The ISC Int'l Journal of Information Security
ISeCure

November 2023, Volume 15, Number 3 (pp. 77–89)
http://www.isecure-journal.org

Presented at the ISCISC'2023 in Tehran, Iran.

A Lightweight Mutual Authentication Scheme for VANETs Between Vehicles and RSUs **

Mohamadreza Amani [1,*], Javad Mohajeri [2], and Mahmoud Salmasizadeh [2]
[1] Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran
[2] Electronics Research Institute, Sharif University of Technology, Tehran, Iran

ARTICLE INFO.

Keywords:
Batch authentication, Department of Motor Vehicles(DMV), Homomorphic hash function, Road-Side Unit(RSU), Sybil attack, Trusted Authority(TA)

Type:
Research Article

doi: 10.22042/isecure.2023.417758.1018

ABSTRACT

Vehicular Ad-hoc Networks (VANETs) have emerged as part of Intelligent Transportation Systems (ITS), offering the potential to enhance passenger and driver safety, as well as driving conditions. However, VANETs face significant security challenges and various attacks due to their wireless nature and operation in free space. Mutual authentication between vehicles and RSUs is one of the most, if not the most, critical security requirements in VANETs. In this process, maintaining resource authenticity, data authenticity and preserving users' privacy, are key concerns. This paper proposes a pseudonym-based authentication scheme for VANETs, built upon existing approaches. The proposed scheme not only ensures the aforementioned security requirements but also meets critical security requirements for the mentioned process in VANETs, such as non-reputation, unlinkability, and unforgeability. Furthermore, the suggested scheme effectively detects and mitigates the Sybil attack in mutual authentication between vehicles and RSU, a well-known and common threat. By comparing the efficiency and security characteristics of the proposed scheme with other existing approaches, it becomes evident that the suggested scheme surpasses previously proposed methods.

1 Introduction

There are numerous autonomous intelligent systems based on IoTs, for example, e-Health care, e-commerce, defense, agriculture, etc. Vehicular Ad-hoc NETworks (VANETs) are one of the important factors of smart and autonomous Intelligent Transport Systems (ITS) [1]. The ITS requires two types of wireless communication: Short range wireless communication and long range communication. Short range communication includes emerging technologies such as Dedicated Short Range Communication (DSRC) and IEEE 802.11b for establishing an Ad hoc network. In contrast, establishing long-range communication depends on existing infrastructure such as cellular networks [2]. The main goal of a vehicular network is to accurately disseminate information about life-threatening events, such as traffic jams and accident

* Corresponding author.
**The ISCISC'2023 program committee effort is highly acknowledged for reviewing this paper.
Email addresses: mohammadreza.amani@alum.sharif.edu, mohajer@sharif.edu, salmasi@sharif.edu
ISSN: 2008-2045

reports, in a short time [3]. A vehicle broadcasts informative messages every 100–300 ms to RSUs or nearby vehicles. As per the DSRC standard, the maximum communication range in VANETs can be up to 1 km, and the transmission speed varies from 6 to 27 Mbps [4].

VANETs mainly consist of three key entities: the Trusted Authority (TA), the Road-Side Unit (RSU), and the vehicles. The commonly used term to describe communication between vehicles and other entities is Vehicle-to-Everything (V2X). V2X includes possible modes of communication in VANETs such as communication pathways between moving vehicles (V2V) equipped with onboard units (OBU) and controller area network (CAN), between vehicles and nearby fixed equipment (V2I), and between moving vehicles and pedestrians (V2P), all of these modes improve road safety, traffic efficiency, and the availability of infotainment services [5]. In case of exception, the vehicle's drivers take an early decision on the basis of transmitted information they received [1]. For instance, when emergency brake is activated in vehicle X, a warning signal will be sent to nearby vehicles in real-time so that other vehicles, particularly that are in front, behind, or beside vehicle X, can take the appropriate actions [6].

With the highly dynamic nature of vehicles and sheer number of vehicles in VANETs, it is a challenge to ensure the truthfulness of passed messages and to maintain vehicles' security [7]. Also, Vehicles communicate with each other through open wireless channels, and attackers can easily alter, intercept and delete transmitted messages [1]. So, security is the biggest challenge of VANETs. The solution to security issues in VANETs required end-to-end authentication to avoid intrusion in the VANETs. It also required, robust and lightweight authentication solutions for resource constraint nodes. Another promising component is the privacy of the individual rights to independent of any record conducted without their consent. The service provider can not mishandle the personal data without the consent of the owner, and necessary measures should be taken to hide the user's real identity [1].

However, vehicle privacy and security are somewhat conflicting, as a "perfect privacy" environment may result in the message generators not being able to be identified. In other words, such a feature can prevent an investigation of a misbehaving vehicle from taking place; thus, the need for "conditional privacy." So there should be certain security mechanisms that detect and prevent the normal network behavior from intruder attacks automatically [6].

Furthermore, it is important to acknowledge that the efficiency of the system is influenced by the computational cost and communication overhead. By reducing the computational cost, vehicular communications can be accelerated. Therefore, it is imperative to implement efficient security mechanisms that can automatically detect and prevent intruder attacks on normal network behavior.

As previously mentioned, end-to-end authentication is a crucial requirement in VANETs. The first step of this authentication process involves mutual authentication between vehicles and RSUs. This paper proposes a lightweight mutual authentication protocol for VANETs that aims to achieve efficient and simultaneous authentication of a group of vehicles entering the domain of an RSU, rather than authenticating them individually.

The organization of the rest of this paper is as follows: Section 2 introduces related work in the field. In Section 3, security goals are introduced. the system architecture and preliminaries are presented in Section 4. The proposed mutual authentication scheme is described in Section 5. In Section 6, a performance evaluation of the scheme is provided. Finally, Section 7 concludes the paper.

2 Related Work

In VANETs, authentication and privacy are the basic security requirements [1]. In [1, 4], classifications on authentication schemes are presented. By and large, these schemes can be categorized into five groups, introduced as follows.

2.1 Symmetric Key Cryptography-based Schemes

These schemes are employed in VANETs due to their lower computational and communication costs, enabling swift verification. In [8, 9], the approach mentioned for VANETs is utilized. These schemes excel in terms of computational efficiency. However, when it comes to important security properties such as non-repudiation and public verifiability, they fall short due to the usage of message authentication codes, hash functions, and secret shared keys. In other words, their primary drawback lies in their security aspect.

2.2 Public-Key Cryptography-based Schemes

Compared to symmetric encryption-based schemes, asymmetric encryption-based schemes incur a higher computational cost on the network. However, when essential security requirements such as non-repudiation and traceability need to be met, asymmetric encryption-based schemes can be utilized to

develop authentication and privacy-preserving mechanisms. In these schemes, a Trusted Authority (TA) controls the composition and distribution of public-private key pairs to valid members for communication purposes. Traceability is achieved through certificates issued by a Certification Authority (CA) [4].

Traditional public-key schemes suffer from critical shortcomings such as overhead from Certificate Revocation Lists (CRL), communication overhead from public-key certificates, and location disclosure, among others. Examples of such schemes include [10, 11], which propose innovative approaches to address the problems associated with public-key encryption, with the aim of designing an efficient scheme.

2.3 Identity-based Cryptography Schemes

There is no need to certificates for authenticating in identity-based public key cryptography. Therefore, it reduces the overhead produced due to certifications. Hence, it improves the efficiency of VANETs [1]. Within these categories, a vehicle's essential information, such as their telephone number or email ID, can be employed for generating its public-key [4].

Schemes [12, 13] serve as examples of such approaches. These schemes are capable of providing privacy preservation, as discussed earlier. They are advantageous in terms of computational overhead due to elimination of certificates. However, it should be noted that many of these schemes rely on bilinear pairing, which imposes considerable computational overhead. Furthermore, considering a vehicle typically possesses a single identity, it may become vulnerable to certain attacks such as linkability.

2.4 Pseudonym-based Cryptography Schemes

The term "pseudonym" is used to refer to an alternative name used in place of a real name. In an organization, entities are identified and referred to by pseudonyms to protect their identity, maintain anonymity, and preserve privacy. It is important to ensure that there is no association between different pseudonyms assigned to a vehicle. The concept of conditional privacy-preserving can be achieved through the use of pseudonyms.

Schemes such as [9, 14–17] employ this approach for designing an effective system. However, it is crucial to acknowledge that such schemes may also have their limitations, including overhead from managing revocation lists and challenges related to public-private key management in certain cases. By and large, these schemes can be considered as a viable solution that offers usefulness in addressing certain challenges. However, it is important to note that they may not be sufficient on their own to tackle all the complexities of the problem at hand.

2.5 Group and Ring Signatures-based Schemes

In group signature, all the group members are allowed to sign the message on behalf of the group leader. A single group public-key is used to verify the signature but the identity of the signer is kept secret. Moreover, it is impossible to judge whether a group member has been issued two signatures. However, in case of any dispute a designated group manager can disclose the real identity of the signer [1]. However, a ring signature scheme offers a distinct advantage by enabling a user to sign a message anonymously within a group of users. This means that the actual signer of the message remains undisclosed, providing an additional layer of anonymity.

Schemes [18, 19] are based on group signature and ring signature, respectively. A group signature-based scheme can fulfill the requirement for conditional privacy preservation, whereas a ring signature does not provide the same level of privacy. However, a common weakness shared by these schemes is their reliance on complex computations and the need for certificates, resulting in high communication and computation overhead.

Based on the explanation provided in Section 2, we have adopted the pseudonym idea as a basis for designing a mutual authentication scheme among vehicles and RSUs in VANETs. By incorporating the pseudonym idea along with other concepts, such as HMAC (Hash-based Message Authentication Code), we have developed an authentication scheme for VANETs.

3 Security Goals

In this section, we will introduce the anticipated security requirements and engage in a discussion of the corresponding attacks. These requirements and attacks are derived from the thorough analyses conducted in [1, 20]. It's important to note that the focus of the proposed paper is solely on the authentication process between vehicles and RSUs. Consequently, this paper does not encompass any contributions related to V2V communication. As a result, certain security requirements and attacks related to V2V communication do not need to be addressed within this context. Each security requirement will be elaborated upon in the following.

- **Message and Source Authentication**: Message and source authentication are essential as-

pects that focus on verifying the legitimacy of the message sender and detecting any modifications made to the message. It is crucial for the recipient to confirm the identity of the sender and ensure the integrity of the received message.

In the proposed scheme, it is imperative for the RSU to ensure that the authentication request originates from a valid vehicle. This step helps establish the trustworthiness of the sender. Additionally, the RSU needs to verify that the authentication request has not been tampered with by an attacker, ensuring the integrity and authenticity of the received message. On the other hand, the vehicle participating in the authentication process should have mechanisms to ensure that a message is sent by the RSU.

- **Privacy Preservation**: Privacy preservation is a crucial requirement in the authentication process due to sensitive data such as the vehicle's real identity, coarse-grained value, and group-key. It is vital to keep this information concealed to prevent potential attacks, as an attacker could exploit knowledge of a vehicle's real identity for malicious purposes.

  However, it is important to acknowledge that achieving perfect privacy preservation may not be entirely useful in the context of mutual authentication. Instead, there is a need for conditional privacy preservation, which allows vehicles to maintain their privacy while still being traceable in situations where they violate laws or regulations.
- **Unlinkability**: Indeed, ensuring that there is no repeated algorithm or pattern in the exchanged messages during mutual authentication processes is crucial. The presence of a common algorithm or pattern can compromise the privacy of a vehicle and make it vulnerable to tracking attacks.

  To mitigate this risk, it is essential to design authentication protocols that employ randomized or non-deterministic elements, making it challenging for attackers to discern any predictable pattern or algorithm. It helps maintaining the unlinkability of the vehicles involved in the mutual authentication process.
- **Confidentiality**: Ensuring the confidentiality of exchanged messages is crucial to prevent unauthorized entities from accessing their contents. In the proposed scheme, for instance, if a vehicle sends its authentication request encrypted to the RSU, it effectively prevents other vehicles from accessing the data within the request, except for the RSU. In this paper, the criterion is to evaluate the confidentiality of the vehicle's authentication request.

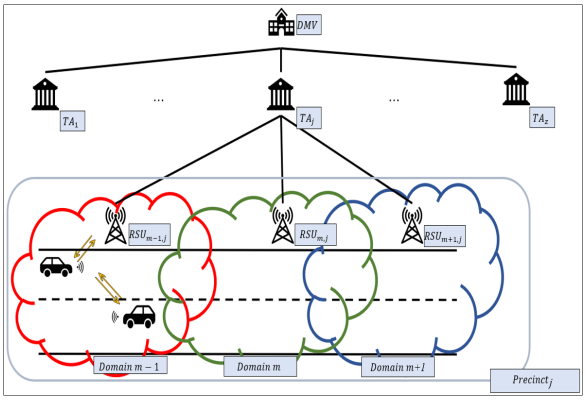


Figure 1. Proposed System Architecture

- **Non-repudiation**: Non-repudiation is a critical concept that ensures an entity cannot deny having sent a specific message. In the proposed scheme, it is essential to establish a mechanism where a vehicle cannot deny sending an authentication request, and the RSU cannot deny sending a message that includes a group key.
- **Unforgeability**: Absolutely, preventing message forgery and entity impersonation is crucial for the network. Unauthorized actions such as forging messages or impersonating entities can lead to chaos and disruption within the network without any accountability for the actual attacker. In the context of the proposed scheme, it is imperative to design mechanisms that prevent attackers from sending authentication requests using identities that do not belong to them.
- **Sybil Attack Resistance**: It is of utmost importance to prevent malicious vehicles within the network from generating valid fake identities that can successfully authenticate with an RSU. These fake identities can create an illusion of multiple vehicles, leading to potential security breaches and disruptions.

  Furthermore, it is essential to thwart attempts by malicious vehicles to deceive the RSU using a group of pseudonyms, thereby creating the perception of multiple distinct vehicles in the network. Such deceptive tactics can have severe implications for the overall security and operation of the network.

4 System Architecture and Preliminaries

4.1 System Architecture

As depicted in Figure 1, The VANET system comprises four key entities: the Department of Motor Vehicles (DMV), the Trusted Authorities (TAs), the fixed Road-Side Units (RSUs), and the Vehicles. Let's provide an explanation of each entity.

DMV: The Department of Motor Vehicles (DMV) serves as a trusted entity within the VANET system. Its primary role is to generate pseudonyms, which are then stored in the vehicle's Tamper-Proof Device (TPD) during periodic inspections. Additionally, the DMV is responsible for generating the security parameters required for secure communication within the network. In essence, it functions as the network manager, overseeing and coordinating various aspects of the VANET network.

TA: Each TA controls a precinct, which consists of multiple domains. Within each domain, there is one Road-Side Unit RSU. TAs receive security parameters from the DMV. They also possess the authority to address vehicles that violate traffic laws or engage in unlawful activities, thereby ensuring overall safety and order within their assigned precincts in the VANET network.

RSU: RSU, a trusted entity, serves as an intermediate component between OBUs and the TA in a trusted manner. It establishes wired connections with the TA while utilizing wireless links to communicate with OBUs. Positioned alongside the road, the RSU functions as a fixed access point. It has the capability to monitor its designated domain and gain access to the messages exchanged within that domain.

Vehicle: Vehicles within the VANET network are considered untrusted entities. Each vehicle is equipped with an On-Board Unit (OBU) and TPD. OBUs are responsible for wireless communication between vehicles and RSUs or other vehicles. On the other hand, TPDs securely store cryptographic parameters required for establishing secure communication within the network.

4.2 Preliminaries

A hash function $H(x)$ is homomorphic if, for any input pair x and y, $H(x+y) = H(x) + H(y)$ for the group operation $+$ in the input and output group [21]. For instance, $l-$bit strings, together with the XOR operation, form an Abelian group so that a hash function $H(x \oplus y) = H(x) \oplus H(y)$ for the bitwise XOR for m(input) and n bits(output) is an additive hash function [21]. This concept is elucidated in refrence [22] as the XOR-linear hash function. In reference [23], an RSA-based hash function is introduced, which can be regarded as a homomorphic hash function. Equation 1 presents the RSA-based hash function, showcasing its mathematical formulation and operation.

$$H(m) = b^m (mod n) \tag{1}$$

5 Proposed Scheme

As mentioned before, this scheme can be characterized as a pseudonym-based scheme that aims to tackle the common issues associated with such schemes and achieve an acceptable level of performance. In this section, we will describe our scheme in the following phases: pseudonym generation, sending authentication request, authenticating vehicle process, batch authentication process, group key distribution, and authenticating RSU by a vehicle, as well as obtaining group key. The notations used throughout this paper are listed in Table 1.

Table 1. Notations

Notations	Descriptions
TA_j	Trusted authority of $j-th$ precinct
$RSU_{m,j}$	$m-th$ road-side unit in $j-th$ precinct
V_i	The real identity of $i-th$ vehicle
Ps_i	$i-th$ pseudonym among all pseudonyms
H_1, H_2	Homomorphic hash function
H_3	Map to point
SF_1	First selection sunction
SF_2	Fecond selection function
K_{glb}	Global Key
K_{prv}	Private Key
C_l	$l-th$ coarse-grained group
c_l	Value of C_l
c_{V_i}	V_i's coarse-grained value
$F_{m,l}$	$m-th$ fine-grained group in the $l-th$ coarse-grained group
$f_{m,l}$	Value of $F_{m,l}$
TS	Time-stamp
TS_i	Sent time-stamp by i
$ID_{RSU_{m,j}}$	Identity of $RSU_{m,j}$
$Ps_{i,j}$	$j-th$ pseudonym of V_i
$Ps_{V_{i_{RSU_{m,j}}}}$	Pseudonym of V_i which is issued by $RSU_{m,j}$
$\oplus$	XOR
$\|$	Concatenation

5.1 Pseudonym Generation

In the first step, pseudonyms are generated by the DMV. The total number of pseudonyms should be an integer multiple of the total number of vehicles. Subsequently, clustering operations are performed on the pseudonyms to prevent easy generation of forged pseudonyms by any vehicle, thereby mitigating the risk of Sybil attacks. This clustering process is accomplished using the method presented in [24, 25]. Initially, the pseudonyms are concatenated with a global key, and the resulting concatenation is hashed. Subsequently, a specific function known as the "First Selection Function" extracts selected bits from the output, it is shown in Equation 2. The global key,

the first selection and hash function function are exclusively accessible to RSUs, TAs, and the DMV.

$$\begin{aligned} &\textit{Selecting a Subset of Bits from the Hash}\\ &\textit{Function Output} = SF_1(H_1(Ps_i \parallel K_{glb})), 1 \leq i \leq y \end{aligned} \tag{2}$$

Considering the characteristics of hash functions, the probability of collision in the output values for each pseudonym is negligible. However, when specific bit positions are chosen from output of each pseudonym, collisions can occur. Pseudonyms with identical selected bits are then grouped together, forming what is known as a coarse-grained group.This process is illustrated in Equation 3.

$$\begin{aligned} &\{Ps_i \mid SF_1(H_1(Ps_i \parallel K_{glb}))\} = c_l\\ &c_l \textit{ is constant and } 1 \leq i \leq y \end{aligned} \tag{3}$$

Next, the existing pseudonyms within each coarse-grained group are concatenated with a private key and the resulting concatenation is hashed. Subsequently, a specific function known as the "Second Selection Function" selects certain output bits, analogous to the process of producing coarse-grained groups. The private key value is exclusively known by the DMV and TAs, while it remains undisclosed to RSUs. Equation 4 illustrates the procedure involved in this step. Notably, this step differs from the previous process in terms of the selection function, the hash function, concatenated key, and the pseudonyms range.

$$\begin{aligned} &\textit{Selecting a Subset of Bits from the Hash}\\ &\textit{Function Output} = SF_2(H_2(Ps_k \parallel K_{prv})), Ps_k \in C_l \end{aligned} \tag{4}$$

The pseudonyms within a coarse-grained group, which share the same output bits as determined by Equation 4, are grouped together into a fine-grained group. This clustering process ensures that each pseudonym is assigned to a unique combination of a coarse-grained group and a corresponding fine-grained group. Subsequently, the pseudonyms within each fine-grained group are allocated to individual vehicles for a specific duration, such as one year. The process of forming a fine-grained group is illustrated in Equation 5.

$$\begin{aligned} &\{Ps_k \in C_l \mid SF_2(H_2(Ps_k \parallel K_{prv}))\} = f_{m,l}\\ &f_{m,l} \textit{ is constant} \end{aligned} \tag{5}$$

The method of clustering pseudonyms is depicted in Figure 2. At specific intervals, each RSU receives the revocation list from the TA. This list enables the revocation of either a specific pseudonym or all the pseudonyms associated with a particular vehicle.

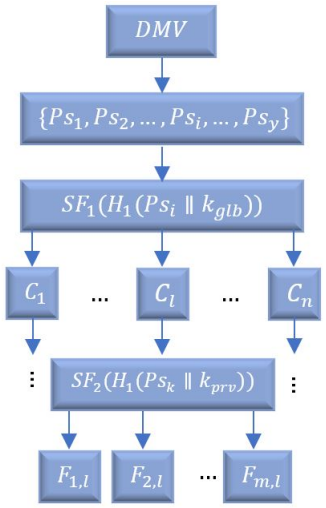


Figure 2. Method of clustering pseudonyms

Notably, RSU has access to the real identity concerned with a pseudonym. The overall function of this scheme is as follows: when a vehicle intends to authenticate itself within the domain, it sends an authentication request to the RSU. The RSU verifies the authentication request and subsequently distributes a group key to legitimate vehicles for secure V2V communication. Additionally, each vehicle is provided with a pseudonym for V2V communication purposes within the domain. In the following paragraphs, we will delve into the details of the proposed scheme.

5.2 Sending Request for Authentication

In this method, authentication requests and other data are transmitted plainly to the RSU without encryption. Consequently, pseudonyms should be utilized in a single-serving manner. When a vehicle enters an RSU domain, it sends an authentication request to the RSU. The format of this message is illustrated in (6).

$$\begin{aligned} &V_i \rightarrow RSU_{m,j} = \{PS_{i,j}, TS_{V_i}, A_i\}\\ &A_i = H_2(c_{V_i} \parallel TS_{V_i}) \end{aligned} \tag{6}$$

5.3 Authenticating Vehicle Process

When the RSU receives an authentication request message, it first examines the timestamp of the message. If the timestamp falls within an acceptable range, the RSU proceeds to verify the pseudonym. The pseudonym should not have been listed on the revocation list. If this stage is successfully passed, the RSU utilizes the first selection function and the global key, which are accessible to the RSU, to validate the accuracy of the request message using Equation 7. If Equation 7 holds true, the authentication of the vehicle is deemed successful.

$$H_2(SF_1(H_1(Ps_{i,j} \parallel K_{glb})) \parallel TS_{V_i}) = A_i \quad (7)$$

5.4 Batch Authentication Process

When a group of cars enters a domain simultaneously and sends their authentication requests, checking these requests individually would result in a loss of network efficiency. In such cases, it is essential for the network to authenticate all vehicles simultaneously and swiftly. This capability is referred to as "Batch Authentication". The use of homomorphic hash functions in this scheme enables the achievement of this goal. The process of batch authentication is outlined from Equations 8 to 13. Equation 12 or 13 serves as the final equation specifically designed for batch authentication. In order to detect Sybil attacks during the batch authentication phase, it is crucial to utilize Equation 10 for the purpose of batch authentication.

$$\begin{aligned} &H_2(SF_1(H_1(Ps_{1,\alpha} \parallel K_{glb})) \parallel TS_{V_1}) \oplus \\ &H_2(SF_1(H_1(Ps_{2,\beta} \parallel K_{glb})) \parallel TS_{V_2}) \oplus \ldots \oplus \\ &H_2(SF_1(H_1(Ps_{n,\gamma} \parallel K_{glb})) \parallel TS_{V_n}) = \\ &A_1 \oplus A_2 \oplus \ldots \oplus A_n \end{aligned} \quad (8)$$

Because H_2 is a homomorphic hash function, it can be factorized.

$$\begin{aligned} &H_2(\ (SF_1(H_1(Ps_{1,\alpha} \parallel K_{glb})) \parallel TS_{V_1}) \oplus \\ &(SF_1(H_1(Ps_{2,\beta} \parallel K_{glb})) \parallel TS_{V_2}) \oplus \ldots \oplus \\ &(SF_1(H_1(Ps_{n,\gamma} \parallel K_{glb})) \parallel TS_{V_n})\ ) = \\ &A_1 \oplus A_2 \oplus \ldots \oplus A_n \end{aligned} \quad (9)$$

Since XOR is a bitwise operation, the equation can be expressed in the format shown in Equation 10.

$$\begin{aligned} &H_2(\ SF_1(H_1(Ps_{1,\alpha} \parallel K_{glb})) \\ &\oplus SF_1(H_1(Ps_{2,\beta} \parallel K_{glb})) \oplus \ldots \oplus SF_1(H_1 \\ &(Ps_{n,\gamma} \parallel K_{glb})) \parallel (TS_{V_1} \oplus TS_{V_2} \oplus \ldots \oplus TS_{V_n})) = \\ &A_1 \oplus A_2 \oplus \ldots \oplus A_n \end{aligned} \quad (10)$$

Also, SF_1 and H_1, which are homomorphic functions, can be factorized. It has shown in Equation 11.

$$\begin{aligned} &H_2(\ SF_1(H_1(Ps_{1,\alpha} \parallel K_{glb}) \oplus (Ps_{2,\beta} \parallel K_{glb}) \\ &\oplus \ldots \oplus (Ps_{n,\gamma} \parallel K_{glb})) \parallel \\ &(TS_{V_1} \oplus TS_{V_2} \oplus \ldots \oplus TS_{V_n})) = \\ &A_1 \oplus A_2 \oplus \ldots \oplus A_n \end{aligned} \quad (11)$$

Similar to the previous parts, in this step, the XOR operation can be performed on pseudonyms and global keys separately. Finally, Equation 12 is achieved. It can be used for batch authentication.

$$\begin{aligned} &H_2(\ SF_1(H_1(Ps_{1,\alpha} \oplus Ps_{2,\beta} \oplus \ldots \oplus Ps_{n,\gamma}) \parallel \\ &(K_{glb} \oplus K_{glb} \oplus \ldots \oplus K_{glb})) \parallel \\ &(TS_{V_1} \oplus TS_{V_2} \oplus \ldots \oplus TS_{V_n})\ ) = \\ &A_1 \oplus A_2 \oplus \ldots \oplus A_n \end{aligned} \quad (12)$$

The result of the XOR will be zero if the number of applicants for the network is even. This could be seen as a positive opportunity for attackers and could facilitate their work. In this situation, RSU can use Equation 13. In this approach, a predefined authentication message has a timestamp and pseudonym set to zero strings, which serve as the identity element for XOR operations.

$$\begin{aligned} &if\ n\ =\ even\ number\ : \\ &H_2(\ SF_1(H_1(Ps_{1,\alpha} \oplus Ps_{2,\beta} \oplus \ldots \oplus Ps_{n,\gamma}) \parallel \\ &(K_{glb}))\ \parallel (TS_{V_1} \oplus TS_{V_2} \oplus \ldots \oplus TS_{V_n})\ ) = \\ &A_1 \oplus A_2 \oplus \ldots \oplus A_n \oplus A_{n+1} \\ &A_{n+1} = \\ &H_2(SF_1(H_1(Ps = 0 \parallel K_{glb})) \parallel TS = 0) \end{aligned} \quad (13)$$

5.5 Group Key Distribution

After successfully authenticating a vehicle or vehicles, the RSU is responsible for sending a group key as a symmetric encryption key to ensure secure communication among the vehicles. However, it is crucial that the transfer of group keys remains confidential, considering the absence of a secure channel between the vehicles and the RSU. To address this requirement, a key between each vehicle and the RSU is necessary to establish encrypted communication. Key establishment protocols can be employed to accomplish this objective. In this case, the key is set to a value of Equation 14, as mentioned before, RSU has access to the real identity concerned with a pseudonym. Subsequently, the RSU sends the value of the group key for secure V2V communication to each vehicle using a message format in (15). A Pseudonym is assigned by the RSU to V_i, for utilization in V2V communications to ensure traceability.

$$K_{RSU_{m,j},V_i} = H_3(ID_{RSU_{m,j}} \parallel V_i) \quad (14)$$

$$RSU_{m,j} \rightarrow V_i = \{K_G, Ps_{V_{i_{RSU_{m,j}}}}, TS_{RSU}\}_{K_{RSU_{m,j},V_i}} \quad (15)$$

5.6 Authenticating RSU and Obtaining Group Key

As soon as the vehicle receives a message from RSU with a group key, it uses $K_{RSU_{m,j},V_i}$ to decrypt the message. After acquiring the group key and pseudonym for V2V communication, vehicles in the

domain will be able to communicate with each other. An overview of the proposed scheme is shown in Algorithm 1.

Algorithm 1 Mutual Authentication Process and Group Key Acquisition

1: $RSU \leftarrow \{Ps_{i,j}, TS_{V_i}, H_2(c_{V_i} \parallel TS_{V_i})\}$
2: **if** TS_{V_i} is acceptable and $Ps_{i,j}$ was not revoked **then**
3: RSU verifies $H_2(SF_1(H_1(Ps_{i,j} \parallel K_{glb})) \parallel TS_{V_i}) = A_i$
4: **if** the equation holds **then**
5: RSU computes $K_{RSU_{m,j},V_i} = H_3(ID_{RSU_{m,j}} \parallel V_i)$
6: RSU sends $\{K_G, Ps_{V_{i_{RSU_{m,j}}}}, TS_{RSU}\}_{K_{RSU_{m,j},V_i}}$
7: **end if**
8: **end if**
9: $V_i \leftarrow \{K_G, Ps_{V_{i_{RSU_{m,j}}}}, TS_{RSU}\}_{K_{RSU_{m,j},V_i}}$
10: **if** TS_{RSU} is acceptable **then**
11: **Output:** Mutual authentication and group key acquisition completed successfully.
12: **end if**

6 Evaluation of Proposed Schemes

In this section, the proposed scheme will be analyzed concerning security requirements, computational cost, and communication overhead, and it will be compared with other pseudonym-based existing schemes which were introduced in Section 2.4.

6.1 Security Analysis

Some security requirements including confidentiality of the group key, the confidentiality of the symmetric key for secure communication between RSU and Vehicle, the value of coarse-grained value, and mutual authentication between the vehicle and RSU will be formally examined, while other security requirements will be assessed informally.

6.1.1 formal Analysis of Proposed Scheme

The formal analysis is performed with AVISPA (Automated Validation of Internet Security Protocols and Applications), which is a toolset for the analysis of security protocols. It provides an environment to model and verify the correctness of cryptographic protocols using different formal methods. As mentioned before, the considered goals in the simulation include the confidentiality of the group key, the confidentiality of the symmetric key for secure communication between RSU and Vehicle, the value of coarse-grained value, and mutual authentication between the vehicle and RSU.

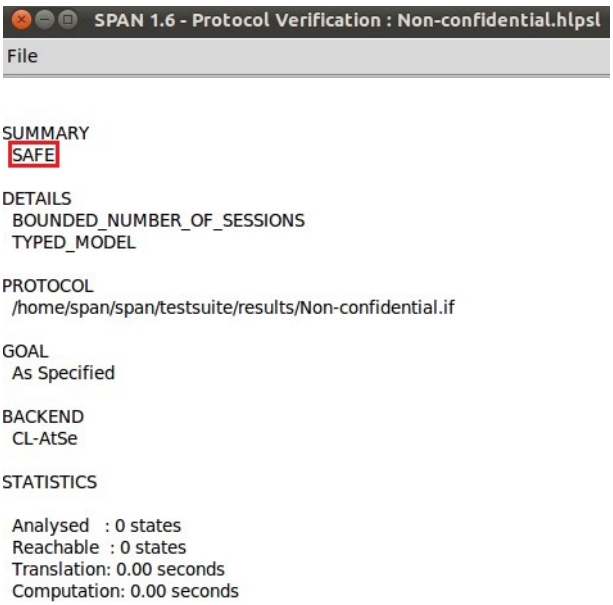


Figure 3. evaluation in AVISPA with ASTE

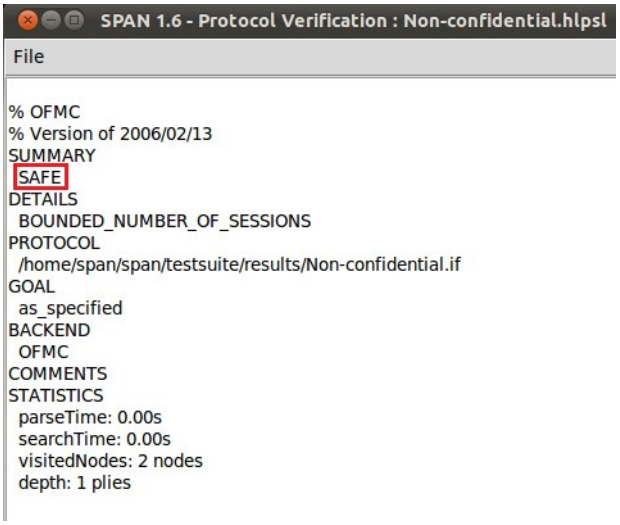


Figure 4. evaluation in AVISPA with OFMC

In this simulation, the channel model is Dolev-Yao, which means that the attacker model is Dolev-Yao. Additionally, the AVISPA tools, OFMC and ASTE, are employed for analyzing protocols related to authentication and key agreement. OFMC and ASTE are powerful tools within the AVISPA framework that provide thorough analysis and verification capabilities for protocol security. The results are shown in Figure 3 and 4. As depicted in the figures, when the executed protocols yield safe results, it signifies the successful achievement of goals.

6.1.2 Informal Analysis of Proposed Scheme

In this section, the considered goals include message authentication, privacy preservation, unlinkability,

Table 2. Comparison of security goals

Scheme	[16]	[17]	[15]	[14]	[9]	Proposed scheme
Message and source authentication	✓	✓	✓	✓	✓	✓
Privacy-preserving and unlinkability	✓	✓	×	✓	✓	✓
Non-repudiation	✓	✓	✓	✓	✓	✓
Sybil attack resistance	×	×	×	×	×	✓
Impersonation attack resistance	✓	✓	×	✓	✓	✓
Confidentiality	×	×	×	×	×	×

collusion resistance, unforgeability, and sybil attack resistance.

- **Message Authentication**: It can also be referred to as integrity assurance. it is advisable to analyze this concept from two perspectives. First, in the authentication request sent by the vehicle, this requirement is fulfilled through the use of HMAC. This process ensures that the RSU can verify whether the message has been tampered with by malicious entities. On the other hand, due to the symmetric key encryption between RSUs and vehicles, any alteration to the message would render it unintelligible. Consequently, integrity can be effectively achieved.
- **Privacy Preservation and Unlinkability**: The primary objective in privacy preservation is to prevent identity disclosure from other vehicles, and this is achieved in the proposed scheme through the use of single-serving pseudonyms. Another crucial aspect is the one-way property of the Hash function, which prevents attackers from accessing the coarse-grained value and ensures privacy preservation. Furthermore, when a vehicle sends an authentication request, it employs different pseudonyms for each request, thereby maintaining anonymity. The randomized output of the hash function ensures that there are no common patterns in the messages, thus preserving unlinkability.
- **Unforgeability**: Since pseudonyms are stored in the TPD, no entity can have access to them. Furthermore, pseudonyms are single-serving, preventing attackers from exploiting them. They exclusively belong to the vehicle, and other vehicles cannot utilize them. Additionally, an attacker cannot generate a valid pseudonym due to the lack of access Global key. Moreover, the hash function, which is a one-way function, prevents attackers from obtaining the coarse-grained value from the exchanged messages.
- **Non-Repudiation**: Due to the storage of pseudonyms in the TPD and their single usage nature, it becomes unfeasible for a malcious vehicle to use them. Furthermore, these pseudonyms are inherently non-forgable. Consequently, the only entity empowered to initiate an authentication request using a valid pseudonym is its rightful possessor. Conversely, the RSU exclusively possesses the ability to respond to an authentication request with a valid encrypted message, thereby negating any possibility of RSU denial in message transmission.
- **Sybil Attack Resistance**: As mentioned earlier, in this attack, the goal of the attacker is to create an illusion of the presence of multiple vehicles. There are several ways in which this can be attempted.

  The first way is by generating valid pseudonyms to deceive the RSU. However, this approach is impossible because the attacker does not have access to the Global key.

  Another approach is to exploit the pseudonyms of other vehicles. However, since pseudonyms are stored in the TPD, they are inaccessible to the attacker, making this method infeasible as well.

  The last approach involves using a group of pseudonyms to deceive the RSU. However, if this occurs, the RSU can detect the presence of multiple pseudonyms with the same coarse-grained value, which raises suspicion. In such cases, the RSU sends the pseudonyms to the TA, which can determine whether they belong to a legitimate group or not. If all the pseudonyms belong to a fine-grained group, a Sybil attack is detected. This process is carried out by the TA to reduce the overhead on the RSU, thereby improving the functionality of the scheme.

  It is important to note that the likelihood of encountering vehicles with identical coarse-grained values is minimal. For instance, considering a 30-bit function as the coarse-grained value, the probability of encountering two pseudonyms with the same coarse-grained value remains low. if it is desired to detect the Sybil attack during the batch authentication phase, the RSU has the option to employ Equation 10. While this choice may entail an increased com-

putational overhead for the RSU, it provides the advantage of enabling Sybil attack detection concurrent with batch authentication. This detection strategy relies on the presence of at least two distinct coarse-grained values, which raises the probability of identifying a potential Sybil attack. However, if the consideration of Sybil attacks is either irrelevant or can be managed independently from the batch authentication process, the RSU has the option to employ Equation 12 or 13 for batch authentication.

Table 2 presents a comparison between the proposed schemes and several pseudonym-based existing schemes in terms of security requirements.

6.2 Computation Cost

For evaluating a scheme in terms of computational overhead, it is necessary to consider the time taken to perform various operations. Table 3 displays the execution time of certain operations. The execution time for operations, excluding XOR, was obtained from the measurements conducted in [9] using an Intel Pentium IV 3.0 GHz processor. The XOR time execution, on the other hand, was measured using an Intel Core i3 processor.

To calculate the XOR execution time in Intel Pentium IV 3.0 GHz, a comparison can be made using the website https://www.cpubenchmark.net/compare/ to obtain the benchmark score for this processor. By referring to the benchmark score, the execution time for XOR on the Intel Pentium IV 3.0 GHz processor can be estimated.

Also, XOR operations cannot be considered negligible, because the proposed scheme heavily relies on XOR operations, and it is important to take into account the computational overhead associated with them.

Table 3. Execution time of operators

Operation	**Execution Time** (ms)
Scalar multiplication in elliptic curves (T_{mul})	0.6
Point addition in an elliptic curve	Ignorable
Hash function (T_H)	0.02
Map to point (T_{M2P})	0.6
Calculating bivariate polynomial	Ignorable
Bilinear pairing (T_{par})	4.5
Selection function	Ignorable
XOR	3.14×10^{-6}

It is evident that the inclusion of operations such as bilinear pairing significantly impacts the efficiency of designing an authentication scheme. In Table 4, the time required for generating an authentication request is presented.

Table 4. Required time for generating an authentication request

Scheme	**Required time**
[9]	$4T_{mul} + T_{M2P} = 3ms$
[15]	$3T_{mul} + 3T_H = 1.86ms$
[14]	$2T_{mul} + 2T_H = 1.86ms$
[16]	$2T_{mul} + 2T_H = 0.64ms$
[17]	$3T_H = 0.06ms$
Proposed scheme	$T_H = 0.02ms$

Table 5 showcases the delay associated with batch authentication.

Table 5. Batch authentication delay

Scheme	**Delay** (n: number of vehicles)
[9]	$3T_{par} + (n+1)T_{mul}$
[15]	$(2n+2)T_{mul} + 2nT_H$
[14]	nT_H
[16]	$2T_{mul} + nT_H$
[17]	nT_H
Proposed scheme	$2T_H + n \times 3.14 \times 10^{-6}$

The delay of batch authentication in the presence of 2 to 100 vehicles within the RSU's domain is illustrated in Figure 5. The chart highlights the performance of four schemes that have the best delay results. It is evident that the proposed scheme outperforms the other schemes in terms of delay.

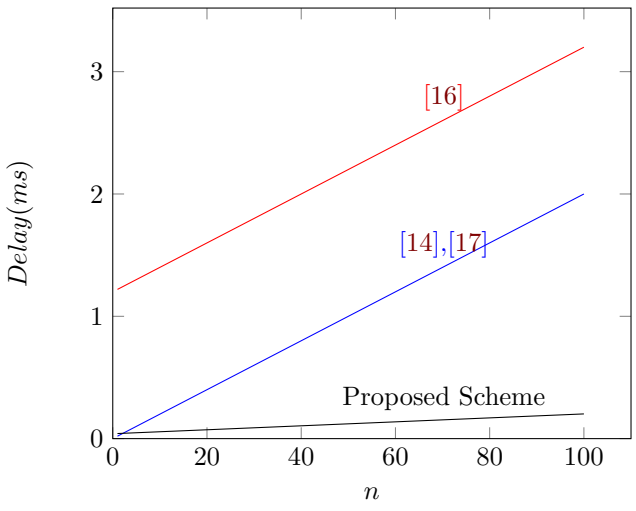


Figure 5. Batch authentication delay for 2 to 100 vehicles

6.3 Communication Overhead

For evaluating the communication overhead, it is necessary to calculate the message size, which can be determined by considering the size of each component. Table 6 provides the size of each component.

Table 6. Message components size

Pseudonym	30B
Coarse-Grained Value	30B
Time Stamp	4B
Symmetric Key	16B
Coarse-Grained Value	4B
Output of H_2	32B

In Table 7, a comparison among schemes in terms of communication overhead is presented. It is important to note that in this scheme, the revocation list overhead is shifted to the RSUs, resulting in improved performance, as vehicles often face constraints in terms of computational resources.

Table 7. The communication overhead of authentication requests

Scheme	Communication Overhead
[9]	$92B$
[15]	$148B$
[14]	$100B$
[16]	$104B$
[17]	$44B$
Proposed Scheme	$66B$

7 Conclusion

In this paper, a scheme is introduced for VANETs that not only meets security requirements and has low communication and computation overhead but also, successfully fulfills desired targets, including batch authentication, resistance against Sybil attacks, and efficient management of revocation lists. Moreover, the scheme achieves the most important goals which are mutual authentication and conditional privacy preservation. By using the concept of the homomorphic hash function, computation overhead significantly reduces. Regarding security goals and computation overhead, the proposed scheme outperforms the other introduced schemes. While is a scheme with lower communication overhead, when considering all aspects, the proposed scheme remains an acceptable choice overall. It strikes a balance between security, computation overhead, and communication overhead, can make it a favorable option for VANETs.

References

[1] Sagheer Ahmed Jan, Noor Ul Amin, Mohamed Othman, Mazhar Ali, Arif Iqbal Umar, and Abdul Basir. A survey on privacy-preserving authentication schemes in vanets: attacks, challenges and open issues. *IEEE Access*, 9:153701–153726, 2021.

[2] Azlan Awang, Khaleel Husain, Nidal Kamel, and Sonia Aissa. Routing in vehicular ad-hoc networks: A survey on single-and cross-layer design techniques, and perspectives. *IEEE Access*, 5:9497–9517, 2017.

[3] Rakesh Shrestha, Rojeena Bajracharya, Anish P Shrestha, and Seung Yeob Nam. A new type of blockchain for secure message exchange in vanet. *Digital communications and networks*, 6(2):177–186, 2020.

[4] Pravin Mundhe, Shekhar Verma, and S Venkatesan. A comprehensive survey on authentication and privacy-preserving schemes in vanets. *Computer Science Review*, 41:100411, 2021.

[5] Sowmya Kudva, Shahriar Badsha, Shamik Sengupta, Ibrahim Khalil, and Albert Zomaya. Towards secure and practical consensus for blockchain based vanet. *Information Sciences*, 545:170–187, 2021.

[6] Lei Zhang, Mingxing Luo, Jiangtao Li, Man Ho Au, Kim-Kwang Raymond Choo, Tong Chen, and Shengwei Tian. Blockchain based secure data sharing system for internet of vehicles: A position paper. *Vehicular Communications*, 16:85–93, 2019.

[7] Otto B Piramuthu and Matthew Caesar. Vanet authentication protocols: security analysis and a proposal. *The Journal of Supercomputing*, 79(2):2153–2179, 2023.

[8] Pandi Vijayakumar, Maria Azees, Victor Chang, Jegatha Deborah, and Balamurugan Balusamy. Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. *cluster computing*, 20:2439–2450, 2017.

[9] Shunrong Jiang, Xiaoyan Zhu, and Liangmin Wang. An efficient anonymous batch authentication scheme based on hmac for vanets. *IEEE Transactions on Intelligent Transportation Systems*, 17(8):2193–2204, 2016.

[10] Arwa Alrawais, Abdulrahman Alhothaily, Bo Mei, Tianyi Song, and Xiaolu Cheng. An efficient revocation scheme for vehicular ad-hoc networks. *Procedia Computer Science*, 129:312–318, 2018.

[11] Marcos A Simplicio, Eduardo Lopes Cominetti, Harsh Kupwade Patil, Jefferson E Ricardini, Leonardo TD Ferraz, and Marcos Vini-

cius M Silva. Privacy-preserving certificate linkage/revocation in vanets without linkage authorities. *IEEE Transactions on Intelligent Transportation Systems*, 22(6):3326–3336, 2020.

[12] Yimin Wang, Hong Zhong, Yan Xu, Jie Cui, and Ge Wu. Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for vanets. *IEEE Systems Journal*, 14(4):5373–5383, 2020.

[13] Lei Zhang, Xinyu Meng, Kim-Kwang Raymond Choo, Yuanfei Zhang, and Feifei Dai. Privacy-preserving cloud establishment and data dissemination scheme for vehicular cloud. *IEEE Transactions on Dependable and Secure Computing*, 17(3):634–647, 2018.

[14] Jie Cui, Wenyu Xu, Yibo Han, Jing Zhang, and Hong Zhong. Secure mutual authentication with privacy preservation in vehicular ad hoc networks. *Vehicular Communications*, 21:100200, 2020.

[15] Hongyuan Cheng and Yining Liu. An improved rsu-based authentication scheme for vanet. *Journal of Internet Technology*, 21(4):1137–1150, 2020.

[16] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks. *Sensors*, 22(5):1696, 2022.

[17] Saad Ali Alfadhli, Songfeng Lu, Kai Chen, and Meriem Sebai. Mfspv: A multi-factor secured and lightweight privacy-preserving authentication scheme for vanets. *IEEE Access*, 8:142858–142874, 2020.

[18] Lili Zhang, Chenming Li, Yueheng Li, Qiaomei Luo, and Rongbo Zhu. Group signature based privacy protection algorithm for mobile ad hoc network. In *2017 IEEE International Conference on Information and Automation (ICIA)*, pages 947–952. IEEE, 2017.

[19] Yi Han, Nuo-Nuo Xue, Bi-Yao Wang, Qi Zhang, Chun-Lei Liu, and Wei-Shan Zhang. Improved dual-protected ring signature for security and privacy of vehicular communications in vehicular ad-hoc networks. *IEEE Access*, 6:20209–20220, 2018.

[20] Ikram Ali, Alzubair Hassan, and Fagen Li. Authentication and privacy schemes for vehicular ad hoc networks (vanets): A survey. *Vehicular Communications*, 16:45–61, 2019.

[21] Juan Carlos Garcia-Escartin, Vicent Gimeno, and Julio José Moyano-Fernández. Quantum collision finding for homomorphic hash functions. *arXiv preprint arXiv:2108.00100*, 2021.

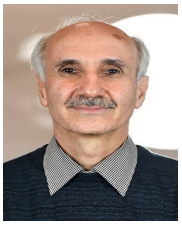
[22] Hugo Krawczyk. Lfsr-based hashing and authentication. In *Annual International Cryptology Conference*, pages 129–139. Springer, 1994.

[23] Young-Sam Kim and Joon Heo. Device authentication protocol for smart grid systems using homomorphic hash. *Journal of Communications and Networks*, 14(6):606–613, 2012.

[24] Anu S Lal and Reena Nair. Region authority based collaborative scheme to detect sybil attacks in vanet. In *2015 International Conference on Control Communication & Computing India (ICCC)*, pages 664–668. IEEE, 2015.

[25] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty. P2dap—sybil attacks detection in vehicular ad hoc networks. *IEEE journal on selected areas in communications*, 29(3):582–594, 2011.

Mohamadreza Amani received the B.Sc. degree in Electrical Engineering from Iran University of Science and Technology, Tehran, Iran, in 2019. Hw received M.Sc. degree from Sharif University of Technology, in 2022. His research interests include Vehicular Ad-hoc Networks (VANET), Security Analysis, Network Protocols, Cryptography, and Blockchain Technology.



Javad Mohajeri is an Assistant Professor with the Electronics Research Institute, Sharif University of Technology, Tehran, Iran, where he is an Adjunct Assistant Professor with the Electrical Engineering Department. His current research interests include Data Security and the Design and Analysis of Cryptographic Protocols and Algorithms. Javad is a Founding Member of the Iranian Society of Cryptology.

Mahmoud Salmasizadeh received the B.Sc. and M.Sc. degrees in electrical engineering from Sharif University of Technology, Tehran, Iran, in 1972 and 1989, respectively. He also received a Ph.D. degree in information technology from Queensland University of Technology, Australia, in 1997. Currently, he is an associate professor in the Electronics Research Institute and an adjunct associate professor in the Electrical Engineering Department, Sharif University of Technology. His research interests include the Design and Cryptanalysis of Cryptographic Algorithms and Protocols, E-commerce Security, and Information-Theoretic Secrecy. He is a founding member of the Iranian Society of Cryptology.