A Study on the Relationship between Properties of the Elliptic Curves and Performance of Elliptic Curve Method (ECM)

Jizhe Cui[1], Seung-won Shin[2] and Jong-Uk Choi[3]
[1]Advanced Information Technology Laboratory, Sangmyung University
Seoul, South Korea 110-743. Phone: +82-2-2287-5214, Fax: +82-2-395-5214, Email: jzcui@ait.re.kr
[2]Advanced Information Technology Laboratory, Sangmyung University
Seoul, South Korea 110-743. Phone: +82-2-2287-5214, Fax: +82-2-395-5214, Email: swshin@ait.re.kr
[3]TrusTech
8-11. 5F, chungha b/d, Chamwon-dong, Seocho-ku, Seoul, South Korea. Phone : +82-2-3445-9194, Fax: +82-2-3445-9195, Email: juchoi@trustech.co.kr

Abstract

Recently encryption algorithms based on difficulties of factorization have been used with popularization. Prime number factorizations are progressed rapidly.
In this paper, characteristics of elliptic curve are analyzed and generation of elliptic curves suitable for prime number factorization is discussed.

Keywords

ECM, algebraically closed field, torsion subgroup, quadratic residue

1. Introduction

Studies on prime number factorization have been actively pursued with popularization of public key algorithms that mainly rely the strength of encryption on difficulties of factorization. However, polynomial algorithms that can drastically reduce computation time have not been developed for the input value. Even though quantum computer-based polynomial time algorithm was suggested by Shor, the quantum computer has not been realized.
Prime number factorizations are classified into algorithms which depend its computation time on the composite number n and algorithms which depend on its prime number. For the former, the number field sieve algorithm is known as the best one, and its complexity is $O(\exp[(64/9)^{1/3}(\ln\ln N)^{2/3}])$. For the latter, ECM (Elliptic Curve Method) is known as the best algorithm and its complexity is $O(L_p[1/2, \sqrt{2}+o(1)])$, if the maximum prime number of the composite number is p. As the ECM depends on ln p, size of p, rather than size of n, fast computation is possible if the size of p is small, even though the size of n is large.

In this paper, characteristics of elliptic curve are analyzed and generation of elliptic curves suitable for prime number factorization is discussed.

2. Elliptic Curve

2.1 Definition of Elliptic Curves and Operation

Definition of Elliptic Curve: Let assume that $p>3$ $p \in prime$, and O is infinite point. When the following conditions are satisfied, the set is defined as elliptic curve on the prime number field $GF(p)$.

$$E(GF(p)) = \{(x,y) \in GF(p)^2 \,|\, y^2 = x^3 + ax + b \mod p,\ a,b \in GF(p),\ 4a^3 + 27b^2 \neq 0 \mod p\} \cup \{O\}$$

The equation is called a definition equation of elliptic curve, and the points that satisfy the equation are called rational point. The number of points on $E(GF(p))$ is called order of curve, being represented by $\#E(GF(p))$. The collection of rational points becomes additive group in the following calculation.

Elliptic Curve group operation: The operation of '+' for $P_3(x_3, y_3)$, which corresponds to $P_1(x_1, y_1)$ and $P_2(x_2, y_2)$ is defined as the following:

* This research was supported by a KOSEF(1999-2-511-001)

1. $P+O=O+P=P(\forall P\in E(GF(p))$ (Infinite point is unit element.)
2. $P=(x,y)\in E(GF(p))$
   $(x,y)+(x,-y)=O(-P=(x,-y))$
3. $P_1=(x_1,y_1)\in E(GF(p))$,
   $P_2=(x_2,y_2)\in E(GF(p))$

$$P_1\neq P_2 \quad P_1+P_2=(x_3,y_3)$$
$$x_3=\lambda^2-x_1-x_2,\quad y_3=\lambda(x_1-x_3)-y_1$$
$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1} & if\ P_1\neq P_2\\ \dfrac{3x_1^{\,2}+a}{2y_1} & if\ P_1=P_2\end{cases}$$

Table 1. Comparison of Finite field($GF(p)$) and Elliptic Curves group($E(GF(p))$)

Group	$GF(p)$	$E(GF(p))$
Group Element	Integer {1, 2, ... ,p-1}	pointer (x, y) and O of E
Group Operation	Multiplication in Mod p	Addition of points
Notation	element: g, h multiplication: g*h inverse element: g^{-1} division: g/h exponent: g^a	element: P_1, P_2 addition: P_1+P_2 inverse element: $-P_1$ subtraction: P_1-P_2 multiple: aP_1

Points on the elliptic curves become Abel group by Elliptic Curve group operation. As to the group elements, the following theorem is made..

Theorem 2.1: $\forall x\in GF(p),\ \exists e\in GF(p) \quad x^e=1$.
In the theorem, 1 is unit element of the group, and if the operation is addition, $ex=x+x+\cdots+x=0$. Especially, the minimum positive integer m, if the condition $mx=0$ is satisfied, is called the number of group element.

2.2 Elliptic Curve on Finite Field

Theorem 2.2 (mordell-Weil) $E(GF(p))$ on elliptic curves are finite Abel group. That is,

$$E(GF(p))=E(GF(p))_{tor}\oplus Z\oplus\cdots\oplus Z$$

where $E(GF(p))_{tor}$ is set whose order is finite. Subgroup $E(GF(p))_{tor}$ is called torsion subgroup of $E(GF(p))$.

The following two theorems on elliptic curves play important roles in explaining the relationship between changes of coefficients in elliptic curves and changes in its order

.

Theorem 2.3(Hasse-weil) The order $\#E(GF(p))$ of the elliptic curve group $E(GF(p))$ defined on finite field $GF(p)$ satisfies the following condition:

$$p+1-2\sqrt{p}\le\#E(GF(p))\le p+1+2\sqrt{p}$$

Theorem 2.4(Deuring) When the coefficients of the elliptic curve a , b modify $GF(p)$, $t=\#E(GF(p))-(p+1)$ is equally distributed in the interval $-2\sqrt{p}\le t\le 2\sqrt{p}$ and takes all the integer values in the interval.
The classification based on torsion subgroup of elliptic curves manly relies on the following theorems.

Theorem 2.5(Mazur): $E(GF(p))_{tor}$, torsion subgroup of elliptic curve defined in rational number field Q becomes an isomorphism of the following 15 groups.

$$\begin{cases} Z/\eta Z & \eta=1,2,\cdots,10,12\\ Z/2Z\times Z/2\eta Z & \eta=1,2,3,4\end{cases}$$

Theorem 2.6(Kamienny-Kenku-Momose) The torsion subgroup $E(GF(p))_{tor}$ defined in quadratic field $Q(\sqrt{m})$ is an isomorphism of the following 26 groups.

$$\begin{cases} Z/\eta Z & \eta=1,\cdots,16,18\\ Z/2Z\times Z/2\eta Z & \eta=1,\cdots,6\\ Z/3Z\times Z/3\eta Z & \eta=1,2 \quad when \quad m=-3\\ Z/4Z\times Z/4Z & when\ m=-1\end{cases}$$

2.3 Division Polynomial

Operation of polynomial ring is defined by addition and multiplication. When the order of the polynomial equation is low, the number of multiplication operation is small, but the number of addition operation is relatively large. If the order of the polynomial equations is high enough, the number of operation can be lowered by dividing the polynomial equations. Divided polynomial equations are defined

in the groups of rational elements in algebraically closed fields. Please refer the book [3].

3. Generation of Elliptic Curve

3.1 ECM (Elliptic Curve Method)

Elliptic Curve Method (ECM) is a prime number factorization algorithm suggested by Lenstra Jr. in 1987[1]. The elliptic curve defined in the rational fields $GF(p)$ for the prime number p satisfies $\#E(GF(p)) \cdot P = O$ for its order and arbitrarily defined point P on the curve. When the number n is factorized into prime numbers, p is not known. The prime number factorization can be applied to the following two types of elliptic curves:

1. When the elliptic curve is considered in the ring of $R = Z / nZ$ and addition operation is conducted, operation of inverse element in mod n is required. However, as there does not exist all inverse elements for each arbitrarily defined element, inverse operation can fail. When the inverse operation fails, operation should stop. Let's assume the number obtained at the stopping point of inverse operation is F. Then, the relationship is satisfied GCD(F, n) = p.
2. Let's assume we want to factorize n into prime numbers, and set the point P and integer number m on the elliptic curve to calculate mP. When $\#E(GF(p)) | m$ is satisfied, $mP = O$ for $E(GF(p))$ and for $E(R)$, resulting into $mP = O$. Thus, the calculation is made impossible and the above process can be applied to obtain the prime number of n.

The process of prime number factorization is ECM.

As discussed above, the following four problems should be should to enhance the performance of elliptic curves.

1. Generation of appropriate elliptic curves
2. Selection of the starting point P on the elliptic curves and selection of the integer number m.
3. Enhancement of computation speed in addition operations.
4. Estimation of range for prime number p.

3.2 Generation of Elliptic Curve

Generation of elliptic curves has the most important effects on the decryption performance. That is, what elliptic curves are to be used in the decryption determined the effectiveness of the ECM. The following three problems should be considered.

1. Generation of elliptic curves to accelerate computation speed of addition operation.
2. Generation of elliptic curves so that $\#E(GF(p))$ in prime number fields is smooth.
3. Optimal implementation of addition operations depending on the computer architecture.

Various approaches have been suggested to selection of elliptic curves for enhancing the computation time in addition operation.

Method [B1]: A typical elliptic curve is one introduced by Montgomery and being popularly used in ECM [2]. The elliptic curves are applied to prime number factorization to reduce computation time.

Method [B2]: Based on the Theorem 2.3 and Theorem 2.4, $\#E(GF(p))$ is possibly random number as large as p. Finding a smooth curve is generally difficult. However, with the use of curve whose order is small divisor d, the size of random changes decreases from p to p/d. Therefore, possibility of successful factorization into prime number increases. Suyama suggested an ECM which renders $d = 12$ at the starting point. After the suggestion, Atkin-Morain suggested a composition method with $d = 16$. As the composition method for the elliptic curves of $d \leq 16$ uses torsion Subgroup suggested by Mazur Theorem, it can be applied to every value of p. On the other hand, as the elliptic curve composition method which is applicable to $d > 16$ uses subgroup employed in the theorem of Kamienny-Kenku-Momose, it can be applied to appropriate p. However, in this case, if the value of d increments, the successful implementation of factorization into prime number is enhanced. The method 3 can be divided into two categories: d=12 and d =18.

Method [B3, B4]: In [B3] *d=12* is used to be compatible with the elliptic curves of Montgomery. It was used also in [B1] to analyze the performance. In [B4] *d=18* is used to compatible with the elliptic curves of Montgomery to analyze the performance.

4. Application Effects of ECM

Currently library functions for 20~35 bit are available in internet. Let's assume that a prime number of 4 – 25 digits and another prime number of 36 digits.

1733(4), 7853(4), 79139(5), 14669(5), 306091(6), 141529(6), 2812583(7), 73629553(8), 53643809(8), 415668563(9), 211941187(9), 3821263937(10), 18546805133(11), 39589685693(11), 499123818241(12), 774017083691(12), 4531100550901(13), 6102530946904l(14), 6896671519701 61(15), 594960058508093(15), 115247030905506311529891723062628161(36)

When a number is generated by multiplying two prime numbers, the number of possible combination is $C_{21}^{2}+21$. For the number, the three methods of [B1], [B2], and [B3, B4] have been applied.

Application and Analysis
System Specification: Pentium II, 8X speed, intel

Table 2 Results of Each Method.

Method	B1	B3	B4
Curve check	345 iterations	320 iterations	341 iterations
Computation Time	1 Min 32 Sec	1Min 21Sec	1Min 37Sec

At the time of prime number factorization, only the number n is known. For the method [B2] it is assumed that it s prime number is p. As it is not certain that (-3) is quadratic residue of , it is assumed that prime numbers of the composite number are known. Then analysis based on elliptic curves is as following:
For $n_1 = p_1 q$, $n_2 = p_2 q$
In the situation

$$p_1 = 499123818241,\ p_2 = 774017083691,$$
$$\text{and } q = 992474642815068364143371,$$

the success rate is lowered in $n_1 = p_1 q$ [4]. In the experiment, it was concluded that B3 is better. It is explained that constratins are enforced on p by the theorem 2.6 (Kamienny-Kenku-Momose), when the elliptic curves are identical to the curves generated by the torsion subgroup $E(GF(p))_{tor}$ and $d \geq 16$ is satisfied.

5. Conclusion

In this paper, a study on the performance of ECM and characteristics of elliptic curves in infinite fields was conducted to enhance the computation time of the prime number factorization. As a result of the experiments, rather than relying on random selection of coefficients of elliptic curves, the system can improve its computation speed by selecting elliptic curves which are can prove addition time. The improvement of computation speed ranges from 6% [Method B2] to 12%[Method B3]. Furthermore, to improve the computation speed, it is desirable to implement with d=16.

Refernces

1. Lenstra Jr. H. W., "Factoring Integer with Elliptic Curves," Annals of Math. 126, 649-673, 1987.
2. Montgomery, P. L. Speeding the Pollard and Elliptic Curve Methods of Factorizations, Math. Comp. 48, 243-264, 1987.
3. Silverman, J. H., "The Arithmetic of Elliptic Curves," GTM 106, Springer, 1991.
4. IZU Tetsuya, "Generation Elliptic Curves Suitable for Factorization," The 2000 Symposium on Cryptography and Information Security Okinawa, Japan, January 26-28, 2000
5. Kazumaro AOKI, Tetsutaro KOBAYASHI and Fumitaka HOSHINO "The Fastest ECC Implementations," The 2000 Symposium on Cryptography and Information Security Okinawa, Japan, January 26-28, 2000