Comparing and Implementation of Public Key Cryptography Algorithms on Smart Card

Zhang Peng
Key Laboratory of Instrumentation Science & Dynamic
Measurement,Ministry of Education
North University of China
Taiyuan, 030051, China
e-mail:zhangpeng@126.com

Jia Jian Fang
Information and Communication Engineering
North University of China
Taiyuan, 030051, China
e-mail:jiajianfang@126.com

Abstract: **As the smart card is used increasingly and widely, security becomes a primary issue for information transmission. public key cryptography is the main research directions of smart card encryption. This article first analysis of the principles of public key cryptography, illustrates two typical cryptographics RSA and ECC. Moreover, comparison and discussion about public key sizes and the security required of these two cryptographics. In the case of Ecc's uses with smaller keys to provide high security and high speed in a low bandwidth, this article select ECC cryptographic to implement the smart card encryption.**

Keywords: Smart card; Public key cryptography; RSA; ECC

I. INTRODUCTION

Similar in size to today's plastic payment card, the smart card has its own CPU, memory and COS, almost equivalent to a computer, and it can implement information storage and data processing. With the development of software and hardware technology,smart card is widely used in medical, transportation, communications, finance, and other areas.

As information technology continues to evolve, people increasingly high demand for information security of smart card.Information security is one of the main directions of smart card, this naturally gives rise to the need for reliable,efficient and convenient cryptograghic algorithms.Since Whitfield Diffie and Martin Hellman first proposed Public Key Cryptography(PKC) algorithm in the paper "New Direction in Cryptography" in 1976[1], many PKC algorithm are arised and widely used.

Smard card is an ideal medium for use with PKI applications. It provide secure storage of confidential data and is capable of executing complex cryptographic algorithms, such as RSA, EIGammal and elliptic curve cryptography(ECC).

This paper describes RSA and ECC algorithms, compares these two cryptosystems performance applicated in smart card, and gives improvement proposal and further development.

II. PRINCIPLES OF PKC

PKC algorithm can be divided into two kinds of public key and private key. In PKC system, public key is open, however private key is kept confidential, and the private key cannot be calculated only from the public key. Anyone who informed the user public key is available to encrypt information for secure information exchange with the user. As the public key and private key are diffident, only the user can decrypt the message, any user who were not authorized and the sender cannot decrypt this message.

The system of PKC is shown in fig 1. If Sender A want to send massage m to Receiver B, he calculate cipher text c with the encryption function of ENCeB (m), then transport cipher text to Receiver B. When Receiver B get massage m', he calculate with the function of DECdB (c) to obtain massage m.

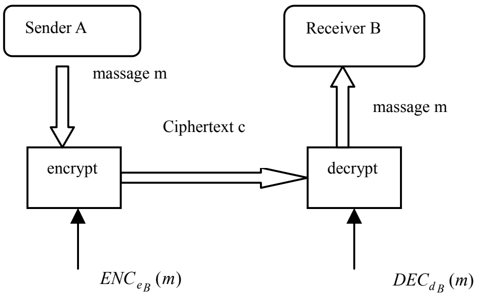

Fig1 PKC encryption

2.1 Theory of RSA Cryptosystem

The RSA cryptosystem was invented in 1977 by Rivest, Shamir and Adleman. It is the best known of the integer factorization family of cryptosystems where the strength of the cryptosystem lies in the mathematical difficulty of factoring large integers.

The RSA key pair generation algorithm is generated by following steps.

(1)Choose two random primes, p and q, of length l/2.

(2)Calculate n=p*q and Φ= (p-1) (q-1).

(3)Choose integer e to meet 1<e<Φ and gcd(e, Φ)=1.

(4)Calculate integer d to meet 1<d<Φ and e*d=1(mod Φ).

(5)Get the public key pair (e,n) and the private key pair (d, n).

Where n is RSA's operation mode, e is signified encryption index, l is signified security parameters and d is signified private key.

RSA encryption scheme is get cipher text by the encryption formula c=me mod n, and get the explicitly by the decryption formula m= cd mod n.

2.2 Theory of ECC Cryptosystem

ECC is a public key primitive that is increasingly important as alternative to RSA. ECC was proposed independently by Miller and Koblitz in 1985, is becoming widely known and accepted. Elliptic curves are mathematical constructions, that can be defined over and field. A field is defined by a set of elements and some operations that have some special properties [2].

Order E is the finite field Fp on the elliptic curve, P is a point on the elliptic curve. E is defined by formula (1).

y2=x2+ax+b (1)

Where a,b∈Fp, and satisfies formula(2).

4a3+27b2≠0(mod p) (2)

Set the order of P is a prime n, so that assemblage P is a cyclic subgroups of elliptic curves which generated by P. Prime P, elliptic curve equation E and order n constitute a public set of parameters. The ECC key pair generation algorithm is generated by following steps.

(1)Choose a random key d in [1,n-1].

(2)Calculate Q=d*p.

(3)Get the public key pair(Q,d).

Where d is signified private key and Q is signified public key.

To achieve the elliptic curve encryption, following steps need to do.

Expressed plaintext m as elliptic curve point M.

(1)Choose a random key k in [1, n-1].

(2)Calculate C1=k*p.

(3)Calculate C2=M+k*Q.

(4)Get the public key pair (C1, C2).

Where C1 and C2 are ciphertexts.

The decryption process is receiver calculate M by formula M= C2+d* C1, then get plaintext m.

III Comparison

RSA and ECC are two public key algorithms. We can comparison these two cryptographic algorithms in key size.

As is shown in table 1[3], if security level is given, ECC has a small parameter than RSA. The higher level of security, the gap of parameters size more obvious. Smaller parameter will make computing faster,shorter keys and smaller key certificates, the computation speed of ECC is many times faster than the RSA. For example, RSA key size is 1024 bit and ECC key size is 160 bit at the 80 security level, their key size ratio is 1 to 6. When the security level is raised to 256, their key size ratio increase of 1 to 30.

Table1 Equivalent key sizes for ECC and RSA

Algori thm	Security(bits)				
	80	112	128	192	256
RSA	1024	2048	3072	8192	15360
ECC	160	224	256	384	512

The advantage of RSA algorithm are simple mathematical principle and easier to achieve in engineering applications.,but its relatively low strength of the unit safety. To ensure the security of use RSA, key size must be increased, generally believed that more than 1024 bit key size is security. However,the increase in key size will led to significantly reduce the speed of encryption and decryption, and hardware becomes more complex.

ECC algorithm can achieve the same encryption results of the RSA algorithm only by use shorter key, this indicates that ECC's safety performance is better. Moreover, ECC's key generation rate is hundred times than RSA's. In addition, ECC occupy a small storage space. These benefits make ECC widespread used.

IV Implementation

At present, smart card is mainly used for electronic identification and storing user information. The security services offered by a smart card often include both data encryption and public key operations. Creation of a digital signature is often the most computationally intensive operation demanded of a smart card.

The hardware resources of smart card are limited; security system is facing the constraints of memory capacity and computing power. ECC encryption is capble of compensate for the limitations of the smart card hardware. On the one hand, the key genertated from ECC is short, which means less storage capacity, faster information transfer rate and computing power can be achieved. On the other hand, the use of ECC in the smart card does not require additional hardware, thereby reducing the cost of hardware and improving the usability.

To implement an ECC, an implementor must select a finite field in which to perform arithmetic calculations. Elliptic curve selection and parameter determination may make difference results, how to improve the efficiency of the cryptosystem become the focus of researchers.

Research in cryptography elliptic curve is essentially a large prime fields GF(p) and is launched on finite field GF(2m) of characteristic 2. We only study the case of characteristic 2 in this paper,.In this case, the formula(1) can be further simplified and shown in formula(3).

y2+xy=x3+a6, a6∈F2m (3)

After the elliptic curve is determined(see formula(3)), order n with SEA algorithm[4]. Next, generate elliptic curve key pair according to the ECC key pair generation algorithm identified in 2.2. Finally, realize smart card information encryption and decrytion by the elliptic curve encryption scheme defined in 2.2.

Implementing ECC on Intel 8051, generate the key pair with encryption took 5.2s, encryption took 21.3s and decryption took 17.1s. The results are basically consistent with the expected.

V Conclusions and outlook

PKC have been proposed by governmental entities all over the world. ECC and RSA are all typical public key cryptosystem. This paper compares the two cryptosystems, indicate that ECC is quicker evolving capacity and by providing arrtactive and alternative way to researchers of cryptographic algorithm than RSA.

This paper applied ECC encryption to the Intel 8051 to achieve encryption and decryption. Although smart card had restricted by hardware, ECC features are capble to compensate for this lack and meet the safety requirements of the smart card.

ECC is a very effective and safe PKC and has gradually become part of the various safety standards. Enhancing comupte power, solving large integer factorization problem and discreting logarithm algorithm will be possible to improve the efficiency of smart card encryption.

REFERENCES

[1]. Diffie,W.and Hellman M., ”New directions in Cryptography”, IEEE Transactions on Information Theory, 1976 22(6), pp:644-654.

[2]. Johan Borst,Bart Preneel,Vincent Rijmen,”Cryptography on smart cards”,Computer Networks, 2001 36,pp:423-435.

[3]. Dr.R.Shanmugalakshmi and M.Prabu, ”Research Issues on Elliptic Curve Cryptography and Its applications”, International Journal of Computer Science and Network Security, 2009 9(6),pp:19-22.

[4]. Lercier R, et al, ”Counting the number of points on elliptic curves over finite fields:Strategies and performances”, Eurocrypto 1995,LNCS 2045,pp:79.