Elliptic Curve Cryptography

Yiqiao Liu
Mathematics, University of Glasgow
* Corresponding author: gaoming@cas-harbour.org

ABSTRACT

Number theory is a very important cornerstone of cryptography. Modern public key cryptography has been applied to many fields due to its security and flexibility. This paper will focus on elliptic curve cryptography. The paper discusses the formula derivation and encryption method of elliptic curve cryptosystem, and then uses the code to implement the elliptic curve cryptosystem, simulates the whole process of encryption and decryption, and proves the security performance of the elliptic curve cryptosystem.

Keywords: Number theory, elliptic curve cryptography, code, security

1.INTRODUCTION

Number theory is the most ancient mathematics, the purest of an important branch of mathematics, mathematics prince Gauss once said, mathematics is the queen of science, number theory is the queen of mathematics. The main task of number theory is to study the nature of integers, because the nature of integers is complex and profound, difficult to consider, so number theory has long been considered a beautiful mathematical discipline. And number theory is not only a pure mathematical subject, but also a subject with strong application. Nowadays, with the rapid development of modern computer network communication, number theory is widely and deeply applied in cryptography.

Three scientists at MIT, R.L. Livest, A.Shamir and L. Ardleman (RSA for short) [1], proposed a practical public key cryptosystem based on the difficulty of integer decomposition, which is now commonly called RSA system. In the RSA system, a large integer (currently usually 1024 bits long) is used, which is the product of two prime numbers. This large integer is disclosed, while its two prime factors are kept secret. If someone could decompose this large integer into its two prime factors, they could break the cryptosystem, so RSA security was based on the problem of factorization of large integers. This is a classical number theory problem, the proposed RSA greatly promoted the large integer factorization algorithm research. So far, there is no very satisfactory fast integer decomposition algorithm. The fastest integer decomposition algorithm in the world is the number field sieve method (NFS) pioneered by J. Collard, and NFS is not very low computational complexity.

The most representative modern public key cryptosystems developed later are based on different number theory problems, such as integer decomposition, discrete logarithms, and discrete logarithms on elliptic curves. Almost all practical public key cryptosystems in the world are basically based on these number theory problems. In other words, the encryption, decryption, deciphering and other problems with the number theory of the solution of a piece of the connection. Codes are hard to crack because number theory is hard to solve. Therefore, number theory and cryptography are closely linked here, because not only the theory and method of number theory itself have practical value, but also the problems in number theory find an ideal application place in real life.

Due to the close relationship between number theory and cryptography, this paper chooses the topic of elliptic curve cryptography to explore, and the following three parts are mainly used for research. Firstly, the origin and characteristics of elliptic curve cryptography are expounded, the advantages compared with RSA are discussed, and the derivation process of elliptic curve cryptography is described from the perspective of formula. Then, the application of elliptic cryptographic curve system in digital currency encryption and decryption is introduced. Finally, the process of encryption and decryption of elliptic cipher curve is realized by using code.

2.ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptosystem is a cryptosystem based on elliptic curves of the finite field to encrypt and decrypt information. It is considered to be relatively safe and practical in the world. In addition, this cryptosystem has a wide range of applications. Elliptic curve public key cryptogram was proposed by Neal Koblitz of The University of Washington and

International Conference on Statistics, Applied Mathematics, and Computing Science (CSAMCS 2021), edited by
Hong-Ming Yin, Ke Chen, Romeo Meštrović, Teresa A. Oliveira, Nan Lin, Proc. of SPIE
Vol. 12163, 121633M · © 2022 SPIE · 0277-786X · doi: 10.1117/12.2628220

Victor Miller of IBM in 1985 [2], after Goldwasser and Killian's primeness test, Lenstra's elliptic curve decomposition of large numbers, Elliptic curve theory is a new application in cryptography, its idea is still in all kinds of public key cryptosystems involving multiplicative group in finite field, using the elliptic curve group in finite field to simulate multiplication group in finite field, so as to obtain similar public key cryptosystems. The security of this kind of system is based on the difficulty of solving the discrete logarithm problem on the elliptic curve. So far, no subexponential time algorithm has been found to solve this problem. Therefore, it has some incomparable advantages over other public key cryptosystems. Elliptic curve cryptosystem has the advantages of short parameters and key size, small computation, fast processing speed and low bandwidth requirements.

3.ANALYSIS ON THE ADVANTAGES OF ELLIPTIC CURVE CRYPTOSYSTEM

There are two potential advantages of using elliptic curves [3] to build cryptosystems: on the one hand, it has inexhaustible elliptic curves which can be used to construct finite point groups; on the other hand, there is no discrete logarithmic subexponential algorithm for calculating finite point groups of elliptic curves. Because of these advantages, elliptic curve cryptosystem has been widely concerned by cryptography, and elliptic curve cryptosystem is considered as the next generation of the most general public key cryptosystem. The following table shows the advantages of elliptic curve encryption over RSA [4]. As shown in table 1, because elliptic curve encryption is based on EC discrete logarithm, it is more difficult and brings higher security. Moreover, the number of keys is much less than RSA. Due to the diversification of elliptic curve, the flexibility is also very high.

Table 1 RSA and elliptic curve encryption contrast

	RSA	**Elliptic curve cryptography**
difficulty	difficult（integer factorization）	more difficult（EC discrete logarithm）
key amount	Large（1024bit）	Little（160bit）
security	high	higher
flexibility	medium	high

3.1 Elliptic curve

An ellipse is defined as the trajectory of a point in the plane whose sum of distances from two dissimilar fixed points (F1 and F2) is constant. The standard equation for an ellipse is as follows:

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1 \tag{1}$$

In which, $F_1=(-c,0)$， $F_2=(0,c)$， $c^2=a^2-b^2$, The circumference formula of the ellipse is:

$$L=4\int_0^{\frac{\pi}{2}}\sqrt{x_t^{'2}+y_t^{'2}}dt \tag{2}$$

When $\theta=\frac{\pi}{2}-t$,then:

$$L=4a\int_0^{\frac{\pi}{2}}\sqrt{1-\frac{a^2-b^2}{a^2}\sin^2\theta d\theta} \tag{3}$$

Because $c^2=a^2-b^2$, eccentricity $e=\frac{c}{a}$, so

$$L=4a\int_0^{\frac{\pi}{2}}\sqrt{1-e^2\sin^2\theta}d\theta=4aE(e,\frac{\pi}{2}) \tag{4}$$

he elliptic integral is defined as:

$$f(x) = \int_c^x R\left|t, \sqrt{P(t)}\right| dt \tag{5}$$

The elliptic integral is defined as: where R is a rational function of its two parameters, P is a polynomial of order 3 or 4 without multiple roots, and c is a constant. By simplifying the formula, elliptic integrals can be reduced to integrals that can be expressed by elementary functions, such as the complete elliptic integrals of the second kind:

$$E = E(k) = E(k, \frac{\pi}{2}) = \int_0^1 \sqrt{\frac{1-k^2x^2}{1-x^2}} dx = \int_0^{\frac{\pi}{2}} \sqrt{1-k^2\sin^2\theta} \tag{6}$$

Then, the circumference formula of the ellipse can be converted to the form of the second kind of complete elliptic integral E:

$$L = 4a\int_0^{\frac{\pi}{2}} \sqrt{1-e^2\sin^2\theta} d\theta = 4aE(e, \frac{\pi}{2}) \tag{7}$$

And because the elliptic integral is a cubic or quartic polynomial of T, then in a binary cubic equation:

$$y^2 + aty + by = t^3 + ct^2 + dt + e \tag{8}$$

Then,

$$f(x) = \int_c^x R\left|t, \sqrt{t^3 + ct^2 + dt + e}\right| dt \tag{9}$$

The above equation is a curve, so a curve in this form is called an elliptic curve.

When a=0, b=0, c=0, then:

$$f(x) = \int_c^x R\left|t, \sqrt{t^3 + dt + e}\right| dt \tag{10}$$

To obtain the elliptic curve commonly used in cryptography:

$$y^2 = x^3 + Ax + B \tag{11}$$

3.2 Discrete logarithm problem

The discrete logarithm problem is given a positive integer x, y, p> 1, find a positive integer k > 1 (if it exists), make it $y \equiv x^k (\bmod p)$.

The mathematical principle of discrete logarithm encryption is as follows:X is the base, k is the private key, y is the public key, given x, k (private key), it is easy to find y (public key), that is, decryption is easy; Given x, y (public key), it is difficult to find k (private key), that is, it is difficult to crack.

3.3 Elliptic curve encryption

The elliptic curve equation commonly used in elliptic curve encryption is:

$$y^2 = x^3 + ax + b(a, b \in GF(p), 4a^3 + 27b^2 \neq 0) \tag{12}$$

Since the number theory is mainly used to study the properties of integers, the point set on the elliptic curve is generally used to encrypt the elliptic curve. Here, let Ep(a,b) represent the point set on the elliptic curve. The steps for finding the point set of Ep(a,b) are as follows: First of all, for each x, calculate $x^3 + ax + b(\bmod p)$, and then determine whether the previous value has a square root under module P, calculate $y^2(\mod p)$, if not, then there is no corresponding point on the curve, if there is, then find the two square roots.

The addition rule in an elliptic curve is different from ordinary addition in algebra. Instead, it uses the line of two addends to intersect with another point of the elliptic curve, and then takes a mapping point for this point, which is the result of the addition of the two. It is this addition rule that creates the asymmetric encryption property of elliptic curve encryption, that is, it is easy to calculate the former from the latter, and almost impossible to calculate backwards. The product rule in elliptic curves is consistent with the addition rule. If you take a tangent line to a point on the curve, the mapping between the tangent line and the intersecting point of the curve is 2 times, and you can continue the addition operation to get the desired product. The finite field of the elliptic curve means that the line between two points does not intersect with the elliptic curve when the addition calculation is carried out. At this time, it is equivalent to folding the coordinate axis somewhere, so that the extension line continues to extend in the finite field until it intersects the elliptic curve.

4.ELLIPTIC CURVE CRYPTOGRAPHY APPLICATION

Elliptic curve encryption has an important application in modern society, which is digital currency encryption. Among them, Bitcoin is using elliptic curve encryption to achieve the effect of internal anti-cheating and external anti-attack [5]. The following will elaborate on the application of elliptic curve encryption in bitcoin [6].

4.1 Blockchain and Bitcoin

A blockchain is a growing list of records linked through cryptography. The first widespread application of blockchain is bitcoin, and it is also being explored in the field of payment, invoice and guessing.

On November 1, 2008, Satoshi Nakamoto formally proposed Bitcoin in his paper "Bitcoin: A peer-to-peer Electronic Cash System", which is the theoretical cornerstone of blockchain. Blockchain was formally and independently proposed in 2015. It aims at a series of disadvantages brought about by the centralization of society, as shown in the table 2.

Table 2 Blockchain technology and now insufficient contrast

	Present deficiency	The advantages of blockchain
process	centralized, intermediary	Decentralize and improve efficiency
consequence	Not open, not transparent	Open, distributed, and unmodifiable
security	information disclosure	privacy protection

Blockchain uses P2P networks, consensus mechanisms, incentives, and smart contracts to form a decentralized process. For results, blockchain has the advantages of being open, distributed, and non-modifiable. For security management blockchain is to use elliptic curve digital signature algorithm to encrypt, elliptic curve encryption to blockchain and digital currency extremely high security.

4.2 The elliptic curve encryption in Bitcoin

Bitcoin is a virtual cryptocurrency in the form of P2P. Its encryption mechanism is using elliptic curve encryption, which is called elliptic curve digital signature algorithm. In real work and life, we use signature to express recognition of a document, other people can identify your signature and can not forge your signature, and digital signature is a kind of electronic implementation of the real signature, it can not only fully achieve the characteristics of the real signature, even can do better. Bitcoin chooses the elliptic curve digital signature algorithm, and the reason why bitcoin chooses the elliptic curve digital signature algorithm is because of its two advantages: when the public key is known, the private key corresponding to the public key cannot be deduced; there are ways to prove that someone has a private key that corresponds to a public key without revealing anything about the private key.

The elliptic curve for Bitcoin is $y^2 = (x^3 + 7) \mod p$, The elliptic curve parameter is Secp256k1, where Secp is Standards for Efficient Cryptography Parameters, 256 is 256 bits, and K is Koblitz curve. The implementation process of the elliptic curve encryption algorithm in Bitcoin is as follows: first, a 256-bit binary number is randomly generated, that is, a private key; then we use elliptic curve encryption to process the number, get the public key, $Pub_{key} = \Pr iv_{key} * G$, The G here refers to the pre-agreed point, called the generator(G); The public key is then hashed twice to get the bitcoin address. The hashing operation can generate a character band of specified length for any length of data.

5.ELLIPTIC CURVE ENCRYPTION DECRYPTION CODE IMPLEMENTATION

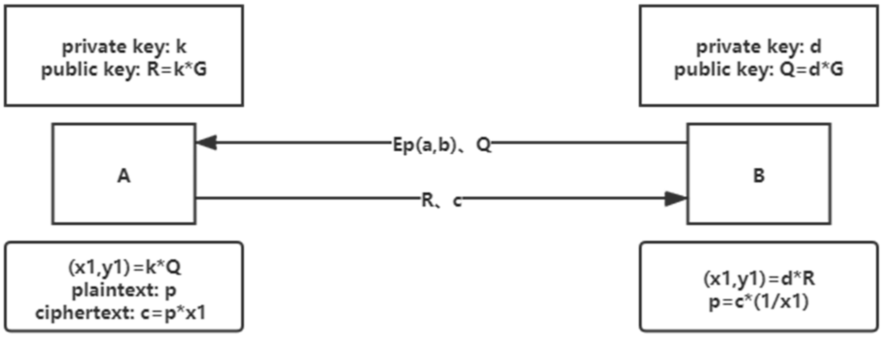
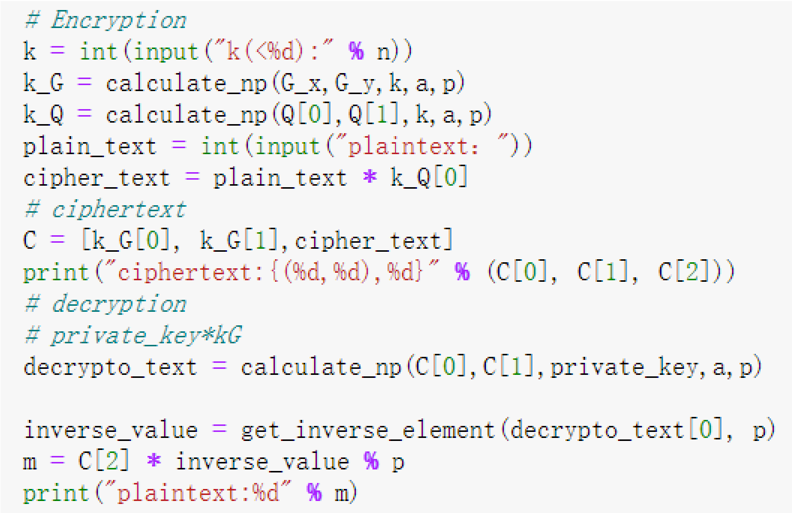


Figure 1 Elliptic curve encryption and decryption process

As shown in figure 1, A and B based on the elliptic curve encryption communication process, the specific steps are as follows, first send A selection of the elliptic curve parameter a, b and B's public key Q, A calculated after receiving the product of its own private key and public key B, $(x1, y1) = k*Q = k*d*G$, the encryption key to unlock the product is communication, A will need to encrypt plaintext p and x1multiplication, You get ciphertext c, and that's the encryption process. When the ciphertext c and public key R is received by B, B multiplies its private key with the public key of A to obtain $(x1, y1) = d*R = d*k*G$. Then, B can solve the ciphertext, $p = c*(1/x1)$ according to the coordinate and obtain the plaintext p. As shown in figure 2, part of the code for encryption and decryption is as follows.

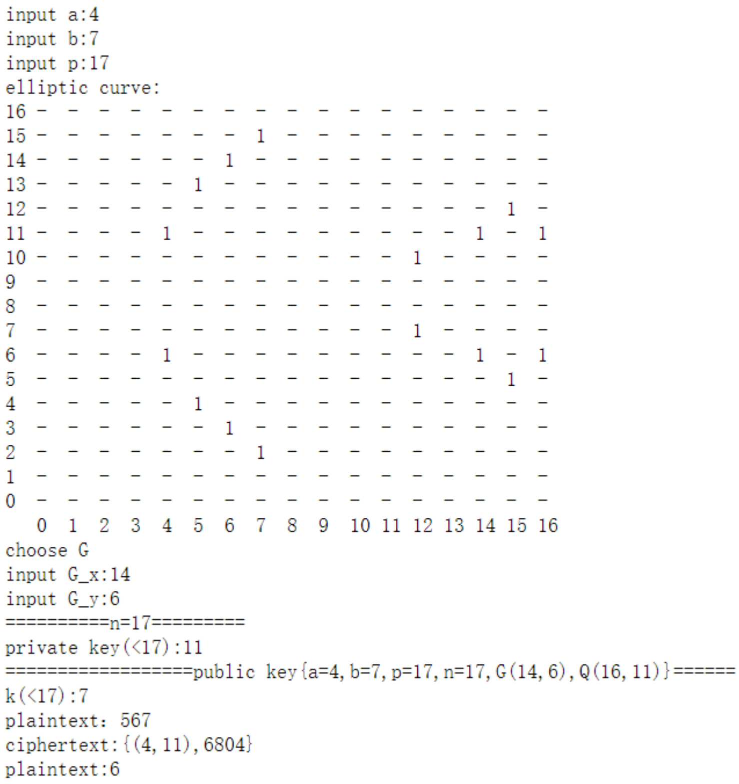


```
# Encryption
k = int(input("k(<%d):" % n))
k_G = calculate_np(G_x, G_y, k, a, p)
k_Q = calculate_np(Q[0], Q[1], k, a, p)
plain_text = int(input("plaintext: "))
cipher_text = plain_text * k_Q[0]
# ciphertext
C = [k_G[0], k_G[1], cipher_text]
print("ciphertext:{(%d,%d),%d}" % (C[0], C[1], C[2]))
# decryption
# private_key*kG
decrypto_text = calculate_np(C[0], C[1], private_key, a, p)

inverse_value = get_inverse_element(decrypto_text[0], p)
m = C[2] * inverse_value % p
print("plaintext:%d" % m)
```

Figure 2 Encrypt the decryption part of the code

As shown in Figure 3, the result of the program run is:



```
input a:4
input b:7
input p:17
elliptic curve:
16 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
15 -  -  -  -  -  -  -  1  -  -  -  -  -  -  -  -  -
14 -  -  -  -  -  -  1  -  -  -  -  -  -  -  -  -  -
13 -  -  -  -  -  1  -  -  -  -  -  -  -  -  -  -  -
12 -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  1  -
11 -  -  -  -  1  -  -  -  -  -  -  -  -  -  1  -  1
10 -  -  -  -  -  -  -  -  -  -  -  -  1  -  -  -  -
9  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
8  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
7  -  -  -  -  -  -  -  -  -  -  -  -  1  -  -  -  -
6  -  -  -  -  1  -  -  -  -  -  -  -  -  -  1  -  1
5  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  1  -
4  -  -  -  -  -  1  -  -  -  -  -  -  -  -  -  -  -
3  -  -  -  -  -  -  1  -  -  -  -  -  -  -  -  -  -
2  -  -  -  -  -  -  -  1  -  -  -  -  -  -  -  -  -
1  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
0  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
   0  1  2  3  4  5  6  7  8  9  10 11 12 13 14 15 16
choose G
input G_x:14
input G_y:6
==========n=17=========
private key(<17):11
=================public key{a=4,b=7,p=17,n=17,G(14,6),Q(16,11)}======
k(<17):7
plaintext： 567
ciphertext:{(4,11),6804}
plaintext:6
```

Figure 3 Encrypted decrypted code run results

Through code simulation of encrypted communication between two points, it can be seen that elliptic curve cryptosystem has high flexibility and security.

6.CONCLUSION

Number theory occupies a pivotal position in the cryptology, for blockchain of elliptic curve encryption, it gives the privacy protection and signature mechanism of modern society provides a good way of thinking. When using code to simulate elliptic curve encryption, it is considered that the security of elliptic curve encryption may be further improved if the parameters of elliptic curve are encrypted simultaneously when the communication is encrypted. Along with the social development, the elliptic curve encryption or encryption algorithm of the other, will get more in-depth application in all fields and recognition.

REFERENCES

[1] Boneh D. Twenty years of attacks on the RSA cryptosystem[J]. Notices of the AMS, 1999, 46(2): 203-213.

[2] Lopez J, Dahab R. An overview of elliptic curve cryptography[J]. 2000.

[3] Lauter K. The advantages of elliptic curve cryptography for wireless security[J]. IEEE Wireless communications, 2004, 11(1): 62-67.

[4] Gura N, Patel A, Wander A, et al. Comparing elliptic curve cryptography and RSA on 8-bit CPUs[C]//International workshop on cryptographic hardware and embedded systems. Springer, Berlin, Heidelberg, 2004: 119-132.

[5] Bos J W, Halderman J A, Heninger N, et al. Elliptic curve cryptography in practice[C]//International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2014: 157-175.

[6] Wang H, He D, Ji Y. Designated-verifier proof of assets for bitcoin exchange using elliptic curve cryptography[J]. Future Generation Computer Systems, 2020, 107: 854-862.