




## Article

# Using Adaptive Zero-Knowledge Authentication Protocol in VANET Automotive Network

Igor Anatolyevich Kalmykov<sup>1,\*</sup> , Aleksandr Anatolyevich Olenev<sup>2</sup> , Natalia Igorevna Kalmykova<sup>1</sup>  
and Daniil Vyacheslavovich Dukhovnyj<sup>1</sup> 

<sup>1</sup> Department of Information Security of Automated Systems, North-Caucasus Federal University Stavropol, 1 Pushkina Str., 355017 Stavropol, Russia

<sup>2</sup> Stavropol State Pedagogical Institute, 417 Lenina Str., 355009 Stavropol, Russia

\* Correspondence: kia762@yandex.ru

**Abstract:** One of the most important components of intelligent transportation systems (ITS) is the automotive self-organizing VANET network (vehicular ad hoc network). Its nodes are vehicles with specialized onboard units (OBU) installed on them. Such a network can be subject to various attacks. To reduce the effectiveness of a number of attacks on the VANET, it is advisable to use authentication protocols. Well-known authentication protocols support a security policy with full trust in roadside unit (RSU) base stations. The disadvantage of these authentication protocols is the ability of the RSU to track the route of the vehicle. This leads to a violation of the privacy and anonymity of the vehicle's owner. To eliminate this drawback, the article proposes an adaptive authentication protocol. An advantage of this protocol is the provision of high imitation resistance without using symmetric and asymmetric ciphers. This result has been achieved by using a zero-knowledge authentication protocol. A scheme for adapting the protocol parameters depending on the intensity of the user's traffic has been developed for the proposed protocol. The scientific novelty of this solution is to reduce time spent on authentication without changing the protocol execution algorithm by reducing the number of modular exponentiation operations when calculating true and "distorted" digests of the prover and verifying the correctness of responses, as well as by reducing the number of responses. Authentication, as before, takes place in one round without changing the bit depth of the modulus used in the protocol. To evaluate the effectiveness of the adaptive authentication protocol, the VANET model was implemented using NS-2. The obtained research results have shown that the adaptation of the authentication protocol in conditions of increased density of vehicles on the road makes it possible to increase the volume of data exchange between OBU and RSU by reducing the level of confidentiality. In addition, a mechanism for verifying the authority of the vehicle's owner for provided services has been developed. As a result of the implementation of this mechanism, vehicle registration sites (VRS) calculate the public key of the vehicle without using encryption and provide necessary services to the owner.

**Keywords:** VANET; authentication; zero-knowledge protocol; authentication protocol adaptation schemes



**Citation:** Kalmykov, I.A.; Olenev, A.A.; Kalmykova, N.I.; Dukhovnyj, D.V. Using Adaptive Zero-Knowledge Authentication Protocol in VANET Automotive Network. *Information* **2023**, *14*, 27. <https://doi.org/10.3390/info14010027>

Academic Editors: Abderrezak Rachedi, Omar Sami Oubbati and Sherali Zeadally

Received: 7 November 2022

Revised: 19 December 2022

Accepted: 29 December 2022

Published: 31 December 2022



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

## 1. Introduction

It is difficult to imagine the modern economy without transportation and its development. According to the data provided in [1], the demand for urban mobility is expected to increase by more than 2.5 times by 2050. To enhance the transportation process efficiency and prevent road accidents in real time, intelligent transportation systems (ITS) are being created [2].

One of the most important components of ITS is the VANET (vehicular ad hoc network). Its nodes are vehicles with specialized communication modules installed on them. The main objectives of such networks are to warn users about emergencies, to enable real-time vehicle monitoring, and to provide an access to the global network [3]. In addition,

the deployment of the VANET network reduces the number of accidents on the road. The paper [4] shows the use of the developed road-accidents-forecasting system. This system is based on hidden Markov networks. It takes into account many factors, such as weather conditions, vehicle speed, and driver fatigue in order to reduce the likelihood of a road accident.

The main elements of the VANET's architecture are specialized telecommunication modules mounted on the vehicles (they are called onboard units, or just OBUs), as well as infrastructure base stations (they are called roadside units, or just RSUs) with a similar set of communication interfaces. OBUs are integrated into a vehicle's onboard system. They have their own computing resources, antenna, and informational display. In addition to firmware modules, the VANET includes communication interfaces that allow these modules to interact with each other. Depending on the direction of information transfer between objects, the following types of interfaces are distinguished [5–7]:

- Vehicle-to-vehicle (V2V): When OBUs are interacting objects. This type of interaction is the main one in the absence of infrastructure base stations. It allows organizing the data exchange between road vehicles to enhance road safety;
- Vehicle-to-infrastructure (V2I): When information is transferred from the OBU to the RSU. It is used to accumulate information in control centers in order to organize a control system for monitoring and managing traffic streams;
- Infrastructure-to-infrastructure (I2I): When RSUs interact with each other. This type of interface allows data exchanging both via wired communication channels and wireless ones;
- Vehicle-to-X (V2X) is a universal interface type that allows organizing the V2V and/or V2I type of interaction.

An autonomous vehicle diagnostic can be performed using V2X interfaces, followed by sending the data to the service department. These interfaces allow expanding the range of services that ensure travel comfort.

Figure 1 shows the structure of the VANET's architecture. Due to the fact that the VANET network provides high-speed wireless connections and exchange of confidential information in real time, such a network can be susceptible to various attacks. The papers [8–10] analyze the VANET's main vulnerabilities and attacks on it. Among them, the following types of attacks can be distinguished: attacks on availability, attacks on confidentiality, attacks on authentication, attacks on data integrity, and attacks on non-repudiation.

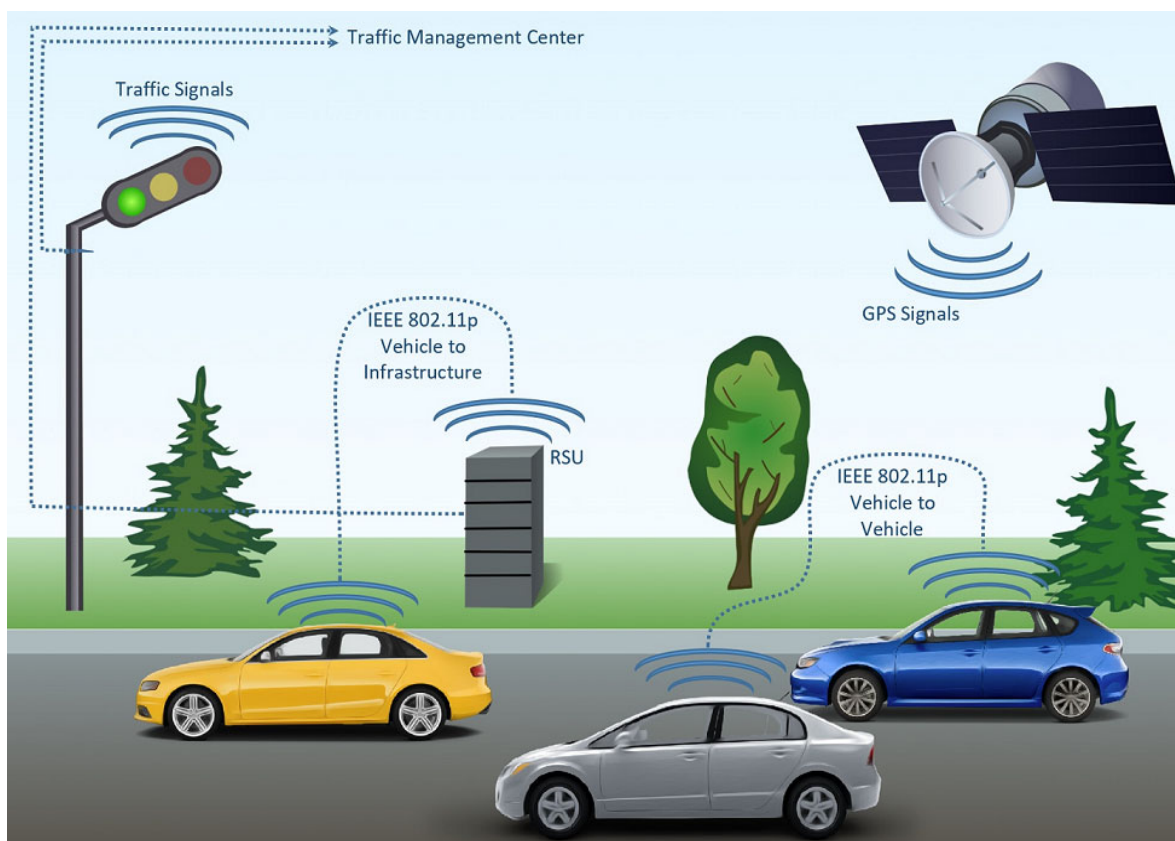
The authentication protocols can be used to reduce the effectiveness of many attacks on the VANET [11,12]. The application of authentication procedures between OBUs and RSUs allows increasing the efficiency of the VANET and will not allow unauthorized content to be imposed.

The requirements for the VANET authentication protocols are the following.

Firstly, authentication methods must have high cryptographic strength without the use of encryption methods. This requirement can eliminate the need for the delivery of private and public keys for telecommunication modules (OBU) and base stations (RSU) to implement authentication.

Secondly, during the authentication process, RSUs should not obtain information about the vehicle and the driver. Failure to comply with this requirement will allow the RSU to calculate the route of any vehicle, which entails a violation of the confidentiality and anonymity of the vehicle's owners.

Thirdly, the authentication protocol must contain a rule that would allow the protocol parameters to be adapted depending on the vehicle traffic intensity. To increase road capacity in high-traffic conditions, RSU devices need to reduce the time required for vehicle identification. This goal can be achieved by changing the protocol's cryptographic strength.



**Figure 1.** VANET's architecture.

Fourthly, the protocol should provide the possibility to deliver services to vehicle's owners through the access to the vehicle registration sites (VRS) that are part of the VANET structure. A service delivery request must be generated in order to receive services. However, the vehicle ID and the required services cannot be transmitted over an open channel due to the threat of message interception or modification. Therefore, the OBU-VRS authentication protocol must use an algorithm that allows the VRS to obtain the vehicle's public key without encryption. Then, based on the calculated public key, the VRS verifies its credentials and provides the required service.

Our contribution is as follows.

1. Taking into account the above requirements for authentication in the VANET, an adaptive authentication protocol was developed, built on zero-knowledge proof. This protocol provides a high degree of anonymity when performing OBU-RSU authentication, RSU-OBU authentication, and OBU-OBU authentication without using encryption methods. In this case, the trusted authorities will not be able to track the vehicle route using the data received by RSUs or OBUs during the authentication process. At the same time, this protocol requires minimal time spent on vehicle authentication. This is achievable by a reduction in the number of execution stages compared to previously known challenge-response protocols.
2. A scheme that allows adapting the protocol's parameters depending on the vehicle traffic intensity. When there is little traffic on the road, the OBU selects a high confidentiality level (level 3). As the traffic congestion increases, the user can lower the confidentiality level (to the level 2). A decrease in this level will reduce the time required for vehicle authentication. A further decrease in confidentiality to the first level ensures minimal time spent on vehicle authentication. It allows RSUs to operate efficiently under high-traffic conditions.

3. A protocol for verifying the authority of the vehicle's owner for requested services. As a result of this protocol implementation, the VRS calculates the public key of the vehicle without using encryption and provides necessary services.

The paper is structured as follows. Section 2 is devoted to authentication methods used in the VANET. Section 3 provides a comparative analysis of zero-knowledge authentication protocols. The main disadvantages of these protocols are shown. Section 4 is focused on the zero-knowledge authentication protocol with minimal authentication time. Section 5 provides an analysis of the scheme that allows adapting the protocol's parameters depending on the traffic intensity. Section 6 presents the protocol for verifying the vehicle's owner's authority for the requested services. The results of the studies and conclusions are presented in Sections 7 and 8, respectively.

## 2. Comparative Analysis of VANET Authentication Methods

The papers [13,14] present authentication protocols based on the idea of full trust in RSU or authentication servers. However, this approach has a disadvantage associated with the possibility to control specific vehicles' movement. At the same time, there is no possibility to choose the level of confidentiality in these protocols.

To reduce the time of the prover's authentication, it is proposed in [15,16] to use symmetric encryption in the authentication protocol. However, this approach has a drawback, which is the necessity to deliver secret keys to authentication objects. In this case, the interception of such keys can lead to the entire VANET being compromised, which entails a decrease in the data exchange security.

Public key encryption systems (PKI) can eliminate this drawback [17,18]. PKI technology makes it possible to unambiguously identify a vehicle. However, this protocol can only be used when OBUs fully trust RSUs. In other words, only RSUs authenticate OBUs. Then, it is necessary to enter the public keys of each OBU into each base station memory during their deployment. Another option is the data exchange between the RSU and the authentication server in real time. As a result, the speed of the authentication procedure decreases, which negatively affects the road capacity. In addition, it is rather difficult to organize data exchange via the OBU-OBU interface when PKI-based authentication protocols are being used.

To reduce the computational load when executing a PKI-based authentication protocol, it was proposed in [19] to use an identity-based batch authentication scheme. This approach allows generating many public and private key pairs without preloading them into OBUs and RSUs and reducing the cost of transferring and verifying PKI certificates.

It is proposed in [20–23] to combine several vehicles into groups in order to reduce the volume of stored keys and minimize computational load. It allows using group digital signatures. However, such solutions have disadvantages. Firstly, the confidentiality of the OBU group depends on the group manager, who possesses the group master key. In this case, there is a possibility of any group member's confidential-data leakage. Secondly, there is a problem of choosing a group manager. Thirdly, the group digital signature strength can be reduced because of the small number of vehicles that make up the group.

It is shown in [24–30] that the PKI does not fully ensure the vehicle's owner's confidentiality. In this case, the attacker will be able to establish a correspondence between the vehicle and the fixed key. To eliminate this drawback, it is proposed to use temporary anonymous certified keys or pseudonym-based authentication. The paper [24] presents an authentication method based on the usage of pseudonyms. With this method, users are autonomous in terms of obtaining public key certificates and pseudonyms, which minimizes data exchange with the certification authority. Pseudonyms allow maintaining anonymous communication between vehicles while keeping OBUs' privacy safe. However, these methods also have a disadvantage. The problem is implicit vehicle authentication. To unambiguously identify the vehicle's owner, it is necessary to use a special trusted authority.

The comparative analysis has shown that to ensure the required level of confidentiality, the above-mentioned authentication methods use various encryption systems that require

the usage of key management systems. It is possible to eliminate this disadvantage by using a zero-knowledge authentication protocol.

### 3. Analysis of Zero-Knowledge Protocols

These protocols involve two parties: the verifier (V) generates random challenges to be responded to by the prover (P). The purpose of this protocol is that P must convince V of the truth of the statement known to P. If the prover is an authorized user, that is, his statements are true, then, with an increase in the number of verification steps, the probability of a statement to be true must tend to one. Otherwise, when the statement provided by P is false, the probability of correctness of the proof will be close to zero [25].

Typically, the implementation of most zero-knowledge proof protocols requires several rounds of verification. Each round requires the following steps:

Step 1. P, who possesses some secret  $S$ , makes a request  $E$ , which is transmitted to V.

Step 2. V sends a challenge  $B$  to P. P computes a response  $W$ .

Step 3. V checks the response and decides whether the current proof is true.

In the Fiat–Shamir and Feige–Fiat–Shamir protocols, it is proposed to perform from 5 to 20 rounds of verification, depending on the size (bit depth) of challenges and responses [25]. Having sufficient cryptographic strength, these protocols are widely used in contactless devices. For example, in [26,27], authentication algorithms used in smart cards are considered. Zero-knowledge protocols make it possible to refuse classic password authentication methods, providing effective protection of smart cards against active parallel attacks, when an attacker can use information that he receives during one session to respond to challenges that arise during the other session.

It should be noted that, recently, the field of automatic identification systems (RFID) has been expanding. With this technology, the data are stored in so-called transponders or RFID tags and are read or written using radio signals. To prevent unauthorized access to the data, it is necessary to authenticate the data receiver. For this purpose, in [28,29], it is proposed to use modified interactive authentication protocols based on zero-knowledge proof. In [30], a modification of the Schnorr protocol is presented, which has a higher speed compared to the Fiat–Shamir and Feige–Fiat–Shamir protocols due to reducing the number of verification rounds. The paper [31] discusses the information security issues of a “smart home” technology. The Feige–Fiat–Shamir protocol helps to solve the problem of the increasing number of secret keys used to authenticate an ever-increasing number of IoT devices. An example of using a modified Feige–Fiat–Shamir protocol is given in [32]. The Feige–Fiat–Shamir authentication protocol has been chosen because IoT devices have limited processing power. The research results presented in the article showed that the authentication scheme effectively resisted brute-force attacks. Thus, using a 20-bit key and 20 rounds of authentication in the protocol did not allow the attacker to obtain the value of the modulus  $n$  and the private key  $S$ .

The ISO/IEC Joint Technical Committee has developed a standard [33] for zero-knowledge authentication protocols. This standard regulates the algorithm for constructing an authentication protocol with zero-knowledge proof based on the public key encryption system (Publ\_Encr). The RSA encryption algorithm can be used as such a system.

In accordance with [33], the following steps must be performed in order to implement a zero-knowledge authentication protocol.

1. The verifier chooses a random number  $A$  and encrypts it using the prover’s public key  $C = E_{K_{public}^p}(A)$ . Then, the verifier calculates a value of the hash function at the number  $A$ , that is,  $H_A = H(A)$ , where  $H$  is the hash function. A pair of the obtained results  $(C, H_A)$  is transmitted to the prover.
2. The prover, having received  $(C, H_A)$ , decrypts the message  $C$  with his secret key and obtains  $A^* = D_{K_{private}^p}(C)$ . Then, the prover calculates a value of the hash function  $H_{A^*} = H(A^*)$ . If an equality  $H_{A^*} = H_A$  is satisfied, the decrypted number  $A^*$  is returned to the verifier.

3. The verifier receives a number  $A^*$  and compares it with his chosen number  $A$ . If equality  $A = A^*$  is satisfied, the verifier reaches a conclusion about the authenticity of the prover.

This protocol is recommended for authentication in various information systems where protocol participants do not trust each other. The VANET can be considered to be such a system. Therefore, zero-knowledge authentication protocols have found application in VANET systems [34–37]. The paper [34] shows the authentication protocol for the VANET system, which is an integration of two cryptographic protocols. The authors propose jointly using the zero-knowledge authentication protocol (ZKAP) and the distance limitation protocol. In this case, two problems are solved at once. First, OBU authentication is performed using ZKAP. Secondly, the distance from the RSU to the vehicle is determined. However, this approach has a disadvantage: the high sensitivity of the protocol’s distance bounding to data-processing delay. As a result, high demands are placed on the synchronization subsystems of radio equipment that are used in OBUs and RSUs.

In [35–37], authentication protocols that can adapt their parameters depending on the intensity of vehicle traffic are presented. The paper [35] presents an iterative protocol in which the reduction in authentication time is achieved by reducing the number of rounds of verification of the prover. At the same time, there is a decrease in the level of confidentiality of the protocol. In [36,37], it is proposed to adapt the protocol by changing the bit depth of the data processed in the protocol. When the bit depth of the signal received from the prover decreases, the speed of authentication increases. However, at the same time, the level of confidentiality decreases. An increase in the bit depth of the prover’s response provides an increase in the level of confidentiality of the protocol, but at the same time, the time of the prover’s verification increases.

The above-mentioned research papers’ analysis has shown that zero-knowledge authentication protocols provide high cryptographic strength without using encryption methods. Moreover, these protocols do not achieve maximal authentication speed due to the iterative verification process. In addition, to ensure high imitation resistance in these protocols, it is required to perform all operations using large modulus. That reduces the speed of an authentication protocol execution. It is due to the fact they do not use session keys that would be changed in different authentication sessions. Therefore, it is necessary to develop a protocol that would allow performing this procedure in fewer steps and with the usage of session keys.

#### 4. Zero-Knowledge Authentication Protocol with Minimal Authentication Time

Preliminary stage goes as follows.

To execute the protocol, each OBU and RSU must have:

- A prime number  $S$ , a modulo in which the calculations in the developed protocol are performed.
- The number  $m$  is the number generating the multiplicative group  $Z_S$ .
- $k_{private}^{OBU}, k_{private}^{RSU}$  are images of the OBU and RSU secret keys, where

$$k_{private}^{OBU} = K_{private}^{OBU} \bmod S, k_{private}^{RSU} = K_{private}^{RSU} \bmod S, \tag{1}$$

where  $K_{private}^{OBU}$  is the OBU secret key;  $K_{private}^{RSU}$  is the RSU secret key; and  $\{k_{private}^{OBU}, k_{private}^{RSU}\} < S - 1$ .

- $D, G$  are the numbers for obtaining OBU and RSU session keys where  $\{D, G\} < S - 1$ .
- $L$  is the number used by the OBU in the protocol for verifying the vehicle user’s credentials for the services provided where  $L < S - 1$ .
- $T$  is the number used by RSU to get the timestamp where  $T < S - 1$ .

To ensure high imitation resistance when calculating session keys, we will use a pseudo-random function (PRF). Its strength should be based on the complexity of solving

the Diffie–Hellman problem. Such a function has been given in [38]. Then, the session keys values will be determined by the expressions

$$D(j) = m^{(D(j-1)+k_{private}^{OBU})^{-1}} \bmod S, G(j) = m^{(G(j-1)+k_{private}^{RSU})^{-1}} \bmod S, \tag{2}$$

where  $D(j - 1)$ ,  $G(j - 1)$  are session key values in the previous authentication session;  $D = D(0)$ ,  $G = G(0)$  are the initial parameters for calculating the OBU and RSU session keys.

Similarly, we obtain

$$L(j) = m^{(L(j-1)+k_{private}^{OBU})^{-1}} \bmod S, T(j) = m^{(T(j-1)+k_{private}^{RSU})^{-1}} \bmod S, \tag{3}$$

Authentication (level 3). OBU (prover) → RSU (verifier).

1. The prover (OBU) calculates its true digest value to perform the  $j$ -th authentication:

$$B(j) = m^{k_{private}^{OBU}(j)} m^{D(j)} m^{L(j)} \bmod S. \tag{4}$$

The true digest is entered in the OBU’s memory.

2. The prover (OBU) chooses random numbers  $\{\Delta k_{private}^{OBU}(j), \Delta D(j), \Delta L(j)\} < S - 2$ , thus “distorting” the protocol’s secret parameters:

$$\begin{aligned} \hat{k}_{private}^{OBU}(j) &= (k_{private}^{OBU} + \Delta k_{private}^{OBU}(j)) \bmod \phi(S), \\ \hat{D}(j) &= (D(j) + \Delta D(j)) \bmod \phi(S), \\ \hat{L}(j) &= (L(j) + \Delta L(j)) \bmod \phi(S), \end{aligned} \tag{5}$$

where  $\phi(S)$  is the value of Euler’s totient function at the number  $S$ . The OBU then calculates the “distorted” digest:

$$\hat{B}(j) = m^{\hat{k}_{private}^{OBU}(j)} m^{\hat{D}(j)} m^{\hat{L}(j)} \bmod S. \tag{6}$$

The “distorted” digest is entered into the OBU’s memory. When the OBU (prover) comes into the range of the RSU (verifier), the following actions are performed:

3. The verifier (RSU) chooses a random number  $M(j) < S - 2$ , which is a challenge. This number is sent to the OBU.
4. The prover (OBU) computes the responses:

$$\begin{aligned} Y_1(j) &= (\hat{k}_{private}^{OBU}(j) - M(j)k_{private}^{OBU}(j)) \bmod \phi(S), \\ Y_2(j) &= (\hat{D}(j) - M(j)D(j)) \bmod \phi(S), \\ Y_3(j) &= (\hat{L}(j) - M(j)L(j)) \bmod \phi(S). \end{aligned} \tag{7}$$

5. The prover (OBU) sends a signal to the RSU:

$$(B(j) || \hat{B}(j) || Y_1(j) || Y_2(j) || Y_3(j)).$$

6. The RSU (verifier) checks the correctness of the response by calculating

$$A(j) = B^{M(j)}(j) m^{Y_1(j)} m^{Y_2(j)} m^{Y_3(j)}. \tag{8}$$

If the calculated value matches the “distorted” digest  $A(j) = \hat{B}(j)$ , then the OBU is authorized. Now, after authentication, the RSU can establish a communication session with the VRS to provide the required service to the vehicle’s owner. At the same time, the

RSU cannot obtain information about the vehicle itself, as well as calculate its route. This ensures the VANET's privacy.

Let us consider the authentication protocol in the opposite direction since OBUs and RSUs do not trust each other.

Authentication (level 3). RSU (prover)  $\rightarrow$  OBU (verifier).

1. Prover (RSU):

$$H(j) = m^{k_{private}^{RSU}(j)} m^{G(j)} m^{T(j)} \bmod S. \quad (9)$$

Prover (RSU):

$$RSU \rightarrow RAM_{RSU} : H(j).$$

2. Prover (RSU):

$$\begin{aligned} \{ \Delta k_{private}^{RSU}(j), \Delta G(j), \Delta T(j) \} &< S - 2, \\ \hat{k}_{private}^{RSU}(j) &= (k_{private}^{RSU} + \Delta k_{private}^{RSU}(j)) \bmod \phi(S), \\ \hat{G}(j) &= (G(j) + \Delta G(j)) \bmod \phi(S), \\ \hat{T}(j) &= (T(j) + \Delta T(j)) \bmod \phi(S). \end{aligned} \quad (10)$$

Prover (RSU):

$$\hat{H}(j) = m^{\hat{k}_{private}^{RSU}(j)} m^{\hat{G}(j)} m^{\hat{T}(j)} \bmod S. \quad (11)$$

Prover (RSU):

$$RSU \rightarrow RAM_{RSU} : \hat{H}(j).$$

3. Verifier (OBU):

$$E(j) < S - 2, \text{ OBU} \rightarrow \text{RSU} : E(j).$$

4. Prover (RSU):

$$\begin{aligned} C_1(j) &= (\hat{k}_{private}^{RSU}(j) - E(j)k_{private}^{RSU}(j)) \bmod \phi(S), \\ C_2(j) &= (\hat{G}(j) - E(j)G(j)) \bmod \phi(S), \\ C_3(j) &= (\hat{T}(j) - E(j)T(j)) \bmod \phi(S). \end{aligned} \quad (12)$$

5. Prover (RSU):

$$RSU \rightarrow OBU : (H(j) || \hat{H}(j) || C_1(j) || C_2(j) || C_3(j)).$$

6. Verifier (OBU):

$$Q(j) = H^{E(j)}(j) m^{C_1(j)} m^{C_2(j)} m^{C_3(j)} = \hat{H}(j). \quad (13)$$

The authentication protocol between the two OBUs is similar to those described above. The only difference is that the verifier and the prover are two different OBUs.

### 5. The Protocol Parameters' Adaptation Depending on Traffic Density

The development of a protocol parameter adaptation scheme is an urgent task since it allows RSUs and OBUs to effectively perform the authentication procedure in different road situations. When there is little traffic on the road, the OBU chooses a high level of confidentiality (level 3). As traffic increases, the user can lower the confidentiality level (level 2). Lowering this level will reduce the time required to authenticate vehicles. A further reduction in confidentiality to the first level ensures minimal time spent on vehicle authentication, which allows RSUs to operate efficiently in conditions of high vehicle traffic.

The authentication protocol that ensures the highest confidentiality level is presented in Section 4. This protocol uses three secret parameters. Therefore, three independent responses have been generated when calculating responses to the given challenge. This ensures maximal confidentiality when checking the received responses to the challenge.



Let us consider a scheme for adapting the protocol’s parameters to the second level. In this case, the secret protocol parameters  $k_{private}^{OBU}$  and  $k_{private}^{RSU}$ , as well as the numbers  $D, G$ , are still used to obtain OBUs and RSUs session keys, where  $\{D, G\} < S - 1$ . Since the protocol is implemented for two directions and has the same algorithm, we will only consider the situation when the OBU is a prover, and the RSU is a verifier.

Authentication (level 2). OBU (prover) → RSU (verifier).

1. Prover (OBU):

$$B(j) = m^{k_{private}^{OBU}(j)} m^{D(j)} \text{ mod } S. \tag{14}$$

Prover (OBU):

$$OBU \rightarrow RAM_{OBU} : B(j).$$

2. Prover (OBU):

$$\{\Delta k_{private}^{OBU}(j), \Delta D(j)\} < S - 2.$$

Prover (OBU):

$$\begin{aligned} \hat{k}_{private}^{OBU}(j) &= (k_{private}^{OBU} + \Delta k_{private}^{OBU}(j)) \text{ mod } \phi(S), \\ \hat{D}(j) &= (D(j) + \Delta D(j)) \text{ mod } \phi(S). \end{aligned} \tag{15}$$

Prover (OBU):

$$\hat{B}(j) = m^{\hat{k}_{private}^{OBU}(j)} m^{\hat{D}(j)} \text{ mod } S. \tag{16}$$

Prover (OBU):

$$OBU \rightarrow RAM_{OBU} : \hat{B}(j).$$

3. Verifier (RSU):

$$M(j) < S - 2, RSU \rightarrow OBU : M(j).$$

4. Prover (OBU):

$$\begin{aligned} Y_1(j) &= (\hat{k}_{private}^{OBU}(j) - M(j)k_{private}^{OBU}(j)) \text{ mod } \phi(S), \\ Y_2(j) &= (\hat{D}(j) - M(j)D(j)) \text{ mod } \phi(S). \end{aligned} \tag{17}$$

5. Prover (OBU):

$$OBU \rightarrow RSU : (B(j) || \hat{B}(j) || Y_1(j) || Y_2(j)).$$

6. Verifier (RSU):

$$A(j) = B^{M(j)}(j) m^{Y_1(j)} m^{Y_2(j)} = \hat{B}(j). \tag{18}$$

It is obvious that reducing the time to calculate the true and “distorted” OBU’s digests, as well as reducing the number of responses to the challenge, reduces the protocol’s confidentiality. However, at the same time, the efficient operation of OBUs and RSUs during intense traffic density is ensured.

Let us consider a scheme for adapting the protocol’s parameters to the first level. In this case, only  $k_{private}^{OBU}$  and  $k_{private}^{RSU}$  remain as secret parameters. Now, we consider the situation when the OBU is a prover, and the RSU is a verifier.

Authentication (level 1). OBU (prover) → RSU (verifier).

1. Prover (OBU):

$$B(j) = m^{k_{private}^{OBU}(j)} \text{ mod } S. \tag{19}$$

Prover (OBU):

$$OBU \rightarrow RAM_{OBU} : B(j).$$

2. Prover (OBU):

$$\{\Delta k_{private}^{OBU}(j)\} < S - 2.$$

Prover (OBU):

$$\hat{k}_{private}^{OBU}(j) = (k_{private}^{OBU} + \Delta k_{private}^{OBU}(j)) \bmod \phi(S). \quad (20)$$

Prover (OBU):

$$\hat{B}(j) = m^{\hat{k}_{private}^{OBU}(j)} \bmod S. \quad (21)$$

Prover (OBU):

$$OBU \rightarrow RAM_{OBU} : \hat{B}(j).$$

3. Verifier (RSU):

$$M(j) < S - 2, \text{ RSU} \rightarrow OBU : M(j).$$

4. Prover (OBU):

$$Y_1(j) = (\hat{k}_{private}^{OBU}(j) - M(j)k_{private}^{OBU}(j)) \bmod \phi(S). \quad (22)$$

5. Prover (OBU):

$$OBU \rightarrow RSU : (B(j) || \hat{B}(j) || Y_1(j)).$$

6. Verifier (RSU):

$$A(j) = B^{M(j)}(j) m^{Y_1(j)} \bmod S = \hat{B}(j). \quad (23)$$

Analyzing expressions (19)–(23), we see that a further decrease in confidentiality to the first level ensures minimal time spent on vehicle authentication, allowing RSU and OBU devices to operate efficiently in conditions of high traffic.

## 6. A Mechanism to Verify the Vehicle Owner's Authority for the Services Provider

Along with the authentication of the OBU embedded in the vehicle, the VANET must provide various types of services. For this purpose, a network of high-performance servers is used that support available services for a given vehicle's owner. Service providers can be both automakers themselves and private firms providing services for vehicles. In addition, government organizations may also be involved as service providers. However, all services should be differentiated according to their priorities and the prices paid by the customers. Therefore, when organizing the data exchange on the provision of services between the OBU and the VRS, the latter must clearly define the OBU's authority for the appropriate services.

To deploy the VANET, each OBU is loaded with a unique 64-bit initialization vector (IV) defined by the vehicle manufacturer. It is the initialization vector that determines the authority of the vehicle's owner to select the appropriate services. Obviously, the IVs should not be available to any RSU and other OBUs to ensure the confidentiality of the vehicle. Therefore, when exchanging the data about the services available to the vehicle's owners, the initialization vector's transfer between the OBU and the VRS via an open channel is impossible. Interception of this information will allow an attacker to gain access to services that were not provided to him initially. To eliminate this drawback, a protocol has been developed to verify the vehicle owner's authority for provided services when using an open communication channel.

Preliminary stage of the protocol.

To execute the protocol, each OBU and RSU must have:

- A prime number  $S$ , a modulo in which the calculations in the developed protocol are performed, where  $\log_2 n > 512$ .
- A number  $a$  generating the multiplicative group  $Z_S$ .

The OBU and RSU public keys are defined as follows:

$$K_{public}^{OBU} = a^{K_{private}^{OBU}} \bmod n, \quad K_{public}^{RSU} = a^{K_{private}^{RSU}} \bmod n. \quad (24)$$

When registering a vehicle in the VANET, its 64-bit initialization vector  $IV = L$  and the OBU's public key  $K_{public}^{OBU}$  are sent to the VRS. To increase the verification protocol confidentiality, a counter will be used showing the  $i$ -th number of the OBU request to the VRS,  $i = 1, 2, \dots$

Protocol to verify the vehicle's owner's authority for the services provider. OBU (prover)  $\rightarrow$  VRS (verifier).

1. Verifier (VRS):

$$X_1(i) < n - 2, VRS \rightarrow OBU : X_1(i).$$

where  $X_1(i)$  is an even integer.

2. Prover (OBU):

$$V_1(i) = K_{public}^{OBU} \left( a^{(L+i+1)^{-1}} \right)^{X_1} \text{mod} n, \quad (25)$$

$$OBU \rightarrow VRS : V_1(i).$$

3. Verifier (VRS):

$$X_2(i) < n - 2, VRS \rightarrow OBU : X_2(i).$$

where  $X_2(i)$  is an odd integer.

4. Prover (OBU):

$$V_2(i) = K_{public}^{OBU} \left( a^{(L+i+1)^{-1}} \right)^{X_2} \text{mod} n, \quad (26)$$

$$OBU \rightarrow VRS : V_2(i).$$

5. Verifier (VRS):

$$K(j) = \left( \frac{V_1^{X_2}}{V_2^{X_1}} \right)^{(X_2 - X_1)^{-1}} \text{mod} n = K_{public}^{OBU}. \quad (27)$$

If the vehicle's owner's public key  $K_{public}^{OBU}$  is obtained during the protocol execution, the VRS determines the initialization vector  $IV$ , which defines the set of available services.

A characteristic feature of the developed protocol is that an open channel has been used when exchanging the data necessary to verify the vehicle's owner's authority. In this case, intercepting the information transmitted from the OBU to the VRS will not allow the attacker to calculate the unique initialization vector, and thus obtain someone else's services.

## 7. Results and Discussion

To evaluate the effectiveness of the proposed authentication protocol, the VANET model was implemented using NS-2. The choice of this simulation system is due to the absence of restrictions in modifying the code and the high adequacy of the models under study. The simulated VANET network includes 10 RSUs and up to 100 OBUs for each RSU. Each OBU and RSU has a developed authentication protocol. A radio communication channel with free signal propagation was allocated to obtain the results. In this case, the transmitting and receiving antennas must be within the line of sight, which ensures the interaction zone radius of 1 km. To simulate the VANET network, a uniform distribution of RSUs located at a distance of 2 km from each other was chosen. The data transfer rate was 1 Mbit/s. The packet size changed from 50 to 200 bytes.

Let us consider the cryptographic strength of the developed authentication protocol and the time spent on its implementation at different confidentiality levels. It is obvious that the protocol's strength in finding the correct answer to the verifier's question will be determined both by the bit length of the module,  $S$ , and the number of answers,  $M(i)$ ,

included in the prover's signal, where  $i = 1, 2, 3$ . Then, the probability of guessing the correct answer will be determined by the expression

$$P = \frac{1}{2^{M(i) \log_2 S}}. \quad (28)$$

Let us consider using a 64-bit module in the developed authentication protocol. When applying the third level of confidentiality, the prover's signal consists of true, "distorted" digests and three answers to the question posed, that is  $M(3) = 5$ . Then, the probability of guessing the prover's signal is  $P_3^{(64)} = 1.08 \cdot 10^{-20}$ . If confidentiality level 2 is used, then the number of responses in the prover's signal is reduced to two, that is  $M(2) = 4$ . Then, the probability of matching the prover's signal is  $P_2^{(64)} = 1.35 \cdot 10^{-20}$ .

A further lowering of confidentiality to level 1 is possible by reducing the number of responses to one, that is  $M(1) = 3$ . Then, the probability of matching the prover's signal is equal to  $P_1^{(64)} = 1.80 \cdot 10^{-20}$ .

Thus, the transition from the third level of confidentiality to the second one reduces the cryptographic strength of the developed protocol by 1.25 times. A further lowering the level of confidentiality reduces the cryptographic strength of the developed protocol by 1.33 times.

However, the authentication protocol using the 64-bit  $S$  module does not provide a high level of confidentiality. The paper [39] presents a program for checking the password strength to brute force. So, with a 56-bit-length password, the time to crack is two hours. Additionally, with an 80-bit password, the time to crack increases to four years. Therefore, it is obvious that the module  $S$  bit depth must be greater than 64 bits. When using a 128-bit module at the third level of confidentiality of the adaptive protocol, the probability of guessing the prover's signal is  $P_3^{(128)} = 5.87 \cdot 10^{-40}$ .

If confidentiality level 2 is used, then the number of responses in the prover's signal is reduced to two, that is  $M(2) = 4$ . Then, the probability of guessing the prover's signal is  $P_2^{(128)} = 7.34 \cdot 10^{-40}$ . Further lowering the confidentiality to level 1 is possible by reducing the number of responses to one, that is  $M(1) = 3$ . Then, the probability of guessing the prover's signal is equal to  $P_1^{(128)} = 9.79 \cdot 10^{-40}$ . Thus, the transition to the 128-bit  $S$  module allows increasing the cryptographic strength of the authentication protocol by 20 orders of magnitude compared to the 64-bit module, which ensures the higher confidentiality of the vehicle route.

To estimate the time spent on the implementation of the developed authentication protocols, a Virtex-6 FPGA (XC6VSX315T) was used. The testing was performed using Xilinx Vivado HLS 2018. Operands and modules were 32-bit. When performing the modular exponentiation, a binary algorithm was used. This algorithm has the maximum computational complexity and allows obtaining the maximum possible time spent on the authentication protocol implementation. The maximum 32-bit prime number  $S = 4294967291$  was chosen as the modulus.

The exponent maximum value was chosen to be 30. During the simulation of the authentication system, it was found that the modular exponentiation was performed using two operations. The first operation was a multiplication of two 32-bit numbers and obtaining a 64-bit result. The second operation was calculating the remainder of the product over a 32-bit modulus. The first operation was performed using the IEEE Numeric\_std standard library. In this case, the multiplication of two 32-bit numbers was executed in  $N_{MUL} = 4$  clock cycles. Computing the remainder of the multiplication  $V^2 \text{ mod } S$  using the binary algorithm requires  $N_{MOD} = 41$  clock cycles. Thus,  $N_{EXP} = N_{MOD} + N_{MUL} = 45$  cycles are required to implement the modular exponentiation. For the selected FPGA, the clock frequency is 10 ns. Thus, the execution time of one modular exponentiation operation for 32-bit numbers is 450 ns. It is proposed in [33] to use an RSA encryption system with a 256-bit key in order to build an authentication protocol with zero-knowledge proof. The simplest method of modular exponentiation is the recursive method. Using this

method, 384 multiplication operations must be performed for a 256-bit key. It is shown in [39] that the use of the M-ary modular exponentiation algorithm reduces the number of multiplication operations to 340. In this case, the execution time of the encryption process alone is 9792  $\mu$ s. In the authentication protocol, one encryption operation and one decryption operation must be performed. Therefore, it takes 19,584  $\mu$ s to perform these two operations. If we take into account that during the authentication process the parties exchange 256-bit signals twice, then the transmission time is 512  $\mu$ s. In this case, the execution time of the protocol (without taking into account the time for calculation of the hash function's value) is 20,096  $\mu$ s. Let us conduct a comparative analysis with the developed adaptive authentication protocol with zero-knowledge proof.

As a result of the studies, the following time costs were obtained for performing basic protocol operations for the confidentiality level 1 (Table 1):

**Table 1.** The time cost for executing a 32-bit module authentication protocol.

$T_1$ , ns	$T_2$ , ns	$T_3$ , ns	$T_4$ , ns	$T_5$ , ns	$T_6$ , ns
13,500	13,900	32,000	500	96,000	27,450

$T_1$  is the time for calculating the true digest;  $T_2$  is the time for calculating the “distorted” digest;  $T_3$  is the time for transmitting the request;  $T_4$  is the time for calculating the response;  $T_5$  is the time for transmitting the response to the request; and  $T_6$  is the time to check the response.

However, the usage of a 32-bit module does not allow for the required level of confidentiality of the developed protocol. Therefore, let us consider the authentication protocol using a 64-bit module. So, when applying the first level of confidentiality, the time spent on protocol execution was  $T_{64}^1 = 138.392 \mu$ s. Increasing confidentiality to the second level led to an increase in time costs up to  $T_{64}^2 = 217.352 \mu$ s. As a result, the protocol execution time increased by 1.57 times. Further raising the confidentiality to level 3 increased time costs to a value of  $T_{64}^3 = 296.312 \mu$ s. It is 1.36 times more than when using confidentiality level 2. The increased time costs are due to both an increase in the computational complexity of the protocol and an increase in the total bit depth of the prover's signals.

To evaluate the effectiveness of the proposed authentication protocol, a simulation model of the VANET was developed. It helped to simulate the process of information exchange between OBUs and RSUs. The data transfer rate was 1 Mbit/s. The OBUs' and PSUs' signals' reception range was 1 km. A discrete interference-free data transmission channel was chosen. The time to live was TTL = 1. To obtain concrete results, 100 tests were carried out.

When simulating the information exchange between an OBU and an RSU, the situation when subscribers do not trust each other is taken into account. That is, the OBU–RSU authentication process takes place first. Then, the RSU–OBU authentication protocol is executed. During the OBU–RSU and RSU–OBU authentication process, no information is transmitted. This leads to a reduction in the amount of information transferred between the VANET nodes. The dependence of the traffic volume available for the information transfer in the VANET system when using a 64-bit authentication protocol is shown in Figures 2–5.

Figure 1 analysis shows that with up to 20 OBUs per 1 km, the transition from the third confidentiality level to the second level allowed increasing the amount of traffic available for information transmission from 126,496.12 bytes/s to 127,698.83 bytes/s. That is, the traffic volume increased by 1.0095 times. Lowering the confidentiality to level 1 made it possible to increase the volume of traffic available for the information transmission to 128,901.55 bytes/s, that is, 1.0094 times compared to level 2.

An increase in the OBUs' density per 1 km increased the gain in the amount of available traffic. Thus, when providing up to 70 OBUs per 1 km, the shift from the third confidentiality level to the second level allowed increasing the available traffic volume from 115,056.42 bytes/s to 119,265.93 bytes/s. That is, the traffic volume increased by 1.037 times.

The further lowering of the confidentiality to the first level allowed increasing the available traffic volume to 123,475.43 bytes/s. That is, the volume of traffic increased by 1.036 times compared to level 2. It should be noted that as the traffic density increases, the benefits from lowering the confidentiality level will increase, allowing for the maximum possible amount of traffic available for the transmission of information.

Figure 2 shows the average number of packets per OBU when using a 64-bit authentication protocol. The results are obtained for the third confidentiality level.

Figure 2 analysis shows that using shorter packets allowed increasing their average value per OBU. So, with small traffic density up to 20 OBUs per 1 km, with a packet size of 50 bytes, there were up to 126 packages per OBU. If the packet size was 120 bytes, then the number of packets was reduced to 52.

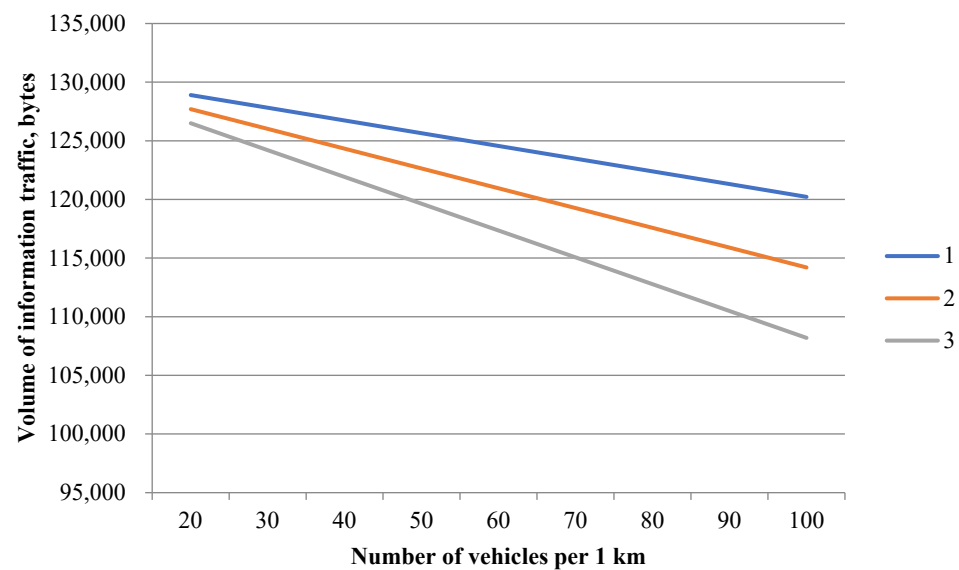


Figure 2. Dependence of the traffic volume available for transmitting information on the number of OBUs per 1 km (1, 2, and 3—confidentiality levels).

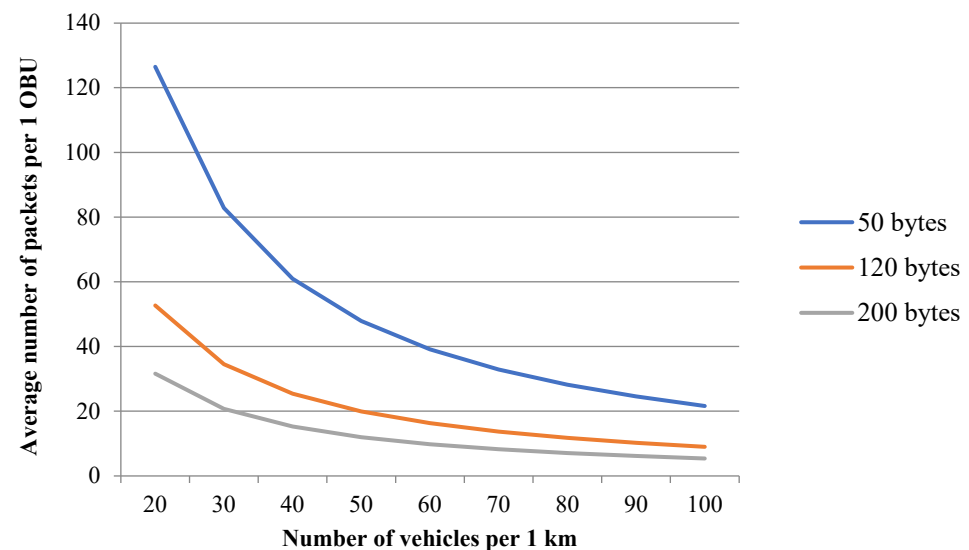
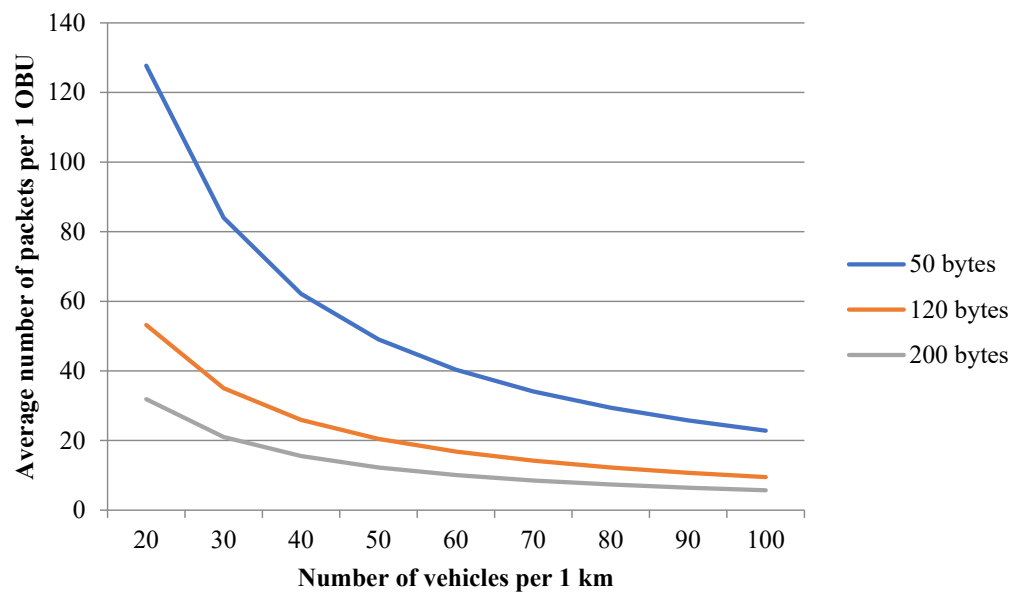
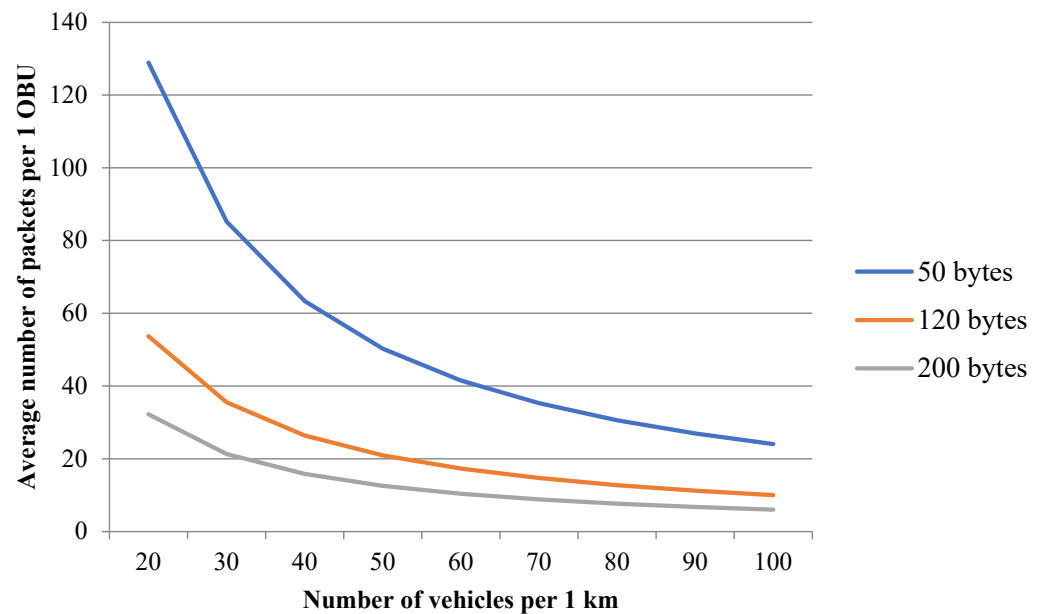


Figure 3. The average number of packets per OBU at the 3rd confidentiality level, 64-bit authentication protocol.



**Figure 4.** The average number of packets per OBU at the 2nd confidentiality level.



**Figure 5.** The average number of packets per OBU at the 1st confidentiality level.

A further increase in the packet size to 200 bytes reduced the average number of packets per OBU to 32. With an increase in the traffic density by 3.5 times, to 70 OBUs per 1 km, the average number of packets per OBU decreased. With a packet size of 50 bytes, there were up to 32 packets per OBU. Increasing the packet size to 120 bytes reduced the packets' average number to 13, and when using 200-byte packets, up to 8 packets. Obviously, reducing the packets' length allows increasing the volume of information exchange between the OBUs and RSUs. However, it should be kept in mind that the network packet consists of service information, including the start bits (preamble), headers, trailer, and payload. Reducing the packet size can lead to a decrease in the amount of useful information and negatively affect the efficiency of the VANET system. Therefore, choosing the optimal packet size for the VANET is an urgent task.

Figures 3 and 4 show the packet distribution for the confidentiality levels 2 and 1 in a 64-bit authentication protocol.

Figures 2–5 analysis confirms the conclusion that lowering the confidentiality level led to an increase in the average number of packets per OBU. If the density of cars was up to 20 OBU/1 km, then with a packet size of 50 bytes, the number of packets per OBU for level 2 increased to 128, and for level 1, up to 129 packets. If the packet size was 120 bytes, then the number of packets reduced to 53 for level 2, and to 54 packets per OBU for the first level. With an increase in the density of vehicles by 3.5 times, to a value of 70 OBU per 1 km, the average number of packets per OBU decreased. With a packet size of 50 bytes, there were up to 34 packets per OBU at confidentiality level 2, and 35 packets at confidentiality level 1. Increasing the packet size to 120 bytes reduced the average number of packets to 14 for confidentiality level 2 and up to 15 packets when using level 1.

So, the choice of the appropriate confidentiality level allows the vehicle's driver to provide the required data-exchange traffic between the OBU and the RSU. This will be especially relevant when the time-to-live increases, that is, when  $TTL > 1$ .

However, using a 64-bit module does not provide high cryptographic strength of the protocol. In [40], services are presented that allow determining the time spent on brute-force password cracking. So, using a Core i5-6600K processor, with a password length of 56 bits, cracking the password will take three hours; with a length of 64 bits, it will take 2 days. Therefore, the size of the module used in the protocol was increased to 128 bits. The dependence of the amount of traffic available for transmitting information in the VANET when using a 128-bit authentication protocol is shown in Figures 6–9.

The analysis of Figure 5 shows that with up to 20 OBUs per 1 km, the transition from the third confidentiality level to the second level allowed increasing the volume of traffic free for information transmission from 115,536.71 bytes/s to 119,676.49 bytes/s. That is, the volume of traffic increased by 1.036 times. Reducing the confidentiality level to 1 increased the volume of traffic available for information transmission to 123,816.27 bytes/s, that is, by 1.035 times compared to level 2. An increase in the OBUs' density per 1 km increased the gain in the amount of available traffic. Thus, with 70 OBUs per 1 km, the transition from the third confidentiality level to the second level increased the available traffic volume from 76,698.51 bytes/s to 91,187.73 bytes/s. That is, the volume of traffic increased by 1.16 times. Further lowering the confidentiality level to 1 made it possible to increase the volume of traffic available for information transmission to 105,676.96 bytes/s. That is, the volume of traffic increased by 1.19 times compared to level 2. The further increase to 100 OBUs per 1 km during the transition from the third confidentiality level to the second level allowed increasing the volume of available traffic from 53,395.58 bytes/s to 74,094.47 bytes/s. That is, the traffic amount increased by 1.38 times. Further lowering the confidentiality level to 1 allowed increasing the traffic volume available for information transfer to 94,793.36 bytes/s. That is, the amount of traffic increased by 1.28 times compared to level 2. The data obtained confirm the previous version that as the vehicle density increases, the gain from lowering the confidentiality level will increase, allowing for the maximum possible amount of traffic available for information transfer.

Figure 6 shows the average number of packets per OBU when using a 128-bit authentication protocol. The results were obtained for the third level of confidentiality.

As can be seen from Figure 6, using shorter packets could increase their average value per OBU. Thus, with a small density of vehicles (up to 20 OBUs per 1 km), with a packet size of 50 bytes, one OBU accounted for up to 115 packets. If the packet size was 120 bytes, then the number of packets was reduced to 48. A further increase in the packet size to 200 bytes reduced the average number of packets per OBU to 14. With an increase in the traffic density by 3.5 times, to 70 OBUs per 1 km, the average number of packets per OBU decreased. With a packet size of 50 bytes, there were up to 21 packets per OBU. Increasing the packet to 120 bytes reduced the average number of packets to nine. Using 200-byte packets reduced the average number of packets to two. Figures 7 and 8 show the packet distribution for confidentiality levels 2 and 1 when using a 128-bit authentication protocol.



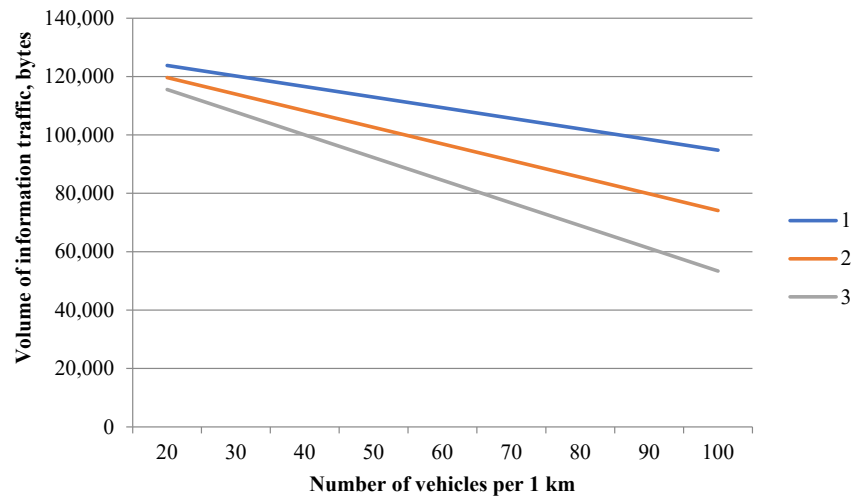


Figure 6. Dependence of the traffic available for transmitting information on the number of OBUs per 1 km (1, 2, and 3—confidentiality levels).

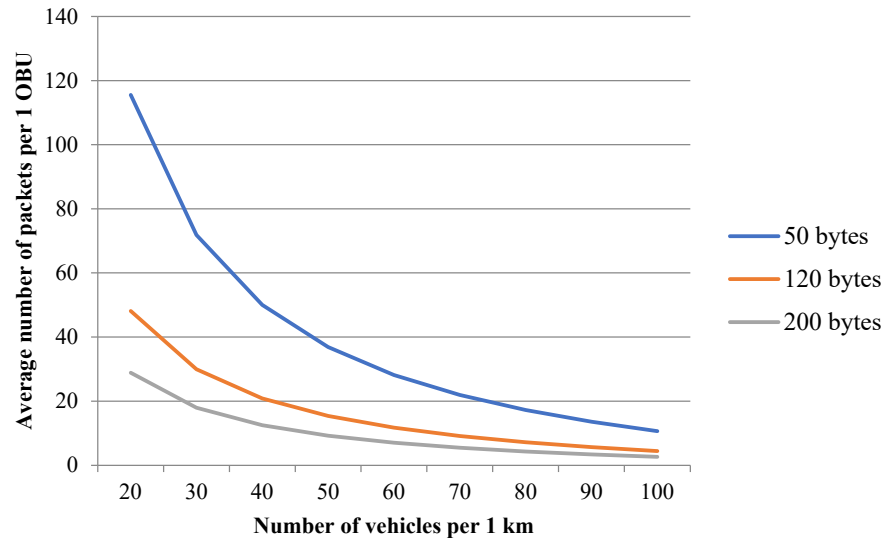


Figure 7. Average number of packets per OBU when using the 3rd confidentiality level.

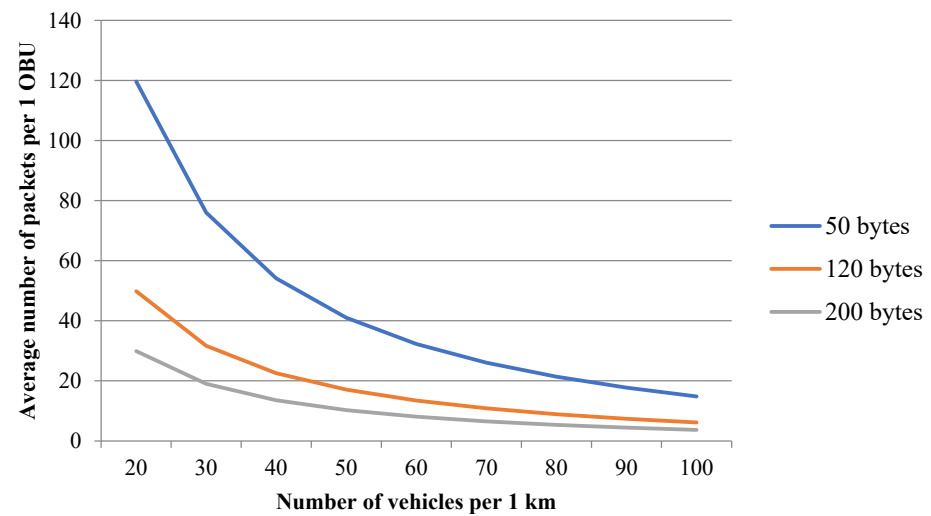
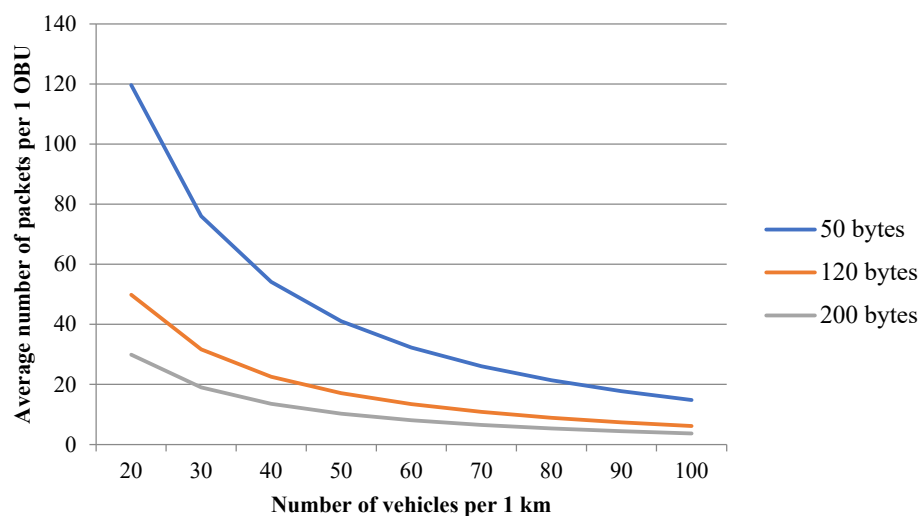


Figure 8. Average number of packets per OBU when using confidentiality level 2.



**Figure 9.** Average number of packets per OBU when using confidentiality level 1.

The analysis of Figures 6–8 confirms the earlier conclusion that a decrease in the level of confidentiality leads to an increase in the average number of packets per OBU. Thus, the following conclusions can be drawn. The developed adaptive authentication protocol for the VANET allows the motor vehicle driver to ensure the required amount of data-exchange traffic between the OBUs and RSUs by choosing the appropriate level of confidentiality. The developed authentication protocol shows the greatest gain when the number of cars on the road increases, that is, when the RSU is located on multi-lane expressways. Application of the developed protocol in a megalopolis (city) allows guaranteeing sufficiently high data-exchange traffic between the OBUs and RSUs, providing the maximum level of confidentiality.

To reduce the negative impact of the developed adaptive authentication protocol on the amount of information transferred between the OBUs and the RSU, it is advisable to consider the following solutions. Firstly, we can try to use parallel pipeline computations based on the residue number system (RNS). These are arithmetic codes that effectively implement modular operations (modular addition, subtraction, and multiplication). Since operands in the RNS code are represented as small-bit residues, and modular operations are performed in parallel, this will reduce the time spent on performing the authentication procedure. Secondly, multiplicative modular operations take a very long time when executing the authentication protocol. In order to speed up the modular exponentiation, it is advisable to use the Montgomery algorithm.

## 8. Conclusions

Based on the analysis of various methods for ensuring privacy in the VANET network, an adaptive authentication protocol was proposed in the article. A characteristic feature of this protocol is the ability to determine the status of the OBU and the RSU without using symmetric and asymmetric encryption systems, providing a sufficient level of cryptographic strength. The developed ZKAP makes it possible to reduce the authentication time compared to the standard [33], in which it is proposed to use public key encryption methods. So, when using a 256-bit key and the RSA encryption algorithm, the authentication time was 20,096  $\mu$ s. Then, using the developed protocol, while ensuring the maximum level of confidentiality, it took 1181  $\mu$ s for authentication. Thus, it is obvious that the developed protocol provides a higher authentication speed compared to the standard for building the ZKAP protocol [33].

At the same time, this protocol allows, by changing the level of confidentiality, increasing the efficiency of information exchange between the OBUs and RSUs. So, when using the third level of confidentiality and a 64-bit module, the probability of finding the prover's answer will be  $P_{64}^3 = 4.68 \cdot 10^{-97}$ , and the transition to level 1 reduces this indicator to a

value  $P_{64}^1 = 1.59 \cdot 10^{-58}$ . This allows increasing the amount of traffic available for data transfer with up to 70 OBUs per 1 km from 115,056.42 bytes/s to 119,265.93 bytes/s. That is, the volume of traffic has increased by 1.073 times. A higher gain is observed with an increase in the bit depth of the module. So, when using the third level of confidentiality and a 128-bit module, the probability of guessing the prover's answer will be  $P_{128}^3 = 8.76 \cdot 10^{-193}$ , and switching to level 1 reduces this value to  $P_{128}^1 = 3.94 \cdot 10^{-116}$ . This allows increasing the amount of traffic available for information transfer with up to 70 OBUs per 1 km from 76,698.51 bytes/s to 105,676.96 bytes/s. So, the volume of traffic increases by 1.38 times. At the same time, with an increase in the density of cars, this gain increases. Thus, if there are up to 100 OBUs per 1 km on the road, the amount of traffic available for information transfer increases from 53,395.58 bytes/s to 94,793.36 bytes/s. That is, lowering confidentiality to a minimum level allows increasing the traffic amount by 1.75 times.

The article presents the most promising methods to increase the efficiency of the developed adaptive authentication protocol. These include a usage of parallel arithmetic RNS codes and the Montgomery algorithm, which reduce the time spent on performing modular multiplicative operations.

**Author Contributions:** Conceptualization, I.A.K.; Data curation, I.A.K., A.A.O. and N.I.K.; Formal analysis, I.A.K.; Investigation, I.A.K., A.A.O. and N.I.K.; Methodology, I.A.K.; Project administration, I.A.K.; Software, N.I.K. and D.V.D.; Supervision, I.A.K.; Validation, D.V.D.; Visualization, D.V.D.; Writing—Original draft, I.A.K. All authors have read and agreed to the published version of the manuscript.

**Funding:** The research was carried out at the expense of a grant from the Russian Science Foundation, grant number 23-21-00036, <https://rscf.ru/en/project/23-21-00036/> (accessed on 8 October 2022).

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** No new data were created or analyzed in this study. Data sharing is not applicable to this article.

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

## References

1. Van Audenhove, F.; Korniiuchuk, O. *Future of Urban Mobility 2.0*; UITP: Brussels, Belgium, 2014; p. 72.
2. Anand, P.; Chilamkurti, N.; Daniel, A.; Rho, S. *Intelligent Vehicular Networks and Communications Fundamentals, Architectures and Solutions*; Elsevier Inc.: Amsterdam, The Netherlands, 2017; p. 227.
3. Stoilova, K.; Stoilov, T.; Ivanov, V. Bi-Level Optimization as a Tool for Implementation of Intelligent Transportation Systems. *Cybern. Inf. Technol.* **2017**, *17*, 97–105. [[CrossRef](#)]
4. Aung, N.; Zhang, W.; Dhelim, S.; Ai, Y. Accident prediction system based on hidden Markov model for vehicular ad-hoc network in urban environments. *Information* **2018**, *9*, 311. [[CrossRef](#)]
5. Zhang, H.; Li, H. Modeling and Topological Properties of a V2I Sub Network in VANET Based on a Complex Network. *Cybern. Inf. Technol.* **2015**, *15*, 149–160. [[CrossRef](#)]
6. *ETSI TS 101 539-1 V1.1.1 (2013-08)*; Intelligent Transport Systems (ITS); V2X Applications; Part 1: Road Hazard Signalling (RHS) Application Requirements Specification. ETSI: Valbonne, France, 2013.
7. *ETSI TS 101 539-3 V1.1.1 (2013-11)*; Intelligent Transport Systems (ITS); V2X Applications; Part 3: Longitudinal Collision Risk Warning (LCRW) Application Requirements Specification. ETSI: Valbonne, France, 2013.
8. Manivannan, S.S.; Sathiyamoorthy, E. A Prevention Model for Session Hijack Attacks in Wireless Networks Using Strong and Encrypted Session ID. *Cybern. Inf. Technol.* **2014**, *14*, 46–60. [[CrossRef](#)]
9. Zeadally, S.; Hunt, R.; Chen, Y.-S.; Irwin, A.; Hassan, A. Vehicular ad hoc networks (VANETS): Status, results, and challenges. *Telecommun. Syst.* **2012**, *50*, 217–241. [[CrossRef](#)]
10. Sheikh, M.S.; Liang, J. A Comprehensive Survey on VANET Security Services in Traffic Management System. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1–23. [[CrossRef](#)]
11. Al-kahtani, M.S. Survey on security attacks in vehicular ad hoc networks (VANET). In Proceedings of the 6th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, GC, Australia, 12–14 December 2012.
12. Singh, U.; Singh, P. Review of solutions for securing the vehicular networks. *Int. J. Comput. Appl. Technol.* **2011**, *2*, 1652–1656.
13. Zhang, C.; Lin, X.; Lu, R.; Ho, P.-H. RAISE: An efficient RSU-aided message authentication scheme in vehicular communication networks. In Proceedings of the IEEE International Conference on Communications, Beijing, China, 19–23 May 2008.

14. Raya, M.; Papadimitratos, P.; Aad, I.; Jungels, D.; Hubaux, J.P. Eviction of misbehaving and faulty nodes in vehicular networks. *IEEE J. Sel. Areas Commun.* **2007**, *25*, 1557–1568. [CrossRef]
15. Al-Mutiri, R.; Al-Rodhaan, M.; Tian, Y. Improving Vehicular Authentication in VANET using Cryptography. *Int. J. Commun. Netw. Inf. Secur.* **2018**, *10*, 248–255.
16. Alaya, B.; Sellami, L. Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks. *J. Inf. Secur. Appl.* **2021**, *58*, 102779. [CrossRef]
17. Liu, Y.-N.; Lv, S.-Z.; Xie, M.; Chen, Z.-B.; Wang, P. Dynamic anonymous identity authentication (DAIA) scheme for VANET. *Int. J. Commun. Syst.* **2018**, *32*, e3892. [CrossRef]
18. Gaiduk, P.; Ranjan, K.R.; Basmer, T.; Tschorsch, F. Privacy-Preserving Public Key Infrastructure for Vehicular Networks. In Proceedings of the IEEE 45th Conference on Local Computer Networks (LCN), Sydney, NSW, Australia, 16–19 November 2020.
19. Zhang, C.; Lu, R.; Lin, X.; Ho, P.-H.; Shen, X. An efficient identity-based batch verification scheme for vehicular sensor networks. In Proceedings of the 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008.
20. Lu, R.; Lin, X.; Zhu, H.; Ho, P.-H.; Shen, X. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In Proceedings of the 27th Conference on Computer Communications, Phoenix, AZ, USA, 13–18 April 2008.
21. Lin, X.; Sun, X.; Ho, P.-H.; Shen, X. GSIS: A secure and privacy preserving protocol for vehicular communications. *IEEE Trans. Veh. Technol.* **2007**, *56*, 3442–3456.
22. Calandriello, G.; Liroy, A. Efficient and Reliable Pseudonymous Authentication. In *Cyber Crime: Concepts, Methodologies, Tools and Applications*; IGI Global: Pennsylvania, PA, USA, 2011; Volume 1, pp. 571–586.
23. Mansour, M.B.; Salama, C.; Mohamed, H.K.; Hammad, S.A. VANET security and privacy—An overview. *Int. J. Netw. Secur. Its Appl. (IJNSA)* **2018**, *10*, 13–34. [CrossRef]
24. Armknecht, F.; Festag, A.; Westho, D.; Zeng, K. Cross-layer privacy enhancement and non-repudiation in vehicular communication. In Proceedings of the 4th Workshop on Mobile Ad-Hoc Networks (WMAN), Bern, Switzerland, 1–2 March 2007.
25. Kahate, A. *Cryptography and Network Security*; Tata McGraw Hill Education Private Ltd.: Hoboken, NJ, USA, 2013; p. 524.
26. Kumari, S.; Chaudhry, S.A.; Wu, F.; Li, X.; Farash, M.S.; Khan, M.K. An improved smart card based authentication scheme for session initiation protocol. *Peer Peer Netw. Appl.* **2017**, *10*, 92–105. [CrossRef]
27. Walshe, M.; Epiphaniou, G. Non-Interactive Zero Knowledge Proofs for the Authentication of IoT Devices in Reduced Connectivity Environments. *J. Ad Hoc Netw.* **2019**, *95*, 36. [CrossRef]
28. Assidi, H.; Ayebe, E.B.; Souidi, E.M. Two Mutual Authentication Protocols Based on Zero-Knowledge Proofs for RFID Systems. In Proceedings of the Information Security and Cryptology—ICISC 2017, Seoul, Republic of Korea, 29 November–1 December 2017.
29. Dossa, R.; Trujillo-Rasua, R.; Piramuthu, S. Secure attribute-based search in RFID-based inventory control systems. *Decis. Support Syst.* **2020**, *132*, 113270. [CrossRef]
30. Al-Adhami, A.H.; Ambroze, M.; Stengel, I.; Tomlinson, M. An Efficient Improvement of RFID Authentication Protocol Using Hash Function ZKP. In Proceedings of the 2nd Scientific Conference of Computer Sciences (SCCS), Baghdad, Iraq, 27–28 March 2019.
31. Park, G.; Kim, B.; Jun, M. A Design of Secure Authentication Method Using Zero Knowledge Proof in Smart-Home Environment. In Proceedings of the UCAWSN CUTE CSA 2016, Seoul, Republic of Korea, 23 November 2016.
32. Maulana, L.; Kusyanti, A.; Bachtiar, F. Implementasi Metode Autentikasi dengan Zero Knowledge Proof menggunakan Protokol Feige-Fiat-Shamir Identification Scheme pada Perangkat Internet of Things. *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.* **2019**, *3*, 8937–8945.
33. ISO/IEC 9798-5:2009; Information Technology—Security Techniques—Entity Authentication—Part 5: Mechanisms Using Zero-Knowledge Technique. International Organization for Standardization: Geneva, Switzerland, 2009.
34. Kim, M.; Choi, K.-C.; You, H.; Jun, M. Design of Authentication Protocol Based on Distance-Bounding and Zero-Knowledge for Anonymity in VANET. In *Advances in Computer Science and Ubiquitous Computing*; Springer: Singapore, 2015; pp. 269–274.
35. Hedge, N.; Manvi, S.S. MFZKAP: Multi Factor Zero Knowledge Proof Authentication for Secure Service in Vehicular Cloud Computing. In Proceedings of the 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), Gangtok, Sikkim, India, 25–28 February 2019.
36. Chisousov, N.K.; Kalmykov, I.A.; Dukhovnyj, D.V.; Kalmykov, M.I.; Olenev, A.A. Adaptive authentication protocol based on zero-knowledge proof. *Algorithms* **2022**, *15*, 50. [CrossRef]
37. Rasheed, A.A.; Mahapatra, R.N.; Hamza-Lup, F.G. Adaptive Group-Based Zero Knowledge Proof-Authentication Protocol in Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2020**, *21*, 867–887. [CrossRef]
38. Dodis, Y.; Yampolsky, A. Verifiable Random Function with Short Proofs and Keys. In *Public Key Cryptography-PKC 2005*; Springer: Berlin/Heidelberg, Germany, 2005; pp. 416–431.
39. Cohen, H. *Course in Computational Algebraic Number Theory*; Springer: Berlin/Heidelberg, Germany, 1993; p. 540.
40. Secure Password Check. Available online: <https://password.kaspersky.com> (accessed on 25 November 2022).

**Disclaimer/Publisher’s Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.