The Overview of Elliptic Curve Cryptography (ECC)

The Overview of Elliptic Curve Cryptography (ECC)

Yuhan Yan

Beijing National Day School, Beijing, China, 100039

13501091160@163.com

Abstract. Elliptic Curve Cryptography (ECC) is one of the strongest and most efficient cryptographic techniques in modern cryptography. This paper gives the following introduction: The introduction of cryptography's development; the introduction of the elliptic curve; the principle of ECC; the horizontal comparison between ECC and other types of cryptography; the modern breakthrough of ECC; the applications of ECC; by using a method of literature review. The study's findings indicate that this factor is responsible for the rapid historical development of cryptography, from the classical password to the leap to modern cryptography. Elliptic Curve Cryptography (ECC), as one of the most important modern cryptographies, is stronger than most other cryptographies both in terms of security and strength, because it uses an elliptic curve to construct and, at the same time, uses mathematical operations to encrypt and generate keys. At the same time, elliptic curve cryptography can continue to improve the speed and intensity with the improvement of accelerators, scalar multiplication, and the speed of order operation. The applications of the elliptic curve in ECDSA and SM2 are very efficient, which further illustrates the importance of elliptic curve cryptography.

Keywords: Elliptic Curve Cryptography(ECC), cryptography, RSA code, Elliptic Curve Digital Signature Algorithm (ECDSA).

1. Introduction

Cryptography is the art of secretly passing information. Nowadays, humans need cryptography to win wars, build the internet, and so on. Cryptography is an essential tool for the development of human society.

In this paper, we summarized the introduction to cryptography, the introduction to the elliptic curves, how ECC works, the comparison between ECC and other codes, the breakthrough of ECC, and the application of ECC by using a method of literature review.

This paper overviews the development of ECC. The comparison can make clear the advantages and disadvantages of ECC. In order to make some direct improvements, the introduction to elliptic curves and how ECC works can make the public know about ECC; the introduction to cryptography can give the public awareness of cryptography; and the application of ECC can make people know how ECC really helps them in their daily life. Above all, this paper makes more people learn about cryptography, especially ECC, and how to make some improvements in the future together. Besides, this paper gives some practical ways and directions for the improvement of ECC by giving a summary of what people did to improve it before.

2. The Introduction of Cryptography

2.1. The Process of The Development of Cryptography

Cryptography is the art of hiding information. People use cryptography to transmit information. Cryptography is becoming increasingly important in wars.

Cryptography has a long history; it has been discovered for about 400 years. Before 1949, people used classical codes. Classical codes have low intensity, which means that they're easy to crack. Between 1950 and 1975, cryptography gradually entered into people's minds and became a science. From 1976 till now, the key in cryptography has made great progress. From that point forward, cryptography began to divide into several branches.

2.2. The Classification of Cryptography

After cryptography started to have branches, cryptography has been specified into symmetric cryptography and asymmetric cryptography (public key cryptography). Among these, public key cryptography is the mainstream direction of cryptography study, and is also the most unbreakable cryptography [2].

2.3. Public Key Cryptography

RSA cryptography and Elliptic Curve cryptography (ECC) are the two main codes in public key cryptography.

Public key cryptography mainly uses mathematical computations to encrypt and decrypt. For instance, RSA cryptography uses a huge number that is difficult to separate by two big prime numbers to make the code stronger.

Public key cryptography is more modern than traditional cryptography, and its security is stronger than that of traditional cryptography because its key length is longer and its deciphering requires more computation. However, public key cryptography will not completely replace traditional cryptography because it consumes a lot of calculation, so it can only be used in signatures and key management.

Table 1. the comparison between traditional cryptography and public key cryptography.

	traditional cryptography	public key cryptography
basic requirements	1. senders and receivers must share the key	1. the sender owns one of the key of encryption or decryption, and the receiver owns the other one.
	2. senders and receivers must uses the same key and the same algorithm	2. the encryption and decrption uses the same algorithm, but different keys
security requirements	1. if one doesn't know the key, one cannot decipher	1. if one doesn't know the key, one cannot decipher
	2. if one only knows the algorithm and several ciphertexts, one cannot confirm the key.	2. if one only knows one key and several ciphertexts, one cannot confirm the other key.
	3. the key has to be kept secretly	3. the private key has to be kept secretly

3. The introduction of Elliptic curves

3.1. The Introduction of Elliptic Curves

Elliptic curve cryptography is an important cryptographic type in public key cryptography, which relies on an elliptic curve to encrypt and decrypt.

An elliptic curve is a smooth affine curve with genus 1 in the domain, and its expression can be written as $y^2 = x(x-1)(x-\lambda), \lambda \neq 0,1$, or $y^2 + ay = x^3 + bx^2 + cx + d$. If the characteristics of the domain are not 2 and 3, then it can also be written as $y^2 = x^3 + ax + b$.

The graphs of elliptic curves change with their coefficients, as shown in the graphs below.

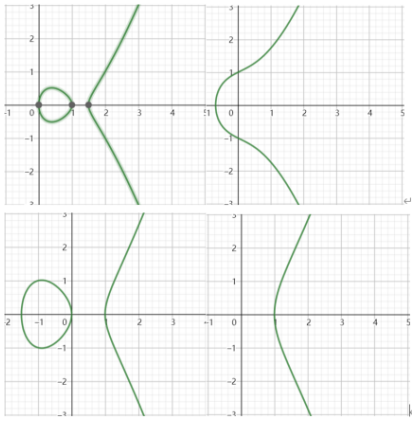


Figure 1. Four different elliptic curves.

Elliptic curves have several applications, such as Elliptic Curve Cryptography (ECC), Elliptic Curve Digital Signature Algorithm (ECDSA), etc.

3.2. The Introduction of Group

To understand elliptic curve cryptography, we also need to know the definition of group.

If an nonempty group G is defined to have an operation "·", and this operation satisfied:

（1） $\forall x,y \in G$， they satisfied $x \cdot y \in G$

（2）$(x \cdot y) \cdot z = x \cdot (y \cdot z)$

（3） $\forall x \in G$， $\exists p$， such that $p \cdot x = x$

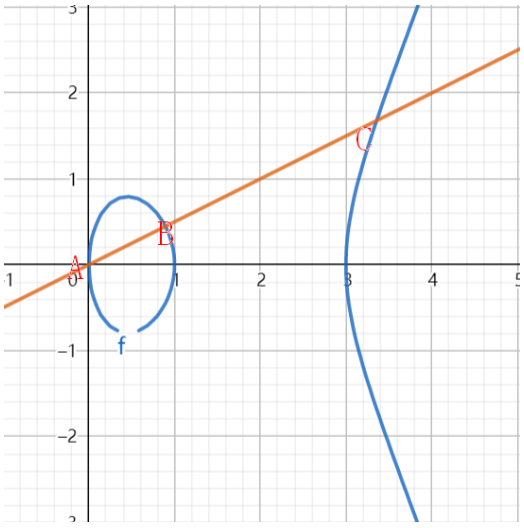
（4） $\forall x \in G, \exists y$, such that $x \cdot y = y \cdot x = q$

then we can say that G is a group about operation "·".

If G also satisfies commutative axiom, then G is an Abelian Group.

3.3. The Additive Group On Elliptic Curves

On an elliptic curve, we need to define an "additive group" for later cryptographic calculations.



$(P + xA) - kxB$

Figure 2. Four different elliptic curves.

On an elliptic curve, we choose two points A, B randomly. Then, draw line AB and intersect the

elliptic curve at point C. Then, define $A+B=C$.

If A and B are the same points, then, C is the intersection point of the tangent line of A and the elliptic curve.

It is proved that the additive group of the elliptic curve conforms to the four requirements of group, so it is a group, and it also conforms to the commutative axiom, so it is an Abelian group.

3.4. The Order of Elliptic Curves

The order of the elliptic curve is also an important basic knowledge of the elliptic curve.

If an elliptic curve exists in finite fields, there is an order. The order is the number of the points on the elliptic curve's limited domain.

4. The Basic Principle of Elliptic Curve Cryptography (ECC)

4.1. The Constituent of Elliptic Curve Cryptography (ECC)

A code system is composed of the plaintext, a key, and ciphertext, in which the key can be public, private, or partially public and partially private.

4.2. The Formation of the Key of Elliptic Curve Cryptography (ECC)

The author chooses two points A and B on the elliptic curve randomly, B is the cardinal point on the elliptic curve, and A satisfies $A=kB$. Then, set the private key to be k, and the public key to be A.

By using the additive group on the elliptic curve, if we only know k and B, it is easy to find A, but if we only know A and B, it is difficult to find k.

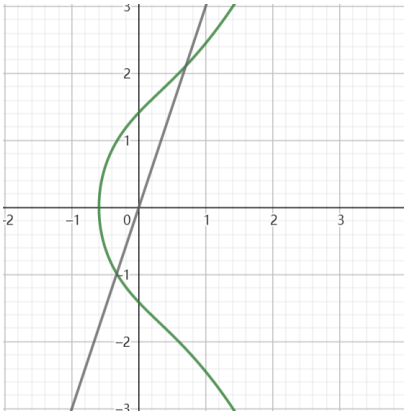


Figure 3. A line passing through an elliptic curve.

4.3. The Encryption of Elliptic Curve Cryptography (ECC)

Firstly, the encoder has to transform the sentences in the plaintext into several numbers through some changes.

Then, the encoder has to find a specific elliptic curve randomly.

Set the plaintext be P, choose a number x ($x<n$, n is the order of the specific elliptic curve) randomly. Through the transformation $Q=(xB, P+xA)$, the encoder transforms the plaintext P into the cyphertext Q. The addition in this transformation is the normal algebraic addition. Then, change the cyphertext Q into words through some changes.

4.4. The Decryption of Elliptic Curve Cryptography

The decoder will receive the private key k, so the decoder can use the equation to find the plaintext P, because $(P+xA)-kxB=P+kxB-kxB=P$.

4.5. The Reason Why ECC uses Elliptic Curves

1) A line passing through a random point on an elliptic curve is likely to have three intersection points with the whole elliptic curve. This satisfies the requirements of the additive on the elliptic curves that ECC requires.

2) There are several shapes of elliptic curves. Changing a coefficient can make the whole elliptic curve change shape.

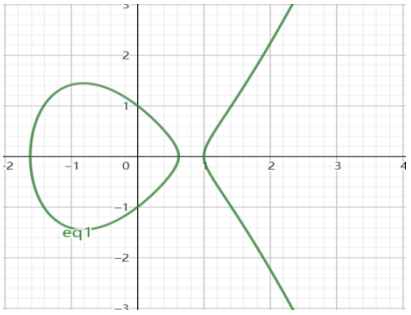


Figure 4. $y^2=x^3-2x+1$.

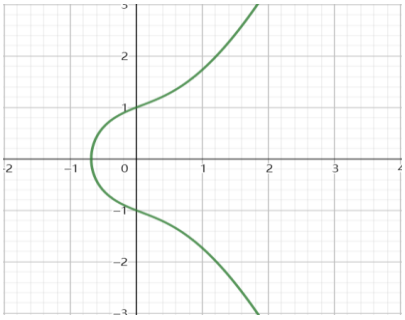


Figure 5. $y^2=x^3+x+1$.

This satisfies the requirement of the variety of elliptic curves in ECC.

5. The Comparison Between ECC and RSA Cryptography

5.1. The Comparison of the Key Points Between ECC and RSA Cryptography

The key of RSA cryptography is that the large number multiplied by two large prime numbers is a public key and that it is difficult to disassemble. However, the efficiency of generating two huge prime numbers is lower than that of elliptic curve cryptography.

Elliptic curve cryptography (ECC) uses the inverse operation of addition in an elliptic curve as the key and can achieve high encryption without complex operations, so its efficiency is relatively higher. Also, ECC has not been found to have any obvious vulnerabilities so far, so it is a relatively reliable modern cryptography [3].

5.2. Analysis of the advantages of elliptic curve cryptography (ECC)

First, Elliptic Curve Cryptography has a better security level. The elliptic curve cryptography system provides stronger protection and is better than any other encryption algorithm at preventing attacks, making websites and infrastructure more secure than traditional encryption methods, allowing ECC to provide a better guarantee for mobile Internet security [4].

Second, elliptic curve cryptography is better for the mobile Internet. Elliptic curve cryptography has a relatively short key of 256 bits, so it takes up less storage space. As more and more users use mobile devices to complete various online activities, elliptic curve cryptography provides a better customer experience for mobile Internet security.

Third, Elliptic Curve Cryptography has better properties. Elliptic curve cryptography can provide better security with shorter key lengths. For example, the key strength of the 256-bit elliptic curve cryptography is about the same as that of the 3072-bit RSA key (currently, the normal RSA key length is 2048 bits). According to the tests of relevant foreign authorities, the response time of a Web server is more than ten times faster than RSA when using the ECC algorithm on Apache and IIS servers.

5.3. Analysis of the disadvantages of elliptic curve cryptography (ECC)

The main disadvantage of elliptic curve cryptography is its low efficiency. Elliptic cryptography relies on mathematical computation to encrypt and decrypt, and its strength depends on the complexity of computation. So its calculation is huge, resulting in low efficiency of transmission, encryption and decryption.

6. Modern Breakthroughs of Elliptic Curve Cryptography (ECC)

6.1. Improvements of the Accelerator

One of the major disadvantages of public key cryptography is that it takes too much computation and consumes too much energy and time, so the improvement of the accelerator is very necessary to improve the efficiency of elliptic curve encryption and decryption and the generations of keys [5]. The current domestic and foreign university students who have a lot of experience in elliptic curve cryptography are committed to researching how to improve efficiency and gradually find out the more suitable accelerator for elliptic curve cryptography. For example, the ASIC method can be used to design and implement hardware accelerators [6].

6.2. Acceleration of scalar multiplication algorithm

The speed of the scalar multiplication algorithm is very important for elliptic cryptography encryption [7]. There are two factors that speed up the scalar multiplication algorithm: coordinate representation and exponential addition chain representation. Inverse coordinate representation can avoid inverse operation in a finite domain. An exponential addition chain can achieve scalar multiplication with as few elliptic curve groups as possible.

At present, the most modern standard is coordinate representation, with odd features using Jacobian coordinates and even features using LD coordinates. The improved speed of the scalar multiplication algorithm can be applied to popular hardware with remarkable effect [8].

6.3. Improvements of the Order of Calculation

Compound by complex multiplication, the method of cryptography, it is easy to find the elliptic curve, but in order to further strengthen the security of the password system, cryptography, the elliptic curve tends to be randomly generated. But the elliptic curves required by elliptic curve cryptography must have the same order, so polarization of order becomes an important effect in generating elliptic curves.

In 1984, Schoof with a polynomial time algorithm is proposed to calculate the order of elliptic curve method, but the actual performance of the algorithm is very poor, so the author cannot get practical application in elliptic curve cryptography. Then, Elkie put forward the Elkie primes and Atkins primes, kay in finite field features a larger context, algorithm is proposed, and greatly improves the efficiency of calculation of elliptic curve order. Similarly, Lecier proposed the method of using form of way to calculate the effect, which had similar results with . Then, more efficient algorithm was put forward by Satoh, Harley and also gave the same promotion of simple and effective calculation method to calculate the effect is more outstanding. So far, this problem has been solved almost perfectly by several cryptographers and mathematicians [8].

7. The Applications of Elliptic Curve Cryptography (ECC)

7.1. Elliptic Curve Digital Signature Algorithm (ECDSA).

A digital signature does not refer to a real signature, but a private key "signs" certain information. Other people (including user B) can verify that the information is actually signed by User A through user A's public key, because the information can be signed only by user A's private key. However, digital signatures can be used for real signatures.

The operator will use Hash-function that is at the security-level to transform signature plaintext P into cyphertext Q. Then, the operator will generate another number k $(0 < k < n)$ randomly, n is the order of the cyclic subgroup.

Then, $A = kB$, the definition of A, B, k is the same with the ones above.

Then, define x_p as the x-coordinate of P, $r = x_p \bmod n$, $s = (z + rd_A) / k \bmod n$.

Then, (r, s) is the signature information [9].

7.2. SM2 Algorithm

SM2 has advantages over RSA in terms of security and properties. Therefore, SM2 can basically replace RSA. SM2 algorithm has many applications, such as information security hardening [10].

There is a relationship between SM2 Algorithm and Elliptic Curve Cryptography (ECC). SM2 Algorithm determines its curve by determine in . Besides, in order to map curves to encryption algorithms, other parameters are identified in the SM2 standard for use by algorithmic programs [11].

8. Conclusion

First of all, cryptography has developed rapidly since ancient times. The leap from classical cryptography to modern cryptography is due to the discovery of the key. The elliptic curveModern cryptography, for example, is one of them. It is one of the most important modern cryptographies. It is stronger than most other cryptographies both in terms of security and strength because it uses elliptic curves to construct and, at the same time, uses mathematical operations to encrypt and generate keys.

Secondly, elliptic curve cryptography can continue to improve the speed and intensity with the improvement of accelerators, scalar multiplication, and the speed of order operation.

Finally, the application of the elliptic curve in Internet digital signature and SM2 is very efficient, which further illustrates the importance of elliptic curve cryptography.

This study has the following two shortcomings: First, no extensive research into the application of elliptic curve cryptography has been conducted, resulting in an incomplete summary of its application; second, other cryptography types in modern cryptography have not been investigated; and third, elliptic curve cryptography is relatively simple when compared to other cryptography. Further research will be conducted on the application of elliptic cryptography and its horizontal comparison with elliptic curve cryptography and other modern ciphers.

References

[1] Wang Zhaohui <A Research on the Securities of Elliptic Curves Cryptosystems>, 2004-04-10, Wuhan University.
[2] Zhou Min <On Digital Signature based on Elliptic Curve Cryptosystem>, 2013-03-01, Qinghai Normal University.
[3] Yu Wei <Research on Some Elliptic Curve Cryptographic Algorithm>, 2013-05, University of Science and Technology of China.
[4] Ye Dingfeng <Advances in Elliptic Curve Cryptography>, 2007-09, Graduate University of the Chinese Academy of Sciences, Communications of China Computer Society.
[5] Niu Yongchuan <Fast Implementation of Public Key Cryptographic Algorithm SM2 based on Elliptic Curves>, 2013-03-20, Shandong University.
[6] Liu Yuxuan<Research on FPGA-based High-performance Elliptic Curve Cryptography Acceleration Technology>, 2021-05, Hefei University of Technology.
[7] Simon Singh <The Code Book>, 2003-08-12, eBooks.
[8] Gao Wei, Luo Yixuan, Li Jiakun, Wu Haixia <High Performance Hardware Implementation of Elliptic Curve Cryptography Point Multiplication over GF(p)>, 2021-09, Beijing Institute of Technology, Transaction of Beijing Institute of Technology.
[9] Tang Siyun <Research on RSA and Elliptic Curve Cryptography Algorithms>, 2003, Hengyang

Normal University.
[10] Wei Wei, Chen Jiazhe, Li Dan, Zhang Baofeng <Research on the Bit Security of Elliptic Curve Diffie-Hellman>, 2020-04-24, Journal of Electronics & Information Technology.
[11] Luo Zhao, Xie Jihua, Gu Wei, Xu Fang, Jin Junhua <Development of power grid information security support platform based on SM2 cryptography system>, 2014-03-25, Automation of Electric Power System.