IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 10 August 2022, accepted 26 August 2022, date of publication 1 September 2022, date of current version 13 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3203580

RESEARCH ARTICLE

An Efficient and Physically Secure Privacy-Preserving Authentication Scheme for Vehicular Ad-hoc NETworks (VANETs)

ALIREZA AGHABAGHERLOO[1], MAHSHID DELAVAR[2], JAVAD MOHAJERI[3], MAHMOUD SALMASIZADEH[3], AND BART PRENEEL[1], (Member, IEEE)

[1]imec-COSIC, Department of Electrical Engineering, KU Leuven, 3001 Leuven, Belgium
[2]Department of Computer Science, University of Warwick, Coventry CV4 7EZ, U.K.
[3]Electronics Research Institute, Sharif University of Technology, Tehran 11155-11365, Iran

Corresponding author: Alireza Aghabagherloo (Alireza.aghabagherloo@esat.kuleuven.be)

This work was supported by in part by the Cyber Security Research Flanders under Grant VR20192203, and in part by the Research Council KU Leuven C1 on Security and Privacy for Cyber-Physical Systems and the Internet of Things under Contract C16/15/058.

ABSTRACT Vehicular ad-hoc networks (VANETs) can substantially improve traffic safety and efficiency by providing a communication platform between vehicles and roadside units (RSUs) to share real-time information on traffic and road conditions. Two essential security requirements for VANETS are data authentication and the preservation of the privacy of vehicle owners. Conditional privacy-preserving authentication (CPPA) schemes address both of these security requirements. The existing CPPA schemes either require a tamper-resistant device (TRD), which is vulnerable to key exposure based on physical attacks, or require continuous communications of vehicles with RSUs, which significantly increases the communication overhead. This paper addresses both of these problems by proposing a provable secure, and efficient CPPA scheme. We prove the privacy-preserving property of our scheme in the random oracle model and show that it offers anonymity, unlinkability, and tamper detection even if a physical attacker succeeds in compromising an individual OBU. Moreover, the performance analysis of our scheme shows a substantial improvement in communication cost, especially in comparison with RSU-aided schemes that require continuous vehicle communication with roadside units and a Trusted Authority (TA).

INDEX TERMS Vehicular ad-hoc networks, privacy-preserving schemes, provable security, authentication, physically secure, fail-stop signature.

I. INTRODUCTION

Many road accidents are caused by the lack of timely information to the vehicle's drivers, resulting in inappropriate or delayed responses to unexpected situations. Vehicular Ad-hoc NETworks (VANETs) can increase safety by transmitting relevant information to drivers in a timely way. Four entities are involved in these networks: drivers (users), On-Board Units (OBU) in vehicles, Road-Side Units (RSU), and a Trusted Authority (TA) [1]. A Tamper Resistant Device (TRD) or Trusted Platform Module (TPM) can be embedded in OBUs. Vehicle drivers are authenticated with a password, a smart card, or a security token (e.g., stored on a smartphone). OBUs and RSUs can establish Vehicle-to-Vehicle (V-2-V) and Vehicle-to-RSU (V-2-R) communications, and RSUs can communicate with the TA over the internet (Figure 1). Each vehicle acts as a node in these networks and sends the information to its closest neighbors.

One of the major concerns in these networks is how to authenticate the sender while protecting the anonymity of vehicles and their drivers. The existing authentication schemes for vehicular ad-hoc networks can be categorized

The associate editor coordinating the review of this manuscript and approving it for publication was Zijian Zhang.

into two categories; symmetric-encryption-based schemes and asymmetric-encryption-based schemes. Symmetric-encryption-based schemes usually have lower computation costs. However, they do not provide public verification and irrefutability properties. Some examples of these schemes are [1], [2], [3], and [4], the first two of which have high communication costs because of the vehicle's continuous communication with RSUs.

Asymmetric-encryption-based schemes can also be categorized into schemes based on Public-Key Infrastructure (PKI) and Identity-based schemes. Identity-based schemes usually have lower communication and computational costs compared to PKI-based schemes [5], [6], [7], which makes them attractive for VANETs. The disadvantage is that a single central party (or a distributed set of such parties) has full knowledge of all secrets. The traditional CPPA schemes which use tamper-resistant devices such as [8], [9], and [10] are some examples of identity-based schemes. The advantage of the schemes introduced in [8], [9], and [10] is their low computational cost obtained by avoiding expensive bilinear maps. Moreover, the ideas presented in [8] have been used in other schemes like [11], [12], [13], [14], [15], and [16].

The main issue of TRD-aided CPPA schemes [8], [9], [10] is their strong assumption on the security of these devices w.r.t. physical attacks. However, it is well known that side-channel and fault injection attacks can extract secret key material from tamper-resistant devices [17], [18]. Although the researches in [4], [14], [19], [20], [21], [22], and [23] tried to address this problem, their proposed schemes, which we call RSU-aided schemes, require continuous vehicle communications with RSUs and the TA. This imposes high communication costs on the network. Since traffic emergency messages need an ultra-low transmission delay, the delay caused by these continuous communications makes these schemes impractical for VANETs. Wei *et al.* in [24] have also addressed the physical security of TRDs by introducing a new CPPA scheme in which TRDs of unrevoked vehicles update their private key securely using Shamir's secret sharing algorithm [25], [26]. Updating the key can reduce the opportunity for and impact of a physical attack; however, if such an attack recovers a private key from a single OBU, the attacker can quickly obtain newly updated keys using the previous key or can even update other vehicles' private key on behalf of the TA using the private key recovered from a single TRD.

One can also classify VANET security solutions based on other aspects, such as the use of blockchain [27], [28], Machine Learning [29], [30], edge computing [29], [30], or the 5G infrastructure [30], [31]. Blockchain-based schemes build on distributed trust and may not require trust in a central authority; whey they offer transparency, decentralization, and security, their design has some challenges, such as storage space, energy efficiency, and delay [32], [33]. Machine learning (ML) algorithms are used in various applications and play an essential role in creating next-generation systems. However, as indicated in [34], to achieve its full potential in VANET, many challenges need to be addressed, such as requiring sufficiently large datasets for a high-scale and heterogeneous network and the development of an appropriate model for collected data; these challenges show that using ML in VANETs still needs further investigation. Lai *et al.* [31] present the infrastructure of 5G-enabled vehicular networks and introduce the essential security and privacy aspects of 5G-V2X; however, as indicated in [31] and [34], despite the great success of 5G-V2X in developing the next generation of VANETs, the security of the overall architecture is still questionable. Cui *et al.* [29] proposed a privacy-preserving data downloading scheme by adopting the concept of edge computing for VANETs, and Zhang *et al.* [30] proposed an authentication scheme by combining 5G technology and edge computing. As mentioned in [35] and [36] similar to RSU-aided schemes, [29] impose a high communicational cost to the system, and once the TRDs of the proposed scheme in [30] fall into the single point of failure, the entire network faces privacy disclosure.

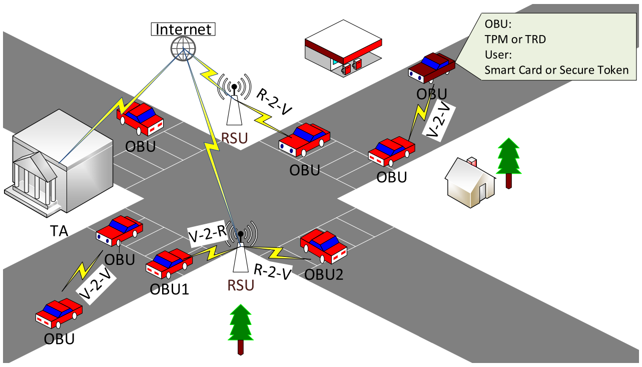


FIGURE 1. The architecture of vehicular ad-hoc networks [8].

A. OUR CONTRIBUTIONS

This paper first shows the shortcomings of existing CPPA schemes. Then, it proposes a new efficient privacy-preserving authentication scheme for VANETs that combines the advantages of both traditional and recently introduced CPPA schemes with additional security and privacy requirements such as anonymity and unlinkability without increasing the performance costs. In addition, the scheme is robust against the compromise of individual TRDs.

The main advantages of our scheme compared to RSU-aided and TRD-aided CPPA schemes can be summarized as follows:

- Our proposal does not require continuous vehicle communication with RSUs and the TA, resulting in a more efficient scheme than the existing RSU-aided schemes.
- By adding tamper detection to existing CPPA schemes, the security and privacy requirements (namely, revealing and revoking the identity of the users who break the rules, detecting forged messages, preserving the identity of other vehicles, and untraceability and unlinkability of

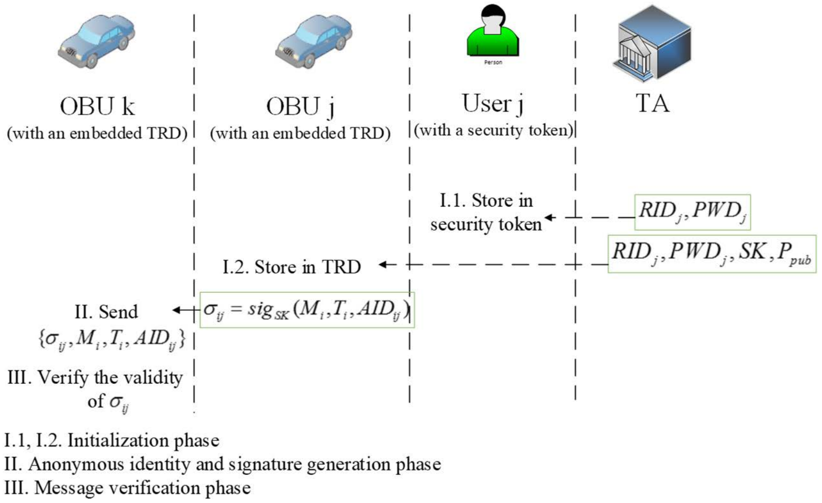

OBU k
(with an embedded TRD)
OBU j
(with an embedded TRD)
User j
(with a security token)
TA
Person
I.1. Store in security token
RID_j, PWD_j
$RID_j, PWD_j, SK, P_{pub}$
I.2. Store in TRD
II. Send $\{\sigma_{ij}, M_i, T_i, AID_{ij}\}$
$\sigma_{ij} = sig_{SK}(M_i, T_i, AID_{ij})$
III. Verify the validity of σ_{ij}
I.1, I.2. Initialization phase
II. Anonymous identity and signature generation phase
III. Message verification phase

FIGURE 2. An overview of traditional TRD-aided CPPA schemes [8], [9], [10], [24].

vehicles) are satisfied even if the private key of an OBU is revealed.

- The opportunity for and impact of physical attacks is reduced with a private key updating mechanism.

The paper is organized as follows: Section II introduces the traditional CPPA schemes based on tamper-resistant devices and the recently introduced RSU-aided CPPA schemes. We also discuss their vulnerabilities and deficiencies. In Sect. III, we introduce our new scheme. Section IV is dedicated to the security and performance analysis of our scheme. We conclude the paper in Sect. V.

II. RELATED WORK

This section provides a brief overview of the most important Conditional Privacy-Preserving Authentication (CPPA) schemes introduced in [4], [8], [9], [10], [14], [19], [20], [21], and [24], and shows their vulnerability. Traditional TRD-aided CPPA schemes have been introduced in [8], [9], and [10]. These schemes can be used for both Vehicle to Vehicle (V-2-V) and Vehicle to Road Side Unit (V-2-R) communications. One of the advantages of these schemes is V-2-V authentication without the RSU's intervention, which leads to a reduced communication overhead.

A. REVIEW OF TYPICAL TRD-AIDED CPPA SCHEMES

These schemes usually consist of three phases:

1) INITIALIZATION

in this phase, the TA sets up the network. It first generates the public and private parameters, including the system private key SK, the corresponding public key P_{pub}, and each vehicle's real identity RID_j. Then, the TA publishes the public parameters in the network and stores SK in each vehicle's TRD together with the identity RID_j of the vehicle. A security token is also stored in the TRD to authenticate the drivers (it could, for example, be a salted hash of a user password).

2) ANONYMOUS IDENTITY AND SIGNATURE GENERATION

in this phase, the TRD authenticates the vehicle's owner by checking the stored parameters in the security token and generates an anonymous identity and a signature for each message that it sends. To this end, OBU_j uses P_{pub} and RID_j to generate the Anonymous ID AID_{ij} for the i-th message. Knowledge of SK is required to derive the value of RID_j by having an AID. After generating AID_{ij}, the OBU_j signs the message M_i, AID_{ij}, and the time stamp T_i using the private key SK stored in its TRD.

$$\sigma_{ij} = sig_{SK}(M_i| |T_i| |AID_{ij}). \tag{1}$$

Finally, the OBU_j broadcasts $\sigma_{ij}| |M_i| |T_i| |T_i| |AID_{ij})$ to the nearest RSU and to the other neighboring vehicles.

3) MESSAGE VERIFICATION

in this phase, the OBU can verify the messages in single and batch mode using the public key $\mathrm{P_{pub}}$. Figure 2 gives an overview of TRD-aided CPPA schemes. The continuous and temporary communications are depicted by solid and dashed lines, respectively.

B. VULNERABILITIES OF TRD-AIDED CPPA SCHEMES

Bayat *et al.* introduced an ID-based CPPA scheme, the security of which is based on tamper-resistant devices [9]. Subsequently, He *et al.* [8] and Zhong *et al.* [10] improved its efficiency. The security of these three schemes has been formally proved. The authors have shown that if the OBU devices are tamper-resistant, the scheme is secure against impersonation, message modification, man-in-the-middle, identity disclosure, and replay attacks. Moreover, it has been shown that only the trusted authority can find out the real identity of the vehicles that break the rules. However, it has been assumed in [14], [21], and [24] that the secret value stored in a tamper-resistant device can be revealed, for example, through physical attacks: in this case, the security of all mentioned schemes is compromised.

As indicated in Sec. II.B, in TRD-aided schemes, the entity with SK can obtain the RID_j corresponding to an AID. Thus, by extracting the secret value SK, a physical attacker can find the real identities of all other vehicles from their Anonymous IDs and track them. Moreover, she can impersonate any vehicle in the network and sign messages on their behalf using the obtained SK.

Moreover, these schemes do not provide any solution for detecting whether a device has been tampered with or not. Therefore, none of the vehicles can prove that they have not sent the forged message. Even if there is a solution to detect the compromised devices, in the case of a compromised OBU, all the stored secret values need to be updated.

In 2021, Wei *et al.* [24] tried to address this problem by updating SK. Although this method does reduce the attack surface, an attacker who recovers a single private key will still quickly obtain newly updated keys using the previous key; this shows that the update approach has strong limitations. The other vulnerability of [24] is that the TA uses the stored private key in TRDs, to sign the private key updating message; hence an attacker who recovers a privacy key from a single TRD will be able to send a private key updating message on behalf of the TA to all other vehicles.

C. REVIEW OF TYPICAL RSU-AIDED CPPA SCHEMES

RSU-aided CPPA schemes [1], [4], [14], [19], [20], [21], [22] are ID-based schemes that support V-2-V and V-2-R communications. These schemes have the same four entities involved and, in most cases, authenticate drivers using a smart card. They typically consist of the following five phases (see Figure 3 for an overview):

1) USER REGISTRATION PHASE

Each OBU and each user's smart card must be registered with the TA once. Here, it is assumed that during registration, there is a secure channel between the TA and the OBU and the TA and the user. Also, it is assumed that only authorized users can register with the TA (and thus, an adversary is not able to do so).

2) USER LOGIN PHASE

In this phase, each user U_j inserts a valid smart card in its OBU. It is assumed that a protocol for entity authentication is executed that resists replay attacks.

3) USER AUTHENTICATION PHASE

Each time an OBU with ID_j enters the range of a new RSU, it must be authenticated with the TA. After that, the OBU obtains a session key shared with the RSU (notice that each vehicle obtains a different key compared to other vehicles in the range of that RSU, and the RSU acts here as an intermediary between OBUs and the TA).

4) DATA AUTHENTICATION PHASE

In this phase, the OBUs communicate with each other and authenticate the transmitted data using the secret session key shared in the previous phase.

5) PASSWORD CHANGING PHASE

In this phase, the vehicle owner who notices her password has been compromised attempts to change her password saved in the smart card.

D. SECURITY AND PERFORMANCE ANALYSIS OF RSU-AIDED CPPA SCHEMES

Aghabagherloo *et al.* have shown in [4] that the schemes of [19] and [20] do not provide unlinkability of messages transmitted within the range of a single RSU since the verifier must use a parameter of the previous message to validate the new message. The scheme of [14] has solved this problem using a Bloom filter with the interposition of the RSU; however, it requires permanent communication between the OBU and the RSU in all V-2-V communications. Moreover, the scheme in [19] does not provide any solution to change the password. The scheme of [14] satisfies most of the security requirements for VANETs. However, similar to [19] and [20], the permanent communications of the vehicles with RSUs make the scheme highly inefficient. These RSU-aided schemes offload the overhead to RSUs and require the dense deployment of RSU [16].

Another issue with the schemes of [19] and [20] is that the TA cannot revoke registered IDs that violate the terms of service since they do not employ a registration list. In 2021 Zhang *et al.* [23] designed a Chinese remainder theorem (CRT) based CPPA scheme in VANETs. Although this scheme needs a realistic TRD, and the master key of the system does not need to be preloaded into the OBUs, similar to RSU-aided schemes, the necessity of obtaining the secret domain key from TA imposes a high communication cost.

Pournaghi *et al.* [26] proposed a scheme that combines RSU-aided and TRD-aided solutions. Their scheme has the property that when a vehicle wants to enter a new RSU range, it should authenticate itself to the RSU, and then the OBU receives a temporary key from the RSU. Although this scheme does not need continuous communication of RSUs with TA, it does not solve the main problem of RSU-aided schemes, which is the necessity of permanent communication of OBUs with RSUs. In fact, in this scheme, RUSs are considered as fully trusted parties, similar to TA. The other weakness of this scheme is that the messages sent by OBUs do not contain any timestamp, and the transmitted messages are valid until the expiration of T_s (Timestamp of the RSU). This can enable a replay attack during the validity period of T_s. To tackle this problem, the timestamp of RSUs must be updated regularly, which will impose high communication costs.

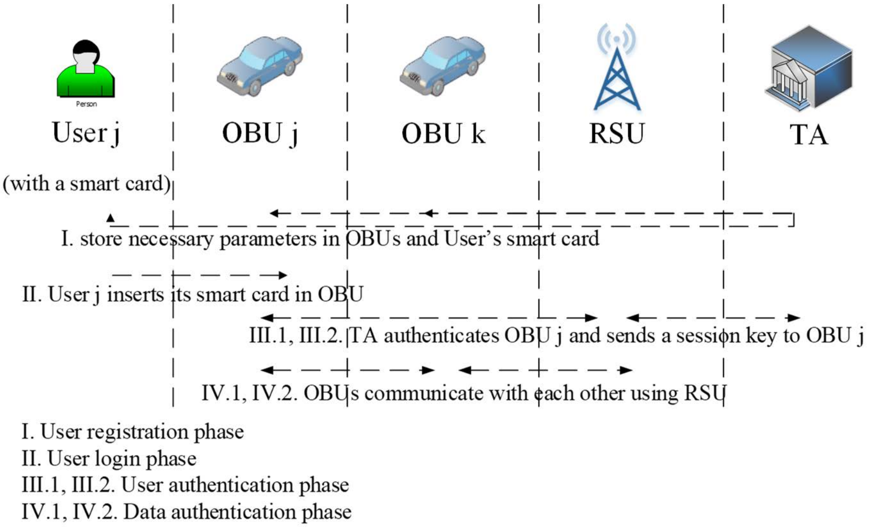

Person
User j
(with a smart card)
OBU j
OBU k
RSU
TA
I. store necessary parameters in OBUs and User's smart card
II. User j inserts its smart card in OBU
III.1, III.2. TA authenticates OBU j and sends a session key to OBU j
IV.1, IV.2. OBUs communicate with each other using RSU
I. User registration phase
II. User login phase
III.1, III.2. User authentication phase
IV.1, IV.2. Data authentication phase

FIGURE 3. An overview of RSU-aided CPPA schemes [1], [4], [14], [19], [20], [21], [22], [23].

TABLE 1. Notation.

Notation	Description
p, q	Two large prime numbers
E	An elliptic curve defined by $y^2 = x^3 + ax + b \bmod p$
RID_{jt}, K_{jt}	The real identity and key of the j-th vehicle in the t-th cluster
AID_{ijt}	The anonymous identity of the j-th vehicle in the t-th cluster in the i-th session
PK_{TA}, SK_{TA}	The master public and private key of the TA
PK_t, SK_t	The public and private keys of t-th cluster
h_1, h_2, h_3, h_4	Cryptographic hash functions

III. THE PROPOSED SCHEME

As mentioned in Section II, traditional CPPA schemes take advantage of a tamper-resistant device in their design. While these schemes are efficient, the compromise of a single OBU undermines the security of the complete system. Moreover, RSU-aided CPPA schemes have high computational and communication overheads since they require continuous communication between the vehicles and RSUs as well as vehicles and the TA.

Here, we propose a novel CPPA scheme with improved security and efficiency. Similar to the other schemes, our scheme consists of the following entities:

A. TRUSTED AUTHORITY (TA)

This entity is responsible for generating public parameters of the network. It is the only entity that can figure out the real identity of the vehicles.

B. ROAD SIDE UNITS (RSUs)

These entities are in wireless communication with other entities in the network. They can authenticate the transmitted messages or send specific messages to the TA.

C. ON-BOARD UNITS (OBUs)

Each vehicle can generate an authenticated message or authenticate the messages received from other vehicles. We assume that a secret value has been stored in each OBU, but we consider that information can leak from OBU.

Unlike RSU-aided CPPA schemes, there is no need for continuous communication between the other entities and the TA in our scheme. Also, tampering with the OBU and extracting secret keys does not compromise the full scheme. However, our scheme has a process in which suspicious messages are verified with the TA: this requires a few rounds of communication between OBU and TA and results in the revocation of OBUs whose secrets have been exposed; this is a major improvement over earlier TRD-aided CPPA schemes.

In other words, our proposed scheme combines the good properties of both types of schemes. Thus, unlike TRD-aided CPPA, information leakage from the OBU does not compromise the security properties of our scheme, and unlike RSU-aided schemes, there is no need for a continuous connection between vehicles and the TA and RSUs.

Our proposed scheme runs in four phases (Figure 4): 1. Initialization; 2. Anonymous ID and signature generation;

3. Message verification; 4. Forgery notification and detection of impersonated messages. In addition, a private key updating algorithm is described at the end of this section: this algorithm mitigate the impact of physical attacks. The private key updating algorithm has been inspired by the algorithm proposed in [24], but we have used SK_{TA} instead of the stored private key in OBUs to sign the private key updating message, which enhances security.

We describe our scheme in an ECC group as an example, but it can be applied in any generic group of prime order in which the discrete logarithm problem is hard.

D. INITIALIZATION

this phase consists of the following steps:

The TA generates two prime numbers p and q, as well as the elliptic curve E defined as:

$$y^2 = x^3 + ax + b \, mod \, p \quad a, b \in F_p. \tag{2}$$

The TA chooses a point P of order q on the elliptic curve E, and defines the cyclic group G as the subgroup generated by $< P >$. Also, the TA chooses as a private key a random number $SK_{TA} \in_R Z_q^*$ and computes the corresponding master public key:

$$PK_{TA} = SK_{TA} \cdot P. \tag{3}$$

The TA categorizes the vehicles into k clusters and generates a secret key for each cluster by picking a random integer $SK_t \in_R Z_q^*$. SK_t is securely stored in the OBU of all vehicles in that cluster. In this regard, first, we categorize vehicles according to their location of registration, and then we put each type of vehicle in one cluster. For example, we can group the vehicles of one country into emergency vehicles such as ambulances or fire engines, police cars, and rescue vehicles, and other types of vehicles such as passenger cars, vans, buses, and trucks.

Next, the public key corresponding to each cluster is generated by the TA as follows:

$$PK_t = SK_t \cdot P. \tag{4}$$

Then the TA defines the following four cryptographic hash functions:

$$h_1 : \{0, 1\}^* \rightarrow \{0, 1\}^* \tag{5}$$
$$h_2 : G \rightarrow Z_q \tag{6}$$
$$h_3 : \{0, 1\}^* \rightarrow Z_q \tag{7}$$
$$h_4 : \{0, 1\}^* \times \{0, 1\}^* \times G \times \{0, 1\}^* \rightarrow Z_q. \tag{8}$$

These hash functions are assumed to be (second) preimage resistant and collision-resistant; in our security proof, they will be modeled as Random Oracles (ROs).

The TA assigns a fixed identity RID_{jt} and a secret key K_{jt} to the j-th vehicle in the t-th cluster and puts them in the corresponding security token to the j-th vehicle. Then, the tuple $(h_1(RID_{jt}, K_{jt}), SK_t)$ is stored in the OBU of that vehicle.

Finally, the following public parameters are sent to all the entities in the network (OBUs and RSUs):

$$parameters = \{p, q, a, b, P, PK_{TA}, PK_t, \\ 1 \leq t \leq k, h_1, h_2, h_3, h_4\}.$$

E. ANONYMOUS IDENTITY AND SIGNATURE GENERATION

in this phase, the user is authenticated; next, the OBU generates the anonymous identity and signature to produce an authenticated message through the following steps.

The authorized user of the vehicle inserts the security token into the OBU's card reader. The OBU executes a protocol for entity authentication that resists replay attacks. In the case of successful authentication, OBU uses K_{jt} in the subsequent steps.

The OBU generates the anonymous identity $AID_{ijt} = \{AID_{ijt,1}, AID_{ijt,2}, AID_{ijt,3}\}$, and the parameters α_{ijt} and s_{ijt} as follows:

$$w_i \in_R Z_q^*, \quad AID_{ijt,1} = w_i P \tag{9}$$
$$AID_{ijt,2} = K_{jt} \oplus h_2(w_i \cdot PK_{TA}) \tag{10}$$
$$AID_{ijt,3} = h_4(K_{jt}, w_i \cdot PK_{TA}, T_i) \tag{11}$$
$$\alpha_{ijt} = h_3(AID_{ijt}, T_i) \tag{12}$$
$$s_{ijt} = w_i + \alpha_{ijt} \cdot SK_t mod \, q. \tag{13}$$

The vehicle uses the values generated in the previous step to generate the signature (σ_{ijt}) on the message M_i using a variant of the Schnorr signature algorithm [37].

$$r_i \in Z_q^*, \quad R_i = r_i P \tag{14}$$
$$\beta_{ijt} = h_4(AID_{ijt}, T_i, R_i, M_i) \tag{15}$$
$$\sigma_{ijt} = s_{ijt} + \beta_{ijt} \cdot r_i mod \, q. \tag{16}$$

Finally, the vehicle sends the anonymous identity, the message, and the signature $\{t, \sigma_{ijt}, M_i, R_i, T_i, AID_{ijt}\}$ to the nearest RSU and the neighboring vehicles.

F. MESSAGE VERIFICATION

this phase includes the verification of a single message and batch verification of multiple messages. Suppose a vehicle or an RSU wants to check the validity of only one message. In that case, it can verify Eqn. (17). If this vehicle or RSU wants to check the validity of multiple messages belonging to one cluster's vehicles, it can verify Eqn. (18).

If the OBU verifies the signature on a single message, each module uses the public key of the cluster to verify that the message has been sent by one of its members.

$$\begin{aligned} \sigma_{ijt}.P &= (s_{ijt} + \beta_{ijt} \cdot r_i) \cdot P \\ &= w_i \cdot P + \alpha_{ijt} \cdot SK_t.P + \beta_{ijt} \cdot r_i \cdot P \\ &= AID_{ijt,1} + \alpha_{ijt} \cdot PK_t + \beta_{ijt} \cdot R_i mod \, q. \end{aligned} \tag{17}$$

If the OBU verifies the signatures on a batch of messages, the module authenticates the messages sent by the vehicles in one cluster using the random vector $v = \{v_1, \ldots, v_n\}$ and the

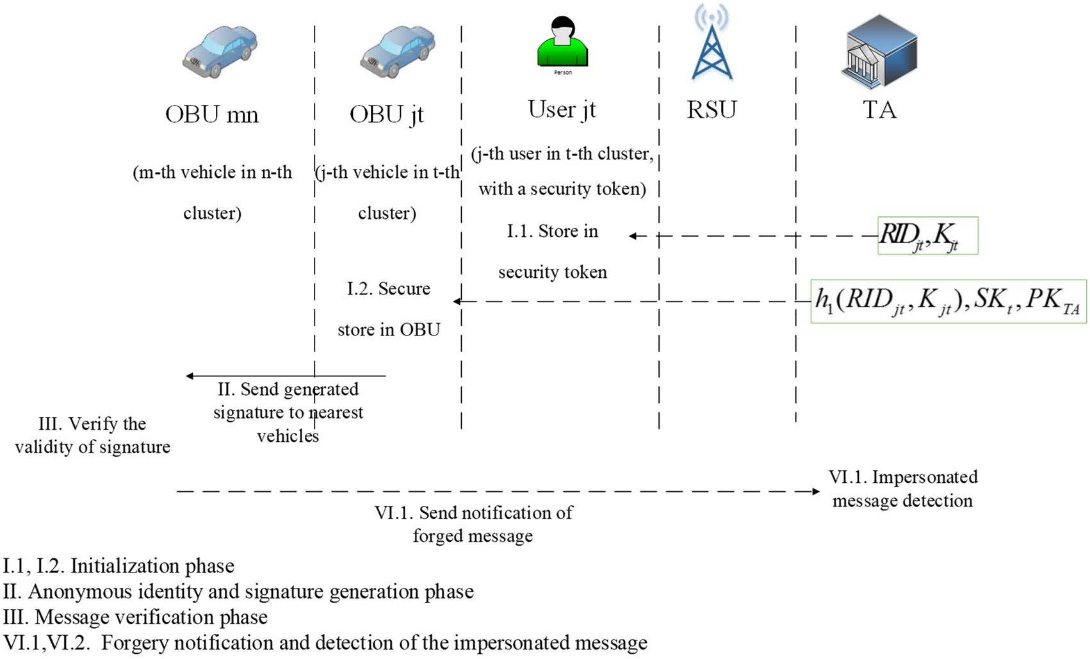

OBU mn
(m-th vehicle in n-th cluster)
OBU jt
(j-th vehicle in t-th cluster)
User jt
(j-th user in t-th cluster, with a security token)
RSU
TA
I.1. Store in security token
RID_{jt}, K_{jt}
I.2. Secure store in OBU
$h_1(RID_{jt}, K_{jt}), SK_t, PK_{TA}$
II. Send generated signature to nearest vehicles
III. Verify the validity of signature
VI.1. Send notification of forged message
VI.1. Impersonated message detection
I.1, I.2. Initialization phase
II. Anonymous identity and signature generation phase
III. Message verification phase
VI.1,VI.2. Forgery notification and detection of the impersonated message

FIGURE 4. An overview of the proposed scheme.

following equation:

$$\left(\sum\nolimits_{i=1}^{n} v_i \cdot \sigma_{ijt}\right)P = \sum\nolimits_{i=1}^{n}(v_i \cdot AID_{ijt,1})\left(\sum\nolimits_{i=1}^{n}(v_i \cdot \alpha_{ijt})\right)PK_t + \sum\nolimits_{i=1}^{n}(v_i \cdot \beta_i \cdot R_i)\,. \quad (18)$$

G. FORGERY NOTIFICATION AND DETECTION OF THE IMPERSONATED MESSAGE

If an adversary obtains the value of SK_t, it can generate an invalid message $\{t, \sigma_{ijt}, M_i, R_i, T_i, AID_{ijt}\}$. In this case, the vehicle owner can generate a notification that an adversary forged her message $\{t, \sigma_{ijt}, M_i, R_i, T_i, AID_{ijt}\}$, the RSU forwards the message to the TA. The TA verifies the message and uses SK_{TA} and the following equations to compute K_{jt}:

$$SK_{TA} \cdot AID_{ijt,1} = SK_{TA} \cdot w_i \cdot P = w_i \cdot PK_{TA} \quad (19)$$

$$K_{jt} = AID_{ijt,2} \oplus h_2\left(SK_{TA} \cdot AID_{ijt,1}\right). \quad (20)$$

If the value of K_{jt} is valid, the TA computes the tuple $(K_{jt}, w_i \cdot PK_{TA}, T_i)$ and compares the hash value of this tuple with $AID_{ijt,3}$. If they are the same, then the message is a valid one. Otherwise, the TA confirms that an attacker has tampered with the OBU, revokes the message, and updates the private keys stored in the vehicles of the compromised cluster. Notice that if it has been detected that the OBU of one of sensitive and emergency type vehicles' clusters (such as ambulances or fire engines, police cars, and rescue vehicles) has been tampered with, TA will invite the corresponding vehicles to update their private keys. If necessary, TA can also update the private keys of vehicles belonging to other clusters.

Private Key Updating Algorithm: in order to mitigate attacks that expose the key SK_t, it can be updated according to a key updating algorithm based on Shamir's secret sharing scheme [25], [26], ensuring that only the unrevoked vehicles can obtain the updated SK_t.

To this end, TA chooses a new $SK'_t \in_R Z_q^*$, computes the corresponding $PK'_t = SK'_t \cdot P$, a random $w_t \in_R Z_q^*$ and computes the corresponding public key $W_t = w_t \cdot P$, and chooses a random nonce $N_t \in_R Z_q^*$ for the t-th cluster; next, it calculates:

$$x_{jt} = PRF\left(h_4\left(K_{jt}, SK_t\right), N_t\right) \quad (21)$$

$$y_{jt} = PRF\left(h_4\left(K_{jt}, SK_t\right), N_t + 1\right). \quad (22)$$

Then the TA calculates the points $P_{jt} = (x_{jt}, y_{jt})(1 \leq j \leq J)$ and $P_{0t} = (0, SK'_t)$ where PRF is a pseudo-random function, generates a J-degree interpolated polynomial $y = f(x) = SK'_t + a_{1t}x + a_{2t}x^2 + \ldots + a_{Jt}x^J$ that passes through $J+1$ points $P_{jt}(0 \leq j \leq J)$, and using the polynomial $y = f(x)$, TA produces J new additional random points $P'_{jt}(1 \leq j \leq J)$ on the interpolated polynomial of degree J: $y'_j = f(j), P'_{jt} = (j, y'_j)\ (1 \leq j \leq J)$.

In the next step, TA signs J additional points $P'_{jt}(1 \leq j \leq J)$ by calculating:

$$\sigma_{TA} = w_t + SK_{TA} \cdot h_4\left(PK'_t, T_{TA}, N_t, P'_{1t}, P'_{2t}, \ldots, P'_{Jt}\right) \times mod\ q. \quad (23)$$

In this equation T_{TA} is the timestamp of TA. Finally, TA sends the updating message $P'_{jt}(1 \leq j \leq J), PK'_t, W_t, N_t, T_{TA}, t$ where t is the cluster number to all corresponding vehicles through the public channel.

Upon receiving the private key updating message, OBU verifies the validity of this message by checking the equation:

$$\sigma_{TA} \cdot P = W_t + h_4\left(PK'_t, T_{TA}, N_t, P'_{1t}, P'_{2t}, \ldots, P'_{Jt}\right) \cdot PK_{TA}. \tag{24}$$

Then OBU calculates $P'_{0t} = \left(PRF\left(h_4\left(K_{jt}, SK_t\right), N_t\right), PRF\left(h_4\left(K_{jt}, SK_t\right), N_t + 1\right)\right)$, and using $J+1$ points $P'_{jt}(0 \leq j \leq J)$ and Lagrange interpolation method calculates SK'_t:

$$SK'_t = \sum\nolimits_{j=0}^{J} (y'_i \cdot \prod\nolimits_{g=0\&g\neq j}^{J} (-x'_g \Big/ \left(x'_j - x'_g\right)). \tag{25}$$

Finally, after checking the validity of the equation $PK'_t = SK'_t \cdot P$ OBU stores newly updated private key SK'_t securely.

IV. SECURITY AND PERFORMANCE ANALYSIS

A. SECURITY ANALYSIS

This section proves that our proposed protocol is privacy-preserving and offers unforgeability and a secure private key updating algorithm. We also show that our scheme provides the following security requirements:

- revealing and revoking the identity of the users who break the rules;
- detecting the impersonated messages;
- preserving the identity of other vehicles (even if the value of SK_t stored in OBUs is leaked); and
- untraceability and unlinkability of vehicles.

We further compare the security properties of our scheme with other relevant schemes.

1) UNFORGEABILITY

The signature generation phase of the proposed scheme has been inspired by Schnorr's signature scheme [37] and the signature generation scheme in [8]. The unforgeability of our scheme can be easily proven using similar techniques as in [8]. Note that, to generate a valid signature, the adversary needs the vehicle's key (K_{jt}) in addition to the secret value SK_t. Hence, even if the information stored in the vehicle's OBU, i.e. $(h_1(RID_{jt}, K_{jt}), SK_t)$ is revealed, the adversary cannot obtain a valid K_{jt} since the cryptographic hash function h_1 has been modeled as RO; therefore, she cannot generate a valid signature. In what follows, having this in mind, we prove our scheme is privacy-preserving even if the OBU is tampered with.

2) SECURE PRIVATE KEY UPDATING ALGORITHM

As has been indicated in Section III, the private key updating algorithm has been inspired by the algorithm proposed in [24], and according to Theorem 2 of this paper, it meets the requirement for a secure private key updating algorithm. The main difference with our proposed algorithm is the use of SK_{TA} instead of the stored private key in OBUs to sign the private key updating message, which will prevent the physical attacker who obtained the private key stored in OBUs from signing the private key updating message on behalf of TA.

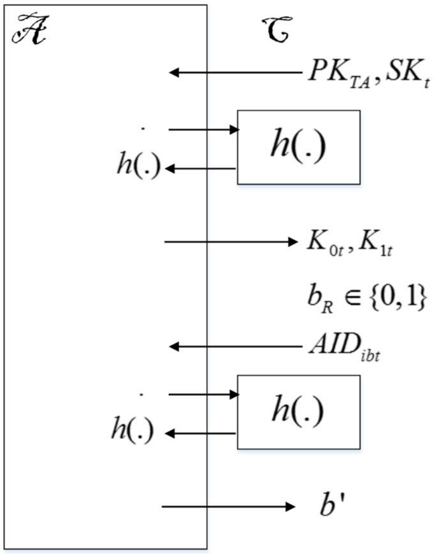


FIGURE 5. Indistinguishability game between Challenger C and Adversary A.

3) PRIVACY-PRESERVING

Formally, privacy-preserving means the adversary who obtained the private key (SK_{jt}) stored in OBUs cannot guess the vehicles' real identity and key (K_{jt}) from their messages; also, this attacker cannot reveal these values from the OBUs alone. We present our proof in the random oracle model. We consider the game in Figure 5, which runs between a probabilistic polynomial-time (PPT) adversary $\mathscr{A}$ and challenger $\mathscr{C}$.

Our scheme is privacy-preserving if the adversary cannot obtain any information from AID_{ijt} about K_{jt} and RID_{jt} having the private key (SK_t); moreover, the adversary cannot compromise any key at the time, and she is not able to deduce which vehicles are close to a single RSU. AID_{ijt} is composed of $AID_{ijt,1}$, $AID_{ijt,2}$ and $AID_{ijt,3}$. $AID_{ijt,3}$ is equal to $h_4\left(K_{jt}, w_i \cdot PK_{TA}, T_i\right)$, and since it has been assumed that the hash functions have been modeled as random oracles, the values of $h_4(K_{jt}, w_i \cdot PK_{TA}, T_i)$ are uniformly distributed, and if the K_{jt} is large enough, according to Theorem 4.1 of [38], the adversary cannot guess the value of K_{jt} from $AID_{ijt,3}$. Therefore it is sufficient to show that the adversary cannot obtain any information about K_{jt} and RID_{jt} from the first and second parts of AID_{ijt}. To achieve this goal, we consider $AID_{ijt,1} = w_i \cdot P$ and $AID_{ijt,2} = K_{jt} \oplus h_2(w_i \cdot PK_{TA})$ as an encryption function, and then we prove that it is secure in the sense that it offers indistinguishability of ciphertext under chosen-plaintext attacks. Therefore, according to the security definition of indistinguishability in [39], we can define the security property of our scheme as follows:

Definition 1 (Privacy-Preserving): Consider our scheme $\pi = (Gen, Enc, Dec)$ (Enc means the production of AID_{ijt} from K_{jt} and Dec means obtaining K_{jt} (AID_{ijt}) from AID_{ijt} using SK_t) is privacy-preserving under Chosen Plaintext Attack (CPA) if for all probabilistic polynomial-time (PPT) adversaries $\mathscr{A}$ there exist a negligible function *negl* such that:

$$pr[privacy - preserving_{A,\pi}^{CPA}(1^{\lambda})] \leq 1/2 + negl(\lambda). \quad (26)$$

Here the probability is taken over the random coins used by a Probabilistic Polynomial Time (PPT) adversary $\mathscr{A}$, and the random coins used in the experiment (for choosing the key, the random bit b, and any random coins used in the encryption process). And $pr[privacy - preserving_{A,\pi}^{CPA}(1^{\lambda})]$ is the probability that the adversary wins the following game:

Setup phase; $\mathscr{C}$ generates the private and public parameters of the system and sends the public parameters and $\mathrm{SK_j}$ stored in the OBU to A, while keeping $\mathrm{SK_{TA}}$secure.

Learning phase; in this phase, $\mathscr{A}$ has access to hash oracles, private keys stored in OBUs (SK_t), the Anonymous Identity and Signature generation oracle queries:

Hash Oracles; $\mathscr{A}$ queries the challenger to run one or some of the hash functions $\mathrm{h_1}$ to $\mathrm{h_4}$ with her chosen inputs.

Anonymous Identity and Signature generation oracle; $\mathscr{A}$ queries the challenger to run this oracle on $\mathrm{M_i}$ and an arbitrary $\mathrm{K_{jt}}$.

Challenge phase; $\mathscr{A}$ queries challenger $\mathscr{C}$ with two $\mathrm{K_{jt}}$. $\mathscr{C}$ chooses one of them uniformly at random and sends its corresponding tuple to $\mathscr{A}$.

Guess phase; $\mathscr{A}$ guesses the $\mathrm{K_{jt}}$ corresponding to the received tuple. A wins the game if she guesses the correct $\mathrm{K_{jt}}$.

This game is illustrated in Figure 5.

Theorem 1: The proposed scheme is privacy-preserving if the hash functions $\mathrm{h_2}$ and $\mathrm{h_4}$ can be modeled as Random Oracles (ROs), and the discrete logarithm problem (DL) in G is hard.

Proof: We prove this theorem by showing that the probability that a PPT adversary wins the game of Definition 1 is negligibly larger than 1/2 in the security parameter λ.

Setup Phase: $\mathscr{C}$ generates the pair of private and public parameters of the system by running the algorithm $(SK_t, PK_t) \leftarrow Gen()$ and $(SK_{TA}, PK_{TA}) \leftarrow Gen()$ and sends the public parameters as well as SK_t stored in the OBU to $\mathscr{A}$. Consider that $\mathscr{C}$ keeps SK_{TA} secure.

1st Query Phase: after receiving the public parameters as well as SK_t, the adversary $\mathscr{A}$ has access to the following oracles for a polynomial bounded number of queries:

Simulating the Hash Oracle: $\mathscr{A}$ queries the challenger to run one of the hash functions $\mathrm{h_1}$ to $\mathrm{h_4}$ with her chosen inputs. If the input in i-th query, $\mathrm{q_i}$, has not been computed before, $\mathscr{C}$ responds with a random response $h_j(q_i)$ chosen uniformly from its output domain, stores the pair $(q_i, h_j(q_i))$ in its database, and sends $h_j(q_i)$ to $\mathscr{A}$. Otherwise, $\mathscr{C}$ sends the $h_j(q_i)$ stored in its database to A.

Simulating Anonymous Identity and Signature Generation Oracle: $\mathscr{A}$ queries the challenger to run this oracle on $\mathrm{M_i}$ and an arbitrary K_{jt}. A receives the tuple $(j, \sigma_{ijt}, M_i, R_i, T_i, AID_{ijt})$ from $\mathscr{C}$.

Challenge Phase: the adversary chooses two K_{jt}s, say K_{0t} and K_{1t}, and asks the challenger to send her back the tuple corresponding to one of them. The challenger chooses one of them uniformly at random and sends the tuple $(t, \sigma_{ibt}, M_i, R_i, T_i, AID_{ibt})$ where b ∈ {0, 1}. The only value in this tuple that includes information about $\mathrm{K_{jt}}$ *and* RID_{bt}, is $AID_{ibt} = \{AID_{ibt,1}, AID_{ibt,2}, AID_{ibt,3}\}$ where $AID_{ibt,1} = w_i \cdot P$, $AID_{ibt,2} = K_{bt} \oplus h_2(w_i \cdot PK_{TA})$ and $AID_{ibt,3} = h_4(K_{bt}, w_i \cdot PK_{TA}, T_i)$.

2nd Query Phase: after receiving the challenge-response exchange $(t, \sigma_{ibt}, M_i, R_i, T_i, AID_{ibt})$, the adversary $\mathscr{A}$ has access to the hash oracle defined in the 1st query phase.

Guess phase; $\mathscr{A}$ guesses the $\mathrm{K_{jt}}$ corresponding to the received tuple. $\mathscr{A}$ wins the game if she guesses the correct $\mathrm{K_{jt}}$. Therefore, to prove Theorem 1, it suffices to show:

$$pr\,[success] = pr[IDpreserving_{A,\pi}^{CPA}(1^{\lambda})] \leq 1/2 + negl\,(\lambda)\,. \quad (27)$$

Here $pr[success]$ is the adversary's probability of winning the privacy-preserving game; we also consider "Query" as querying the correct $w_i \in_R Z_q^*$ from the Oracles.

As we know; $pr[success] = pr[success \cap Query] + pr[success \cap \overline{Query}] \leq pr[Query] + pr[success \cap \overline{Query}]$ which result in:

$$pr[success] \leq pr[success|\overline{Query}] + pr[Query]. \quad (28)$$

Here, the probability of the attacker's success without querying the correct w_i is equal to a random guess, therefore:

$$pr[success|\overline{Query}] = 1/2. \quad (29)$$

Also, if $Q(\lambda)$ is the number of queries from "generating anonymous ID and signature Oracle," and pr[Solving-DL-Problem] is the probability of solving the DL problem, the probability of querying the correct w_i from the Oracles will be computed as:

$$\begin{aligned} pr[Query] &= Q(\lambda)/2\hat{}\lambda + \Pr[Solving - DL - Problem] \\ &= negl(\lambda). \end{aligned} \quad (30)$$

As a result of (29) and (30), we have:

$$pr\left[ID - preserving_{A,\pi}^{CPA}\left(1^{\lambda}\right)\right] \leq 1/2 + negl\,(\lambda) \quad (31)$$

Thus, adversary $\mathscr{A}$ cannot do better than randomly guessing the value of b, if the hash functions can be modeled as random oracles and if solving the discrete logarithm problem is hard. Therefore, obtaining K_{jt} and RID from the anonymous ID is impossible for the PPT attacker, and the proposed scheme is privacy-preserving. □

In the following, we use Theorem 1 to explain the unique properties of the proposed scheme compared to other schemes:

Revealing the identity of violators and revoking their identities. After verifying the suspicious messages and ensuring no information has been leaked from an OBU, the TA can find out the key (K_{jt}) of the vehicle using Eqn. (19) and (20). Then, it can obtain the corresponding RID from its database. This property is one of the advantages of our scheme compared to other TRD-aided CPPA schemes. In those schemes,

TABLE 2. Comparison of security properties of the schemes in the literature with our novel scheme in the case of tampering.

Scheme	Tamper detection	Anonymity and privacy-preserving	No identity leakage and impersonation of vehicles	Impersonated messages detection	Unlinkability
He et al. [8]	×	×	×	×	×
Bayat et al. [9]	×	×	×	×	×
Zhong et al. [10]	×	×	×	×	×
Zhong et al. [14]	NA	√	√	√	√
Chen et al. [19]	NA	√	√	√	×
Ying et al. [20]	NA	√	√	√	×
Wei et al. [24]	×	×	×	×	×
Proposed	√	√	√	√	√

TABLE 3. The definition of the operations used in the protocols.

Notation	Definition	Notation	Definition
T_m	Elliptic curve scalar multiplication	T_{enc}	Symmetric-key encryption
T_h	Hash function	T_{MAC}	Message Authentication Code
T_{eca}	Elliptic curve point addition	T_p	Modular exponentiation
$T_{\oplus}$	Binary addition	T_{R-O}	Communication's delay between the vehicle and RSUs
T_{bp}	Bilinear map	T_{T-R}	Communication's delay between RSUs and the TA
T_{mp-bp}	Multiplication on a group over the bilinear map	$\mathrm{T}_{\mathrm{O-O}}$	Communication's delay between a vehicle and another vehicle
T_{mtp}	The map-to-point operation used in [9]	T_{RNM}	Releasing notification messages, used in [14]

the violator can claim that the message has been sent by an attacker who obtained some information from TRD.

In other words, the proposed scheme adds a property similar to a fail-stop signature [40] to the existing TRD-aided CPPA schemes, which allows the owner of the vehicle to prove that she didn't sign the impersonated message.

Detecting the impersonated messages. As described, during forgery notification and the detection of the impersonated messages, TA can verify the validity of the suspicious messages using the private key SK_{TA} and determine whether a message is an impersonated or valid message. Hence, TA will be able to detect whether tampering has occurred.

No leakage of information about the identity of other vehicles and no impersonation of other vehicles by leakage of information from an OBU. Even if the value of SK_t stored in OBU is leaked to an adversary, she cannot compute the K_{jt} of other vehicles: indeed, the adversary cannot find the private key of the TA; moreover, K_{jt} and RID_{jt} have not been stored in the OBU. Moreover, Eqns. (9-11) show that the adversary needs a valid K_{jt} added to SK_t to impersonate a valid vehicle which is impossible, as has been shown in the proof of Theorem 1.

Untraceability of vehicles by an adversary and unlinkability of vehicle identities even if the secret information is leaked from an OBU. Even if the adversary obtains the stored values in the OBU, since she cannot compute RID_{jt} and K_{jt} using this information and since AID_{ijt} is updated based on each timestamp, the adversary cannot trace the vehicle. In contrast, in TRD-aided CPPA schemes [9], [10], [11], [24], the adversary can trace other vehicles by obtaining the information stored in the TRD. Moreover, in RSU-aided schemes [19], [20], the unlinkability property of the messages issued from a vehicle in an area covered by an RSU has not been considered. In contrast, the proposed scheme provides this property by using a pseudonymous identity, that varies with the time stamp. Table 2 compares the security properties of the proposed scheme with some other related works.

TABLE 4. The estimated computational time (in ms) of each protocol for sending *n* messages in the range of a single RSU.

Scheme	OBU side	RSU side	TA side	Total cost
He et al. [8]	$6nT_m + 3nT_{\mathrm{eca}} + 2nT_h = 2.65\mathrm{n}$	0	0	2.66n
Bayat et al. [9]	$3\mathrm{n}T_{\mathrm{bp}} + 3nT_{mtp} + 6nT_{mp-bp} = 36.1n$	0	0	36.1n
Zhong et al. [10]	$5nT_m + 3nT_{\mathrm{eca}} + 2n\mathrm{T}_h = 2.22n$	0	0	2.23n
Zhong et al. [14]	$3T_m + (7+2n)T_h = 1.32 + 2 \times 10^{-4}n$	$T_m + 10^3 nT_h + nT_{RNM} = 0.44 + 0.55$	$2T_m + 9T_h = 0.88$	$2.59 + 0.55n$
Chen et al. [19]	$6T_p + (2+n)T_{MAC} + (6+n)T_h = 2.7 + 8 \times 10^{-4}n$	0	$3T_p + 6T_h = 1.35$	4.05
Ying et al. [20]	$4T_p + T_{enc} + (9+n)T_{MAC} + (2+n)T_h = 2.5 + 8 \times 10^{-4}\mathrm{n}$	$T_h = 10^{-4}$	$T_p + T_{enc} + 8T_h = 1.15$	3.65
Wei et al. [24]	$6nT_m + 2nT_{\mathrm{eca}} + 7n\mathrm{T}_h = 2.65\mathrm{n}$	0	0	2.66n
Proposed	$6nT_m + 4nT_h + 2nT_{eca} = 2.65n$	0	0	2.66n

TABLE 5. The estimated communicational imposed delay (in ms) and total delay (in ms) of each protocol for sending *n* messages in the range of a single RSU.

Scheme	Imposed delay			Total delay
	$\mathrm{T_{dO\text{-}O}}$	$\mathrm{T_{dR\text{-}O}}$	$\mathrm{T_{dR\text{-}T}}$	
He et al. [8]	n	0	0	$\mathrm{nT_{dO-O}}$
Bayat et al. [9]	n	0	0	$\mathrm{nT_{dO-O}}$
Zhong et al. [10]	n	0	0	$\mathrm{nT_{dO-O}}$
Zhong et al. [14]	n	$2n+2$	2	$\mathrm{nT_{dO-O}} + (2\mathrm{n}+2)\mathrm{T_{dR-O}} + 2\mathrm{T_{dR-T}} = \mathrm{nT_{dO-O}} + 1000\,n$
Chen et al. [19]	n	2	2	$\mathrm{nT_{dO-O}} + 2\mathrm{T_{dR-O}} + 2\mathrm{T_{dR-T}} = \mathrm{nT_{dO-O}} + 1000$
Ying et al. [20]	n	2	2	$\mathrm{nT_{dO-O}} + 2\mathrm{T_{dR-O}} + 2\mathrm{T_{dR-T}} = \mathrm{nT_{dO-O}} + 1000$
Wei et al. [24]	n	0	0	$\mathrm{nT_{dO-O}}$
Proposed	n	0	0	$\mathrm{nT_{dO-O}}$

B. PERFORMANCE ANALYSIS

In the proposed scheme, unlike the RSU-aided schemes [1], [4], [14], [19], [20], [21], the vehicles need to establish a communication with the TA for verifying only the suspicious messages. This improves the efficiency of our scheme compared to RSU-aided CPPA schemes.

Here, we compare the efficiency of the proposed scheme with competing schemes. We use the notation of Table 3 for the execution time of operations as well as the delay required to establish communication between the entities in the network to compute the efficiency of each scheme. According to [8] and [20], the execution time of each of the operations mentioned in Table 3 using the Miracl library running on an Intel Core i7-4770 at 3.4 GHZ with 4 GB memory are as follows: $T_h = 0.0001\,(ms)$, $T_m = 0.442\,(ms)$, $T_{eca} = 0.0018\,(ms)$, $T_{bp} = 4.2\,(ms)$, $T_{mtp} = 4.406\,(ms)$, $T_{mp-bp} = 1.7\,(ms)$, $T_{enc} = 0.7\,(ms)$, $T_{MAC} = 0.00074\,(ms)$, $T_p = 0.45\,(ms)$. Note that the execution time of the binary addition ($T_{\oplus}$) is

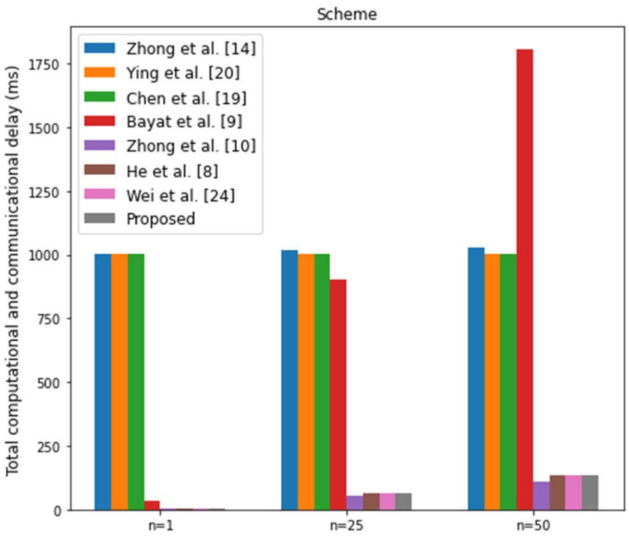


FIGURE 6. **Total computation time and communication delay of each protocol.**

negligible, and to have a fair comparison with the introduced schemes in [14], [19], and [20], according to [41], we choose 0.5*s* as the optimum value for $2T_{dR-O} + 2T_{dR-T}$, so that the delay time of these schemes will be minimum.

According to [10], we assume that one notification message is released per ten traffic information messages; hence we can consider that T_{RNM} equals $0.1T_p$. Tables 4 and 5 show the computational cost and communication delay of the schemes.

In our scheme, vehicles do not need to be authenticated in each RSUs range; therefore, as shown in Table 5, the estimated time cost of our scheme is significantly less than that of [14], [19], and [20].

In [14], it is assumed that the distance between two contiguous RSUs is 600 meters, and the speed of one vehicle is between 0-120 km/h; therefore, in the RSU-aided schemes, each vehicle should be authenticated every 36 seconds, and these vehicles can send maximum 50 messages in the range of each RSU ($0 \leq n \leq 50$). This necessity of permanent communication with the TA and RSUs imposes much higher communication costs on network elements.

As shown in Table 4, the proposed scheme is comparable with the schemes of [8], [10], and [14] in terms of computational overhead. Still, Table 5 shows that in our scheme, and the schemes in [8], [10], and [24], there is no communication between "vehicle and RSU" and between "RSU and TA," contrary to the scheme [14], [19], [20] which needs permanent communication between "RSU and TA" and "vehicle and RSU." Table 2 also shows that the schemes in [8], [9], [10], [19], [20], and [24] cannot provide unlinkability, while this is a critical privacy requirement for VANETs. Our novel scheme provides the necessary security and privacy requirements, including unlinkability, detection of forged messages, protection against identity leakage and impersonation of vehicles, anonymity, and the privacy-preserving property of Definition 1.

The scheme introduced in [14] provides similar security and privacy properties to the proposed scheme and has the lowest computational cost. However, Table 5 shows that in this scheme, each OBU needs $2n+2$ communications to send n messages while traveling inside the range of an RSU, which imposes a significant delay.

Therefore, our scheme is more efficient than the scheme in [14]. Figure 6 shows the total computation time and communication delay of each protocol for sending n messages in the range of a single RSU. As indicated, vehicles can send a maximum of 50 messages in the range of each RSU ($0 \leq n \leq 50$); therefore, we have computed the values for n=1, 25, and 50. Also, in Figure 6, the amount of nT_{dO-O} has been ignored because it is equal in all schemes.

V. CONCLUSION

This paper proposes a novel privacy-preserving authentication scheme that takes advantage of the existing RSU-aided and TRD-aided CPPA schemes while improving their security and efficiency. We proved the security of our scheme in the random oracle model and showed it provides the security and privacy requirements of VANETs. Our performance comparison results show that our scheme has a lower computational and communication cost compared to RSU-aided schemes, and its cost is comparable to that of TRD-aided CPPA schemes.

ACKNOWLEDGMENT

The authors would like to thank Mahdi Sedaghat for the interesting discussions he shared about the proof section of the article.

REFERENCES

[1] O. Mirzamohammadi, A. Aghabagherloo, J. Mohajeri, M. Salmasizadeh, and M. R. Aref, "Analysis and improvement of the SPACF scheme in vehicular ad-hoc networks," in *Proc. 18th Int. ISC Conf. Inf. Secur. Cryptol. (ISCISC)*, Sep. 2021, pp. 68–74, doi: 10.1109/ISCISC53448.2021.9720470.

[2] F. Farouk, Y. Alkady, and R. Rizk, "Efficient privacy-preserving scheme for location based services in VANET system," *IEEE Access*, vol. 8, pp. 60101–60116, 2020, doi: 10.1109/ACCESS.2020.2982636.

[3] N. V. Vighnesh, N. Kavita, S. R. Urs, and S. Sampalli, "A novel sender authentication scheme based on hash chain for vehicular ad-hoc networks," in *Proc. IEEE Symp. Wireless Technol. Appl. (ISWTA)*, Sep. 2011, pp. 96–101, doi: 10.1109/ISWTA.2011.6089388.

[4] A. Aghabagherloo, J. Mohajeri, M. Salmasizadeh, and M. M. Feghhi, "An efficient anonymous authentication scheme using registration list in VANETs," in *Proc. 28th Iranian Conf. Electr. Eng. (ICEE)*, Aug. 2020, pp. 1–5, doi: 10.1109/ICEE50131.2020.9260801.

[5] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Jun. 2017, doi: 10.1109/TVT.2017.2718101.

[6] A. Wasef and X. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 78–89, Jan. 2013, doi: 10.1109/TMC.2011.246.

[7] Y. Park, C. Sur, C. D. Jung, and K. H. Rhee, "An efficient anonymous authentication protocol for secure vehicular communications," *J. Inf. Sci. Eng.*, vol. 26, no. 3, pp. 785–800, 2010.

[8] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 12, pp. 2681–2691, Dec. 2015, doi: 10.1109/TIFS.2015.2473820.

[9] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, ''A secure authentication scheme for VANETs with batch verification,'' *Wireless Netw.*, vol. 21, no. 5, pp. 1733–1743, Dec. 2014, doi: 10.1007/s11276-014-0881-0.

[10] H. Zhong, J. Wen, J. Cui, and S. Zhang, ''Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET,'' *Tsinghua Sci. Technol.*, vol. 21, no. 6, pp. 620–629, 2016, doi: 10.1109/TST.2016.7787005.

[11] M. Azees, P. Vijayakumar, and L. J. Deboarh, ''EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017, doi: 10.1109/TITS.2016.2634623.

[12] I. Ali and F. Li, ''An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs,'' *Veh. Commun.*, vol. 22, Apr. 2020, Art. no. 100228, doi: 10.1016/j.vehcom.2019.100228.

[13] C. Sun, J. Liu, X. Xu, and J. Ma, ''A privacy-preserving mutual authentication resisting DoS attacks in VANETs,'' *IEEE Access*, vol. 5, pp. 24012–24022, 2017, doi: 10.1109/ACCESS.2017.2768499.

[14] H. Zhong, B. Huang, J. Cui, Y. Xu, and L. Liu, ''Conditional privacy-preserving authentication using registration list in vehicular ad hoc networks,'' *IEEE Access*, vol. 6, pp. 2241–2250, 2018, doi: 10.1109/ACCESS.2017.2782672.

[15] S. A. Eftekhari, M. Nikooghadam, and M. Rafighi, ''Security-enhanced three-party pairwise secret key agreement protocol for fog-based vehicular ad-hoc communications,'' *Veh. Commun.*, vol. 28, Apr. 2021, Art. no. 100306, doi: 10.1016/j.vehcom.2020.100306.

[16] D. Manivannan, S. S. Moni, and S. Zeadally, ''Secure authentication and privacy-preserving techniques in vehicular ad-hoc NETworks (VANETs),'' *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100247, doi: 10.1016/j.vehcom.2020.100247.

[17] R. Anderson and M. Kuhn, ''Low cost attacks on tamper resistant devices,'' in *Proc. Int. Workshop Secur. Protocols*, 1997, pp. 125–136.

[18] S. Kaur, B. Singh, and H. Kaur, ''Stratification of hardware attacks: Side channel attacks and fault injection techniques,'' *Social Netw. Comput. Sci.*, vol. 2, no. 3, pp. 1–13, Mar. 2021, doi: 10.1007/s42979-021-00562-3.

[19] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, ''A secure authentication protocol for Internet of Vehicles,'' *IEEE Access*, vol. 7, pp. 12047–12057, 2019, doi: 10.1109/ACCESS.2019.2891105.

[20] B. Ying and A. Nayak, ''Anonymous and lightweight authentication for secure vehicular networks,'' *IEEE Trans. Veh. Technol.*, vol. 66, no. 12, pp. 10626–10636, Dec. 2017, doi: 10.1109/TVT.2017.2744182.

[21] W. Xiong, R. Wang, Y. Wang, F. Zhou, and X. Luo, ''CPPA-D: Efficient conditional privacy-preserving authentication scheme with double-insurance in VANETs,'' *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3456–3468, Apr. 2021, doi: 10.1109/TVT.2021.3064337.

[22] S. M. Pournaghi, B. Zahednejad, M. Bayat, and Y. Farjami, ''NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET,'' *Comput. Netw.*, vol. 134, pp. 78–92, Apr. 2018, doi: 10.1016/j.comnet.2018.01.015.

[23] J. Zhang, J. Cui, H. Zhong, Z. Chen, and L. Liu, ''PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks,'' *IEEE Trans. Dependable Secure Comput.*, vol. 18, no. 2, pp. 722–735, Mar./Apr. 2021, doi: 10.1109/TDSC.2019.2904274.

[24] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, ''Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs,'' *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1681–1695, 2021, doi: 10.1109/TIFS.2020.3040876.

[25] A. Shamir, ''How to share a secret,'' *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176.

[26] A. Khalesi, M. Mirmohseni, and M. A. Maddah-Ali, ''The capacity region of distributed multi-user secret sharing,'' *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 3, pp. 1057–1071, Sep. 2021, doi: 10.1109/JSAIT.2021.3102967.

[27] X. Feng, Q. Shi, Q. Xie, and L. Liu, ''An efficient privacy-preserving authentication model based on blockchain for VANETs,'' *J. Syst. Archit.*, vol. 117, Aug. 2021, Art. no. 102158, doi: 10.1016/j.sysarc.2021.102158.

[28] C. Lin, X. Huang, and D. He, ''EBCPA: Efficient blockchain-based conditional privacy-preserving authentication for VANETs,'' *IEEE Trans. Dependable Secure Comput.*, early access, Apr. 5, 2022, doi: 10.1109/TDSC.2022.3164740.

[29] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu, and L. Liu, ''Edge computing in VANETs—An efficient and privacy-preserving cooperative downloading scheme,'' *IEEE J. Sel. Areas Commun.*, vol. 38, no. 6, pp. 1191–1204, Jun. 2020, doi: 10.1109/JSAC.2020.2986617.

[30] J. Zhang, H. Zhong, J. Cui, M. Tian, Y. Xu, and L. Liu, ''Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks,'' *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 7940–7954, Jul. 2020, doi: 10.1109/TVT.2020.2994144.

[31] C. Lai, R. Lu, D. Zheng, and X. Shen, ''Security and privacy challenges in 5G-enabled vehicular networks,'' *IEEE Netw.*, vol. 34, no. 2, pp. 37–45, Mar. 2020, doi: 10.1109/MNET.001.1900220.

[32] J. Xie, H. Tang, T. Huang, F. R. Yu, R. Xie, J. Liu, and Y. Liu, ''A survey of blockchain technology applied to smart cities: Research issues and challenges,'' *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2794–2830, 3rd Quart., 2019, doi: 10.1109/COMST.2019.2899617.

[33] S. Meisami, M. Beheshti-Atashgah, and M. R. Aref, ''Using blockchain to achieve decentralized privacy in IoT healthcare,'' 2021, *arXiv:2109.14812*.

[34] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, ''A survey on the current security landscape of intelligent transportation systems,'' *IEEE Access*, vol. 9, pp. 9180–9208, 2021, doi: 10.1109/ACCESS.2021.3050038.

[35] M. A. Al-Shareeda, M. Anbar, I. H. Hasbullah, and S. Manickam, ''Survey of authentication and privacy schemes in vehicular ad hoc networks,'' *IEEE Sensors J.*, vol. 21, no. 2, pp. 2422–2433, Jan. 2021, doi: 10.1109/JSEN.2020.3021731.

[36] X. Feng, Q. Shi, Q. Xie, and L. Wang, ''P2BA: A privacy-preserving protocol with batch authentication against semi-trusted RSUs in vehicular ad hoc networks,'' *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3888–3899, 2021, doi: 10.1109/TIFS.2021.3098971.

[37] C. P. Schnorr, ''Efficient signature generation by smart cards,'' *J. Cryptol.*, vol. 4, no. 3, pp. 161–174, Jan. 1991, doi: 10.1007/bf00196725.

[38] R. Impagliazzo and S. Rudich, ''Limits on the provable consequences of one-way permutations,'' in *Proc. 21st Annu. ACM Symp. Theory Comput. (STOC)*, 1989, pp. 44–61.

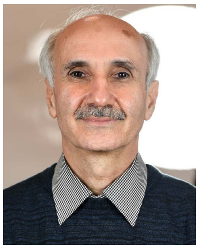
[39] J. Katz, *Introduction To Modern Cryptography*. Boca Raton, FL, USA: CRC Press, 2019.

[40] T. P. Pedersen and B. Pfitzmann, ''Fail-stop signatures,'' *SIAM J. Comput.*, vol. 26, no. 2, pp. 291–330, Mar. 1997.

[41] C. Guo, D. Li, X. Chen, and G. Zhang, ''An adaptive V2R communication strategy based on data delivery delay estimation in VANETs,'' *Veh. Commun.*, vol. 34, Apr. 2022, Art. no. 100444, doi: 10.1016/j.vehcom.2021.100444.

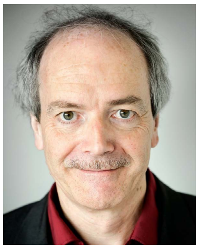
ALIREZA AGHABAGHERLOO received the B.Sc. degree in electrical engineering from the University of Tabriz, Tabriz, Iran, in 2018, and the M.Sc. degree in electrical engineering with a specialization in cryptography and secure communications from the Sharif University of Technology, Tehran, Iran, in 2020. He is currently pursuing the Ph.D. degree with the imec-COSIC Research Group, KU Leuven, Leuven, Belgium. His major research interests include analysis and improvement of cryptographic protocols in VANET, and using the capabilities of artificial intelligence (AI) to defend computers, servers, mobile devices, electronic systems, networks, and data against malicious attacks.

MAHSHID DELAVAR received the Ph.D. degree from the Iran University of Science and Technology, Tehran, Iran, in 2016. She is a Research Fellow with the Computer Science Department, University of Warwick, Coventry, U.K. Her research interests include hardware security, cryptographic protocols, and quantum cryptography.



JAVAD MOHAJERI is an Assistant Professor with the Electronics Research Institute and an Adjunct Assistant Professor with the Electrical Engineering Department, Sharif University of Technology, Tehran, Iran. He is the author/coauthor of over 120 research articles in refereed journals/conferences. He has authored three books and is one of the Founding Members of the Iranian Society of Cryptology. His research interests include design and cryptanalysis of cryptographic algorithms, and protocols and data security.

MAHMOUD SALMASIZADEH received the B.S. and M.S. degrees in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 1972 and 1989, respectively, the Ph.D. degree in information technology from the Queensland University of Technology, Australia, in 1997. Currently, he is an Associate Professor with the Electronics Research Institute and an Adjunct Associate Professor with the Electrical Engineering Department, Sharif University of Technology. His research interests include design and cryptanalysis of cryptographic algorithms and protocols, e-commerce security, and information theoretic secrecy. He is a Founding Member of Iranian Society of Cryptology.



BART PRENEEL (Member, IEEE) is currently a Full Professor with KU Leuven, Leuven, Belgium, where he heads the imec-COSIC Research Group. He has authored over 450 scientific publications and is the inventor of five patents. His main research interests include cryptography, information security, and privacy. He was the program chair of more than 20 international conferences. He has been an invited speaker at over 120 conferences in 50 countries. He was the President of the International Association for Cryptologic Research (IACR) and is the Co-Founder and the Chairperson of the Board of the Information Security Cluster LSEC. He is a member of the Advisory Group of ENISA and of the Academia Europaea. He is a member of the Knowledge Center of the Belgian Data Protection Authority. In 2015, he was elected as fellow of the IACR. He received the RSA Award for Excellence in the Field of Mathematics in 2014, the IFIP TC11 Kristian Beckman Award in 2015 and the ESORICS Outstanding Research Award in 2017.