Hindawi
Journal of Sensors
Volume 2024, Article ID 9804382, 1 page
https://doi.org/10.1155/2024/9804382

Retraction

Retracted: Hardware Optimization and System Design of Elliptic Curve Encryption Algorithm Based on FPGA

Journal of Sensors

Received 23 January 2024; Accepted 23 January 2024; Published 24 January 2024

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope
(2) Discrepancies in the description of the research reported
(3) Discrepancies between the availability of data and the research described
(4) Inappropriate citations
(5) Incoherent, meaningless and/or irrelevant content included in the article
(6) Manipulated or compromised peer review

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] J. Li and W. Gao, "Hardware Optimization and System Design of Elliptic Curve Encryption Algorithm Based on FPGA," *Journal of Sensors*, vol. 2022, Article ID 9074524, 12 pages, 2022.

Hindawi
Journal of Sensors
Volume 2022, Article ID 9074524, 12 pages
https://doi.org/10.1155/2022/9074524

Research Article

Hardware Optimization and System Design of Elliptic Curve Encryption Algorithm Based on FPGA

Jiakun Li[1] **and Wei Gao**[2]

[1]*National Institute of Natural Hazards, Ministry of Emergency Management of China, Beijing 100085, China*
[2]*School of Integrated Circuits and Electronics, Beijing Institute of Technology, Beijing 100081, China*

Correspondence should be addressed to Jiakun Li; jiakunli@ninhm.ac.cn

Received 9 August 2022; Revised 25 September 2022; Accepted 27 September 2022; Published 11 October 2022

Academic Editor: Yaxiang Fan

Since entering the era of big data, the degree of information sharing is getting higher and higher; the information exchange is becoming more and more convenient, but at the same time, personal information is also easy to be exposed to the network environment, if it is used by criminals to lead to information leakage, and then bring certain risks. Therefore, it is in the information age and do a good job of network information security and confidentiality. At present, the security and secrecy of network information are mainly realized by cryptography. Public key cryptography can encrypt information and ensure the security of information transmission, so it is widely used in the contemporary society. At present, elliptic curve encryption is highly respected in the research field of public key cryptosystem. Elliptic curve encryption is divided into two main points, multiplication and inversion, respectively. Through the comparison of these two algorithms, it can be found that there are several choices if the main research objective is to save time, and the Euclidean extension method is mainly discussed in this paper. In other words, more efficient algorithms are used in the hardware implementation process, and a variety of algorithms can be used instead of a single curve algorithm. In this process, we can find the special features of upper level operation and bottom level finite operation. The upper level operation is KP operation, while the bottom level operation is fast calculation of four kinds of K in finite field operation, and finally realize FPGA algorithm. With the help of Quartus ii developed by predecessors, the upper and lower operations of elliptic curve are carried out using VHDL language. Combined ANXIX9.62 in the elliptic curve of each module to test, so as to ensure the accuracy of the data, reduces the error. According to the test results, the designed chip can efficiently complete the elliptic curve encryption system in the whole process. And the average KP operation time can reach 15.15 ms at 20 MHz frequency. At the same time, the chip can complete the operation on ECC public key with any variable curve in F domain less than 256. Therefore, this chip is a high-speed elliptic curve cryptographic chip with optional system parameters. Based on this, this article on the elliptic curve encryption algorithm based on FPGA hardware implementation of system design, from the view of mathematical study analysis, was carried out on the elliptic curve cryptosystem, according to the above two big difficulty, namely, the polynomial of GF(2), the finite field multiplication, and inversion; there will be a detailed studies of discussion, through software comparison to find the differences between different software, especially the software implementation performance level. In addition, it will also focus on the design of elliptic curve algorithm PGA, so as to explore the solution of the algorithm hardware.

1. Introduction

With the continuous improvement of the degree of social information, the ways of people's life, production, and communication have changed dramatically. Computer network has become an indispensable information communication medium in life and study and is an irreplaceable information product for people at present. Openness is both the advantage and disadvantage of computer network, especially when it is violated by network security [1, 2]. This disadvantage is more obvious. At present, it can take the solution measures that personnel management measures cannot fundamentally solve the problem; it is difficult to prevent the computer network security to be violated again, but the emergence of password technology can solve this problem, so in the password technology used in computer network security is more and more important. This is shown in Figure 1.

It was not until 1976 that network secure communication public key cryptography [3] was formally paid attention to by people. After that, more and more implementation schemes of public key cryptography [4] became applicable to various professional fields, and the technology became more and more mature. At present, it can be roughly divided into three categories: (1) the decomposition of large numbers as the idea; (2) take the discrete number pairs in finite domain as the idea; (3) take the discrete number pairs of elliptic curves as the idea. The above classification is mainly based on the mathematical problems of the nature of their schemes, and these schemes have certain security and realizability. It is worth noting that in the above classification, the scheme based on the discrete number pairs of elliptic curves is a kind of cryptosystem. According to the latest academic research, it is concluded that the security of elliptic curve cryptography data transmission with different bit lengths can keep the same basically. For example, there is no significant difference between the security of 160 bit and 1024 bit keys. It can be understood that the key length is 210 bits, and the security is equivalent to the key length of 2048 bits. By contrast, it shows that elliptic curve cryptography is far superior to other public key cryptosystems. People are becoming aware of the commercial and military value behind elliptic curves. Although the 13th Five-Year Plan adjusted the national development of the important task, information network security as one of the key tasks, but the research on elliptic curve discrete logarithm public key cryptography still needs to be developed.

2. The Research Background

Although the emergence of cryptography [4] has a history of thousands of years, during which some people have taken it as a research direction and produced practical applications, the real development of cryptography as a discipline was actually in the middle of the 20th century. Nowadays, cryptography is not only limited to the original political, diplomatic, and military fields but has been developed more widely, becoming an interdisciplinary subject including computer, electronic communication, mathematics, microelectronics, and other technologies. Its function is far more than encrypting information and even can avoid the loss of information data, attack and theft, and so on. Figure 2 shows the first proposed secure communication information model. In the Figure 2, the plaintext M refers to the sender sending, and then C is used for encryption to ensure the security of data transmission. The security factor of the whole system is not related to the encryption system and the confidentiality principle of the algorithm, only depends on the key itself. In other words, even if the encryption and decryption algorithms are exposed, if you want to restore the ciphertext to the plaintext, you must know the composition of the key. In addition, for the concepts of encryption algorithm and decryption algorithm, in fact, they are essentially the parameters used by the algorithm, which have similarities but also differences. According to the characteristics of the key, the algorithm of the password is different. According to the characteristics, it can be divided into two cryptographic algorithms: symmetric key algorithm and public key algorithm. As shown in Figure 2.

If analyzed from the perspective of encryption, the private key cipher can be refined into sequence cipher and block cipher. The principle of sequential cryptography is that after the seed key is transmitted to the sender and receiver through a secure channel, the key stream generator generates the key stream needed for encryption and decryption. But encryption and decryption are a simple modular operation. As for the mathematical model of block cipher, the plaintext is converted into a sequence of numbers by encoding technology and divided into N groups of a certain length, and each group has M bytes. Each group is transformed into an output digit sequence of equal length under the control of the key.

If the same key is used in the process of encryption and decryption, it can be called symmetric encryption system [5]. Therefore, the sender and receiver must select and preserve the shared key, and both parties must have full trust to each other, believe that the other party will not disclose the key, so as to ensure the security and integrity of the information data. Asymmetric cryptographic algorithm can be understood as public key cryptographic algorithm or two-key cryptographic algorithm. According to the classification of algorithms, encryption key and decryption key are two different concepts. In addition, the encryption key has the characteristics of openness, can get rid of time and region restrictions, and can be disclosed, but the decryption key is different and needs to ensure its privacy. Because of the public nature of the encryption key itself, it is also called public key. The decryption key is also known as the private secret key. Among them, the advantage of the private key cryptography algorithm is that the operation process is simple, and the complexity is not high. The disadvantage is that the distribution and management of the key are relatively complex, and it will be slightly difficult to apply in the large-scale network. In addition, it cannot verify the integrity of the sender's identity, so it cannot be applied to digital signature. In contrast, public key cryptography perfectly handles these two problems, and more solutions can be explored. It can be seen that the public key cryptography algorithm has higher application value than the private key cryptography algorithm, but it is a pity that the public key cryptography algorithm has great space complexity and time complexity. Compared with conventional algorithms, the computational cost of public-key cryptography algorithm is larger. For example, the computational cost of DES algorithm is several powers higher. Based on this feature, the application scope of public key is mainly concentrated in the fields with low workload and less data transmission, such as digital signature. This is shown in Figure 3.

In general, the antiattack strength [6] of an algorithm can reflect the security performance of an encryption algorithm, which is an important index to measure. ECC has a strong advantage over RSA, DSA, and other public key systems in this respect. RSA, for example, is one of the most

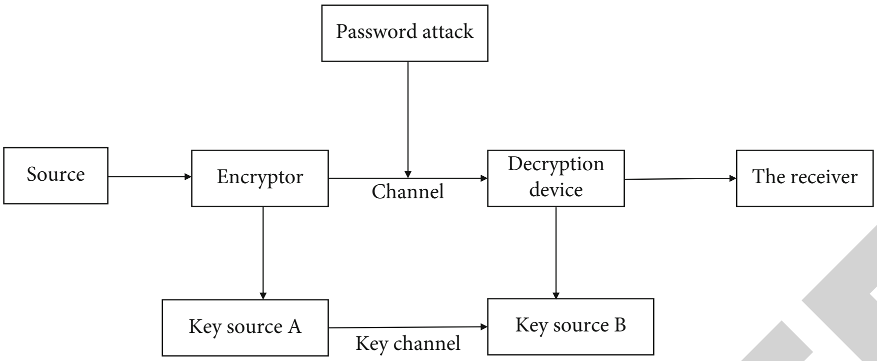

Figure 1: Cryptosystem model.

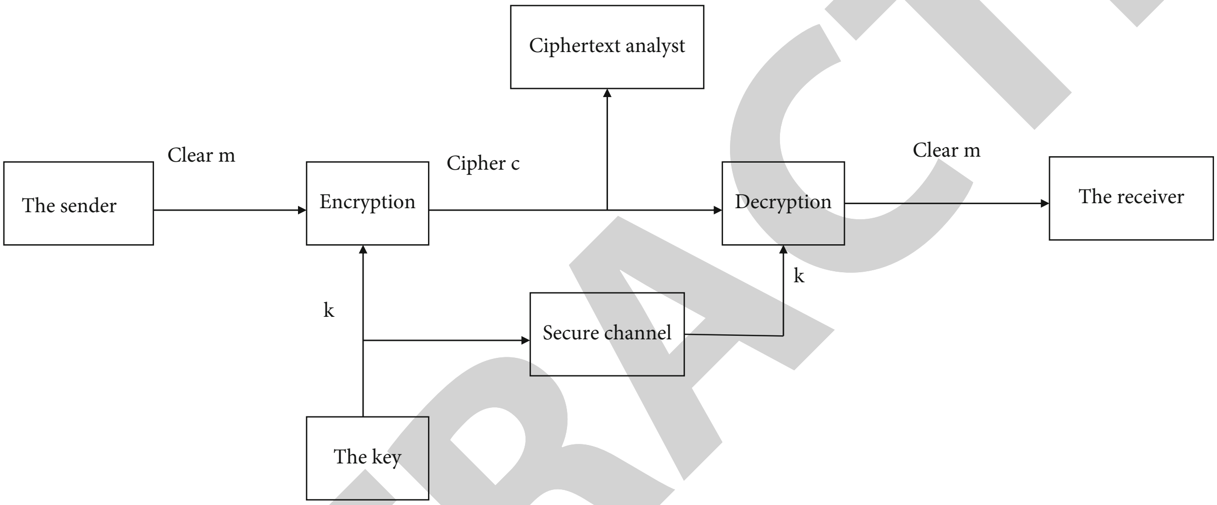

Figure 2: Shannon's secure communication model.

widely used public key systems because of its simple mathematical principles and applications. Subsequently, due to the continuous optimization and modification of the positive factorization scheme and the continuous development of the running speed of the computer, the large number of RSA encryption and decryption security requirements are much larger than before, and the natural need to increase the length of the key to ensure the security of RSA. Generally speaking, only the key length [7] above 1024 bits is secure enough. Unfortunately, because the key length is inversely proportional to the decryption speed, the longer the key length is, the slower the decryption speed is, and the hardware is difficult to realize, which undoubtedly brings great difficulties to the RSA application and greatly affects the RSA application. At this time, the advantages of elliptic curve are highlighted; under the same security strength, the key length of RSA and DSA is much longer than that of ECC, which proves the advantages of ECC. At the same time, elliptic curve encryption can achieve lower bandwidth and smaller storage space to deal with the same problem. Bandwidth and storage space are critical for applications where processor performance, network bandwidth, and hardware storage are limited. For example, web server. Key length of ECC and RSA/DSA is under the same security conditions.

3. Materials and Methods

3.1. Principle of Elliptic Curve Encryption (ECC)

3.1.1. Elliptic Curve. The elliptic curve equation referred to in everyday life often refers to the Wirtschaftsler equation. This equation is expressed mathematically as a series of formulas that satisfy specific conditions within a defined plane curve. In a given number field, it is studied which number couples can be points on an elliptic curve in that field of action. Also, this field of action can be a field of rational numbers (infinite field) or a finite field (finite number of elements in this field). An elliptic curve is a curve symmetric about the x coordinate. In addition to the points of the curve on the coordinate system, the elliptic curve defines an additional point (at infinity), denoted as 0. That is, the elliptic curve is composed of a number of points that meet certain conditions.

About Weierstrass equation:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, a_1 \in K. \tag{1}$$

An algebraic curve with genus 1 defined in a K-field (for a given field) can be determined by a cubic equation. The specific formula is as above. If and only if the discriminant

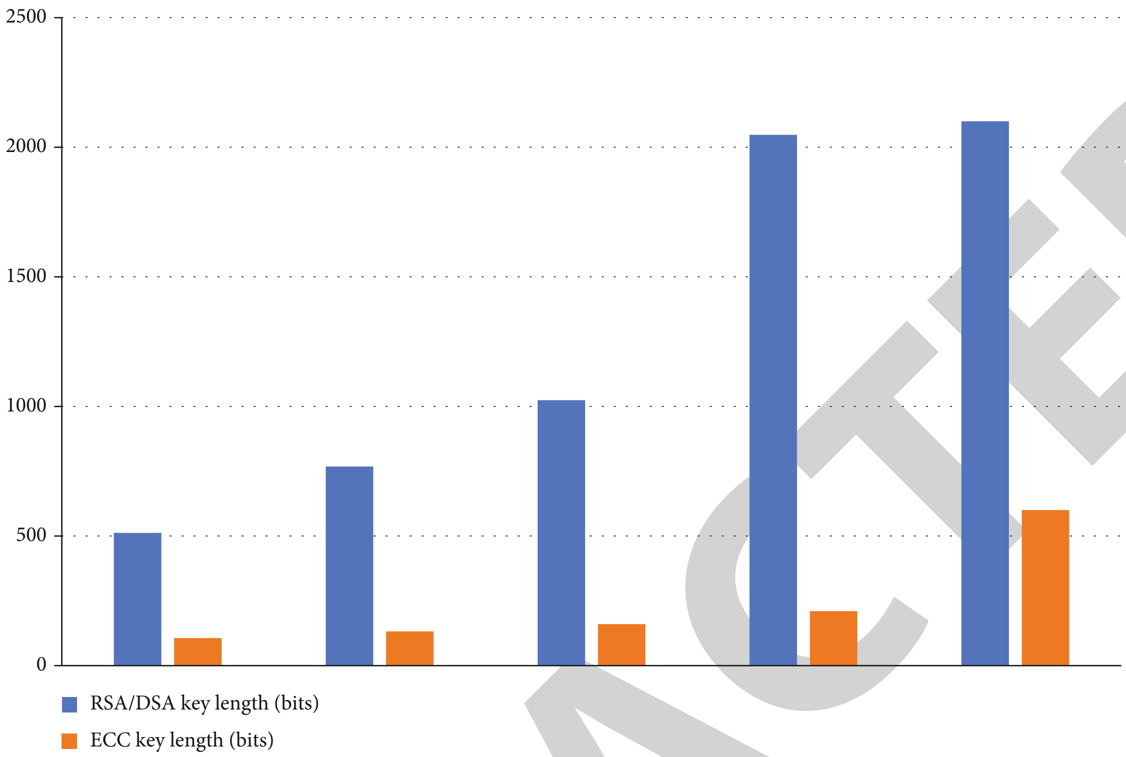

Figure 3: Key length diagram of ECC and RSA/DSA with the same security strength.

of the equation is not equal to 0, it is a nonsingular curve, and the others are singular curves. The group of elliptic curves is defined as the group of operations on the domain K. The elliptic curve has a point $P^2(\bar{K})$ O (0, 1, 0) in the projective plane, which is called the point of infinity. There are two kinds of point operations in elliptic curves, namely, point plus operations and double point operations. In general, finite field operations and point operations on elliptic curves are the basis of ECC. Encryption systems GF(p) for elliptic GF(2^n) curves in finite fields and over finite fields.

The group of elliptic curves in GF (p) in the prime field [8]:

Let P be a prime number less than 3 and $A4a^3 + 27b^2 \neq 0$ and $B \epsilon \mathrm{GF}\,(p)$ satisfy, then A and B will determine that an elliptic curve is the set of points formed by Equation (2) on GF (p):

$$y^2 = x^3 + ax + b. \tag{2}$$

In the formula of elliptic curve, the definition of adding this symbol is that three points on the elliptic curve are on the same line, and their sum is O. This rule is also known as the rule of "tangent string [9]."

From (2) according to Haas theorem (where the point set of GF (p) is denoted by #GF (p)):

$$p + 1 - 2\sqrt{p} \leq \#\mathrm{GF}(p) \leq p + 1 + 2\sqrt{p}. \tag{3}$$

3.1.2. Comparison between ECC and RSA. The security of RSA system is still high; this is because the large integer factorization is very difficult, and it means that the operation process is more complex, so in today's mathematics is still difficult to attack the problem, and there is no relevant personage also gets the corresponding solution, so relatively speaking, the safety factor of the system is higher and is widely used in the encryption system, to better protect confidential resources. In addition to the security aspects of the RSA system, the operating principle and operation of the system are simple. Even nonprofessionals can quickly master the RSA system after training. However, with the advent of the era of data, as well as the in-depth research of science and technology, the work efficiency of large integer decomposition has been rapidly improved. The large integer decomposition work can be decomposed by multiple computers at the same time, and the decomposition speed is greatly accelerated, which affects the confidentiality of the system. Therefore, the encryption security of RSA system is faced with certain challenges. In order to ensure the system security and prevent data leakage, the number of key bits is increasing, which greatly reduces the efficiency of cracking speed and makes the hardware implementation more difficult. In this case, the RSA system is difficult to adapt to some industries, such as e-commerce. If the system is continued to be used, the application scope of the system will become more narrow, which is not conducive to its business expansion. In comparison, elliptic curve encryption method has more application advantages than RSA, as shown in Figure 4.

In elliptic curve encryption system, there are three main aspects of hierarchy, including encryption layer, group operation layer, and arithmetic operation layer. Firstly, the encryption system parameters of elliptic curve

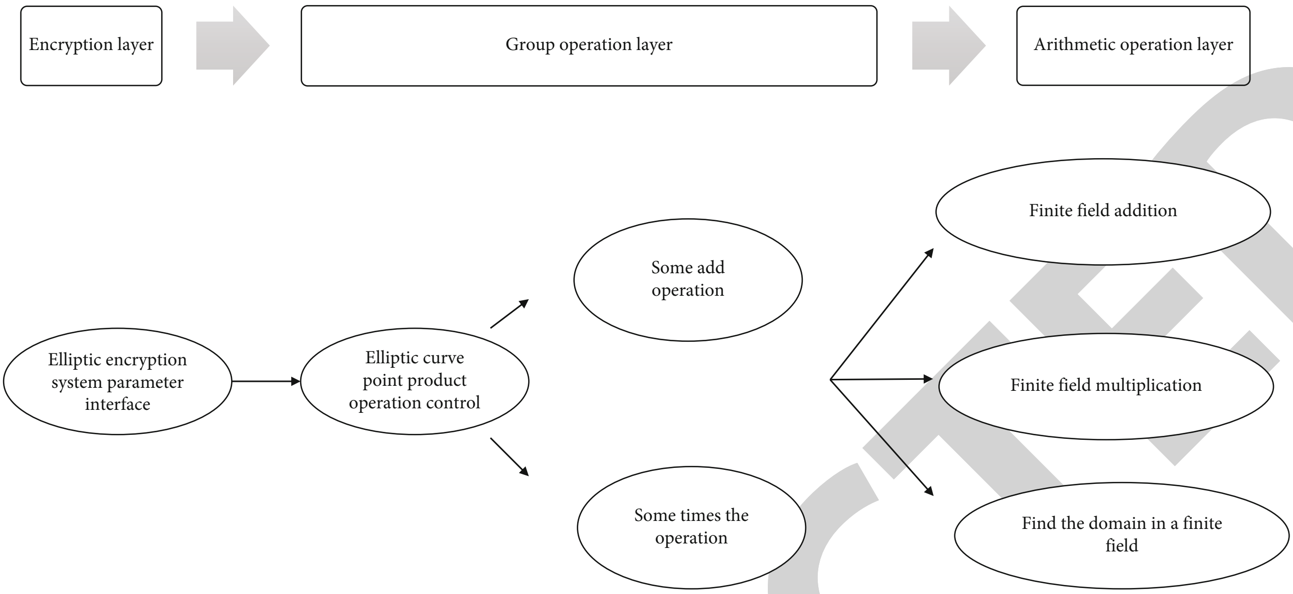
Encryption layer
Group operation layer
Arithmetic operation layer
Elliptic encryption system parameter interface
Elliptic curve point product operation control
Some add operation
Some times the operation
Finite field addition
Finite field multiplication
Find the domain in a finite field

Figure 4: Hierarchy of elliptic curve encryption system.

in encryption layer are obtained by the point multiplication operation of elliptic curve in group operation level. Then the arithmetic operation level will be divided into finite field addition and finite field multiplication and finite field domain.

(i) Higher security performance. The security to run and use is significantly higher than that of RSA systems. The security performance of the encryption algorithm is positively proportional to the attack strength of the algorithm. The higher the attack strength is, the higher the security performance of the encryption algorithm is. For example, the public key of 160 bit ECC is equal to the public key of 1024 bit RSA and DSA and has the same security strength. 210 bit ECC has the same safety strength as 2048 bit RSA and DSA. The comparison of the security performance of symmetric cipher [10], ECC, and RSA/DSA is shown in Figure 5

(ii) The calculation is simplified, and the amount of calculation is smaller. RSA can improve the processing speed of encryption and signature verification by selecting relatively small ones, which has the advantage of competing with ECC. However, if the design of private key processing, that is, decryption and signature, it does not have any advantage, because ECC has higher processing efficiency

Computation is directly related to computation overhead. The key length of the public and private keys depends on the computational overhead. For example, the ECC160 bit key length, 1024 bit RSA key length, and DSA key length correspond to different security indices, because the corresponding systems and keys are different.

The computation overhead of ECC and RSA systems can be compared and studied in Figure 6, where Q is the 160 bit key, and the corresponding data table is the number of operation units. However, due to the particularity of the specific situation, the data have certain errors. As shown in Figure 6.

(iii) The storage space is greatly reduced, and the key occupies a smaller proportion of the memory, which can produce more advantages in the encryption algorithm. The storage space is defined as follows. The plaintext of different encryption algorithms forms the plaintext space of the corresponding algorithm, and all the ciphertext after encryption forms the ciphertext space. Different key spaces are formed according to the length of the key. In particular, the recommended number of rounds of encryption will vary with the length of the key. The key length, key pair, and system parameters have special bits. The corresponding parameters of the three systems are shown in Figure 7. It can be seen that the system parameters used by ECC are shorter than those required by the other two systems. As shown in Figure 7

(iv) Significant changes in bandwidth requirements, especially for short message applications. In the decryption state of long messages, the bandwidth requirement of ECC is the same and does not change significantly, but in the application of short messages, the bandwidth requirement of ECC is significantly reduced. At present, the public key encryption system is more widely used in short messages, for example, the digital signature [10] used in the bank for some business, which is realized by key transfer. Because of the low bandwidth requirement

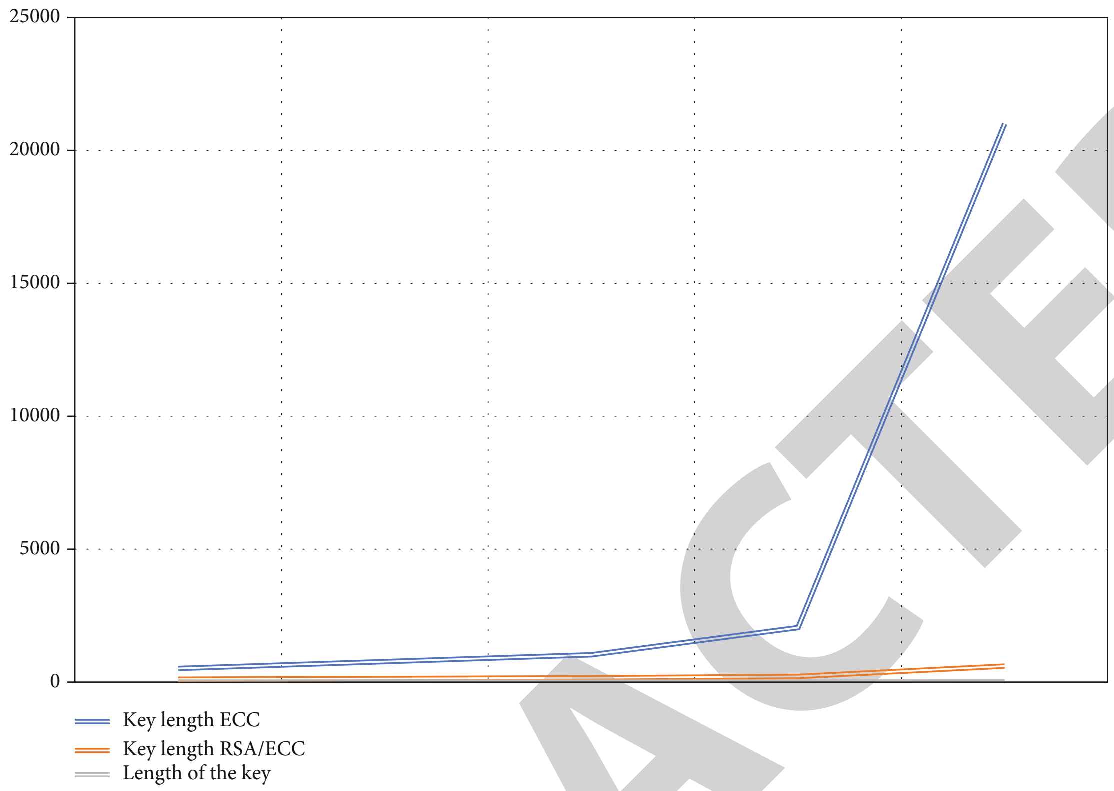

Figure 5: Comparison of safety performance.

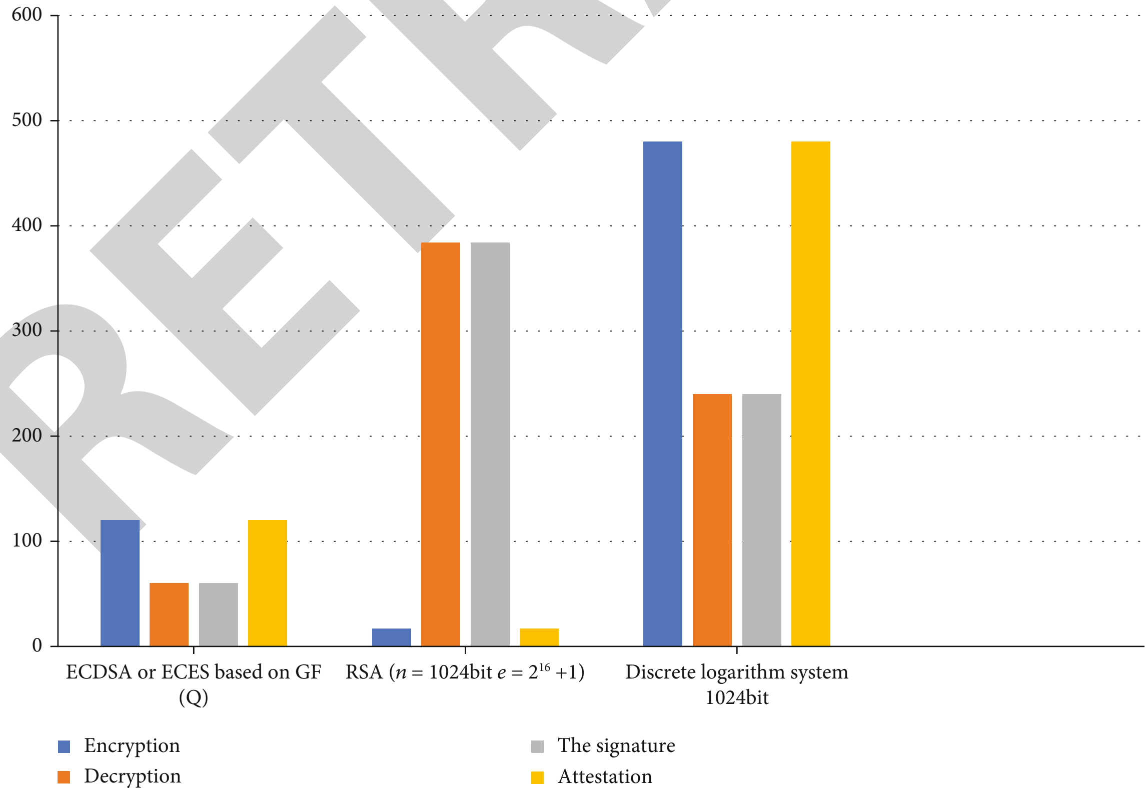

Figure 6: Comparison of processing speed.

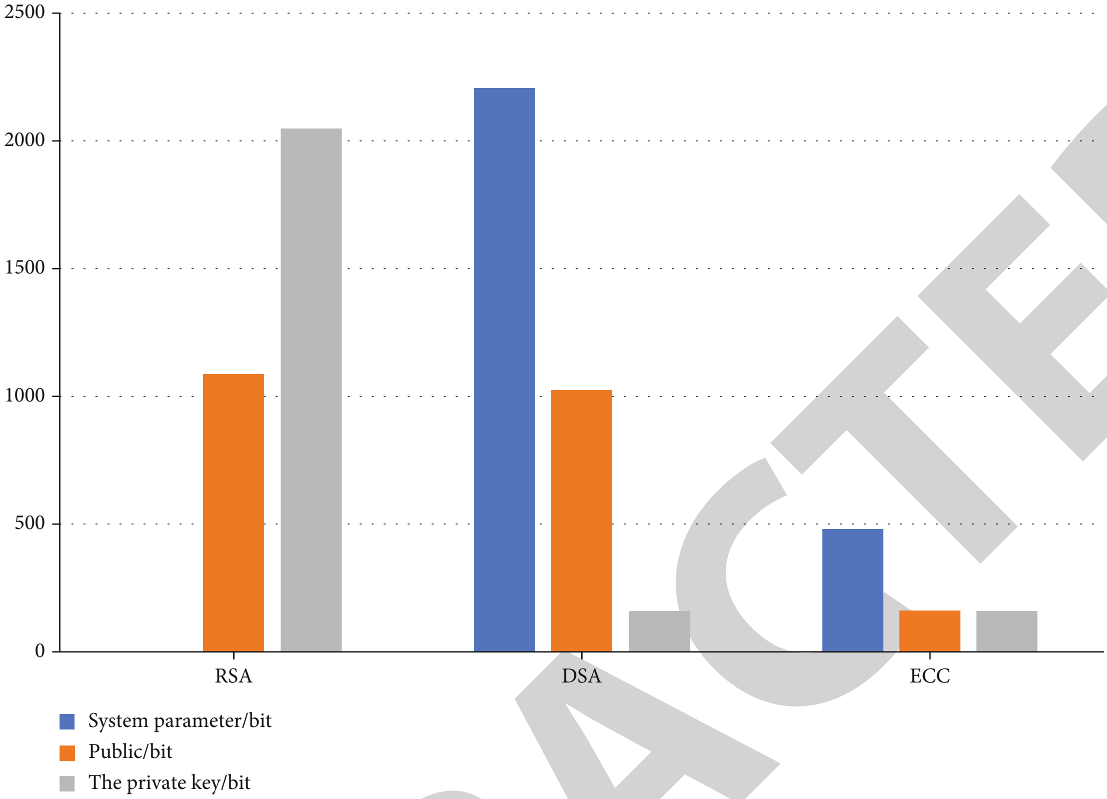

Figure 7: Comparison of system parameters and key pair length.

of public key encryption system, ECC has a great development space in wireless network applications. Based on the above characteristics, elliptic decurving cryptography has received high attention and praise. Nowadays, the cryptographic circles even think that RSA will be replaced in the market position, and the makers of SET (Secure E-lectronic Transactions) protocol have regarded it as the next generation of public key cryptographic algorithm of SET protocol. For specific comparison, it is assumed that the message to be signed is 2 000 bit long, and the message to be encrypted is 100 bit long. The details of the length analysis of the signed and encrypted messages in several cases are shown in Figure 8

As can be seen from Figure 8, when short messages are converted by ECC, the bandwidth demand can be optimized to the best extent. In addition, the point compression technology of ECC also has the advantages of saving the space and bandwidth of storing key certificates. Through the above analysis and comparison, it can be seen that ECC has more obvious application advantages, mainly reflected in high-strength encryption, efficient execution [11], and key. Therefore, compared with other public key encryption systems, ECC can achieve relatively high security with less overhead and delay, that is to say, it has higher cost performance and can be widely used in computing power, such as IC cards and some computer networks.

3.2. Application System Verification. After the hardware implementation of elliptic encryption, the corresponding verification work is still needed to further verify the accuracy of the experimental results. Therefore, by constructing serial port encryption experiment [12] version, the success of elliptic encryption system hardware test is further confirmed.

4. Results and Discussion

The research content of this chapter is mainly carried out around the system simulation test and operation. The research work is centered on the system test and extended in two directions, namely, functional test and performance test. In the function test, the function module is tested, the operation effect of the function module is detected, and the function requirement standard of the module is accurately judged. The problem of high memory usage is studied in performance test. At the same time, the corresponding solution is discussed through the analysis of test results. Finally, through the whole system running effect test, it shows that the system has a strong stability.

For FPGA hardware implementation, the elliptic curve encryption control system module [13] is very important in the system, which is the key to the operation of the whole system. That is, when ready is true, the system contacts information and reads data for storage. When PP = R and PQ = R are entered into the operation, the module will select the appropriate data source corresponding selector for cyclic

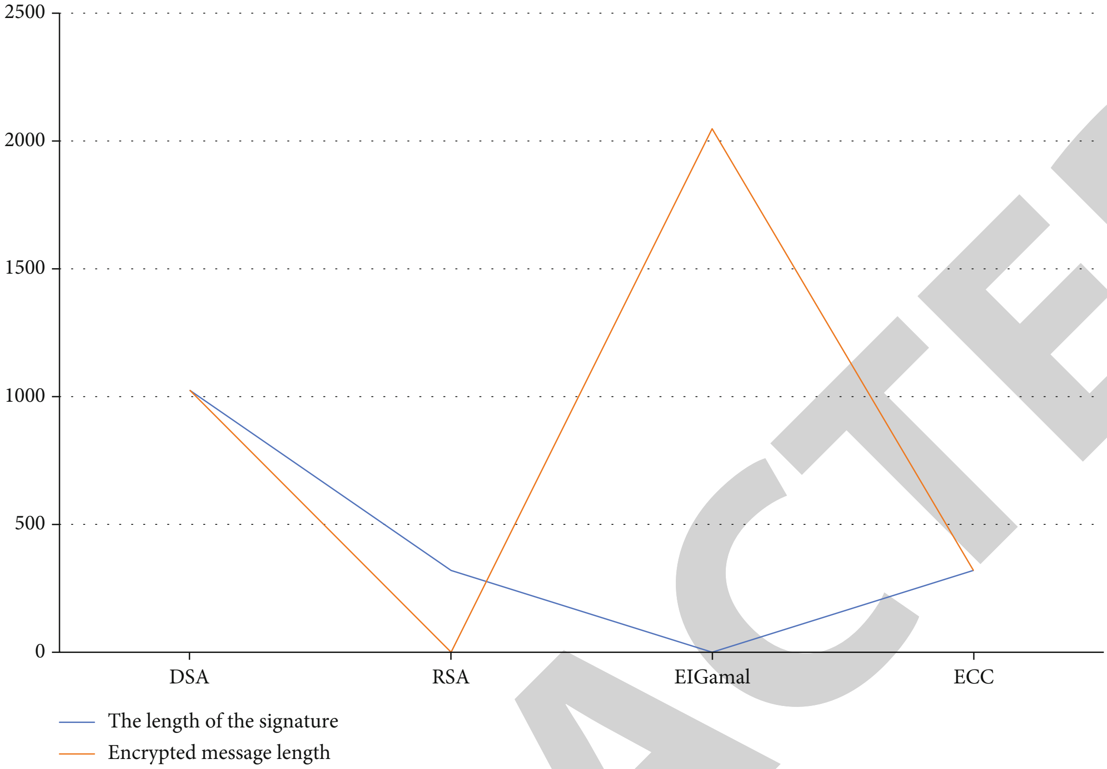

Figure 8: Length analysis of signed and encrypted messages.

control, and after obtaining the operation result, it will output through Qut_ signal. The subsequent control will always enter the control link, which will be controlled according to PP = R module [14] and PQ = R module [15] combined with specific instructions and provide data flow. In the end, to calculate the add operation on the elliptic curve, they need to combine the above two modules and the county in addition and multiplication, and the addition of points on elliptic curve and speed of system performance is a direct connection; if subsequent output data flow is not accurate, there is a big error that will affect the operation rate and cannot reach high operation speed. In short, different memory modules correspond to different instructions, so the results of subsequent operations are also different.

Cryptographic algorithm is a mathematical function that needs to be applied in the process of encryption and decryption. In terms of current research and application, there are many cryptographic algorithms used, such as block cipher and public key cipher. The function of the cryptographic algorithm is actually to serve the transmission of information and ensure the security of information. It will screen the received information and then encrypt the accepted content into ciphertext through the algorithm. For example, if I want to send information with the help of a social media device, so you can use the password algorithm encryption processing, the content of the information in this process can produce relatively after another a cipher text, also is the key, then the information of the receiver will be through another cipher, use the key to restore the content. In this way, information can be transmitted securely. Among the cryptographic algorithms established on the basis of elliptic curve, there are three common cryptographic algorithms: key pair generation algorithm, signature algorithm, and encryption algorithm. Firstly, the elliptic curve version of digital signature ECDSA includes signature operation and verification operation. Let A and B be two communicating parties on a common communication channel, where they have the same elliptic curve parameters (Fq, E, n, h, and G). E is the elliptic curve, G is the base point of Eq. N is the order of the elliptic curve. The encryption process is explained by referring to elliptic curve parameters [16], and H is the cofactor. If A uses a random number dA as its private key, the public key $PA = dA{\cdot}G$ is calculated. The private key and public key are the key pair of A. As mentioned above, public keys are publicly available. Assume that A signs to B, and the signature and verification process will be as follows.

The first part of signature is input the private key dA, and the signature message M contains the authentication information of A and output the signature data (r, s). After the operation, the signature of this message is sent to B. Part 2 verification: input public key PA (r, s) and message M; then the validity judgment result of the signature is output. The second public key encryption algorithm assumes that two communication parties A and B have the same elliptic curve parameters on the common communication channel. B takes a random number dB as the private key and calculates PB = $dB{\cdot}G$. That is, the private key and public key are the key pair of A. The public key in the pair is public. ECES A sends a packet M to B. The process for encrypting and decrypting the packet is as follows. First, the ECES encryption algorithm is used. The unencrypted ECES and public key PB are input, and the encrypted data C is output. Second, B runs ECES decryption algorithm, and input the obtained encrypted data C and private key dB. Packet M was outputted or decrypted. The last procedure is the key pair generation algorithm; the two algorithms mentioned above are digital signature verification algorithm and encryption and decryption algorithm, that is, a pair of public and private keys. So you have the key that generates the algorithm, and the service that generates the algorithm that generates the key. The specific process of the key pair generation algorithm is as follows. Input a random number d, which ranges from 1 to n-1 and input an elliptic curve base point G. output D and Q. D and Q are obtained by the algorithm $Q = dG$.

Like other encryption techniques, elliptic curve encryption is a kind of encryption technique, but its theoretical basis is derived from elliptic curve. In the whole encryption process, it is expanded by points in a finite field. It is necessary to carry out operation and discretization on these points and build corresponding modules, so as to build a special cryptographic system to encrypt and decrypt various information resources. In the process of encryption and decryption, the need to use function means, but generally speaking, are one-way functions; therefore, compared with other systems, its content and operation degree is more complex. To perform an elliptic curve encryption system (ECC), the following steps will be taken: (1) determine the elliptic curve parameters, which are finite field, elliptic curve, and base point; (2) key pair and the relationship between private key and public key is: $Q = kP$. The private key K is a domain element of a finite field, and the public key Q is a point of an elliptic curve. In the previous assumption relationship, A and B are communicating parties, so the parameters of elliptic curve domain can be shared. A is a positive integer as the private key, and the public key can be calculated through the formula. With the private key and public key, the key pair of A can be generated as the public key, and the corresponding key pair of B can be known. Elliptic curve encryption system mainly has the following types: (1) key sharing system: key sharing system is a very important research project in the field of cryptography and has been used in many fields, in life, more common is access control, scheme authentication, etc. One of the key sharing schemes uses the formula ($Q \neq 0$) to share information. However, although this method can achieve password sharing, it is vulnerable to the attack and destruction of the "middle man". To solve this problem, another scheme is proposed; (2) double keys can be constructed according to the specific situation, which are static keys and dynamic keys, respectively (dynamic keys are real-time characteristics, with indeterminate nature); (3) ECES encryption system: checks the MAC addresses to determine the identity of the sender and the sender and generates message masks through the mask function. The plaintext M and the message mask are XOR operation, and the ciphertext is obtained. This is the encrypted process. The next step is the decryption process. After the ciphertext is transmitted to the field of B. The MAC can be obtained through the public key, and the decrypted data will be analyzed and compared with the accepted data. If there is a big difference, the operation will be stopped. If no data error exists, the mask information is calculated and analyzed. The plaintext can be recovered by XOR operation of the mask message and the received encrypted message. It should be noted that the same mask function should be used in the process of encryption and decanting [17].

Theoretical research and calculation need to be verified by experiments, so later hardware operation needs to be verified by software model. In software model verification, addition over finite fields is indispensable. Multiplication and inversion are the key to finite field operations, and the focus of work should be placed in the later resource consumption of hardware, so it is necessary to set up more efficient algorithm programs. Therefore, the particularity generated by GF ((2n)m) in the composite domain is emphatically explored, which can efficiently carry out multiplication and inversion operations and effectively save working time.

In combination with what has been discussed above, we chose the Viretex II device, ISE4.1, developed by XILNX, as the development platform, where the development language is VHDL. The problem faced in this process is mainly the 168-bit elliptic curve encryption algorithm, which involves a huge amount of computation at this point, and therefore, if it is to be implemented, the wiring needs to be considered in a comprehensive manner, and fortunately, Virtex, which provides more extensive wiring resources. Virete can provide and meet most of the features of the FPGA (Field Programmable Gate Way) application market. Especially in the same generation of other products of the same type of chip, the series in the use of the second generation of advanced chip combination module physical architecture. It includes five subseries platforms that implement different functions. The series focuses on the rich resources of FPGAs; each subseries has a high degree of freedom to complement the lack of functionality and resource consumption of the other four series. The corresponding index data are obtained in Modelsim, and the overall operation rate is relatively high. However, if it is the first encryption or decryption, a certain buffer time is needed, but the subsequent plaintext decryption only needs 2 ms. Therefore, this high rate can be adapted to a variety of different occasions. Since the advent of the concept of public key cryptography, quite a few public key cryptosystems have been developed. The security of almost all of these developed systems depends on a different mathematical problem. So far, part of the public key system has been successfully decoded. Of all the remaining public key systems, only the following three are recognized as safe and effective:

(i) IFP, integer factorization, stands for RSA, and so on

(ii) DLP, discrete logarithm, stands for DSA, etc.

(iii) ECDLP, discrete logarithm of elliptic curve, stands for elliptic curve (ECDSA), etc.

To solve the above problems, mathematicians and computer scientists in academia and the world have not found an efficient algorithm after years of calculation, although all these problems have not been proved to be difficult to solve mathematical problems. When the concept of elliptic curve cryptosystem was first put forward, the concept of elliptic curve only stayed in the field of mathematics, lacking the concrete conditions for practical implementation. Due to the security of ECC itself, there is no obvious vulnerability, and the ECC system has been developed rapidly later. Since 1985, ECC has gradually come into the eyes of many cryptographers, computational scientists, and mathematicians and has received full attention. Until today, ECC has become an efficient public key cryptosystem. ECC stands out from many cryptosystems because of its low time complexity in solving mathematical problems. Here, RSA and DSA are taken as examples. The algorithms of these two systems are the same, and they share the same academic source, namely, the time algorithm of subexponential [18]. This shows that the difficulty and length of the problem are directly proportional, that is, the difficulty increases with length. Therefore, although ECC has the same security as IFP and DLP [19], the key length of ECC is much smaller than that of IFP and DLP. Elliptic curve encryption is related to software implementation. The advantage of software implementation is short development time, but the disadvantage is slow encryption speed, which makes the practicality of elliptic curve encryption greatly reduced. The EPGA approach is optimized for this purpose, incorporating the advantages of flexibility and security, faster encryption, and greater advantages in cryptographic applications than ASics.

The characteristics of EPGA hardware and the construction of the model are not completely stripped of the software model, but still need to be based on the software model, and on which to maximize the optimization. At the same time, according to the elliptic curve encryption algorithm, the encryption system can realize modular design, so that different modules can not interfere with each other, complete the setting task independently, but also can share data with each other, coordinate processing, and timing control, so as to improve the encryption effect and improve the security of data transmission.

The application value of ECC far exceeds other traditional public key encryption algorithms, so it has a strong competitive advantage in the field of public key encryption. If purely from the perspective of data encryption, development, and continuous use of ECC is based on the data transmission, the cause of the high safety coefficient is relative to other key system; the system of safety index is higher and can meet the demand of different occasions data transmission, more importantly, the system does not need to be additional to add. Before the ECC system started to be applied, many new public key cryptosystems appeared. However, after the establishment and use of these systems, the risk of being breached is very high, which increases the execution cost. Therefore, ECC has more prominent advantages in key, and the implementation of hardware can further expand its development space.

Among public key encryption algorithms, elliptic curve encryption has high application performance and high encryption effect, so it is widely used in all walks of life. From the point of view of encryption, the ECC system has a higher cost performance ratio, and it can have high security without additional assistance under the established system relationship and meet the security expectations of users. Compared with other public key cryptosystems, even if the system has been established with additional overhead, there is still a large risk of data being breached in the later operation, so the application cost is high. In comparison, ECC system has more prominent advantages and higher cost performance, so it has a broader development space.

ECC system still has higher development potential in the future, because some areas of the system still need to be improved. First is programmable logic devices. In the subsequent research work, it will focus on the aspects of higher gate number and fast rate devices, so as to improve the operation rate of the system. Second is elliptic curve cryptosystem. Elliptic curve cryptosystems still have a lot of room for development, as long as in-depth research and technological development, then can be adapted to more application areas. Third is the hardware implementation of finite field mathematical operation. The hardware implementation algorithm can be improved in the later stage to solve more operational shortcomings and adapt to various forms of key forms. In a word, with the development of modern information technology and science and technology, as well as the change of modern social needs, ECC system will be constantly improved.

5. Conclusion

To sum up, this paper takes ECC system as the research center and discusses in detail the details of each field of the system, operation module design, encryption system implementation, etc. Thesis research results as follows: (1) basic knowledge through research and in-depth analysis of ECC system theory, combining the application problems in the field of e-commerce obtained corresponding solutions, you can use the digital signature, the elliptic curve encryption algorithm, and the combination of symmetric encryption methods; to improve the system in the field of electronic commerce in the encryption speed, reduce the complexity of curve encryption system algorithm; (2) the research object is the modular design of hardware algorithm for elliptic curve encryption system. The influence of finite field selection on the establishment of elliptic curve and the generation of key is analyzed, and the module design of finite field addition, multiplication, and division is optimized. In this process, the realization of FPGA hardware further optimized the design combination of the operation module, and then improved the initial rate, and the system's algorithm logic synthesis ability and simulation can be realized.

In the information age, the risk of data transmission is always greater, and the loss of data once lost or leaked to individuals or enterprises is inestimable. Therefore, in the network era, more emphasis should be placed on network security, do a good job in the research of elliptic curve cryptosystem, and do not use curve cryptosystem to optimize hardware and software equipment, to ensure the security of information transportation and storage.

In many fields, the use is still more traditional algorithms, such as DES, RSA, and so on, because these algorithms themselves are not complex, less computing time. Due to the complexity of its own operation and the limitation of operation time [20], public key cryptosystem is used in few occasions, mainly focusing on digital signature and other places where identity verification is required. However, the update of the algorithm can improve the user experience of password, and the new algorithm can optimize the process and improve the security of information transmission.

ECC has shorter keys and higher security, so it has strong core competitiveness in this field, and its application scope is constantly expanding. Although the research content of this paper can provide suggestions for the future development of EC, there are still many areas that need to be further studied as follows. First, the number of programmable logic gate has expanded space, and the emergence of faster rate devices has become inevitable. Second, the improvement of elliptic curve cryptography should be paid more attention to. Third, the module design of finite field mathematical operation hardware needs continuous optimization.

Data Availability

The experimental data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declared that they have no conflicts of interest regarding this work.

Acknowledgments

This work was supported by National Key Technologies Research and Development Program 2021YFC3001901.

References

[1] L. Hao, S. Li, B. Feng, and J. Li, "An enhanced sensorless control based on active disturbance rejection controller for a PMSM system: design and hardware implementation," *Assembly Automation*, vol. 42, no. 4, pp. 445–457, 2022.

[2] K. Jongbae and S. O. Choi, "Design and implementation of IoT platform education system based on open source hardware," *International Journal of Software Innovation (IJSI)*, vol. 10, no. 1, pp. 1–10, 2022.

[3] D. F. Roberto, D. V. Massimo, and V. Paolo, "A BLE-connected piezoresistive and inertial chest band for remote monitoring of the respiratory activity by an android application: hardware design and software optimization," *Future Internet*, vol. 14, no. 6, p. 183, 2022.

[4] A. Majdi, "Assessing the changeability of component-based system design: a controlled experiment," *International Journal of Computers and Applications*, vol. 44, no. 6, pp. 513–520, 2022.

[5] L. Chuanqi, Z. Yulin, and L. Yan, "System design and research of multi-channel electroacupuncture instrument," *Journal of Physics: Conference Series*, vol. 2290, no. 1, article 012043, 2022.

[6] S. Manoj, K. Shivam, P. Prakhar, and G. Vishal, "Efficient pipelined FFT hardware design for IEEE 754 single precision computing," *Journal of Information and Optimization Sciences*, vol. 43, no. 3, pp. 629–634, 2022.

[7] X. Guo, Z. Bensong, F. Xiaofei, S. Pan, and W. Haowen, "Research and design of scalable advanced application based on dual-core smart meter," *Journal of Physics: Conference Series*, vol. 2264, no. 1, p. 012015, 2022.

[8] S. Erman, A. Musa, and U. Aybars, "Design and implementation of a real-time LDWS with parameter space filtering for embedded platforms," *Journal of Real-Time Image Processing*, vol. 19, no. 3, pp. 663–673, 2022.

[9] Z. Long, "Evaluation system of college physical education teaching reform based on wireless sensor network," *Journal of Computational Methods in Sciences and Engineering*, vol. 22, no. 2, pp. 373–384, 2022.

[10] Z. Monji, B. Imen, A. R. M. Ibrahim, S. M. Z. Mohammed, and U. Mohammed, "Low power hardware design and its mathematical modeling for fast-exact geolocalization system in wireless networks," *International Journal of Communication Systems*, vol. 35, no. 9, p. 35(9), 2022.

[11] J. Wang, C. Zhannan, J. Guo, Y. Dong, J. Yu, and Z. Runan, "Design of wind turbine parameter monitoring and early warning software system based on deep learning modeling," *Journal of Physics: Conference Series*, vol. 2179, no. 1, article 012041, 2022.

[12] Z. Mehdi, A. Ebrahim, and F. Mehdi, "Design and implementation of an intelligent multi-input multi-output Sugeno fuzzy logic controller for managing energy resources in a hybrid renewable energy power system based on Arduino boards," *Soft Computing*, vol. 26, no. 3, pp. 1459–1473, 2022.

[13] Y. Liu, P. Pan, Y. Huang et al., "Unlimited mouse quit wireless smart travel," *International Core Journal of Engineering*, vol. 8, no. 1, pp. 160–166, 2022.

[14] P. Arató, Z. Á. Mann, and A. Orbán, "Algorithmic aspects of hardware/software partitioning," *ACM Transactions on Design Automation of Electronic Systems*, vol. 10, no. 1, pp. 136–156, 2005.

[15] M. Armin, K. Y. Seifi, and N. Ehsan, "VLCIoT: design and implementation of a visible light communication system for indoor Internet of things applications," *Applied Optics*, vol. 60, no. 36, article 11094, 2021.

[16] H. Takayuki, Y. Rentaro, K. Yukihide, and T. Shingo, "Cooperative design of devices and services to balance low power and user experience," *Journal of Low Power Electronics and Applications*, vol. 12, no. 1, p. 15, 2022.

[17] W. Yin, S. Tang, F. Bonini et al., "Hardware design of the generic rear transition module for the global trigger system of the ATLAS phase II upgrade," *Journal of Instrumentation*, vol. 17, no. 3, 2022https://iopscience.iop.org/article/10.1088/1748-0221/17/03/C03017.

[18] Y. F. Chung, K. H. Huang, F. Lai, and T. S. Chen, "ID-based digital signature scheme on the elliptic curve cryptosystem," *Computer Standards and Interfaces*, vol. 29, no. 6, pp. 601–604, 2007.

[19] W. N. Chelton and M. Benaissa, "Fast elliptic curve cryptography on FPGA," *IEEE transactions on very large scale integration (VLSI) systems*, vol. 16, no. 2, pp. 198–205, 2008.

[20] X. Fukang, Z. Zheng, B. Ma, and L. Bingzheng, "Design and implementation of endogenous security container based on union file system," *Journal of Physics: Conference Series*, vol. 2078, no. 1, article 012080, 2021.