Image Processing, Electronics and Computers
L. Trajkovic et al. (Eds.)

doi:10.3233/ATDE240515

Design and Implementation of User Authentication Mechanism for Vehicle-to-Everything Based on FPGA

Changrong YU and Xuxiu ZHANG[1]
School of Automation and Electrical Engineering, Dalian Jiaotong University, Dalian 116052, PR China

Abstract. Aiming at the problem that the current vehicle communication authentication mechanism lacks hardware verification, this paper proposes a new Vehicle-to-Everything(V2X) user authentication mechanism based on FPGA (Field Programmable Gate Array), aiming at improving the safety and reliability of vehicle communication. The mechanism adopts One-Time Password (OTP), Elliptic curve cryptography (ECC) and Secure Hash Algorithm 2 (SHA-2) to realize a highly secure authentication process, and the above algorithms are implemented in FPGA. Compared with the security and resource cost of using a single cryptography mechanism, this paper is effective in authentication, collision resistance, replay attack, man-in-the-middle attack and identity forgery attack, and completes information encryption processing in microsecond level, which improves the performance and reduces the resource occupation, which proves the security and effectiveness of the proposed method in the case of vehicle-mounted equipment with limited resources.

Keywords. FPGA, Internet of vehicles, Vehicle communication, Authentication

1. Introduction

In recent years, car networking technology, as an important branch of the Internet of Things, is developing rapidly and profoundly changing people's travel modes and traffic safety standards. Among them, scenes such as Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V) and Vehicle-to-Pedestrian (V2P) not only improve the efficiency of traffic management, but also improve the efficiency of traffic management[1-3].

The rapid development of the internet of vehicles has provided important support for the realization of intelligent transportation system[4], and it has become a reality to remotely control vehicle driving by mobile phone. For example, users can remotely start the vehicle, unlock the door and even control the driving of the vehicle through smart phones[5]. However, with the wide application of V2X technology, this convenience has also brought security risks, and the security problem of user authentication in the communication process has become increasingly prominent.

The realization of V2X communication technology mainly depends on two technologies: dedicated short range communications (DSRC) and Cellular-Vehicle-to-

[1] Corresponding Author: Xuxiu Zhang, zhangxuxiu@163.com

Everything (C-V2X). DSRC is a wireless communication technology based on IEEE 802.11p standard, which can provide high-speed and low-delay communication services in a short distance[6]. C-V2X is a communication mode based on cellular network technology, which provides a wider communication coverage for vehicles by using LTE or 5G network[7]. These two technologies have their own advantages. DSRC has better communication performance in densely populated areas, while C-V2X can achieve wider geographical coverage. The main application scenarios of V2X communication include but are not limited to: vehicle safety early warning, traffic signal priority control, intelligent navigation, road condition monitoring, etc. By exchanging information such as vehicle position, speed and driving direction in real time, V2X technology can effectively prevent traffic accidents, improve road capacity and reduce energy consumption. However, at the same time of data interaction, user identity verification is indispensable.

There are some security risks in traditional user authentication methods, such as password leakage, man-in-the-middle attack and so on. In order to solve these security problems, Khalid H and others proposed a Time-based One-time Password (TOTP) authentication mechanism[8]. OTP is a temporary password, which will generate an unrepeatable password every time it is used, effectively preventing the risk of password theft. However, at present, most authentication schemes based on OTP are mainly implemented by software, which is vulnerable to malicious software attacks. Unauthorized access may lead to vehicle theft or malicious manipulation, and cyber attacks may threaten the safety of vehicles and their passengers[9]. Therefore, it is very important to study a safe and reliable V2X user authentication mechanism to ensure the safety of remote control of vehicle driving by mobile phone. The traditional V2X user authentication method mainly relies on the combination of user name and static password, which is realized by software and network protocol[10]. This method is simple and easy to use, but its security is low, and it is vulnerable to violent cracking and stealing attacks. In addition, there is an authentication method based on Public Key Infrastructur (PKI), which verifies the identity of users through digital certificates[11]. Although PKI method improves security to some extent, its certificate management process is complex and requires high computing resources.

As a programmable hardware platform, FPGA has been applied in many fields. It has high flexibility and programmability, can realize parallel processing, effectively support complex algorithms, improve calculation efficiency, and reduce delay and resource consumption[12]. In recent years, researchers began to explore the application of FPGA in the field of authentication and encryption to improve security and performance[13]. However, most research focuses on traditional encryption algorithms, such as the performance optimization of AES and RSA(Ron Rivest, Adi Shamir, Leonard Adleman)[14]. There is little research on the combination of one-time password and ECC.

In order to further improve the security of V2X user authentication, this paper proposes a new user authentication mechanism based on FPGA combined with OTP, ECC and SHA-2 hash function algorithm. The results of performance analysis show that, compared with using single cryptography, the verification mechanism in this paper has multiple security improvements, such as authentication, collision resistance, replay attack, man-in-the-middle attack and identity forgery attack, etc. At the same time, it can complete information encryption processing at microsecond level, and the resource occupation is reduced while improving performance. Therefore, this scheme

has important theoretical significance and application value in the environment of vehicle-mounted equipment with limited resources.

2. Related Algorithm

2.1. OTP

OTP algorithm is a dynamic password mechanism. Every authentication will generate a new password, which will change in the next authentication, thus increasing security. The security of OTP algorithm is based on the unpredictability and one-time use of keys, which can effectively prevent password theft and replay attacks[15]. OTP algorithm can be based on time, such as TOTP, or counting, such as HOTP (HMAC-based one-time password), in which TOTP is the most common form. The following is the formula of TOTP algorithm combined with SHA-2:

$$TOTP = (HMAC - SHA - X(K, T)\ [Truncate]\ )\ \mathrm{mod}\ M \tag{1}$$

Where k is a key share between that vehicle-mounted terminal and the user terminal, and the key is use for generating and verifying a one-time password. T is the current timestamp. HMAC-SHA-X(K, T) is used to hash the time stamp t using hash-based message authentication code (hmac) and hash functions (such as SHA-224 and SHA-256), and the key is K.X represents the selected SHA-2 variant (e.g. 224, 256, 384, 512). Truncate is a truncation operation, which removes the last n bits of SHA-X hash value (n depends on the required one-time password length). For example, if a 6-digit password is required, the last 20 digits of the hash value may be taken (6 digits correspond to 20 binary digits). M is the modulus, which is usually a power of 10 (for example, for a 6-digit password, m = 10 6). (HMAC-SHA-X(K, T) [Truncate]) mod M is to modulo m the truncated SHA-X hash value to get the final one-time password.

This paper will choose TOTP, which provides a good balance between security and performance. The server will finally generate OTP according to the current timestamp and the specific information of users (such as user information and vehicle authentication code). This password will only be used once in the authentication process, and then it will expire immediately, which is used to provide an additional layer of security during the user authentication process. In addition, the vehicle terminal, the user terminal and the server need to keep time synchronization to ensure the accuracy, consistency and timeliness of the one-time password.

2.2. SHA-2

SHA-2 is a set of cryptographic hash functions. SHA-2 includes several different variants, including SHA-224, SHA-256, SHA-384, SHA-512, etc. The most commonly used ones are SHA-256 and SHA-512. The core principle of SHA-2 algorithm includes the following steps:

(1)Padding: The input message is padded to a multiple of 512 bits, and the length of the original message is represented by adding a 1, followed by several 0s, and finally a 64-bit length field.

(2)Initializing hash value: An initial 256-bit hash value is used according to the used SHA-2 variant SHA-256.

(3)Segmentation: The filled message is divided into 512-bit blocks, and each block is further divided into a plurality of 32 bits (for SHA-256).

(4)Message expansion: For SHA-256, 16 32-bit words in the message block are expanded to 64.

(5)Processing message blocks: Each message block is processed through a series of complex functions, including bit operations (such as XOR, AND, NOT, OR) and modular addition.

(6)Loop iteration: For each input block, the algorithm performs a series of loop iterations, and the hash value is updated every iteration. After the above processing, a hash value is finally generated.

SHA-256 algorithm will be selected as SHA-X in TOTP algorithm. In the process of identity verification, the vehicle takes the generated TOTP and related user information as input and uses SHA-2 algorithm to process it. Compared with other hash algorithms (such as MD5, SHA-1 and SHA-3), SHA-2 has the following advantages:

(1)Security: SHA-2 is more secure than MD5 and SHA-1. Both MD5 and SHA-1 have been proved to have many vulnerabilities, such as collision attack, that is, the possibility of finding two different input messages but producing the same hash value is very low. SHA-2 has not found an effective attack method so far.

(2)Output length: SHA-2 provides output options with different lengths (such as SHA-224, SHA-256, SHA-384, SHA-512), which provides flexibility for different application scenarios.

(3)Performance: By implementing SHA-2 algorithm on FPGA, the speed of hash calculation can be improved, and real-time hash calculation can be realized, which is very important for application scenarios that need rapid response. Compared with SHA-3, its performance is usually not as good as SHA-2, especially in hardware implementation, and some scenarios need more resources. In a word, SHA-2 algorithm has obvious advantages over other algorithms in terms of security and performance, and the implementation of SHA-2 algorithm on FPGA can further improve the performance, security and flexibility, so it is suitable for many occasions, especially in the environment that requires high security, and can reduce the use of resources.

2.3. ECC

ECC is a public key encryption technology based on elliptic curve mathematics, which provides an efficient and safe method for encryption, decryption, digital signature and other cryptographic operations. The basic principle, formula and definition of ECC are as follows:

$$y^2 \equiv x^3 + ax + b \pmod{p} \tag{2}$$

Among them, p is a big prime number, a and b are constants defined on a finite field, and the recommended field widths are n=163, 233 and 283.

(1) point addition operation: For two points on the elliptic curve P=(x1,y1) and Q=(x2,y2), the point addition operation P+Q is defined as: when q is an infinite

Identity Element, P+Q = P When q is not an infinite point and P ≠ Q, calculate the slope.

$$e = (y2 - y1) / (x2 - x1) \tag{3}$$

Then calculate the result point R = (x3, y3), where:

$$x3 = e^2 - x1 - x2 \pmod p \tag{4}$$

$$y3 = e * (x1 - x3) - y1 \pmod p \tag{5}$$

(2) Point multiplication operation: For the point p on the elliptic curve and an integer n, nP means to add the point p to itself repeatedly for n times. The calculation of point multiplication can be carried out by double addition algorithm.

(3) Key Generation: Select an elliptic curve e and a base point g, where the Order of g is n, randomly select a private key d, and if $1 < d < n$, calculate the public key k = d * g.

In this paper, the key pair will be generated by ECC, and then the OTP message will be processed by SHA-2 algorithm by using elliptic curve digital signature algorithm (ECDSA), and then the digital signature will be generated by using the private key of vehicle-mounted FPGA ECC, and then the shared secret key P = d*K_other will be generated by combining with the public key of mobile ECC to encrypt the message. Compared with RSA encryption, it has lower computational complexity[16], and is more concerned in resource-constrained environments, especially in signature and verification operations. ECC has the following advantages:

(1)Resource consumption: ECC provides the same security level as RSA, but the required key length is shorter. The key size of ECC is usually smaller than RSA, and ECC can use shorter keys under the same security level. For example, a 256-bit ECC key provides security equivalent to a 3072-bit RSA key. On FPGA, a shorter key means less consumption of hardware resources.

(2)Computational efficiency: The operation of ECC can be completed in a fixed time, which makes the implementation of ECC on FPGA more efficient.

(3)Performance: The implementation of ECC algorithm on FPGA usually has low energy consumption, which is an important advantage for battery-powered mobile devices and vehicle-mounted systems that need to run for a long time. And the operation speed of ECC is usually faster than RSA, and the operation of ECC (encryption, decryption, signature and signature verification) involves simpler mathematical operations, so it is more efficient than RSA. Because of the higher computational efficiency, ECC usually consumes less energy when performing encryption operations.

3. Design of System Architecture and Verification Mechanism

3.1. System Architecture

In this paper, FPGA is integrated into vehicle ECU(Electronic Control Unit) as a hardware accelerator to realize the processing of one-time password, ECC and SHA-2

algorithm. At the same time, in order to meet the requirements of V2X communication, FPGA will integrate cellular modules. By offloading these computationally intensive tasks to FPGA, the power consumption and delay of the system can be reduced. In addition, the programmable characteristics of FPGA allow the system to flexibly adapt to different security requirements without changing the hardware, update or upgrade the algorithm through reconfiguration, realize customized hardware optimization, and further improve the system performance. FPGA can realize low-latency calculation, which is very beneficial for applications with high real-time requirements.

The system structure is shown in Figure 1. The system consists of mobile devices (such as smart phones), vehicle-mounted FPGA, cellular network base station and server. The mobile device sends a request command to communicate with the vehicle motherboard through the cellular network. The vehicle-mounted FPGA generates and processes the time-based one-time password and its signature, ECC key pair and SHA-2 algorithm, and the server is used for verification and transmission. Thus, a basic framework of V2X communication authentication model is formed.

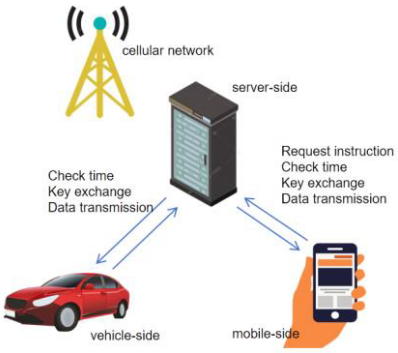

Figure 1. System Structure Diagram.

3.2. Authentication Mechanism

This paper combines FPGA technology with OTP, ECC and SHA-2 for the first time. This combination not only improves security, but also makes full use of the parallel processing ability of FPGA, improves the speed and efficiency of identity verification, and realizes a multi-level efficient and secure protection mechanism. At the same time, it meets the following three requirements of Shannon's indestructible security guarantee[17]: (1) the key must be generated randomly, (2) the key must not be reused, and (3) the key must be safely distributed to the encryption and decryption endpoint devices. Specific verification steps and flow chart (as shown in Figure 2):

Step 1 User request: The user selects the temporary SMS verification code mode in the vehicle control software of the mobile terminal for identity verification, sends a request instruction and preset user information to the vehicle-mounted server, and the system checks the current time.

Step 2 key generation and exchange: when receiving the verification request, detect whether the user equipment information matches. If not, reject the request and authenticate more preset information. When they are consistent, the vehicle-mounted FPGA and the mobile device are initialized, and a pair of new ECC keys, including a private key D and a public key K, are generated respectively. At the same time, it is

necessary to check whether the initialization is completed. The private key of vehicle-mounted FPGA is used to create a digital signature, and its public key is sent to the server for subsequent verification of the digital signature. The public key of the mobile device is sent to the vehicle-mounted FPGA through the server to encrypt the information sent to the mobile device, and its private key is used to decrypt the received encrypted information.

Step 3 message generation: the vehicle-mounted FPGA generates a TOTP based on time and time stamp to ensure that the password generated each time is unique, and digitally signs the TOTP with its private key to create a signed TOTP message.

Step 4 Message encryption: The vehicle-mounted FPGA uses the public key of the mobile device combined with its own private key to generate a shared key, and then encrypts the signed message by ECC. This ensures that only the mobile device with the corresponding private key can decrypt the message.

Step 5 Transmission: The encrypted message is sent from the vehicle-mounted FPGA to the mobile device by wireless communication.

Step 6 The mobile terminal decrypts the message: after receiving the encrypted message, the mobile terminal of the mobile phone decrypts it with its private key to obtain the signed message.

Step 7 Authentication: The mobile device uses the public key of the vehicle-mounted FPGA to verify the signed message to ensure that the message has not been tampered with and really comes from the vehicle-mounted FPGA. (1) Time stamp verification: Time-based OTP has a limited validity period, and its time stamp is verified during authentication. Once it expires, it cannot be used again. (2) Digital signature verification: use the public key of vehicle-mounted FPGA to verify whether the digital signature content is consistent. (3) Verification of verification code: enter the verification code, and the server verifies whether the received verification code matches the verification code sent to the user.

When all the verifications pass, the server confirms the identity of the user, communicates with the mobile terminal of the vehicle terminal and authorizes the mobile device to perform corresponding control operations. If any link fails to verify, the server rejects the request and asks the user to resend the request for re-authentication.

Step 8 Perform vehicle control operation: If the verification is successful, the mobile device can continue to perform vehicle control operation processes, such as starting, stopping, locking, unlocking and moving.

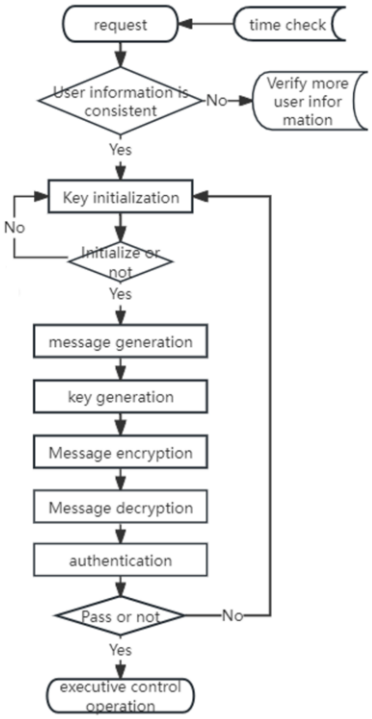

Figure 2. Verification flow chart.

4. FPGA Design and Implementation

4.1. FPGA Related Design

In order to realize the encryption and authentication mechanism based on FPGA, this paper chooses Altera Cyclone IV E P4 CE 115 F 29 C 9L, Quartus II18.0 as the experimental platform, AMD Ryzen 7 4800 U with radeon Graphics 16 Gram as the PC, uses Verilog hardware description language to write the algorithm, and generates the engineering files that can be loaded into FPGA through the steps of synthesis, layout and wiring.

The main modules on FPGA and their corresponding descriptions are as follows:

(1)OTP module: Time stamp, user information and time synchronization signal are used as input data, while clock signal and asynchronous reset signal are input. After being processed by pseudo-random number function realized by Linear congruential generator (LCG), a 32-bit one-time password, a private key D meeting ECC requirements, an OTP valid signal valid_otp and a private key valid signal valid_d are output. The schematic diagram of OTP circuit module is shown in Figure 3 below.

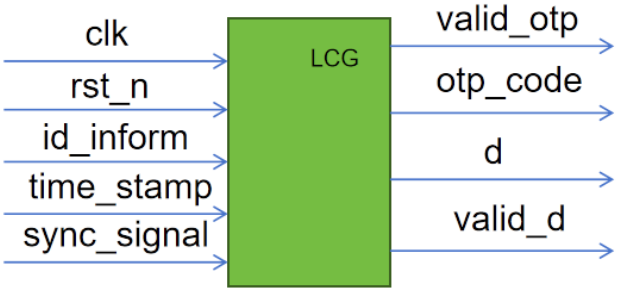

Figure 3. Schematic diagram of OTP module.

(2)SHA-256 module: This module takes otp_code generated by OTP as input data, inputs clock signal, reset signal and OTP valid signal vaild_otp at the same time, performs logic operations such as bit padding, and finally outputs a 256-bit (32-byte) hash message hash_data, a data overflow detection signal overflow_err and a hash completion signal hash_done. The schematic diagram of SHA-256 circuit module is shown in Figure 4 below.

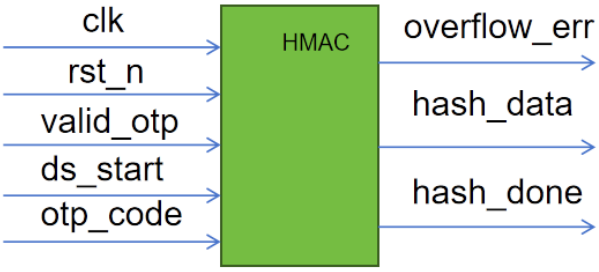

Figure 4. Schematic diagram of SHA-256 module.

(3)ECC module: This module takes point P on the curve, curve coefficient, base point G, private key D and hash message hash_data as input data, and inputs clock signal, reset signal and mode selection signal at the same time. The mode signal is set to 01/10, and when mode=01, it is the public key generation mode, that is, the R point, the public key K and the public key completion signal K _ Done are output through ECC logical operation; When mode=10, it is a digital signature mode, that is, the signature message ds_data and the signature completion signal ds_done are output through the logical operation of elliptic curve digital signature. Based on the existing equipment resources and system performance: when the domain width is 163 bits, it provides enough security to resist the currently known attack methods; Elliptic curves with smaller domain width can provide faster operation speed. Smaller domain width means less resources are occupied in hardware implementation, which is especially important in limited environments, such as embedded systems or car networking devices. Therefore, the domain width will be set to 163 bits, and the schematic diagram of ECC circuit module is shown in Figure 5.

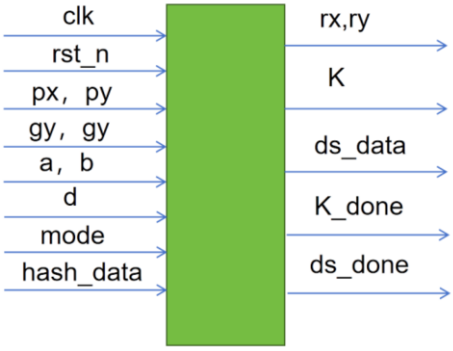

Figure 5. Schematic diagram of ECC module.

4.2. Overall Design

The state transition diagram of the system is shown in Figure 6. Multi-state machines and hierarchical nesting are used in the coding process to improve the processing speed and reduce the use of resources. The start state is ILDE standby sleep state. When receiving the request signal req sent by the server, the system wakes up and enters the OTP module through the synchronization signal sync_signal. OTP sends out a signal valid_otp to enter hash SHA-256 module after calculation, and OTP outputs a private key completion signal d_done to transmit to ECC module at the same time; SHA-256 module sends mode=01 signal to ECC module after completion; ECC module generates a public key and sends out a K_done signal when it receives the signal d_done. When it receives the signal mode=01, it switches to the signature mode mode=10 and starts digital signature. After the signature is completed, the output signal ds_done enters the encryption module encrypt ; . After the encryption is completed, the signal en_done will be output, and it will enter the vehicle-side completion state v_done. The signature message will be sent to the server, and the waiting request signal wait_req will be sent, whether to proceed with the next operation through verification or re-verification, and enter the IDLE state.

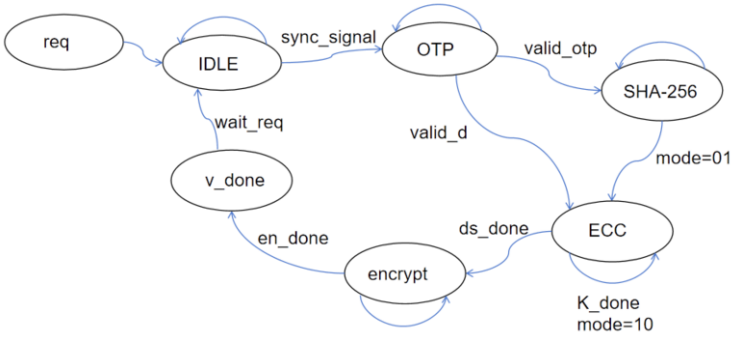

Figure 6. State transition diagram.

5. Performance Analysis

5.1. Security Analysis

5.1.1. Ability to resist replay attacks

Replay attack is an attack method in which an attacker intercepts a packet and resends it at a later time to impersonate a legitimate user. In the authentication mechanism, by using TOTP and SHA-2 combined with ECC, our authentication mechanism will generate a new digital signature every time we communicate, so as to effectively resist replay attacks. Because each authentication request will generate a new authentication message, there is no correct timestamp and one-time password, and it cannot pass the authentication. Even if an attacker intercepts a valid message, due to its one-off nature, the message will be invalid in the next communication, so it cannot be used again.

5.1.2. Ability to resist middleman attacks

Man-in-the-middle attack is an attack method in which attackers secretly intercept and possibly tamper with the communication content between the two parties. By implementing ECC encryption and decryption process on FPGA, the system ensures that the data transmission between the two communication parties is encrypted. Even if the attacker can intercept the data packet, he can't decipher its contents because he doesn't have the corresponding private key to decrypt the information.

5.1.3. Ability to resist collision attack

Collision attack is an attack in which an attacker tries to find two different inputs so that they produce the same output (i.e. hash value or hash value) through a hash function. With the improvement of computing power and the development of attack technology, some hash functions may become unsafe. SHA-2 introduces many design improvements and uses a mechanism called Extended Message Block, XMB), which divides the original message into 512-bit blocks and processes each block. This treatment makes it more difficult to find the collision. It is more secure than the previous version (SHA-1,Secure Hash Algorithm 1), and it is difficult to find two different inputs to produce the same hash value, which helps to prevent the forgery of hash values.

5.1.4. Ability to resist tampering attacks

Tampering attack is that an attacker tries to modify or tamper with information without being detected. The purpose of this kind of attack is to change the content, structure or attribute of information, so as to achieve the attacker's purpose, such as misleading the receiver, destroying the service, stealing sensitive information or committing fraud. Digital signature is a cryptographic technology used to verify the integrity of messages and provide non-repudiation. It can be used to resist tampering attacks, that is, an attacker tries to modify the content of a message without being detected. And the signature message contains timestamp to prove that the signature was generated at a specific time, which further improves the ability to resist tampering attacks.

5.1.5. Ability to resist forged identity attacks

Fake identity attack is an attack method in which an attacker tries to gain unauthorized access by impersonating a legitimate user or device. In our system, we use a complicated authentication process that combines TOTP, ECC key pair and SHA-2 hash algorithm, which makes it difficult for attackers to forge their identities. First of all, the dynamic generation mechanism of TOTP makes it impossible for attackers to predict the next valid password. Secondly, the public key of ECC key pair is unique and associated with a specific user identity. Finally, SHA-2 hashing algorithm ensures the integrity and authenticity of all transmitted data.

See Table 1 for the security comparison of the verification mechanism in this paper with the schemes in references [15], [16] and [18].

Table 1. Safety comparison.

safety performance	The scheme of this paper	References [15]	References [16]	References [18]
Resistance to replay attacks	✓	✓	✓	✓
Resistance to man-in-the-middle attack	✓	✓	✓	✓
Resistance to collision attack	✓	✓	✓	✓
Resistance to tampering attacks	✓			✓
Resist forged identity attacks	✓	✓	✓	✓
Mutual authentication	✓		✓	

5.2. Simulation Result Analysis

Through the comprehensive simulation test of FPGA, as shown in Figure 7, the engineering analysis comprehensive diagram shows the situation of the current design, and Figure 8 shows the situation of the main sub-modules ECC and SHA's ALUTS(Adaptive Look Up Tables). The results are analyzed as follows:

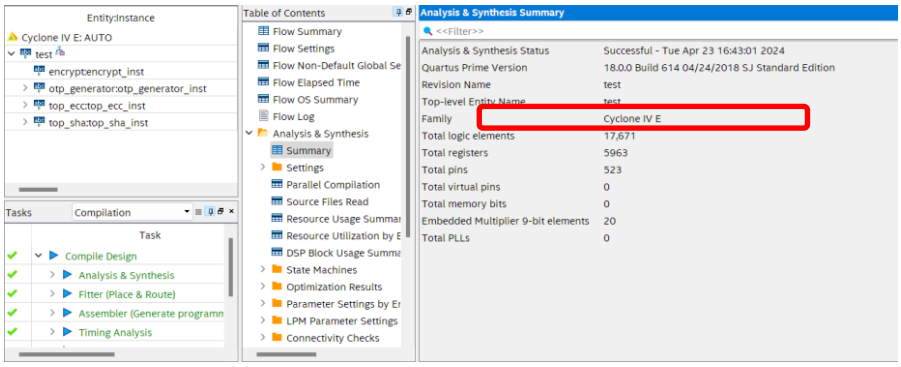

Figure 7. Analysis synthesis figure A.

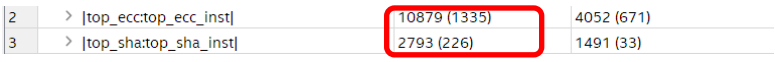

Figure 8. Analysis synthesis figure B.

(1) Processing speed: By measuring the response time required by FPGA to process data requests, the response speed of system authentication is evaluated. The results show that the authentication mechanism based on FPGA in this paper can complete data generation and processing in milliseconds, which meets the real-time requirements.

(2) Resource consumption: By analyzing the resource usage on FPGA, the total logical unit of engineering file is 17671, of which ECC module ALUTS occupies 10879 and SHA-256 module ALUTS occupies 2793, and the peak frequency is 38.97 MHz. Literature [19] the ALUTS which implements ECC algorithm on virtex-5 occupies 18,459, and its peak frequency is 106 MHz ; . The ALUTS implemented on virtex-7 occupies 12272, and its peak frequency is 159 MHz. Literature [20] the logical unit of SHA-256 algorithm implemented in Stratix ii EP2S60F672C3N occupies 4934. Compared with the literature, the hardware consumption of the two main sub-modules is reduced by 41%, 6% and 43%. The design in this paper takes up fewer logic units under the premise of realizing the security function, which can effectively reduce the use of logic resources and can be better applied to the equipment conditions with limited resources.

6. Conclusion and Summary

In this paper, the design of V2X user authentication mechanism based on FPGA has achieved a highly secure user authentication scheme. The combination of one-time password, ECC and SHA-2 algorithm can effectively prevent password leakage and malicious attacks. Through a series of performance evaluations, it has been proved that its efficiency can complete data processing and calculation within milliseconds, and it has multiple security in authentication, collision attack resistance, replay attack, man-in-the-middle attack and forged identity attack. The algorithm realized by FPGA has improved performance and occupied some resources. Analysis and test show that the method proposed in this paper can not only improve the security and reliability of V2X communication, but also provide new ideas and methods for the research and practice of V2X user authentication, and promote the security, reliability and development of intelligent transportation system.

References

[1] Houmer M, Ouaissa M, Ouaissa M. Secure authentication scheme for 5G-based V2X communications. Procedia Computer Science, 2022, 198: 276-281.
[2] Xiong C L. Research on the Application of V2V Technology in Lane Change assistance for autonomous vehicles. Information and Communication, 2020, (02): 15-16.
[3] Malik R Q, Ramli K N, Kareem Z H, et al. An overview on V2P communication system: Architecture and application. 2020 3rd International Conference on Engineering Technology and its Applications (IICETA). IEEE, 2020: 174-178.
[4] Wen X, Li Y. Qualcomm: Using C-V2X technology to improve the future transportation environment. Intelligent Connected Vehicle, 2023,(06):40-42.
[5] Xin Y N, Liu J, Li Q, et al. Design of mobile phone digital key remote control vehicle system. Automotive Engineer, 2018, (10): 23-27.

[6] Li Z J. Research on reliability analysis model of vehicle security communication and security application based on DSRC. Harbin Engineering University, 2022.
[7] Yuan G Y. Technology application of V2X vehicle networking communication module based on 5G. Electronic Technology, 2023, 52(07): 56-57.
[8] Khalid H, Hashim S J, Ahmad S M S, et al. New and simple offline authentication approach using time-based one-time password with biometric for car sharing vehicles. 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE, 2020: 1-7.
[9] Sawade O, Radusch I, Hauswirth M. V2x attack vectors and risk analysis for automated cooperative driving. 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring). IEEE, 2021: 1-6.
[10] Wang X H, Li G C, Wang B H, et al. Application of electronic authentication in V2X Vehicle networking security. Information Security Research, 2020, 8(05): 500-505. (in Chinese)
[11] Yan Se. Research and Application of messaging and Identity authentication Scheme in Vehicle networking environment. Northwest normal university, 2023. DOI: 10.27410/,dcnki.Gxbfu.2023.001435.
[12] Tan B L, Mok K M, Chang J J, et al. RISC32-LP: Low-power FPGA-based IoT sensor nodes with energy reduction program analyzer. IEEE Internet of Things Journal, 2021, 9(6): 4214-4228.
[13] Sureshkumar V, Chinnaraj P, Saravanan P, et al. Authenticated key agreement protocol for secure communication establishment in vehicle-to-grid environment with FPGA implementation. IEEE Transactions on Vehicular Technology, 2022, 71(4): 3470-3479.
[14] La Manna M, Treccozzi L, Perazzo P, et al. Performance evaluation of attribute-based encryption in automotive embedded platform for secure software over-the-air update. Sensors, 2021, 21(2): 515.
[15] Kurniawan D E, Iqbal M, Friadi J, et al. Login security using one time password (OTP) application with encryption algorithm performance. Journal of Physics: Conference Series. IOP Publishing, 2021, 1783(1): 012041.
[16] Khan M A, Quasim M T, Alghamdi N S, et al. A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEE Access, 2020, 8: 52018-52027.
[17] Shannon C E. Communication theory of secrecy systems. The Bell system technical journal, 1949, 28(4): 656-715.
[18] Michail H E, Athanasiou G S, Kelefouras V, et al. On the exploitation of a high-throughput SHA-256 FPGA design for HMAC. ACM Transactions on Reconfigurable Technology & Systems, 2012,5(1):1-28.
[19] Ewing Z, Ge H B. High-performance FPGA implementation of Elliptic curve cryptographic ECC over binary domain. Computer Science, 2019,47(08):127-131.
[20] Li N. Research and FPGA implementation of MD5 and SHA-256 algorithms. Hunan university, 2021. DOI: 10.27135 /, dcnki. Ghudu. 2021.001027.