Computers, Materials & Continua
DOI:10.32604/cmc.2022.023476
Article

Tech Science Press

An Enhanced Privacy Preserving, Secure and Efficient Authentication Protocol for VANET

Safiullah Khan[1], Ali Raza[2,3] and Seong Oun Hwang[4,*]

[1]Department of IT Convergence Engineering, Gachon University, Seongnam, 13320, Korea
[2]ENSAIT, GEMTEX-Laboratoire de Genie et Materiaux Textiles, University of Lille, Lille, F59000, France
[3]School of Computing & Institute of Cyber Security (ICSS), University of Kent, United Kingdom
[4]Department of Computer Engineering, Gachon University, Seongnam, 13320, Korea
*Corresponding Author: Seong Oun Hwang. Email: sohwang@gachon.ac.kr
Received: 09 September 2021; Accepted: 20 October 2021

Abstract: Vehicular ad hoc networks (VANETs) have attracted growing interest in both academia and industry because they can provide a viable solution that improves road safety and comfort for travelers on roads. However, wireless communications over open-access environments face many security and privacy issues that may affect deployment of large-scale VANETs. Researchers have proposed different protocols to address security and privacy issues in a VANET, and in this study we cryptanalyze some of the privacy preserving protocols to show that all existing protocols are vulnerable to the Sybil attack. The Sybil attack can be used by malicious actors to create fake identities that impair existing protocols, which allows them to imitate traffic congestion or at worse cause an accident that may result in the loss of human life. This vulnerability exists because those protocols store vehicle identities in an encrypted form, and it is not possible to search over the encrypted identities to find fake vehicles. This attack is serious in nature and very prevalent for privacy-preserving protocols. To cope with this kind of attack, we propose a novel and practical protocol that uses Public key encryption with an equality test (PKEET) to search over the encrypted identities without leaking any information, and eventually eliminate the Sybil attack. The proposed approach improves security and at the same time maintains privacy in VANET. Our performance analysis indicates that the proposed protocol outperforms state-of-the-art protocols: The proposed beacon generation time is constant compared to a linear increase in existing protocols, with beacon verification shown to be faster by 7.908%. Our communicational analysis shows that the proposed protocol with a beacon size of 322 bytes has the least communicational overhead compared to other state-of-the-art protocols.

Keywords: VANET; authentication protocol; cryptanalysis; privacy preserving; intelligent systems

1 Introduction

Vehicular ad hoc networks (VANETs) are a subset of Mobile ad hoc networks (MANETs) in which smart vehicles act as mobile nodes with their movement governed by road topologies. The vehicles communicate with each other using Vehicle-to-vehicle (V2V) communication and with Road-side unit (RSU), known as Vehicle-to-infrastructure (V2I) communication. Each vehicle is equipped with an On board unit (OBU) that can perform computations and establish communication. A vehicle in a VANET periodically broadcasts messages containing information related to its speed, location, traffic and accidents, known as beacons [1].

Despite these advantages, authentication, security and privacy are critical challenges for VANETs [2]. VANETs have an additional number of challenges, particularly in the domain of authentication, privacy and security [3]. Unauthenticated information in the network may lead to malicious attacks and service abuses that pose a threat to users [4]. In contrast to classical wired networks that have protections in terms of firewalls and gateways, security attacks on such wireless networks could come from various sources to target all nodes [5,6]. Additionally, VANETs are an instance of mobile ad hoc networks. Consequently, they inherit all known and unknown security flaws, such as Sybil attacks that are associated with MANETs [7]. VANETs are more challenging to secure due to their distinct characteristics and features, such as the high mobility of the end users and wide area of the network [8]. Therefore, a new mechanism to provide the desired security, including authentication, integrity, and nonrepudiation, needs to be proposed prior to the practical deployment of VANETs [9].

With regards to issues such as authentication privacy and security, researchers have proposed a number of protocols [10,11]. In [10], the authors proposed a hierarchical privacy preserving pseudonymous authentication protocol for the VANET. Their protocol makes use of two different types of pseudonyms, one is referred to as the primary pseudonym and the second is the secondary pseudonym. A primary pseudonym is provided to a vehicle upon successful verification by the Certification authority (CA). Using this primary pseudonym, the vehicle can request the RSU for a secondary pseudonym that is then broadcast along with the beacons in the VANET. Each pseudonym is associated with an expiration time after which the vehicle has to request new primary and secondary pseudonyms. Primary pseudonyms are associated with a relatively longer expiration time than the secondary pseudonyms.

Furthermore, in [10], the authors provided a brief security analysis to claim the security of the proposed protocol. Usually, in VANETs (e.g., in [10,11]), authorities (such as a CA and Social network (SN), respectively) store the real identities of the vehicles in an encrypted form. Consequently, searching on encrypted data becomes complicated because these authorities are required to first decrypt the encrypted identity prior to searching [12–15] work based on a fully trusted authority. If the trusted authority is compromised, these protocols do not provide security and privacy. We need protocols which can provide privacy even if partially/fully trusted authorities are compromised. Sometimes in an Internet of things (IoT) era (e.g., Internet of vehicles (IoV), smart grids, healthcare, etc.) we need a balance between user privacy and access to information by authorities (CA and SN). Searchable encryption is a cryptographic scheme that provides this kind of balance [16–22]. Public key encryption with equality test (PKEET) is a special type of searchable encryption scheme [23], with a kind of Public key encryption (PKE) that allows to check whether two ciphertexts are encrypted under (possibly) different public keys contain the same message. In other words, searchable encryption is a positive way to protect users' sensitive data, while preserving search ability on the server side. It allows the server to search encrypted data without leaking any information in plaintext data. For more in-depth information about searchable encryption, readers are encouraged to read [24].

We have surveyed many VANET related protocols and classify them into two categories. The protocols in the first category do not encrypt the real identities of vehicles, including [25,26], which can reveal information about the vehicle's daily route. Therefore, they do not provide privacy preservation. The protocols in the second category encrypt the real identities in order to preserve the privacy of the vehicles, which is more desirable for state-of-the-art methods. However, we found that a number of existing protocols including [10,11] in the second category are vulnerable to the Sybil attack since the identities are encrypted and cannot be verified. Thus, a malicious vehicle can create many fake identities, exploiting this vulnerability which may result in fake congestion in the network and subsequently cause serious accidents. To address this problem, we present a novel privacy-preserving protocol secure against the Sybil attack with practical performance. Therefore, this paper not only shows that the protocols are vulnerable against the Sybil attack, but also provides a novel protocol with stronger security along with efficient authentication, beacon generation and beacon verification. In addition, other parameters for the proposed algorithm like the transmit power and scheduling are based on adaptive-transmit power control algorithm [27], while radio resource allocation is performed using a supervised deep learning technique [28].

The contributions of this paper can be summarized as follows:

1. In this paper, we cryptanalyze existing protocols that protect privacy by encrypting vehicles' real identities and are claimed to be secure and efficient protocols for VANETs. We show for the first time that they are vulnerable to the Sybil attack because they cannot verify the vehicle identity during primary pseudonym generation, which is encrypted. This attack may result in fake congestion in the network and subsequently cause catastrophic consequences, which should be resolved. However, protecting such protocols from the Sybil attack is complicated in nature because the vehicle identities in the existing protocols such as [10,11] are encrypted to protect user privacy. It is difficult to protect both user privacy and security against the Sybil attack at the same time. Hence, we present a new research direction when designing a secure and privacy-preserving protocol for VANET.
2. We propose a novel privacy-preserving protocol secure against the Sybil attack by introducing searchable encryption that allows for verification of encrypted vehicle identities. This proposed method is generic in the sense that it can be applied to all protocols vulnerable to the Sybil attack due to encrypted vehicle identities. We examine various attack scenarios and prove that the proposed protocol is secure against the Sybil attack along with satisfying the general security requirements for VANET protocols.
3. We also perform an in-depth analysis of the proposed protocol in terms of the performance over time. The proposed beacon generation has constant time with an increasing number of beacons, in contrast to the linearly increasing time for existing protocols. Regarding beacon verification time, it outperforms existing protocols by 7.908%. We also show that the proposed protocol with a beacon size of 322 bytes has the least communicational over-head compared to other state-of-the-art protocols. The proposed protocol shows its practical applicability in VANET as the beacons are generated and verified on a massive scale.

The rest of the paper is organized as follows: The background and relevant studies are introduced in Section 2. A cryptanalysis of the existing protocols is provided in Section 3. Section 4 defines the proposed protocol. Section 5 presents the analysis of the proposed protocol. Section 6 concludes the paper.

2 Background

In this section, we present background knowledge on a conventional VANET architecture as well as the assumptions and cryptographic tools used in this work.

2.1 Conventional VANET Architecture

Fig. 1 depicts a conventional VANET architecture, where a vehicle first needs to be registered with the Registration authority (RA) in order to receive and send the beacons in the VANET. According to [29], each vehicle has a unique identifier associated with it. In this paper, we refer to it as VID_i. VID_i, is an electronic license plate, and can be issued and installed in the vehicle's OBU by the vehicle registration authorities. VID_i serves as a real identity of a vehicle and uniquely identifies it. A vehicle in our model is required to provide VID_i to RA for registration. Our system model consists of the following participants.

1. Registration authority (RA): During the registration, RA generates a public/private key pair using PKEET [30] and encrypts the VID_i with a public key and sends the encrypted VID_i to the initial vehicle (V_i) and a trapdoor T to CA through a secure channel. Upon the request of legal authorities, RA provides the decryption key to reveal the VID_i.
2. Certification authority (CA): CA issues the primary pseudonyms and keeps associations between the encrypted VID_i and the primary pseudonym. Each primary pseudonym has an expiration time (T_{CA}), after which a vehicle needs to get a new primary pseudonym. This can be done by two means: first by requesting through the RSU located in the area where the vehicle is currently traveling and the other by directly requesting it to CA through 3G/4G communication.
3. Roadside units (RSUs): Secondary pseudonyms are issued by RSU upon request from a vehicle. RSU maintains the association between the primary pseudonyms and secondary pseudonyms. Upon the request of secondary pseudonyms, RSU checks the validation of primary pseudonyms and issues the secondary pseudonyms if they are valid. Each secondary pseudonym has an expiration time (T_{RSU}) relatively smaller than T_{CA}. Once T_{RSU} expires, the vehicle needs to acquire a new secondary pseudonym from RSU.
4. Sender/Initial vehicle: The sender vehicle, denoted by V_i in the rest of the paper, generates the beacons and broadcasts them.
5. Receiver vehicle: The receiver vehicle, denoted by V_r in the rest of the paper, verifies the received beacon. In case the message is forged, it reports this message to RSU. If T_{RSU} expires, the beacon is discarded.

2.2 Assumptions

We have made a number of assumptions that underpin the cryptanalysis and the proposed protocol, and these are outlined next.

1. An honest but curious behavior is expected from CA, RA, and RSU.
2. We assume that CA, RA, and RSU do not collude.
3. Cryptographic credentials are kept safe by all parties.
4. All parties have synchronized clocks.
5. CA, RA, and RSU use a secure channel to communicate.

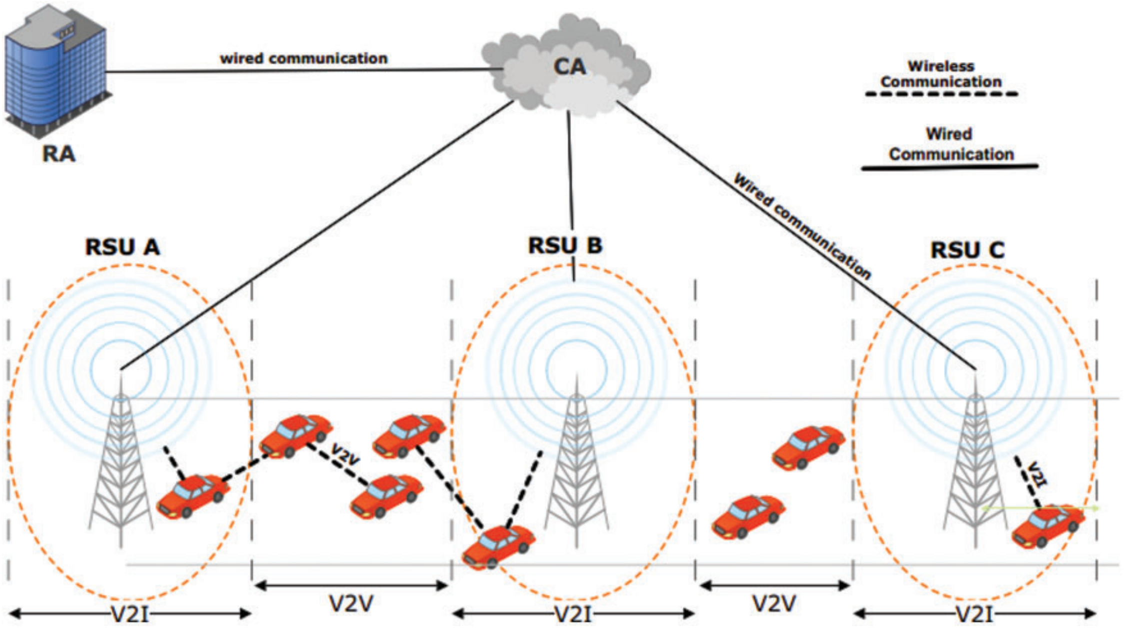


Figure 1: Conventional VANET architecture

2.3 Cryptographic Tools

Elliptic curve cryptography (ECC) is one of the most used cryptographic schemes in security because it provides a high level of security and efficiency. However, it doesn't provide search over encrypted data, which is sometimes required. To provide search over encrypted data, researchers have proposed schemes like PKEET. Therefore, we use two different cryptographic schemes. We use PKEET if there is need to search over encrypted data, and we use ECC if there is no need to search over encrypted data, because it is computationally efficient compared to PKEET. Each of the cryptographic schemes is given as follows:

1. Elliptic curve cryptography (ECC): ECC [31,32] is widely used to implement encryption algorithms and digital signatures. Assume that F_p is a finite field where p is a large prime number. E denotes an elliptic curve over F_p and it is defined by the following equation.

$$y^2 = x^3 + ax + b \ mod \ p \tag{1}$$

Here, $(4a^3 + 27b^2) \ mod \, p \neq 0$ and $x, y, a, b \ \varepsilon \ F_p$. Let us suppose that O be an infinite point, G be an additive group with order q and generator p. Let P and Q be two points on E; then point addition operation in G is defined as $P + Q = R$. The Elliptic curve discrete logarithmic problem (ECDLP) [33] is computationally infeasible. Scalar multiplication in G is given by the following equation.

$$s.P = P + P + \cdots + P \ (s \ times) \tag{2}$$

Given the points P and Q from G, ECDLP is to find $s \ \varepsilon \ F_p$ such that $s.P = Q$. ECC consists of the following algorithms:

a) *Setup* (π)*:* It takes security parameter π as input and outputs the public parameter

b) *KeyGen (pp):* It takes the public parameter *pp* as input, and outputs a public/secret key pair *(Pk, Sk)*.
c) *Encrypt (m, Pk):* It takes a message *m* and the receiver's public key *Pk* as input and outputs a ciphertext *C*.
d) *Decrypt (C, Sk):* It takes a ciphertext *C* and the receiver's secret key *Sk* as input and outputs a plaintext *m*.
e) *Signature Generation (C, Sk):* It takes a ciphertext *C* and the sender's secret key *Sk* as input and outputs a signature *s*.
f) *Signature Verification (s, Sk):* It takes a signature *s* and the sender's public key *Pk* as input and outputs 1 if the signature *s* is true otherwise 0.

Although the complete description of these modules is out of the scope of this paper, interested readers are encouraged to read [34] for more information about these modules.

2. Public key encryption with equality test (PKEET): This is a special type of searchable encryption scheme that allows checking whether two ciphertexts encrypted under (possibly) different public keys contain the same message or not. The scheme in [23] does not provide a trapdoor for authorization to perform an equality test. Later, Ma et al. [30] proposed a variant of PKEET with different authorization methods that provide more control to the user over authorization. It consists of the following algorithms:
   a) *Setup* (λ)*:* It takes security parameter λ as input and outputs the public parameter *pp*.
   b) *KeyGen (pp):* It takes the public parameter *pp* as input and outputs a public/secret key pair *(Pk, Sk)*.
   c) *Encrypt (M, Pk):* It takes a message *M* and the receiver's public key *Pk* as input and outputs a ciphertext *C*.
   d) *Decrypt (C, Sk):* It takes a ciphertext *C* and the receiver's secret key *Sk* as input and outputs a plaintext *M*.
   e) Aut_1 (SK_i): It takes the secret key SK_i as input and outputs a trapdoor $T_{1,i}$ for user U_i.
   f) $Test_1(C_i, T_{1,i}, C_j, T_{1,j})$: It takes U_i's ciphertext C_i, the trapdoor $T_{1,i}$, U_j's ciphertext C_j and the trapdoor $T_{1,j}$ as inputs, and outputs 1 if C_i and C_j contain the same message and 0 otherwise.

Note that [30] is only used by RA and CA in our scheme.

2.4 Security and Privacy Requirements

Both security and privacy are important for secure communications in VANETs. According to the latest research efforts [35–38], a scheme for VANET should meet the following requirements:

1. Message authentication: RSUs are able to check the validity of the messages sent by vehicles. In addition, RSUs are able to detect any modification of the received message.
2. Privacy preservation: RSUs and other vehicles are not able to extract the vehicle's real identity. Any third party is not able to get the vehicle's real identity by analyzing intercepted messages.
3. Traceability/Vehicle revocation: The protocol is able to extract the vehicle's real identity by analyzing its messages when it is necessary. e.g., when a malicious vehicle sends a false or forged message to mislead others.
4. Un-linkability: RSUs and malicious vehicles are not able to link two messages sent by the same vehicle, i.e., they cannot trace the vehicle's action through its messages.

5. Resistance to attacks: The scheme is able to withstand various common attacks such as the Sybil attack that exist in VANETs.

3 Cryptanalysis

In this section, we cryptanalyze and demonstrate with an example how to mount the Sybil attack in one of the state-of-the-art protocols [10], because in a VANET, Sybil attacks are very important to address. In the Sybil attack, the attacker subverts the reputation of a network service by creating a large number of pseudonymous identities and uses them to gain a disproportionately large influence. For an easy explanation, we assume the following scenario from [10] (The complete description of [10] is out of the scope of this research article. However, we encourage interested readers to read [10,11] to completely understand the attack). Let us suppose that in the step of primary pseudonym generation in [10], a malicious (internal) initial vehicle V_i wants to authenticate a fake vehicle V_f. V_i generates two random numbers *n, n'*, public/private ECC key pairs $PK_i/_{SK_i}$ and $PK_i'/_{SK_i}'$. V_i sends the information along with VID_i to *CA* in the following two steps.

Step 1: $V_i \rightarrow CA: n \,||\, PK_i \,||\, VID_i$.

RA generates a number of public/private ECC key pairs and provides CA the public keys that are later used by CA for VID_i encryption. CA validates the VID_i. Upon verification, it encrypts VID_i with one of the public keys of RA. CA encrypts *n* with its paillier homomorphic encryption public key PKCAP, generates an expiration time TCA and creates the following database entries as shown in Tab. 1.

Table 1: Examples of the CA database with attack scenario in [10]

User serial	Data
n	$(VID_i)_{PK_{RA}} \,||\, T_{CA} \,||\, PK_i$

CA signs $(T_{CA} \,||\, PK_i \,||\, (n)_{PK_{CAP}})$ and assigns it to V_i as its primary pseudonym. Note that CA has VID_i in encrypted form using RA's public key. Hence, CA cannot see VID_i once encrypted (until RA provides the corresponding private key). Now V_i again sends *n'*, PK_i', and VID_i to *CA* in order to get another valid primary pseudonym.

Step 2: $V_i \rightarrow$ *CA: n`* || $PK_i$ `|| VID_i.

CA validates VID_i. CA can not check whether VID_i is already in its database or not because VID_i is in encrypted form in its database. Upon verification, it encrypts VID_i with one of the public keys generated by RA, encrypts *n'* with its Paillier public key PK_{CAP}, generates an expiration time T'_{CA} and creates the following database entries as shown in Tab. 2.

Table 2: Examples of the CA database with attack scenario in [10]

User serial	Data
n	$(VID_i)_{PK_{RA}} \,||\, T_{CA} \,||\, PK_i$
n'	$(VID_i)_{PK_{RA}} \,||\, T'_{CA} \,||\, PK'_i$

CA signs $(T'_{CA} \,||\, PK'_i \,||\, (n)'_{PK_{CAP}})$ and assigns it to V_i as its primary pseudonym. Hence, V_i has successfully obtained two valid primary pseudonyms at a time. V_i can give one of its primary pseudonyms to V_f. Using this primary pseudonym, V_f can obtain a secondary pseudonym and can communicate in the network. V_i can create many numbers of such fake authenticated vehicles in the network and can cause fake congestion. The Sybil attack is shown in Fig. 2.

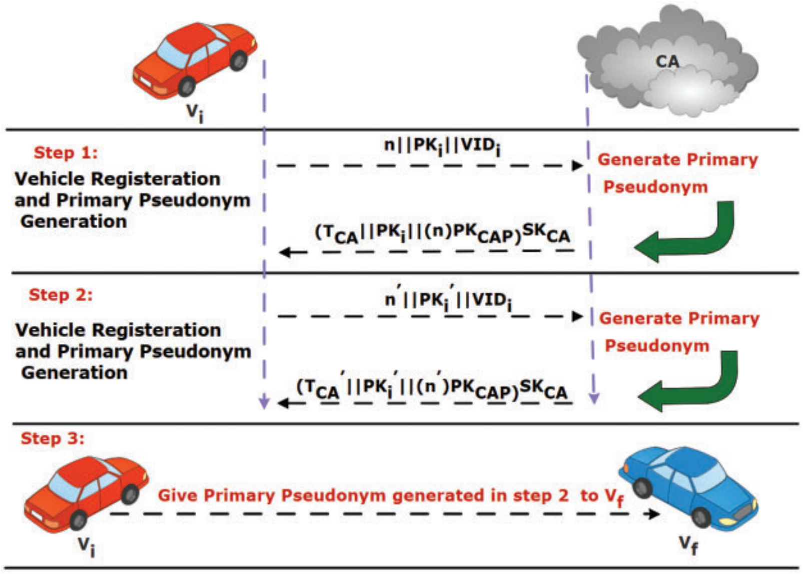

V_i
CA
Step 1:
Vehicle Registeration and Primary Pseudonym Generation
$n||PK_i||VID_i$
Generate Primary Pseudonym
$(T_{CA}||PK_i||(n)PK_{CAP})^{SK_{CA}}$
Step 2:
Vehicle Registeration and Primary Pseudonym Generation
$n'||PK_i'||VID_i$
Generate Primary Pseudonym
$(T_{CA}'||PK_i'||(n')PK_{CAP})^{SK_{CA}}$
Step 3:
Give Primary Pseudonym generated in step 2 to V_f
V_i
V_f

Figure 2: Demonstration of sybil attack in [10]

4 Proposed Protocol

In this section, we propose a new protocol that uses PKEET to eliminate the Sybil attack. The proposed protocol provides improved efficiency, security and maintains privacy in the VANET. The dynamic network architecture of the proposed protocol is shown in Fig. 3 and the protocol is given as follows:

4.1 Off-line Registration and Initialization

At the time of offline registration, CA broadcasts security parameters. Each entity creates its public/private key pairs using ECC. In the case of RA, it also creates public/private key pairs using PKEET. V_i contacts RA with its VID_i and public key PK_i through a secure channel (e.g., by physically visiting). RA uses (PKEET) [30] to encrypt and sign the VID_i and gives it to V_i. Furthermore, RA gives the trapdoor T of its private key PK_{RA} to CA through a secure channel (Note that, in [10,11], RA gives just its public keys to CA and SN, respectively). We use PKEET in [30], which allows to stop the Sybil attack by using the equality test.

Step 1: $V_i \rightarrow RA{:}\ VID_i \,||\, PK_i$.

Step 2: $RA \rightarrow V_i{:}\ (PKEET(VID_i\ )_{PK_{RA}})_{SK_{RA}}$.

Step 3: $RA \rightarrow CA{:}\ T$.

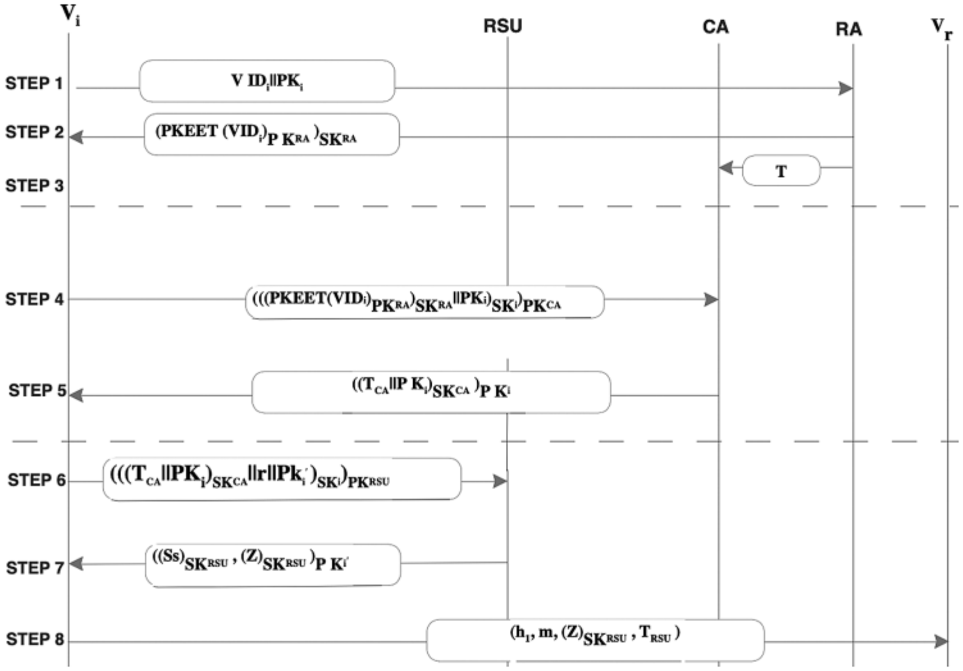

V_i
RSU
CA
RA
V_r
STEP 1
V ID_i||PK_i
STEP 2
(PKEET (VID_i)_P K_RA)_SK_RA
T
STEP 3
STEP 4
(((PKEET(VID_i)_PK_RA)_SK_RA||PK_i)_SK_i)_PK_CA
STEP 5
((T_CA||P K_i)_SK_CA)_P K_i
STEP 6
(((T_CA||PK_i)_SK_CA||r||Pk_i′)_SK_i)_PK_RSU
STEP 7
((Ss)_SK_RSU , (Z)_SK_RSU)_P K_i′
STEP 8
(h_1, m, (Z)_SK_RSU , T_RSU)

Figure 3: Working of proposed protocol

4.2 Primary Pseudonym Generation

V_i signs $(PKEET(VID_i\ )_{PK_{RA}})_{SK_{RA}} \,||\, PK_i$ using its private key $_{SK_i}$ and encrypts it using CA's public key PK_{CA} and sends it to CA to get a primary pseudonym for the first time (i.e., initially but only once).

Step 4: $V_i \rightarrow (((PKEET(VID_i\ )_{PK_{RA}})_{SK_{RA}} \,||\, PK_i)_{SK_i}\ )_{PK_{CK}}$.

CA verifies the signature of RA and checks using the equality test function whether $PKEET(VID_i\ )_{PK_{RA}}$ exists in its database or not. If it does not exist, then CA issues the primary pseudonym $(T_{CA} \,||\, PK_i)_{SK_{CK}}$ and stores it in its database as shown in Tab. 3.

CA encrypts $(T_{CA} \,||\, PK_i)_{SK_{CK}}$ using PK_i and sends it to V_i.

Step 5: $CA \rightarrow V_i{:}\ ((T_{CA} \,||\, PK_i)_{SK_{CK}}\ )_{PK_i}$.

Table 3: Example of the CA database in the proposed protocol

User serial	Data	Primary pseudonym
n	$PKEET(VID_i\ )_{PK_{RA}}$	$(T_{CA} \,\|\|\, PK_i)_{SK_{CK}}$

4.3 Secondary Pseudonym Generation

V_i decrypts the primary pseudonym, generates a random number r and a new public/private key pair Pk'_i, Sk'_i, and then concatenates r and Pk'_i with the primary pseudonym. Thereafter, V_i signs it using $_{SK_i}$, encrypts it using the public key PK_{RSU} of RSU and sends it to RSU.

Step 6: $V_i \rightarrow RSU$: $(((T_{CA} \| PK_i)_{SK_{CK}} \| r \| Pk'_i)_{SK_i})_{PKRSU}$.

RSU decrypts $(((T_{CA} \| PK_i)_{SK_{CK}} \| r \| Pk'_i)_{SK_i})_{PKRSU}$ and verifies the signatures SK_{CA} and $_{SK_i}$. If T_{CA} is valid, RSU generates a secondary pseudonym $Ss = (T_{RSU} \| PK'_i)$ and signs it using its private key SK_{RSU}. RSU also computes $Z = Ss + r$ and signs it using SK_{RSU}. RSU sends $((Ss)_{SKRSU})$, $((Z)_{SKRSU})$ by encrypting it using PK'_i to V_i. RSU maintains its database as shown in Tab. 4.

Step 7: $RSU \rightarrow V_i$: $((Ss)_{SKRSU}, ((Z)_{SKRSU})_{PK'i}$.

Table 4: Example of the RSU database in the proposed protocol

User serial	Data	Secondary pseudonym
n	$((T_{CA})\|\|PK_i)_{SK_{RA}}$	$(Ss)_{SKRSU}$, Z

4.4 Beacon Generation

V_i computes $h_1 = H(Ss + r + m + T_{RSU})$, where m is a beacon message and H is a hash function. V_i then sends $(h_1, m, (Z)_{SKRSU}, T_{RSU})$ to V_r.

Step 8: $V_i \leftarrow V_r$: $(h_1, m, (Z)_{SKRSU}, T_{RSU})$.

4.5 Beacon Verification

V_r checks if T_{RSU} is valid. If it is valid, V_r verifies the signature SK_{RSU} and computes $h_x = H(Z + m + T_{RSU})$. If $h_1 = h_x$, Vr accepts the beacon. Otherwise it rejects the beacon.

4.6 Renewal of Primary Pseudonym

Once the T_{CA} expires, V_i requests CA via 3G/4G communication or RSU for a new primary pseudonym. V_i generates a new public/private key pair PK''_i/SK''_i, concatenates PK''_i with its current primary pseudonym, signs it using current PK_i, encrypts it using PK_{CA} and sends it to CA. CA generates a new primary pseudonym using PK''_i and new expiration time T'_{CA} and signs it using SK_{CA}. CA encrypts it using PK''_i and sends the new primary pseudonym to V_i. CA then updates the corresponding primary pseudonym with a new primary pseudonym in its database.

$V_i \rightarrow CA$: $(((T_{CA} \| PK_i)_{SK_{CK}} \| PK''_i)_{SK_i})_{PKCA}$.

$CA \rightarrow V_i$: $(((T'_{CA}) \| PK''_i)_{SK_{CK}})_{PK''i}$.

4.7 Renewal of Secondary Pseudonym

To renew a secondary pseudonym, once the T_{RSU} expires, V_i generates a new public/private key pair $PK'''i/SK'''i$ and a random number r'. V_i then concatenates $PK'''i$ and r' with its current secondary pseudonym and signs it using the current PK'_i. V_i then encrypts them using PK_{RSU} and sends them to RSU. RSU checks the signatures SK_{RSU} and SK'_i. RSU creates a new secondary pseudonym with new expiration time $T_{RSU'}$. RSU generates $Z' = Ss' + r'$, where $Ss' = (T_{RSU'} \| PK_{i'''})$. RSU signs Z' and Ss' using SK_{RSU}. RSU then sends the signed Z' and Ss' to V_i by encrypting them using $PK_{i'''}$. RSU updates the corresponding secondary pseudonym in its database with the new one. The optimal time to refresh the secondary pseudonym is 1.4 s, which means that each V_i requests for secondary pseudonym after approximately 7 beacons. In case V_i tries to use expired secondary pseudonym, it will not be accepted by RSU as all the entities are synchronized. Thus, the vehicle using the expired secondary pseudonym will not be able to communicate.

5 Analysis of Proposed Protocol

This section provides an analysis of our protocol with two perspectives. First is the security analysis, where we provide various attack scenarios and explain the resilience of our protocol against those attacks to show the effectiveness of the protocol in accordance with the design goals. Next, we provide the computational and communicational efficiency in form of the computational time and communicational bytes required for beacon generation and verification.

5.1 Security Analysis

1. Message Integrity: The receiving vehicles ensure the integrity of the received message by verifying the signature of the RSU and comparing h_1 and h_x.
2. Vehicle Authentication: V_r authenticates V_i by verifying the signature of RSU in secondary pseudonym and validity of T_{RSU}.
3. Non-repudiation: V_i broadcasts the beacons by computing h_1 using r (which is only known to V_i) with its secondary pseudonym, m and T_{RSU}. Hence it provides non repudiation. T_{RSU} is valid for very short time. Therefore, each beacon is unique itself and it also prevents the replay attack and keeps the vehicle anonymous.
4. Privacy Preserving: The primary pseudonym and secondary pseudonym are changing very often, which makes it very difficult to track a particular device. Even if RA, CA, or RSU are compromised, the privacy of the vehicles remains secure.
5. Vehicle Revocation: If V_i is involved in a malicious activity, V_r reports it to the RSU with its secondary pseudonym. RSU blocks the malicious vehicle and sends it primary pseudonym to CA which also blocks it and reports it to RA. Then RA can reveal its real identity by sharing the respective private key of PKEET with CA. Thus, the offender's vehicle is revoked.
6. Conditional Anonymity: The real identity of the offender vehicle in our scheme is traced and revoked from the VANET when malicious activities are detected, as described above.

5.2 Attack Scenarios

We show how the proposed protocol defends against the following attack scenarios.

Theorem 1: Sybil attack is not feasible in the proposed protocol.

Proof: If V_i tries to get another primary pseudonym by the Sybil attack, CA will check if $PKEET(VID_i\ )_{PK_{RA}}$ exists in its database or not by using the equality test. If it exists, CA will not issue the primary pseudonym. Hence, the Sybil attack is not feasible.

Theorem 2: Communication between all the participants is secure.

Proof: All the communication in our protocol is encrypted using ECC cryptography. According to the Diffie-Hellman Problem, given an element h and the value h_x, it is computationally infeasible for an attacker to compute secret x. Therefore, all the communication is secure.

Theorem 3: V_r cannot correlate the secondary pseudonyms of V_i.

Proof: V_i changes the secondary pseudonyms after a few beacon broadcasts. Thereafter, V_r receives the beacons containing different secondary pseudonyms. Therefore, it is very hard for a V_r to establish any correlation between rapidly changing secondary pseudonyms.

Theorem 4: If an attacker succeeds in compromising RSU, no valuable information is leaked.

Proof: RSU only stores the mapping between the current primary pseudonym and secondary pseudonym. The primary pseudonyms are changed after a short period of time. Therefore, it is very hard for an attacker to get any useful information by compromising any of the RSUs.

Theorem 5: If an attacker succeeds in compromising the CA database, no valuable information is leaked.

Proof: Since the database of CA contains encrypted VIDs of vehicles, no valuable information is leaked even though CA is compromised.

Theorem 6: Even if an RSU tries to correlate the pseudonyms of an initiator. it hardly establishes the linkability between them.

Proof: RSUs only issue secondary pseudonyms on the basis of a primary pseudonym. An initiator only uses a primary pseudonym for a short period of time, after which it securely gets another primary pseudonym from CA without the knowledge of RSU. It is, therefore, very hard for the RSU to establish any link between two primary pseudonyms.

If any vehicle is involved in malicious activity, the malicious participant can be reported to RSU with its secondary pseudonym. RSU can then report it to the CA which will further cooperate with RA to get the associated encryption key for primary pseudonym. Thereafter, they can revoke/track the malicious participant using its ID in primary pseudonym.

Tab. 5 shows the comparison of the proposed solution with [10,11]. We observed that the protocols in [10,11] are vulnerable to the Sybil attack. However, the proposed solution in this study is resistant to against the possible Sybil attack. If CA and SN are compromised in [10,11], respectively, they do not provide privacy preservation because V_i sends its VID_i in plaintext. In the proposed solution, since CA is given an encrypted form of VID_i, a compromised CA cannot leak any valuable information regarding VID_i.

Table 5: Comparison with [10,11]

Characteristics	[10]	[11]	Proposed
Security against sybil attack	No	No	Yes
Privacy preserving (under compromised CA or SN)	No	No	Yes
Authentication	Yes	Yes	Yes

5.3 Performance Evaluation

We evaluate the performance of our proposed scheme using our testbed. Our testbed includes an Intel i5 processor with 8 GB of RAM and the computation is carried in a C++, as C++ supports a rich set of cryptographic libraries [39]. Execution time for the cryptographic operations is given in Tab. 6.

We compare the computational overhead for generation and verification of broadcasted beacons in [10,11] with our proposed protocol.

Table 6: Execution time and descriptions of cryptographic operations

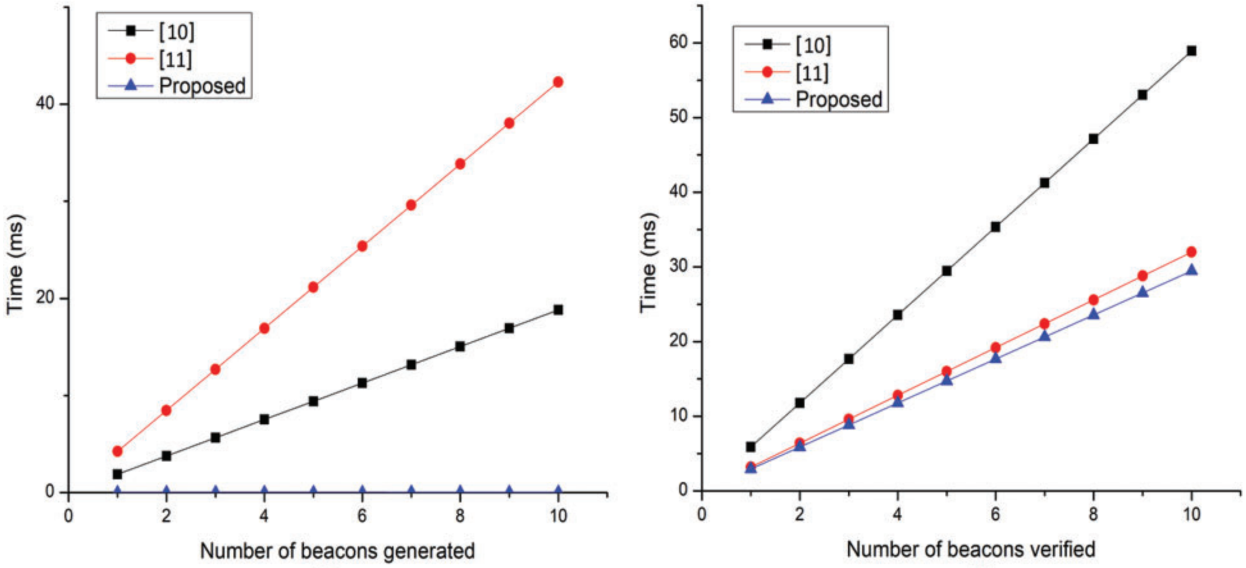
Description	Execution time (ms)
ECC Pk/Prk generation	2
ECC signature generation	1.88
AES encryption	0.357
ECC signature verification	2.946
AES decryption	0.253
AES key generation	0.01289
ECC encryption	9.267
ECC decryption	7.814
Hash function (H)	0.0001

Beacon generation: In Fig. 4a, it is evident that the proposed protocol outperforms others in terms of beacon generation. For beacon generation, [10] computes one signature, so the total time required for beacon generation is 1.88 ms, whereas [11] computes one signature, one AES encryption, and one ECC key generation. Hence, the total time required for beacon generation is $1.88 + 0.357 + 2 \approx 4.237$ ms. For beacon generation, the proposed protocol only computes one hash (H), so the total time required is 0.0001 ms. Hence, the proposed protocol is the most efficient in beacon generation, taking almost constant time, which means that, unlike [10,11], the time for beacon generation does not increase linearly with an increase in the number of beacons generated because the proposed method uses only one hash for beacon generation whereas others use signature verification along with encryption, which are computationally inefficient.

Beacon verification: For beacon verification, as shown in Fig. 4b, [10] computes two signature verifications, so the total time required for beacon verification is $2.946 + 2.946 \approx 5.892$ ms, whereas [11] computes one signature verification and one AES decryption for beacon verification, hence the time required for beacon verification is $2.946 + 0.253 \approx 3.199$ ms. For beacon verification, the proposed protocol computes one hash and one signature verification, so the total time required for message verification is $2.946 + 0.0001 \approx 2.9461$ ms. The proposed protocol provides 7.908% faster time for beacon verification compared to [11], because the proposed protocol uses hash which is computationally efficient compared to AES decryption in [11].

5.4 Communication Overhead

In this section, we evaluate and compare the size of beacons and show that the proposed protocol has the most efficient communicational overhead. Description of size for each element in a beacon is given in Tab. 7. The the size of beacon in the proposed protocol is 322 bytes, whereas the size of beacon in [10,11] is 362 and 364 respectively, as shown in Tab. 8. Hence the proposed protocoloutperforms others in terms of communicational overhead.



(a)

(b)

Figure 4: Computational overhead for: (a) beacon generation, (b) beacon verification

Table 7: Size of elements

Description	Size (bytes)
Signature	64
Beacon data	200
Random number (r)	2
T_{RSU}	2
$PK_i/_{SK_i}$	32
Padding	14
Hash operation (h)	20
Nonce	2
VID_i	4
Nonce	2

The corresponding hardware implementations for this protocol consist of hash function for the beacon generation, and hash function and signature verification for beacon verification. The associated hardware requirements can be accomplished using one hash; the light weight hash function as implemented in [40] can serve as the best option for this case in FPGA platform. Similarly for the signature verification case, the ECC can be employed, where the efficient implementations can be found in [32]. Later, we intend to design the whole protocol in hardware that can utilize the resource sharing techniques for the efficient implementation of the protocol.

Table 8: Communicational overhead comparison

Scheme	Beacon elements (bytes)	Total size (bytes)
[10]	$T_{RSU} = 2$, $PK_i = 32$, signature = 64, beacon data = 200, signature = 64	362
[11]	signature = 64, beacon data = 200, $PK_i^* = 64$, $_{SK_i} = 32$, $VID_i = 4$	364
Proposed	$Hash = 20,$ beacon data = 200, $r = 2$, $T_{RSU}{}^*2 = 4$ signature = 64, $PK_i = 32$	322

6 Conclusions and Future Work

In this paper, our cryptanalysis results found that the VANET authentication protocols are vulnerable to Sybil attacks. To remove this flaw, we proposed a novel protocol using searchable encryption by enabling search over encrypted identities. As a result of that, the security is improved while maintaining the privacy. The proposed solution is generic and can be applied to existing protocols that are vulnerable to Sybil attack. Simulation results show that the beacon generation time is constant while the beacon verification time is 7.908% faster compared to the state-of-the-art protocols. In addition, the beacon size is also reduced to 322 bytes, indicating that the protocol is efficient enough to be used for practical applications. In the future, we intend to adopt lightweight authentication [41] to improve the speed of the beacon verification in the proposed protocol. Efficient implementation techniques can also be developed for specialized hardware (GPU and FPGA) to enhance the speed performance and allow for large scale adoption. Furthermore, we will extend our proposed protocol to other applications such as bluetooth low energy [42] to make them secure from such attacks.

Acknowledgement: We thank our families and colleagues who provided us with moral support.

Funding Statement: This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2021-0-00540, Development of Fast Design and Implementation of Cryptographic Algorithms based on GPU/ASIC).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] F. J. Ros, P. M. Ruiz and I. Stojmenovic, "Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 1, pp. 33–46, 2010.

[2] W. Li and H. Song, "Art: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2015.

[3] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria Engineering Journal*, vol. 54, no. 1, pp. 1115–1126, 2015.

[4] H. E. Sayed, M. Chaqfeh, H. E. Kassabi, M. A. Serhani, H. Alexander *et al.,* "Trust enforcement in vehicular networks: Challenges and opportunities," *IET Wireless Sensor Systems*, vol. 9, no. 5, pp. 237–246, 2019.

[5] I. Memon, “A secure and efficient communication scheme with authenticated key establishment protocol for road networks,” *Wireless Personal Communications*, vol. 85, no. 3, pp. 1167–1191, 2015.

[6] H. Sedjelmaci, S. M. Senouci and M. A. A. Rgheff, “An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks,” *IEEE Internet of Things Journal*, vol. 1, no. 6, pp. 570–577, 2014.

[7] E. C. Eze, S. Zhang, E. Liu and J. C. Eze, “Advances in vehicular ad-hoc networks: Challenges and road-map for future development,” *International Journal of Automation and Computing*, vol. 13, no. 1, pp. 1–18, 2016.

[8] X. Cheng, C. Wang, H. Wang, X. Gao, X. You *et al.,* “Cooperative mimo channel modeling and multi-link spatial correlation properties,” *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 2, pp. 388–396, 2012.

[9] L. Zhang, Q. Wu, A. Solanas and J. D. Ferrer, “A scalable robust authentication protocol for secure vehicular communications,” *IEEE Transactions on Vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2010.

[10] U. Rajput, F. Abbas and H. Oh, “A hierarchical privacy preserving pseudonymous authentication protocol for vanet,” *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[11] S. A. Shah, C. Gongliang, L. Jianhua and Y. Glani, “A dynamic privacy preserving authentication protocol in vanet using social network,” in *Int. Conf. on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, Springer, Cham, pp. 53–65, 2019.

[12] D. He, S. Zeadally, B. Xu and X. Huang, “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, 2015.

[13] J. Zhang, J. Cui, H. Zhong, Z. Chen, L. Liu *et al.,* “Pa-crt: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 2, pp. 722–735, 2019.

[14] J. Cui, L. Wei, H. Zhong, J. Zhang, Y. Xu *et al.,* “Edge computing in vanets-an efficient and privacy-preserving cooperative downloading scheme,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 6, pp. 1191–1204, 2020.

[15] J. Cui, J. Zhang, H. Zhong and Y. Xu, “Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter,” *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10283–10295, 2017.

[16] C. Hu and P. Liu, “An enhanced searchable public key encryption scheme with a designated tester and its extensions,” *Journal of Computer*, vol. 7, no. 3, pp. 716–723, 2012.

[17] D. Boneh, G. D. Crescenzo, R. Ostrovsky and G. Persiano, “Public key encryption with keyword search,” in *Int. Conf. on the Theory and Applications of Cryptographic Techniques*, Berlin, Heidelberg, pp. 506–522, 2004.

[18] X. Guibao, M. Yubo and L. Jialiang, “Inclusion of artificial intelligence in communication networks and services,” *Itu Journal: Ict Discoveries*, no. vol. 1, pp. 1–6, 2017.

[19] R. Chen, Y. Mu, G. Yang, F. Guo, X. Wang *et al.,* “A new general framework for secure public key encryption with keyword search,” in *Australasian Conf. on Information Security and Privacy*, Springer, Cham, pp. 59–76, 2015.

[20] L. Fang, W. Susilo, C. Ge and J. Wang, “Public key encryption with keyword search secure against keyword guessing attacks without random oracle,” *Information Sciences*, vol. 238, pp. 221–241, 2013.

[21] C. Hu and P. Liu, “Decryptable searchable encryption with a designated tester,” *Procedia Engineering*, vol. 15, pp. 1737–1741, 2011.

[22] C. Liu, L. Zhu, M. Wang and Y. Tan, “Search pattern leakage in searchable encryption: Attacks and new construction,” *Information Sciences*, vol. 265, pp. 176–188, 2014.

[23] S. Ma, Q. Huang, M. Zhang and B. Yang, “Efficient public key encryption with equality test supporting flexible authorization,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 458–470, 2014.

[24] Y. Wang, J. Wang and X. Chen, “Secure searchable encryption: A survey,” *Journal of Communications and Information Networks*, vol. 1, no. 4, pp. 52–65, 2016.

[25] J. Huang, L. Yeh and H. Chien, “Abaka: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks,” *IEEE Transactions on Vehicular Technology*, vol. 60, no. 1, pp. 248–262, 2010.

[26] D. A. Rivas, J. M. B. Ordinas, M. G. Zapata and J. D. M. Pozo, “Security on vanets: Privacy, misbehaving nodes, false information and secure data aggregation,” *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1942–1955, 2011.

[27] H. Amir and S. Hwang, “Adaptive transmit power control algorithm for sensing-based semi-persistent scheduling in c-v2x mode 4 communication,” *Electronics*, vol. 8, no. 8, pp. 1–18, 2019.

[28] S. Ali, A. Haider, M. Rahman, M. Sohail, Y. B. Zikria *et al.,* “Deep learning based joint resource allocation and rrh association in 5 g-multi-tier networks,” *IEEE Access*, vol. 9, pp. 118357–118366, 2021.

[29] J. Petit, F. Schaub, M. Feiri and F. Kargl, “Pseudonym schemes in vehicular networks: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 228–255, 2014.

[30] S. Ma, Q. Huang, M. Zhang and B. Yang, “Efficient public key encryption with equality test supporting flexible authorization,” *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 458–470, 2014.

[31] V. S. Miller, “Use of elliptic curves in cryptography,” in *Conf. on the Theory and Application of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 417–426, 1985.

[32] S. Khan, K. Javeed and Y. A. Shah, “High-speed fpga implementation of full-word montgomery multiplier for ecc applications,” *Microprocessors and Microsystems*, vol. 62, pp. 91–101, 2018.

[33] S. D. Galbraith and P. Gaudry, “Recent progress on the elliptic curve discrete logarithm problem,” *Designs, Codes and Cryptography*, vol. 78, no. 1, pp. 51–72, 2016.

[34] S. Vasundhara, “The advantages of elliptic curve cryptography for security,” *Global Journal of Pure and Applied Mathematics*, vol. 13, no. 9, pp. 4995–5011, 2017.

[35] N. Lo and J. Tsai, “An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2015.

[36] J. K. Liu, T. H. Yuen, M. H. Au and W. Susilo. “Improvements on an authentication scheme for vehicular sensor networks,” *Expert Systems with Applications*, vol. 41, no. 5, pp. 2559–2564, 2014.

[37] Z. Jianhong, X. Min and L. Liying, “On the security of a secure batch verification with group testing for vanet,” *International Journal of Network Security*, vol. 16, no. 5, pp. 351–358, 2014.

[38] X. Lin, X. Sun, P. Ho and X. Shen, “Gsis: A secure and privacy-preserving protocol for vehicular communications,” *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, 2007.

[39] M. Scott, “Support for fp8, new bestpair program,” *Github*, 2018. [Online] Available: https://github.com/miracl/MIRACL/blob/master/readme.txt.

[40] S. Khan, W. Lee and S. O. Hwang, “A flexible gimli hardware implementation in fpga and its application to rfid authentication protocols,” *IEEE Access*, vol. 9, pp. 105327–105340, 2021.

[41] K. M. Kay, L. Bassham, M. S. Turan and N. Mouha, “Report on lightweight cryptography,” *NIST Internal Interagency Report 8114*, National Institute of Standards and Technology, pp. 1–23, 2016.

[42] A. Raza, S. Khan and S. O. Hwang, “A secure authentication protocol against the co-located app attack in ble,” *IEIE Transactions on Smart Processing & Computing*, vol. 9, no. 5, pp. 399–404, 2020.