020**, *2020*, 1. [CrossRef]
32. Gaurang, B.; Naren, N.; Chamola, V.; Sikdar, B.; Kumar, N.; Guizani, M. Lightweight mutual authentication protocol for V2G using physical unclonable function. *IEEE Trans. Veh. Technol.* **2020**, *69*, 7234–7246.
33. Maes, R. Physically unclonable functions: concept and nonstructions. In *Physically Unclonable Functions: Constructions, Properties and Applications*; Springer: Berlin, Germany, 2012; ISBN 978-3-642-41395-7.
34. Naveed, M.; Chaing, K.; Sikdar, B. Mutual authentication in IoT systems using physical unclonable functions. *IEEE Internet Things J.* **2017**, *4*, 1327–1340.
35. Gope, P.; Lee, J.; Quek, T.Q. Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 2831–2843. [CrossRef]
36. Delavar, M.; Mirzakuchaki, S.; Mohajeri, J. A ring oscillator-based PUF with enhanced challenge-response pairs. *Canadian J. Electr. Comput. Eng.* **2016**, *39*, 174–180. [CrossRef]
37. Gope, P.; Sikdar, B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. *IEEE Internet Things J.* **2018**, *6*, 580–589. [CrossRef]
38. Kaveh, M.; Aghapour, S.; Martin, D.; Mosavi, M.R. A secure lightweight signcryption scheme for smart grid communications using reliable physically unclonable function. In Proceedings of the IEEE International Conference on Environment and Electrical Engineering and IEEE Industrial and Commercial Power Systems Europe, Madrid, Spain, 9–12 June 2020; pp. 1–6.
39. Gao, Y.; Su, Y.; Xu, L.; Ranasinghe, D.C. Lightweight (reverse) fuzzy extractor with multiple reference PUF responses. *IEEE Trans. Inf. Forensics Secur.* **2018**, *14*, 1887–1901. [CrossRef]
40. Pandey, S.; Deyati, S.; Singh, A.; Chatterjee, A. Noise-resilient SRAM physically unclonable function design for security. In Proceedings of the IEEE 25th Asian Test Symposium (ATS), Hiroshima, Japan, 21–24 November 2016; pp. 55–60.

41. Jeon, D.; Baek, J.H.; Kim, D.K.; Choi, B.D. Towards zero bit-error-rate physical unclonable function: Mismatch-based vs. physical-based approaches in standard CMOS technology. In Proceedings of the 2015 Euromicro Conference on Digital System Design, Madeira, Portugal, 26–28 August 2015; pp. 407–414.
42. Chuang, K.H.; Bury, E.; Degraeve, R.; Kaczer, B.; Linten, D.; Verbauwhede, I. A physically unclonable function using soft oxide breakdown featuring 0% native BER and 51.8 Fj/Bit in 40-Nm CMOS. *IEEE J. Solid State Circuits* **2018**, *54*, 2765–2776. [CrossRef]
43. Lu, X.; Hong, L.; Sengupta, K. CMOS optical PUFs using noise-immune process-sensitive photonic crystals incorporating passive variations for robustness. *IEEE J. Solid State Circuits* **2018**, *53*, 2709–2721. [CrossRef]
44. Wang, W.C.; Yona, Y.S.; Diggavi, N.; Gupta, P. Design and analysis of stability-guaranteed PUFs. *IEEE Trans. Inf. Forensics Secur.* **2017**, *13*, 978–992. [CrossRef]
45. Jindal, A.; Kumar, N.; Singh, M. Internet of energy-based demand response management scheme for smart homes and PHEVs using SVM. *Future Gener. Comput. Syst.* **2018**, *108*, 1058–1068. [CrossRef]
46. ArduinoLibs: Cryptographic Library. 2019. Available online: http://rweather.github.io/arduinolibs/crypto.html (accessed on 11 June 2020).
47. Herder, C.; Yu, M.D.; Koushanfar, F.; Devadas, S. Physical unclonable functions and applications: A tutorial. In Proceedings of the IEEE, Istanbul, Turkey, 3–5 April 2014; pp. 1126–1141.
48. Abbasinezhad-Mood, D.; Nikooghadam, M. Efficient design of a novel ECC-based public key scheme for medical data protection by utilization of NanoPi fire. *IEEE Trans. Reliab.* **2018**, *67*, 1328–1339. [CrossRef]
49. Zhu, H.; Zhang, Y.; Xia, Y.; Li, H. Password-authenticated key exchange scheme using chaotic maps towards a new architecture in standard model. *IJ Netw. Secur.* **2016**, *18*, 326–334.