electronics

MDPI

Article

Lightweight Cryptography for Connected Vehicles Communication Security on Edge Devices

Sahbi Boubaker [1,*], Faisal S. Alsubaei [2], Yahia Said [3] and Hossam E. Ahmed [3]

[1] Department of Computer & Network Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah 21959, Saudi Arabia
[2] Department of Cybersecurity, College of Computer Science and Engineering, University of Jeddah, Jeddah 23218, Saudi Arabia; fsalsubaei@uj.edu.sa
[3] Electrical Engineering Department, College of Engineering, Northern Border University, Arar 91431, Saudi Arabia; yahia.said@nbu.edu.sa (Y.S.); hossam.ahmed@nbu.edu.sa (H.E.A.)
* Correspondence: sboubaker@uj.edu.sa

Abstract: Recent advances in mobile connection technology have been involved in every aspect of modern life. Even vehicles are becoming more connected, with the ability to communicate without human intervention. The main idea of connected vehicles is to exchange information to avoid a potential collision or to warn the driver about stop signs/lights. To achieve a wide range of connections between vehicles, they must be equipped with connected devices such as Bluetooth, wi-fi, and cellular connectivity. However, communication raises security issues with regard to cybersecurity attacks that attempt to collect confidential information or to take control of the vehicle by forcing unintended braking or steering. In this paper, we proposed a secure vehicle-to-vehicle (V2V) communication approach by deploying a secure communication protocol based on a key management process and a cryptography system to encrypt exchanged data. The proposed key management process was designed to resist many attacks and eliminate connections to the infrastructure for key generation. Since vehicles are equipped with embedded devices with limited computation resources, a lightweight cryptography algorithm was used. The light encryption device (LED) block cipher was used to encrypt exchanged data. The LED has a low implementation area on hardware and low power consumption. It is considered to be a perfect solution for security issues in connected vehicles. The proposed data encryption algorithm was synthesized with VHDL on the Xilinx Zynq-7020 FPGA using the Vivado HLS tool. The encryption algorithm was implemented only on the logic of the device. The achieved results proved that the proposed algorithm is suitable for implementation in vehicles due to its low implementation requirements and low power consumption in addition to its high security level against cyber-attacks.

Keywords: connected vehicles; vehicle to vehicle communication; security; data encryption; FPGA

Citation: Boubaker, S.; Alsubaei, F.S.; Said, Y.; Ahmed, H.E. Lightweight Cryptography for Connected Vehicles Communication Security on Edge Devices. *Electronics* **2023**, *12*, 4090. https://doi.org/10.3390/electronics12194090

Academic Editor: Mohamed Karray

Received: 1 September 2023
Revised: 20 September 2023
Accepted: 26 September 2023
Published: 29 September 2023

1. Introduction

Emerging technologies are leading the automotive industry to a significant transformation. Those technologies have changed vehicle concepts by improving efficiency, safety, and performance. Most recent vehicles are becoming more intelligent due to the embedded emerging technologies [1] such as intelligent vision [2,3]. Modern vehicles can talk to each other through wireless and cellular connectivity. Technologies like wi-fi and 5G have made vehicle communication easier.

Connected vehicles share relevant information, such as traffic lights and signs, position, and speed. Considering that the main focus of connected vehicles is to improve safety, V2V communication plays an important role in preventing accidents by avoiding potential collisions. To achieve high reliability of data sharing, wireless or cellular connectivity must be established. However, this communication presents security issues because they

are exposed to cyber-attacks. Therefore, data security is critical and must be considered carefully to ensure the highest levels of safety.

Recent findings have demonstrated the effects of cyber-attacks on connected vehicles and how they menace driver safety. Koscher et al. [4] explained the possibility of hacking the vehicle's internal network, which allows one to manipulate essential functionalities such as brakes, steering, and the engine. In such a case, the hacker can control the vehicle aggressively, disable some functionalities, or stop the engine. In [5], a remote attack to control the vehicle was applied through the exploitation of different connection devices, such as Bluetooth and cellular. This attack allowed the hacker to access all devices connected to the car, such as smartphones, and to collect relevant information such as location and destination. As proved in the mentioned studies, connected cars present security issues that must be considered and solved [6].

Based on many studies, connected cars have a higher risk of causing accidents. For example, according to the German Federal Highway Research Institute (BASt), the involvement of connected vehicles in traffic accidents is eight times more than ordinary vehicles. This is due to receiving wrong alerts or due to driver behavior in emergency cases. Connected vehicles must communicate under real-time conditions to avoid data transfer delays and prevent dangerous situations.

V2V communication allows connected cars to interact to share warnings, such as collision warnings and blind-spot warnings, to prevent accidents. Moreover, it can share traffic information, such as congestion, emergency braking, and pavement defects. However, receiving a wrong warning or traffic information may lead to a disaster. Hence, V2V communication must be secured, and cyber-attacks must be avoided. Thus, establishing a secure communication protocol is a necessary step to guarantee safety. Therefore, considering that V2V communication can be achieved through wireless devices such as Bluetooth and wi-fi without the need for an internet connection, we have proposed a security protocol to authenticate V2V communication. The proposed protocol was designed to run under real-time constraints with a minimal implementation area on the hardware and low power consumption. To achieve such features, lightweight cryptography was proposed as a solution. Lightweight cryptography algorithms are characterized by a high security level and a high throughput in addition to low power consumption.

In this paper, we proposed the encryption of V2V communication through a lightweight cryptography [7] algorithm that is characterized by high throughput and low power consumption in addition to the small hardware implementation area. The light encryption device (LED) [8] block cipher was used as an encryption algorithm for V2V communication. LED is a lightweight encryption algorithm from the substitution permutation network (SPN) family [9]. It has two key lengths, 64-bit and 128-bit, that define the size of the input plaintext. If the 64-bit key length is used, then the plaintext size is 64 bits, and, if the 128-bit key length is used, then the plaintext size is 128 bits. The total number of rounds depends on the key length. For 128 bits, the number of rounds is 48, and for 64 bits, only 32 rounds are performed.

The LED was proposed for effective data encryption while reducing the computational overhead and cost compared to existing V2V communication protocols. The above-mentioned factors prove that the proposed protocol is very flexible and can be easily integrated into connected cars to authenticate communication.

To achieve high efficiency and reliability, we proposed a communication protocol based on a temporary private key. The proposed protocol aims to allow vehicles in a communication group to generate their private keys without sharing them. Initially, each vehicle has a public key that allows it to communicate with a group manager vehicle that is responsible for managing group members and private key generation. After group establishment and group manager vehicle election, the vehicles send their identity to the group manager vehicle for an authorization check. Next, after the vehicles are checked, they send a private key request, and the group manager vehicle responds with the pseudo

key used to generate the final private key. Finally, vehicles generate their private keys through the Mix-Columns function of the LED block cipher.

The proposed protocol was tested on the Xilinx Zynq-7020 FPGA board using VHDL. The hardware implementation proved that the proposed solution is very effective, with a very small implementation area, low power consumption, and a very high throughput.

The main contributions of this work are the following:

- Proposing a data encryption protocol for V2V communication;
- Proposing the use of lightweight cryptography algorithm for data encryption;
- Evaluating the performance of the proposed algorithm with a hardware implementation;
- Achieving high performance with a low implementation area, low power consumption, and high throughput.

The rest of the paper is organized as follows: Section 2 is reserved for related works. The proposed method is explained and detailed in Section 3. In Section 4, experiments and results are presented and discussed. Conclusions are provided in Section 5.

2. Related Works

Smart cities are becoming a reality which includes smart vehicles with communication ability. However, this communication raised security concerns that must be solved to ensure safety and efficiency. In this context, many works have been proposed to guarantee communication security.

Vasudev et al. [10] proposed a lightweight mutual authentication protocol to secure V2V communication. The proposed protocol was based on cryptographic hash functions and XOR operations. The protocol was composed of two phases, and each phase has many steps. The first phase is registration, which aims to register the connected vehicle in the server through a registration authority. If the registration goes well, a smart card with the authentication parameters is generated. The registration phase has three main steps. First, the driver fixes an identifier and a password and sends them to the registration authority through a secure channel such as SSH or TLS. Second, the registration authority generates a smart card that contains the authentication parameters and is transmitted to the trusted authority which controls data transfer between devices and to the driver. Third, an additional parameter is defined for further communications. The second phase is the login, authentication, and communication, which aims to ensure a secure login and authentication of the driver for possible communication. This phase is composed of six steps. First, the driver logs in to the already-registered account using their identification and password. If this is performed, a message is sent to the trusted authority through an insecure channel. Second, the trusted authority verifies the login through verification of the authentication parameters and sends a message to the server. Third, the server generates a secret key and shares it with the driver to facilitate secure communication. Fourth, the trusted authority verifies the secret key if it has been received by the driver. Fifth, the secret key is stored in the vehicle system for V2V communication. Finally, if the vehicle sends a message to another vehicle, the secret key is used to encrypt the message and transmit it. The proposed protocol was very complicated and needed a lot of server communication and computation.

Secure V2V communication using group key management was proposed in [11]. The proposed method was based on data encryption and group key management to avoid secret key sharing and to ensure authenticity. The data encryption was performed using a matrix-based encryption algorithm. Assuming a group of vehicles that moves in the same direction is established, one of those vehicles is responsible for key generation and distribution to ensure smooth and secure communication. The selected vehicle must be stable and trusted to be considered as a group manager. Once the vehicle is selected, it generates a public key and distributes it to the surrounding vehicles in the group. The key is used to decrypt group key requests. After all members receive the public key, they configure security parameters and start requesting private keys. Once all members send a key request, the group manager verifies the identity of the group members and

responds with a message that contains a new public key encrypted using the old public key. Then, each member generates their private key using the newly received public key. The generated private key is used to encrypt group messages without sharing its key with other group members.

Han et al. [12] proposed a secure V2V vehicle-to-infrastructure (V2I) communication protocol based on physical layer key generation. The proposed protocol was used for long-range communication. The physical layer presents a different scheme compared to the traditional encryption method since it is based on information theory and wireless channels' random features. To obtain the needed randomness, vehicles that try to communicate start by sending and receiving test signals between each other. For each received signal, the channel parameters are measured and stored. Since the measured parameters are not synchronous between the sender and receiver, they propose calculating the estimate of all measurements and considering them for further processing. If the parameters of the sender and receiver are highly correlated, a key is generated. The level-crossing algorithm [13] is used for key generation. The proposed protocol posed many difficulties, both spatially, for moving vehicles, and in the limited time to share information. It cannot be implemented for real-time use due to the extensive computation time needed to calculate the channel randomness parameters.

The study in [14] was developed to establish safe communication between vehicles (V2V) in Vehicular Ad Hoc Networks (VANETs). VANETs are a type of network in which automobiles establish communication with one another in order to improve road safety, manage traffic, and facilitate many other applications. The suggested approach emphasizes the attainment of mutual authentication, which entails the verification of identities by both communicating vehicles to build a foundation of confidence. The protection of privacy is given significant importance in order to protect the identity of the vehicles involved in communication. The approach tries to strike a compromise between the requirement for security and the desire to minimize computational overhead, delay, and resource consumption by integrating efficient cryptographic algorithms. The achievement of these objectives is likely facilitated by the utilization of cryptographic primitives, including digital signatures, public-key infrastructure (PKI), and secure key exchange mechanisms. The primary focus of the aforementioned study revolves around the development of a privacy-preserving mutual authentication system that ensures safe vehicle-to-vehicle (V2V) communication inside VANETs. However, it is imperative to acknowledge the limitations associated with this approach, including computational complexity, scalability, and the dynamic characteristics inherent in vehicular networks.

Yao et al. [15] introduced a secure transmission scheme that utilizes both radar and communication technologies within the framework of Mobile Vehicular Networks (MVNs). MVNs are composed of cars that are outfitted with radar and communication systems. These systems enable vehicles to communicate information with each other for a range of objectives, such as enhancing road safety, managing traffic, and avoiding collisions. The suggested solution utilizes the combined capabilities of radar and communication systems to augment the security of information transmission inside MVNs. Radar systems are commonly employed for the purpose of detecting and tracking objects, whilst communication systems facilitate the transmission of data between vehicles, such as traffic information or collision alerts. The integration of these two technologies is intended to enhance the dependability and confidentiality of communication inside the network. The technique may incorporate essential elements like radar-assisted authentication, which utilizes radar data to authenticate the identity and location of adjacent cars before transferring confidential data. Furthermore, the proposed approach can utilize cryptographic methodologies and robust communication protocols to safeguard the transmission of data across vehicles, hence guaranteeing both confidentiality and integrity. The present study centers on an investigation of a secure transmission strategy that utilizes both radar and communication technologies within the context of Mobile Vehicular Networks (MVNs). While this methodology presents the possibility of enhanced security, it is important to

take into account its constraints, such as financial implications, coverage distance, network saturation, and computing demands.

The primary objective of implementing a D2D-compatible jammer is to augment the level of security in V2V communication environments. The purpose of the proposed system [16] is likely to mitigate jamming assaults, which include malevolent organizations attempting to interrupt communication between vehicles (V2V). The D2D-friendly jammer has been specifically developed to effectively fight and minimize the adverse impacts of jamming, therefore guaranteeing the secure continuation of genuine vehicle-to-vehicle (V2V) communication. In order to bolster security measures, the system incorporated methods for secure key management. This encompasses techniques for establishing secure key exchange protocols across cars or for identifying and addressing illegal access attempts. To guarantee that cars can trust the communication partners they are communicating with, robust authentication systems are applied. This measure aids in the prevention of spoofing and illegal access. Although the proposed method has potential advantages in terms of security, it is important to acknowledge its shortcomings in several aspects, such as jammer detection, resource use, complexity, privacy, interoperability, and the effectiveness of countermeasures against persistent jammers.

Most of the proposed protocols have focused on key management and generation, which pose serious problems in real-time communication and the limited time available to achieve the communication due to the mobility of the vehicle. In this work, we considered all the mentioned problems and proposed a solution based on a lightweight cryptography algorithm with temporary private key management.

3. Proposed Method

A secure V2V communication requires a combination of security and privacy. Cryptography is considered to be solution for both issues. However, traditional cryptography presents an extensive computation overhead for encrypting and decrypting messages. In normal cases, a connected vehicle sends a message each 100 to 300 ms [17]. Encrypting a message for each 100 ms does not matter, but decrypting hundreds of messages is a hard challenge that must be solved to achieve reliable V2V communication under real-time constraints. Moreover, all vehicles are equipped with edge devices with limited computation resources and energy. Therefore, a V2V communication protocol must be lightweight, fast, and secure to achieve the desired performance. The main workflow of the proposed protocol is presented in Figure 1.

The number of connected vehicles is extensively growing with the availability of new communication technologies. Most methods for signing and verifying messages are not efficient enough to achieve a high security level. The security of messages is a critical task to ensure safety. Since traditional cryptography is not scalable for the existing traffic density, it is essential to find a solution that satisfies the presented requirement of low commutation overhead and real-time processing in addition to a high security level and a lightweight size to fit into edge devices.

Hence, a lightweight cryptography algorithm was proposed to solve the mentioned issues and satisfy the desired requirements. In this work, we proposed a communication protocol based on a lightweight cryptography algorithm for data encryption and decryption with a temporary group key management that works in an offline scenario.

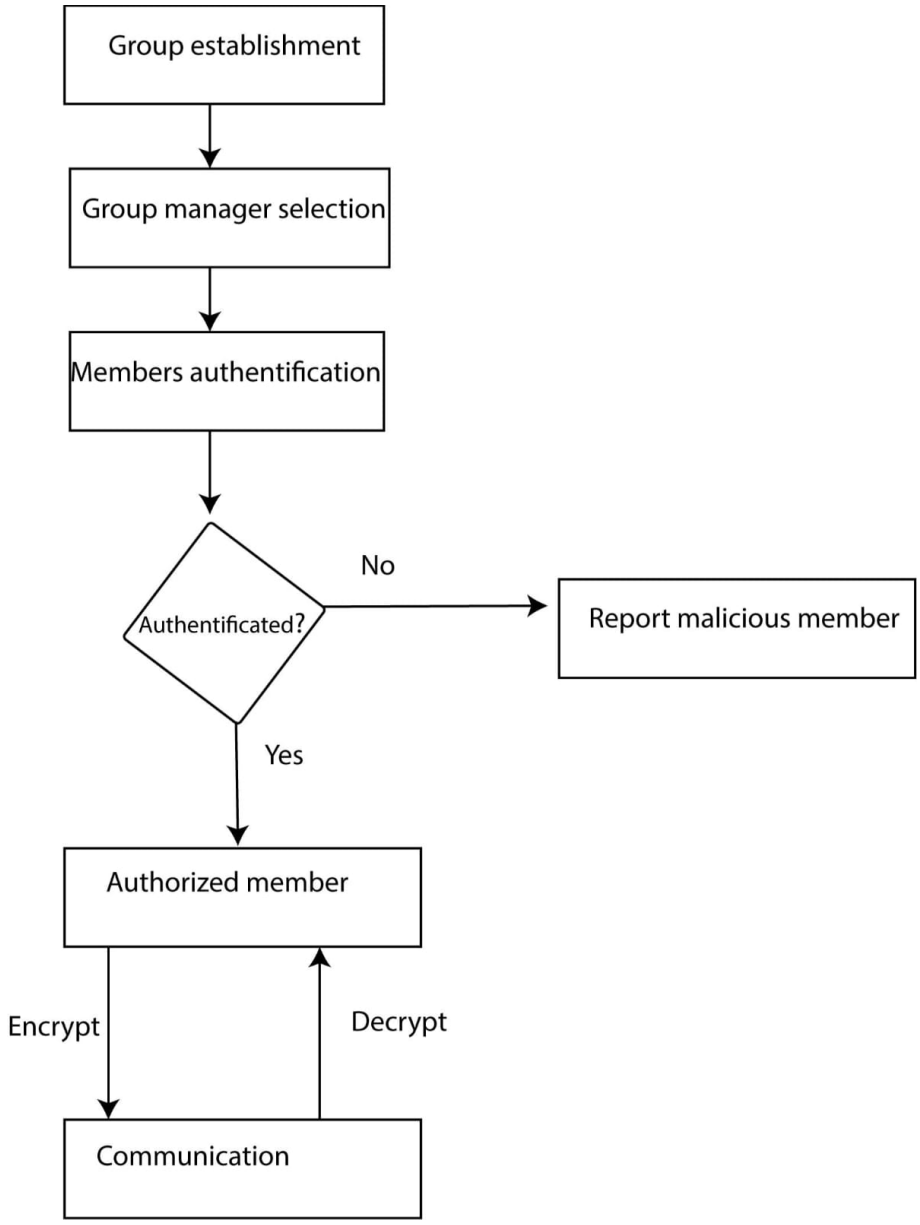

Figure 1. Workflow of the proposed protocol.

3.1. Lightweight Encryption Algorithm

Lightweight cryptography is featured with a small footprint and low power consumption in addition to a good security level. In this work, we proposed the use of the light encryption device (LED) block cipher [8]. The LED block cipher is a symmetric-key encryption technique that has been specially developed for the purpose of lightweight cryptography. The design of this technology was specifically tailored to provide a combination of security and efficiency, rendering it particularly suitable for devices with limited resources, such as Internet of Things (IoT) devices, RFID tags, and sensors. The LED encryption algorithm functions by processing data in 64-bit blocks and offers key sizes of 64 and 128 bits. The utilization of longer keys results in enhanced encryption strength. The employed structure of the system is a Substitution–Permutation Network (SPN), which incorporates a lightweight S-box to introduce non-linearity and a bit-wise permutation to facilitate diffusion in every cycle. The encryption method of LED encompasses several critical components, including key expansion, beginning and final permutations, a predetermined number of rounds (usually 48), and bitwise XOR operations using round

keys. The process of decryption involves reversing the steps of encryption, employing an equal number of rounds and round keys in the opposite sequence. Extensive investigation has been conducted on LED to evaluate its resilience against well-known cryptographic techniques, such as differential and linear cryptanalysis. The aforementioned cipher, which possesses a relatively low computational burden, is particularly suitable for safeguarding data on devices that possess constrained processing capabilities. It achieves a harmonious equilibrium between straightforwardness and the robustness of cryptographic measures.

The LED has a novel design with no key scheduling process, which makes it fast and reliable. It is based on the substitution and permutation network (SPN). LED is composed of four main functions, which are Add-Constant, S-Box, Shift-Row, and Mix-Columns. The S-Box design was inspired by the PRESENT algorithm [18], the Shift-Row was reproduced from the light Advanced Encryption Standard (AES) [19], and the Mix-Columns function was taken from the hash function PHOTON [20]. This collection has allowed the LED to have a small footprint, good software performance, and a high security level. Mainly, the LED uses data blocks of 64-bits and two key sizes, which are the 64-bit key and the 128-bit key. The number of rounds depends on the key size. For the 64-bit key, the number of rounds is 32, and, for the 128-bit key, the number of rounds is 48. To reduce the hardware implementation area, we proposed the use of the 64-bit key version. The architecture of the LED block cipher is presented in Figure 2.

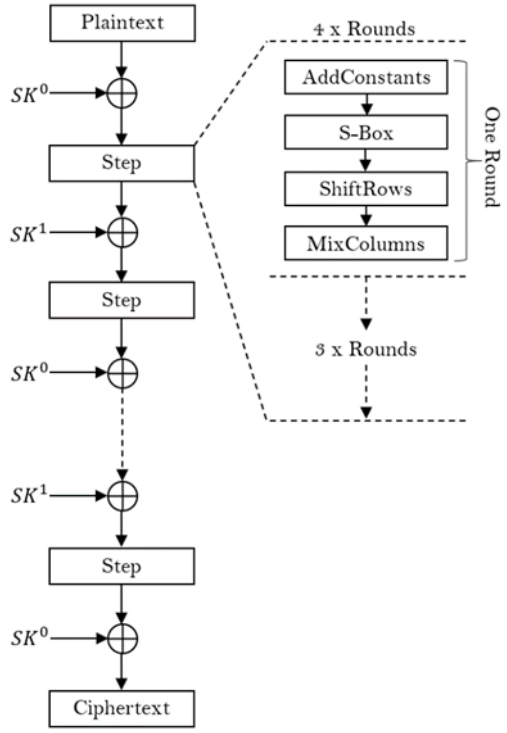

Figure 2. Encryption process of the LED block cipher.

The LED block cipher presents good resistance against many attacks, such as side-channel attacks and replay attacks. Its combination of the SPN and the hash function raises its security level compared to other lightweight cryptography algorithms. The LED block cipher was proposed for V2V communication security due to its low computation overhead and its high security level. It allows encrypting/decrypting messages in real time while preserving confidentiality.

3.2. Temporary Group Key Management

Generally, each connected vehicle is registered to a trusted authority with a unique identity. For V2V communication, the real identity of the vehicle stays anonymous, and a

pseudo-identity is used instead. Connected vehicles have a data table that contains security parameters. The data table is updated regularly each time that the vehicle connects to the trusted authority for security purposes. In the proposed method, we consider that all vehicles in the communication group have a public key.

To start V2V communication, a group of vehicles must be established. Vehicles in the predefined area can communicate with each other. There are many group establishment techniques, so we assume that the most powerful group establishment technique was applied, and we did not consider this task in the proposed method. A group establishment example is presented in Figure 2. Communication between the vehicles can allow sharing of warning messages and media content.

After the group's establishment, one of the vehicles in the group is elected to be the group manager. This vehicle is responsible for communication organization and key management. Clustering algorithms [21] are the most used for group manager vehicles. The election of the group manager vehicle is based on many features, such as stability and confidentiality. The group manager vehicle election was not considered in this work, and we assume that one of the existing algorithms was applied to choose the group manager.

Assuming that all vehicles in the group have the proposed encryption algorithm, each vehicle will generate a temporary private key to join the group communication. Also, we assume that all vehicles have uploaded the public key from a trusted authority or service provider in the registration step. Registration and identification are beyond the scope of this work.

The group manager vehicle collects the identities of the vehicles that joined the group. Each vehicle requests to join the group through an encrypted message based on the public key. After group establishment and the establishment of the group manager vehicle, each vehicle of the group starts requesting private key messages and sends them to the group manager vehicle. After that, it generates response messages to enable group vehicles to generate private keys. Each vehicle in the group computes its private key for V2V communication. The private key allows vehicles to communicate with each other, not like the public key, which allows the vehicles to communicate only with the group manager vehicle.

To generate the private key, the group manager vehicle responds to key requests with a message containing a pseudo key used to generate the private key. Then, vehicles compute the PHOTON hash function of the LED block cipher on the response message from the group manager vehicle. In LED, this function is called Mix-Columns, which is a multiplication of the input by a 4×4 matrix. The multiplication matrix M is presented in Equation (1).

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 4 & 1 & 2 & 2 \end{pmatrix}^4 = \begin{pmatrix} 4 & 1 & 2 & 2 \\ 8 & 6 & 5 & 6 \\ B & E & A & 9 \\ 2 & 2 & F & B \end{pmatrix} \quad (1)$$

The generated private key is used to decrypt messages from vehicles in the group and encrypt messages sent by the vehicle.

To eliminate potential attacks, we proposed regenerating the private keys each minute or in case of detecting a malicious vehicle or unauthorized access. In both cases, the group manager vehicle sends a warning message to all members. After that, the members send key requests, and the group manager vehicle responds with the pseudo keys. Finally, the vehicles compute their new private keys and communicate as normal. The proposed mechanism allows for avoiding many types of attacks.

3.3. Security Analysis

To prove the efficiency of the proposed protocol, we investigated its resistance against many types of attacks. In most attacks, the hacker will try to modify the message or distribute the wrong warning messages. Therefore, it will try to enter the communication

as a member or group manager. In this section, we investigate each attack type and the resistance of the proposed protocol against this attack.

3.3.1. Impersonation Attack

In this type of attack, the hacker tries to act as a member of the communication group. There are two cases of this attack. First, the hacker tries to act as one of the communication members. It will try to randomly guess the private key. The proposed protocol presents a good resistance against this type of attack, since the private key is generated through a hash function that impersonates each vehicle and is not shared, which makes it too hard to guess it. Second, the hacker tries to act as the group manager's vehicle by intercepting the communication between members and the group manager's vehicle. In this case, the real group manager vehicle will detect the potential attack and will send warning messages to all members, and the rekeying process will be enabled if the attack fails.

3.3.2. Stolen Identity Attack

This attack is based on stealing the identity of one of the vehicles in the communication group. Even in case the hacker steals the identity, it cannot communicate with the group for a long duration. When the rekeying process is activated, the group manager vehicle will detect the replicated identity and will block the access of the malicious vehicle.

3.3.3. Public Key Guessing Attack

The hacker will try to guess the public key that joined the communication group. In this case, the public key allows communication with the group manager vehicle only. Then, it will verify the identity of the joining vehicle. Therefore, in the case of an unregistered vehicle, the attack fails.

3.3.4. Untraceable Attack

This attack is performed by collecting communication messages and interrupting them to detect repeated information. The keys are updated each minute, and this results in different messages. The proposed protocol is based on generating random pseudo keys for a private key generation, which makes it resistant to untraceable attacks.

3.3.5. Man-in-the-Middle Attack

In this type of attack, the hacker alters the communication between vehicles by making an independent connection that allows it to control the communication. In the proposed protocol, communication with the group manager cannot be established without passing by the group manager vehicle, which checks the identity of the members. This makes the proposed protocol able to avoid this type of attack.

3.3.6. Eavesdropping

Adversaries engage in the interception and surveillance of V2V communication in order to obtain confidential data. The aforementioned assault undermines the preservation of secrecy and has the potential to result in breaches of privacy. The proposed protocol presents a reliable key-generation process that prevents attackers from extracting confidential data.

3.3.7. Message Tampering

The content of messages transmitted between cars can be modified by malicious actors. The potential consequences of tampering with safety-critical communications include the dissemination of inaccurate traffic information, the provision of misleading warnings, and the increased risk of accidents. The proposed protocol was designed to guarantee safe communication by blocking any malicious member that tries to enter the group.

3.3.8. Replay Attacks

Replay attacks include the unauthorized acquisition and subsequent retransmission of authentic communications by malicious actors at a later point in time. This phenomenon can lead to the recurrence of activities or the introduction of inaccurate information into the network. The proposed protocol has the potential to detect such attacks, since the group manager is charged with regulating the communication process.

3.3.9. Denial of Service (DoS) Attacks

The V2V communication network experiences a significant influx of traffic from malicious actors, resulting in the saturation of communication channels and consequent disruption of the timely delivery of valid communications. The aforementioned phenomenon has the potential to negatively impact the efficiency and effectiveness of traffic control systems, as well as compromise safety applications. The proposed key regeneration process was designed to eliminate such attacks by regenerating the public key frequently.

3.3.10. Sybil Attacks

Sybil attacks include the fraudulent representation of several genuine vehicles by a single hostile entity, resulting in the transmission of misleading information, traffic congestion, and potential accidents caused by the dissemination of faulty data. This attack is avoided by the reliable authentication process and private key generation process.

3.3.11. Message Fabrication

Attackers engage in the production and insertion of fabricated communications inside the V2V network. These communications have the potential to disseminate false information, generate ambiguity, or impede the smooth flow of traffic. Even if this attack is achieved, it will be removed in the next key regeneration process by blocking the malicious member.

3.3.12. Key Compromise

In the event that the encryption keys employed to safeguard V2V communication are compromised, malevolent actors possess the ability to illicitly infiltrate the network, decipher sent communications, and conceivably execute additional offensive maneuvers. The proposed protocol was developed with security concerns in mind; this attack was eliminated by the proposed public key sharing and private key generation.

3.3.13. Physical Layer Attacks

Adversaries possess the capability to impede the physical layer of V2V communication through signal jamming, interference induction, or radio frequency disruption. These assaults have the potential to negatively impact the dependability of communication. This attack is avoided through the authentication of trusted members.

4. Experiments and Results

In this section, we present the experiment environment used to simulate the proposed protocol and we investigate the achieved results with a deep discussion. The proposed protocol was evaluated in terms of computation overhead, cost, power consumption, and processing time. Then, a comparison against the most recent works was conducted.

The proposed protocol was implemented using VHLD on the Xilinx Zynq-7020 board. Vivado HLS software (Version 2019.2) was used to synthesize the proposed protocol. The hardware device is a low-power FPGA with high capabilities that allow it to achieve high performance with a minimum cost and energy consumption.

We start by evaluating the performance in terms of computation overhead and cost. The hardware implementation of the proposed protocol was divided into three parts, and each was evaluated separately. The first part is the encryption process by the LED block cipher. The second part is the decryption process of the encryption algorithm. The last

part is the proposed protocol with encryption, decryption, and key generation processes. Table 1 presents the achieved results of the implementation area of the encryption process. This process has equipped only 140 LUT Flip Flop Pairs, which is less than 0.3% of the total available pairs.

Table 1. Implementation area of the encryption process.

Name	Slice LUTs (53,200)	Slice Register (106,400)	Slice (13,300)	LUT as Logic (53,200)	LUT Flip Flop Pairs (53,200)	Bonded IOB (125)	BUFGCTRL (32)
Top-level	365	210	106	365	140	29	1
Control unit	104	12	49	104	6	0	0
Datapath	261	198	100	261	55	0	0

Table 2 presents the results of the implementation area of the decryption process. A total of 138 LUT Flip Flop Pairs were used for the implementation of the decryption process, which is similar to the encryption process due to the use of the same path for encryption and decryption on the LED block cipher. The main difference is in the control unit, which requires more pairs in the decryption process.

Table 2. Implementation area of the decryption process.

Name	Slice LUTs (53,200)	Slice Register (106,400)	Slice (13,300)	LUT as Logic (53,200)	LUT Flip Flop Pairs (53,200)	Bonded IOB (125)	BUFGCTRL (32)
Top-level	364	210	104	364	138	29	1
Control unit	80	12	34	80	7	0	0
Datapath	284	198	198	284	67	0	0

Table 3 presents the results of the implementation area of the proposed protocol, including the encryption–decryption and key generation processes. The proposed protocol occupied a total of 212 LUT Flip Flop Pairs. The proposed protocol required only 0.39% of the available resources. Only 30 Input/Output Blocks (IOB) were required from the 125 available ones. A low number of slice registers was required, with a less than 0.1% utilization rate. The results show that the proposed protocol achieved a high balance between the security level and the implementation area. It was proven that the proposed protocol has a low computation overhead and cost.

Table 3. Implementation area of the proposed protocol.

Name	Slice LUTs (53,200)	Slice Register (106,400)	Slice (13,300)	LUT as Logic (53,200)	LUT Flip Flop Pairs (53,200)	Bonded IOB (125)	BUFGCTRL (32)
Top-level	608	214	162	608	212	30	1
Control unit	184	16	63	184	16	0	0
Datapath	424	198	154	424	67	0	0

To the best of our knowledge, we are the first to investigate a hardware implementation of a V2V communication protocol. Most of the existing work focuses on the software implementation of their proposed protocols. Therefore, the implementation area cannot be used as a comparison metric against state-of-the-art methods.

More evaluation metrics have been investigated to prove the efficiency of the proposed protocol. We moved on to evaluating the power consumption of the proposed protocol, since it is a critical metric that decides the efficiency of the communication protocol. Figure 3 presents the power consumption of the encryption process. This process has a static power of 1.04 watts and a dynamic power of 17.962 watts.

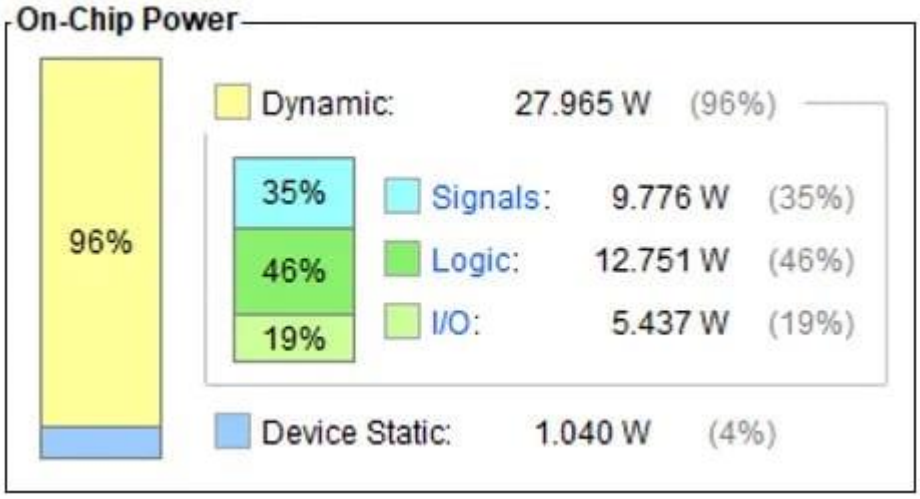

Figure 3. Power consumption of the decryption process.

Figure 4 presents the power consumption of the proposed protocol. The static power remained the same for the encryption and decryption process, and the dynamic power consumption was raised to 35.110 watts. That is due to the presence of the key generation process that runs dynamically. The achieved results of the power consumption have proved the efficiency of the proposed protocol for implementation on edge devices with limited power resources. All of the proposed V2V communication protocols were evaluated on desktops or laptops, which makes it impossible to estimate their power consumption values. Therefore, the proposed protocol cannot be compared to existing protocols based on power consumption.

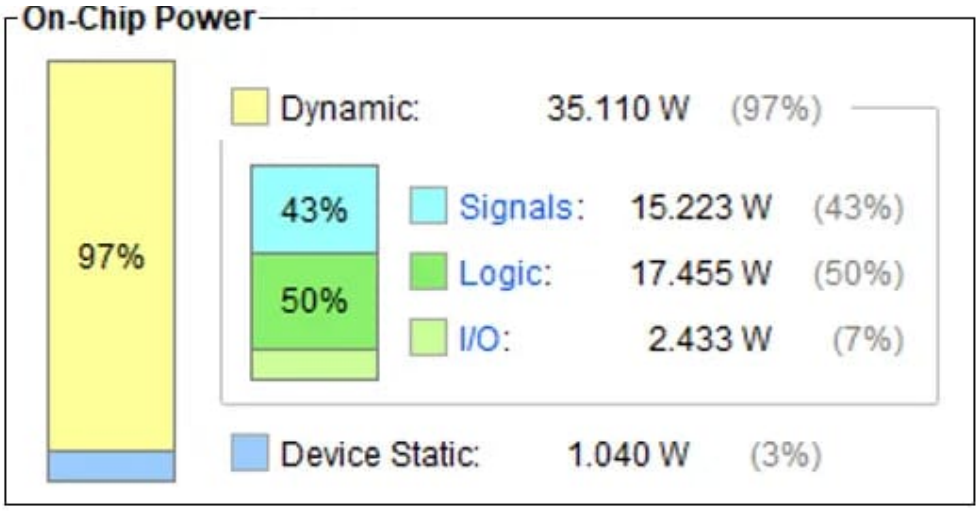

Figure 4. Power consumption of the proposed protocol.

A very critical metric that decides the performance of a communication protocol is the processing time. We have evaluated the processing time of all processes, including the encryption, decryption, and protocol. Figure 5 presents the processing time of the encryption process. This process requires only 8.728 ns to perform, which is a very fast processing time.

```
Timing Report

Slack:                    inf
  Source:                 Inst_control_unit/round_count_reg[0]/C
                            (rising edge-triggered cell FDCE)
  Destination:            Inst_Datapath/state_reg_reg[54]/D
  Path Group:             (none)
  Path Type:              Max at Slow Process Corner
  Data Path Delay:        8.728ns  (logic 1.169ns (13.394%)  route 7.559ns (86.606%))
  Logic Levels:           9  (FDCE=1 LUT2=1 LUT4=3 LUT5=3 LUT6=1)
```

Figure 5. Processing time of the encryption process.

Figure 6 presents the processing time of the decryption process. This process requires 8.332 ns to perform. Such a processing time easily allows for achieving real-time processing. Each vehicle can decrypt more than a thousand messages without any delay.

```
Timing Report

Slack:                    inf
  Source:                 Inst_control_unit/round_count_reg[1]/C
                            (rising edge-triggered cell FDCE)
  Destination:            Inst_Datapath/state_reg_reg[27]/D
  Path Group:             (none)
  Path Type:              Max at Slow Process Corner
  Data Path Delay:        8.332ns  (logic 1.226ns (14.715%)  route 7.106ns (85.285%))
  Logic Levels:           8  (FDCE=1 LUT2=1 LUT3=1 LUT4=1 LUT5=1 LUT6=3)
```

Figure 6. Processing time of the decryption process.

Figure 7 presents the processing time of the proposed protocol. Only 13.619 ns are needed to run the proposed protocol. The achieved results proved that real-time processing is guaranteed with the proposed communication protocol. The hardware implementation was optimized to achieve high performance while focusing on the high security level.

```
Timing Report

Slack:                    inf
  Source:                 Inst_control_unit/round_count_reg[0]/C
                            (rising edge-triggered cell FDCE)
  Destination:            Inst_Datapath/state_reg_reg[52]/D
  Path Group:             (none)
  Path Type:              Max at Slow Process Corner
  Data Path Delay:        13.619ns  (logic 2.158ns (15.845%)  route 11.461ns (84.155%))
  Logic Levels:           15  (FDCE=1 LUT2=1 LUT4=4 LUT5=4 LUT6=5)
```

Figure 7. Processing time of the proposed protocol.

Since all proposed protocols have reported their processing time, we compared the achieved results with state-of-the-art protocols. Table 4 presents a comparison of the achieved results in terms of processing time against state-of-the-art protocols.

Table 4. Comparative study according to the processing time.

Protocol	Key Generation	Encryption	Decryption
Huang et al. [22]	20.4 ms	6.55 ms	3.65 ms
Aliev et al. [11]	0.75 µs	2.85 µs	6.42 µs
Proposed	5.34 ns	8.728 ns	8.332 ns

The timing performance of the proposed protocol outperforms state-of-the-art protocols by a big margin. The key generation process in existing methods depends on the connection to the trusted authority. Huang et al. [22] have a slow key generation time due to the communication to the trusted authority through roadside units. The key generation time grows according to the number of connected vehicles to the group. Aliev et al. [11] have a better processing time but are still slow due to the need for a connection to the trusted authority for each key generation. For the proposed protocol, the key generation process does not need any external connection, and the group manager vehicle is responsible for initial key generation and distribution. Then each vehicle generates its private key for communication. Moreover, the key generation process was not affected by the number of connected vehicles. The proposed protocol can run in areas without an internet connection or roadside infrastructure. Moreover, the proposed protocol was implemented in hardware with the desired specifications, which makes it more suitable than software-designed protocols.

5. Conclusions

Connected vehicles are the future of transportation and play a big role in accident prevention and enhancing the performance of autonomous vehicles. However, V2V communication raises security issues. The communication must be secure and authenticated. In this paper, we proposed a secure communication protocol based on temporary private key management and a lightweight cryptography algorithm for message encryption. The proposed key management was designed to eliminate communication with the infrastructure to achieve real-time processing and more reliability. The light encryption device (LED) block cipher was used for data encryption. LED is featured with a small footprint, low power consumption, and a high security level, which make it suitable for V2V communication based on edge devices with limited resources. Reported results of the implementation of the proposed protocol prove its efficiency in terms of implementation area, power consumption, and processing time. Compared to state-of-the-art protocols, the proposed protocol has better performance and is considered more reliable due to its resistance to many types of attacks. In future works, the proposed protocol will be extended for vehicle-to-everything (V2X) and vehicle-to-infrastructure (V2I) communication. In this context, we will investigate the integration of cellular communication, such as LTE and 5G.

Author Contributions: Conceptualization, S.B. and Y.S.; data curation, F.S.A.; formal analysis, H.E.A.; funding acquisition, S.B. and F.S.A.; investigation, F.S.A.; methodology, Y.S. and H.E.A.; project administration, S.B.; resources, F.S.A. and H.E.A.; software, F.S.A.; supervision, S.B.; validation, S.B. and Y.S.; visualization, Y.S.; writing—original draft, Y.S. and H.E.A.; writing—review and editing, Y.S. and S.B. All authors have read and agreed to the published version of the manuscript.

Funding: Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia—project number MoE-IF-UJ-22-04220772-5.

Data Availability Statement: Data will be made available on request.

Acknowledgments: The authors extend their appreciation to the Deputyship for Research & Innovation, Ministry of Education in Saudi Arabia for funding this research work through project number MoE-IF-UJ-22-04220772-5.

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

References

1. Coppola, R.; Morisio, M. Connected car: Technologies, issues, future trends. *ACM Comput. Surv. (CSUR)* **2016**, *49*, 1–36. [CrossRef]
2. Ayachi, R.; Said, Y.; Ben Abdelaali, A. Pedestrian Detection Based on Light-Weighted Separable Convolution for Advanced Driver Assistance Systems. *Neural Process. Lett.* **2020**, *52*, 2655–2668. [CrossRef]
3. Ayachi, R.; Afif, M.; Said, Y.; Abdelali, A.B. Real-time implementation of traffic signs detection and identification application on graphics processing units. *Int. J. Pattern Recognit. Artif. Intell.* **2021**, *35*, 2150024. [CrossRef]
4. Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; et al. Experimental security analysis of a modern automobile. In Proceedings of the 2010 IEEE Symposium on Security and Privacy (SP), Berleley/Oakland, CA, USA, 16–19 May 2010; pp. 447–462.
5. Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.; Koscher, K.; Czeskis, A.; Roesner, F.; Kohno, T. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the USENIX Security Symposium, San Francisco, CA, USA, 8–12 August 2011; Volume 4, pp. 447–462.
6. Ghafarian, A.; Sardari, S. An Analysis of Connected Cars Technology and Security. In Proceedings of the Teoksessa International Conference on Cyber Warfare and Security, Norfolk, VA, USA, 12–13 March 2020; Volume 14, pp. 195–203.
7. McKay, K.; Lawrence, B.; Meltem, S.T.; Nicky, M. *Report on Lightweight Cryptography. No. NIST Internal or Interagency Report (NISTIR) 8114 (Draft)*; National Institute of Standards and Technology: Gaithersburg, MA, USA, 2016.
8. Guo, J.; Peyrin, T.; Poschmann, A.; Robshaw, M. The LED block cipher. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Springer: Berlin/Heidelberg, Germany, 2011.
9. Miles, E.; Emanuele, V. Substitution-permutation networks, pseudorandom functions, and natural proofs. *J. ACM (JACM)* **2015**, *62*, 1–29. [CrossRef]
10. Vasudev, H.; Deshpande, V.; Das, D.; Das, S.K. A Lightweight Mutual Authentication Protocol for V2V Communication in Internet of Vehicles. *IEEE Trans. Veh. Technol.* **2020**, *69*, 6709–6717. [CrossRef]
11. Aliev, H.; Kim, H.; Choi, S. A Scalable and Secure Group Key Management Method for Secure V2V Communication. *Sensors* **2020**, *20*, 6137. [CrossRef] [PubMed]
12. Han, B.; Peng, S.; Wu, C.; Wang, X.; Wang, B. LoRa-based physical layer key generation for secure v2v/v2i communications. *Sensors* **2020**, *20*, 682. [CrossRef] [PubMed]
13. Yuliana, M. An Efficient Key Generation for the Internet of Things Based Synchronized Quantization. *Sensors* **2019**, *19*, 2674. [CrossRef] [PubMed]
14. Wu, L.; Sun, Q.; Wang, X.; Wang, J.; Yu, S.; Zou, Y.; Liu, B.; Zhu, Z. An efficient privacy-preserving mutual authentication scheme for secure V2V communication in vehicular ad hoc network. *IEEE Access* **2019**, *7*, 55050–55063. [CrossRef]
15. Yao, Y.; Shu, F.; Li, Z.; Cheng, X.; Wu, L. Secure Transmission Scheme Based on Joint Radar and Communication in Mobile Vehicular Networks. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 10027–10037. [CrossRef]
16. Kumar, J.S.; Gupta, A.; Tanwar, S.; Kumar, N.; Akleylek, S. Security enhancement in cellular networks employing D2D friendly jammer for V2V communication. *Clust. Comput.* **2023**, *26*, 865–878. [CrossRef]
17. Tayeb, S.; Pirouz, M.; Esguerra, G.; Ghobadi, K.; Huang, J.; Hill, R.; Lawson, D.; Li, S.; Zhan, T.; Zhan, J.; et al. Securing the positioning signals of autonomous vehicles. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 4522–4528.
18. Reddy, V.K.; Surya, R.; Reddy, A.; Kumar, P.S. FPGA Implementation of Present Algorithm with Improved Security. In Proceedings of the 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 12–14 June 2019; pp. 404–409.
19. Moradi, A.; Poschmann, A.; Ling, S.; Paar, C.; Wang, H. Pushing the limits: A very compact and a threshold implementation of AES. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, 15–19 May 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 69–88.
20. Guo, J.; Peyrin, T.; Poschmann, A. The PHOTON family of lightweight hash functions. In *Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2011*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 222–239.
21. Jiankang, Y.; Yingying, C.; Shifeng, S. Research of clustering and group leader election algorithm on hierarchy Ad Hoc Network. In Proceedings of the 2016 15th International Conference on Optical Communications and Networks (ICOCN), Hangzhou, China, 24–27 September 2016; pp. 1–3.
22. Huang, Q.; Yang, Y.; Shi, Y. SmartVeh: Secure and efficient message access control and authentication for vehicular cloud computing. *Sensors* **2018**, *18*, 666. [CrossRef] [PubMed]