# On the coefficients of the polynomial in the number field sieve ⋆

Yang Min [a], Meng Qingshu [b,*], Wang Zhangyi [b], Li Li [a], Zhang Huanguo [b]

[a] *International School of Software, Wuhan University, Hubei, China, 430072*

[b] *Computer School, Wuhan University, Hubei, China, 430072*

**Abstract**

Polynomial selection is very important in number field sieve. If the yield of a pair of polynomials is closely correlated with the coefficients of the polynomials, we can select polynomials by checking the coefficients first. This can speed up the selection of good polynomials. In this paper, we aim to study the correlation between the polynomial coefficients and the yield of the polynomials. By theoretical analysis and experiments, we find that a polynomial with the ending coefficient containing more small primes is usually better in yield than the one whose ending coefficient contains less. One advantage of the ending coefficient over the leading coefficient is that the ending coefficient is bigger and can contain more small primes in root optimizing stage. The number of real roots can be determined by only the last two or three coefficients of the polynomial if it is skewed. All these observations can be used to speed up the search of good polynomials for the number filed sieve.

*Key words:* cryptography, integer factorization, number field sieve, polynomial selection, coefficients

## 1 Introduction

The general number field sieve[1,2] is known as the asymtotically fastest algorithm for factoring large integers. It is based on the observation that if

⋆ This work is supported in part by the National Natural Science Foundation of China(No.61003267, No.61202385, No.21202386) and the Fundamental Research Funds of Central Universities

* Corresponding author

*Email address:* mqseagle@yahoo.com (Meng Qingshu ).

$a^2 = b^2 \, mod \, N$ and $a \neq b$, $gcd(a - b, N)$ will give a proper factor of N with at least a half chance. The number field sieve starts by choosing two irreducible and coprime polynomials f(x) and g(x) over Z which share a common root $m$ modulo $N$. Let $F(x, y) = y^{d_1} f(x/y)$ and $G(x, y) = y^{d_2} g(x/y)$ be the homogenized polynomials corresponding to $f(x)$ and $g(x)$ respectively, where $d_1$ and $d_2$ are the degree of $f(x)$ and $g(x)$ respectively. We want to find many coprime pairs $(a, b) \in Z^2$ such that the polynomials values $F(a, b)$ and $G(a, b)$ are simultaneously smooth with respect to some upper bound B and the pair $(a, b)$ is called a relation. An integer is smooth with respect to bound $B$ (or $B$-smooth) if none of its prime factors are larger than $B$. If we find enough number of relations, by finding linear dependency[3,4] we can construct:

$$\prod_{(a,b)\in S} (a - b\alpha_1) = \beta_1^2, where \ f(\alpha_1) = 0, \beta_1 \in Z[\alpha_1]$$

$$\prod_{(a,b)\in S} (a - b\alpha_2) = \beta_2^2, where \ g(\alpha_2) = 0, \beta_2 \in Z[\alpha_2].$$

As there exist maps such that $\varphi_1(\alpha_1) = m \ mod \ N$ and $\varphi_2(\alpha_2) = m \ mod \ N$, we have $\varphi_1(\beta_1^2) = \varphi_2(\beta_2^2)$. We can obtain the square root $\beta_1$ and $\beta_2$ from $\beta_1^2$ and $\beta_2^2$ respectively using method in [5]. If we let $\varphi_1(\beta_1) = x$ and $\varphi_2(\beta_2) = y$, then $y^2 = x^2 \, mod \, N$, and we have constructed a congruent squares and so may attempt to factor $N$ by computing $gcd(x - y, N)$.

In order to obtain enough relations, selecting a polynomial with high probability of being smooth is very important. A good polynomial not only can decrease sieving time, but also can reduce the expected matrix size[6]. The polynomial selection is now a hot research area. Based on base-m method and with translation and rotation technique[6], non-skewed or skewed polynomial can be constructed, where one polynomial $f(x)$ is nonlinear and the other $g(x)$ is monic and linear. If the linear polynomial is nonmonic, the size of nonlinear polynomial can be greatly reduced[7,1]. The two methods above are called linear method. Montgomery[8] proposed the nonlinear method, where the two polynomials are both nonlinear. Recently several papers[9–11] address nonlinear polynomials construction problem.

The concept of evolutionary cryptography was proposed in [12] and its idea was used to design cryptographic functions[13,14] or cryptographic algorithm[15]. The capabilities of evolutionary cryptosystem against linear and differential cryptanalysis were given in [16,17] respectively. To search for good polynomials for number field sieve with evolutionary computing, we need to solve the difficulty that the space of candidate polynomials is too huge. With the idea similar to [13], we study if there exists any correlation between the polynomial coefficients and the yield of the polynomials. If they are closely related, we can search for polynomials by checking the coefficients first before calcu-

lating its alpha value[6]. Therefore we can search for good polynomials in a smaller space. This would speed up the selection of polynomials. By theoretical analysis and experiments, we find that the yield of polynomial is closely related to the coefficients of the polynomial. The polynomial with ending coefficient containing more small primes usually have better yields. We also find that the number of real roots can be determined by partial coefficients of the polynomial if it is skewed.

The rest of the paper is organized as follows. In Section 2 we review elements related to the yield of a polynomial. In Section 3 we recite the number of real roots of a rational polynomial. In Section 4 we analyze the effect of the ending coefficient and leading coefficient on the yield respectively. In Section 5 we analyze the effects of coefficients on the number of real roots and on the yield. Finally we make a conclusion in Section 6.

## 2 Elements related to smoothness of a polynomial

An integer is said to be B-smooth if the integer can be factored into factors bounded by B. By Dickman function, given the smooth bound B, the less the integer is, the more likely the integer is B-smooth. In number field sieve, we want the homogenous form $F(x, y) = a_d x^d + \cdots + a_1 x y^{d-1} + a_0 y^d$ of the polynomial $f(x) = a_d x^d + \cdots + a_1 x + a_0$ to be small. In [6], the size and root property are used to describe the quantity. By size we refer to the magnitude of the values taken by $F(x, y)$. By root property we refer to the distribution of the roots of $F(x, y)$ modulo small $p^k$, for p prime and $k \geq 1$. If $F(x, y)$ has many roots modulo small $p^k$, values taken by $F(x, y)$ "behave" as if they are smaller than they actually are. That is, on average, the likelihood of $F(x, y)$ values being smooth is increased. It has always been well understood that size affects the yield of $F(x, y)$. In [18], the number of real roots, the order of Galois group of $f_1(x)f_2(x)$ were taken into account. By the number of real roots, if $a/b$ is near a real root, the value $F(a, b)$ will be small and will be smooth with high chance. By the order of Galois group of $f_1 f_2$, it is better to chose polynomial for which the order of Galois group of $f_1 f_2$ are small, because they provide more free relations.

Obviously, if the coefficients of $f(x)$ are small, $F(x, y)$ would have good size property. In order to obtain polynomial with small coefficients, we can search extensively, or let the linear polynomial be nonmonic as suggested in [1,7]. In order to obtain good root property, usually it is required that the leading coefficient contains many small prime as its factors[6]. The paper[19,20] discussed other ways to improve root property. As for the number of the real roots, it is left as random.

## 3 The number of real roots of a polynomial

In [21,22],the number of real roots or roots distribution of a rational polynomial is given by $CDS$(complete discrimination system).

In degree 3, take polynomial $f(x) = ax^3 + bx^2 + cx + d$ as example. The $CDS$ is

$$\Delta = 18abcd - 4b^3d + b^2c^2 - 4ac^3 - 27a^2d^2.$$

The root distribution is as follows.

(1) If $\Delta > 0$, the equation has three distinct real roots.
(2) If $\Delta = 0$, the equation has a multiple root and all its roots are real.
(3) If $\Delta < 0$, the equation has one real root and two nonreal complex conjugate roots.

In degree 4, take $f(x) = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0, (a_4 \neq 0)$ as example. Its $CDS$ is as follows:

$$D_2 = 3a_3^2 - 8a_2a_4,$$

$$D_3 = 16a_4^2a_0a_2 - 18a_4^2a_1^2 - 4a_4a_2^3 + 14a_4a_1a_3a_2 - 6a_4a_0a_3^2 + a_2^2a_3^2 - 3a_1a_3^3,$$

$$\begin{aligned} D_4 = {} & 256a_4^3a_0^3 - 27a_4^2a_1^4 - 192a_4^2a_1a_0^2a_3 - 27a_3^4a_0^2 - 6a_4a_3^2a_0a_1^2 + a_2^2a_1^2a_3^2 - 4a_4a_2^3a_1^2 + \\ & 18a_2a_0a_3^3a_1 + 144a_4a_2a_0^2a_3^2 - 80a_4a_2^2a_0a_3a_1 + 18a_4a_2a_1^3a_3 - 4a_2^3a_0a_3^2 - 4a_3^3a_1^3 + \\ & 16a_4a_2^4a_0 - 128a_4^2a_2^2a_0^2 + 144a_4^2a_2a_0a_1^2, \end{aligned}$$

$$E = 8a_4^2a_1 + a_3^3 - 4a_4a_3a_2.$$

The numbers of real and imaginary roots and multiplicities of repeated roots in all cases are given as follows:

| | |
|---|---|
| (1) $D_4 > 0 \bigwedge D_3 > 0 \bigwedge D_2 > 0$ | $\{1,1,1,1\}$, |
| (2) $D_4 > 0 \bigwedge (D_3 \leq 0 \bigvee D_2 \leq 0)$ | $\{\}$, |
| (3) $D_4 < 0$ | $\{1,1\}$, |
| (4) $D_4 = 0 \bigwedge D_3 > 0$ | $\{2,1,1\}$, |
| (5) $D_4 = 0 \bigwedge D_3 < 0$ | $\{2\}$, |
| (6) $D_4 = 0 \bigwedge D_3 = 0 \bigwedge D_2 > 0 \bigwedge E = 0$ | $\{2,2\}$, |
| (7) $D_4 = 0 \bigwedge D_3 = 0 \bigwedge D_2 > 0 \bigwedge E \neq 0$ | $\{3,1\}$, |
| (8) $D_4 = 0 \bigwedge D_3 = 0 \bigwedge D_2 < 0$ | $\{\}$, |
| (9) $D_4 = 0 \bigwedge D_3 = 0 \bigwedge D_2 = 0$ | $\{4\}$, |

where the column on the right side describes the situations of the roots. For example, $\{1,1,1,1\}$ means four real simple roots and $\{2,1,1\}$ means one real double root plus two real simple roots.

In degree 5, take $f(x) = x^5 + px^3 + qx^2 + rx + s$ as example. Its $CDS$ is as follows:

$$D_2 = -p$$

$$D_3 = 40rp - 12p^3 - 45q^2$$

$$D_4 = 12p^4r - 4p^3q^2 + 117prq^2 - 88r^2p^2 - 40qp^2s + 125ps^2 - 27q^4 - 300qrs + 160r^3$$

$$D_5 = -1600qsr^3 - 3750ps^3q + 2000ps^2r^2 - 4p^3q^2r^2 + 16p^3q^3s - 900rs^2p^3 + 825q^2p^2s^2 + 144pq^2r^3 + 2250q^2rs^2 + 16p^4r^3 + 108p^5s^2 - 128r^4p^2 - 27q^4r^2 + 108q^5s + 256r^5 + 3125s^4 - 72p^4rsq + 560r^2p^2sq - 630prq^3s$$

$$E_2 = 160r^2p^3 + 900q^2r^2 - 48rp^5 + 60q^2p^2r + 1500rpsq + 16q^2p^4 - 1100qp^3s + 625s^2p^2 - 3375q^3s$$

$$F_2 = 3q^2 - 8rp$$

The numbers of real and imaginary roots and multiplicities of repeated roots of polynomial in all cases are given as follows:

| | | |
|---|---|---|
| (1) | $D_5 > 0 \bigwedge D_4 > 0 \bigwedge D_3 > 0 \bigwedge D2 > 0$ | $\{1, 1, 1, 1, 1\}$ |
| (2) | $D_5 > 0 \bigwedge (D_4 \leq 0 \bigvee D_3 \leq 0 \bigvee D_2 \leq 0)$ | $\{1\}$ |
| (3) | $D_5 < 0$ | $\{1, 1, 1\}$ |
| (4) | $D_5 = 0 \bigwedge D_4 > 0$ | $\{2, 1, 1, 1\}$ |
| (5) | $D_5 = 0 \bigwedge D_4 < 0$ | $\{2, 1\}$ |
| (6) | $D_5 = 0 \bigwedge D_4 = 0 \bigwedge D_3 > 0 \bigwedge E_2 \neq 0$ | $\{2, 2, 1\}$ |
| (7) | $D_5 = 0 \bigwedge D_4 = 0 \bigwedge D_3 > 0 \bigwedge E_2 = 0$ | $\{3, 1, 1\}$ |
| (8) | $D_5 = 0 \bigwedge D_4 = 0 \bigwedge D_3 < 0 \bigwedge E_2 \neq 0$ | $\{1\}$ |
| (9) | $D_5 = 0 \bigwedge D_4 = 0 \bigwedge D_3 < 0 \bigwedge E_2 = 0$ | $\{3\}$ |
| (10) | $D_5 = 0 \bigwedge D_4 = 0 \bigwedge D_3 = 0 \bigwedge D_2 \neq 0 \bigwedge F_2 \neq 0$ | $\{3, 2\}$ |
| (11) | $D_5 = 0 \bigwedge D_4 = 0 \bigwedge D_3 = 0 \bigwedge D_2 \neq 0 \bigwedge F_2 = 0$ | $\{4, 1\}$ |
| (12) | $D_5 = 0 \bigwedge D_4 = 0 \bigwedge D_3 = 0 \bigwedge D_2 = 0$ | $\{5\}$ |

## 4 The yield and the ending coefficient

Let $f(x) = a_d x^d + \cdots + a_1 x + a_0$ be a nonlinear polynomial. Let $F(x, y) = a_d x^d + \cdots + a_1 xy^{d-1} + a_0 y^d$ be the homogenous form of polynomial f(x). Let $p_q$ be the number of roots of the homogeneous polynomial F modulo p and let

$$\alpha(F) = \sum_{small\, prime\, p} (1 - p_q \frac{p}{p+1}) \frac{\log p}{p-1}.$$

In order to make $\alpha(F)$ small, we can increase the value of $p_q$. Equation $F(x, y) = 0 \, mod \, p$ has three kind of roots.

(1) If $p|b$ and $p|a_d$, the pair (a,b) is called the projective root.
(2) If $p|a$ and $p|a_0$, the pair (a,b) is called the zero root.
(3) The rest of pairs (a,b) satisfying $F(a, b) = 0 \, mod \, p$ are called ordinary roots, or simply roots.

Correspondingly, there are three methods to increase the value of $p_q$. The first method is already known that the leading coefficient $a_d$ containing many small primes can increase the number of projective roots. For example, the leading coefficient usually is the multiple of 60[7]. As for the ordinary roots,we refer to [19,20].We propose the third method that if the ending coefficient contains many small primes, the number of zero roots can be increased. As $f(x)$ is skewed with $a_d << a_0$, $a_0$ can contain more small primes than $a_d$ can. The number of pair (a,b) satisfying second case would be much more than the one in the first case, especially after the optimization of root properties.

In order to check whether the above analysis is right, we do many experiments. In our experiments, we let N be an integer of about 30 digits. In Experiment 1, the polynomials are generated by base-m method as described in [6], but without the optimization step.

**Experiment** 1:

(1) Generate polynomial as [6]. For each leading coefficient $a_d$ below a bound, we examine

$$m \approx \lfloor (\frac{N}{a_d})^{\frac{1}{d}} \rfloor.$$

Check the magnitude of $a_{d-1}$, and of $a_{d-2}$ compared to $m$, by computing the integral and non-integral parts of

$$\frac{N - a_d m^d}{m^{d-1}} = a_{d-1} + \frac{a_{d-2}}{m} + O(m^{-2}).$$

If these are sufficiently small, accept $a_d$ and $m$, and we get a polynomial $f(x)$ by the expansion of $N$ in base $m$ and with leading coefficient $a_d$.

(2) Collect relations. For each above polynomial, skew the sieving area with skewness$=\sqrt[d]{\frac{a_0}{a_d}}$. Randomly choose enough pair of coprime (a,b) in sieving area and check if they form relations. For each polynomial,we denote the number of relations by $num_{rel}$.

(3) For each polynomial, there is a row corresponding to it. It includes the following items: the number of relations $num_{rel}$, the number of small primes contained in $a_d$ below a predefined bound, denoted by $num_{a_d}$, the number of small primes in $a_0$ below a predefined bound, denoted by $num_{a_0}$. A file is formed.

(4) Sort the above file in ascending order with $num_{rel}$ as key word. From the sorted file, we can find the parameter $num_{a_0}$ and $num_{a_d}$ both are in ascending order, but not strictly. In order to obtain an obvious impression, we divide the sorted file by rows into many length-equal parts, each of which contains equal number of rows and calculate the sum of the parameters $num_{a_d}$ and $num_{a_0}$ in each part respectively.

Table 1
The trend of three parameter(256 rows/block)

| *Block num* | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $num_{ad}$ | 670 | 670 | 718 | 743 | 785 | 771 | 805 | 818 | 959 | 946 |
| $num_{a0}$ | 484 | 482 | 451 | 580 | 622 | 702 | 638 | 710 | 784 | 817 |
| $num_{root}$ | 428 | 462 | 442 | 460 | 440 | 494 | 476 | 482 | 498 | 538 |

Table 1 lists the sums of $num_{a_d}$ and $num_{a_0}$ respectively, where the parameters are as follows. $N = 39327284784436337729633$( an integer in example 3 [9] ). The degree of the nonlinear polynomial is 3. Sieving area is $2A \times A$, where $A = 4000$, coprime pair $(a, b)$ are chosen randomly from sieving area in a way like "for(a=-$A \times s$;a< $A \times s$;a+=rand()%6+1) for(b=1;b< $A/s$;b+=rand()%6+1), where $s = \sqrt[6]{a_0/a_3}$". From Table 1 we find that the ending coefficients correlate with the yields of polynomials as the leading coefficient does. For polynomial of degree 4 or 5, we get similar results.

For nonmonic linear polynomial generated as suggested in [1,7], we can get similar results. For nonlinear polynomials as suggested in[9], we don't do the experiments. We conjecture the results should be similar.

By the analysis above and the experiments, we have:

**Observation 1**: Increasing the number of small primes which are contained in the ending coefficient as factors may increase the yield.

**Remark 1**: In [6], it is said that computing the ideal decomposition for ideals corresponding to projective roots requires more effort than those corresponding to non-projective roots. Therefore, increasing zero roots is a better choice.

**Remark 2**: If the size of N, the integer to be factored, gets larger, the skewness of the polynomial would become larger, and $a_0$ can contain more small primes than $a_d$ can. This can be used in optimization of root properties. The advantage of ending coefficient over leading coefficient will be more obvious in term of relation yield.

## 5 The number of real roots and the coefficients

A polynomial with more real roots are preferable in number field sieve because if $a/b$ is near a real root, the value $F(a, b)$ will be small and will be smooth with high possibility. Usually the number of real roots is left as random in polynomial generation. In [21,22],the number of real roots or roots distribution of a rational polynomial is given by $CDS$. From $CDS$, the number of

real roots should depends on all coefficients of the polynomial. However, the polynomial for NFS is not randomly generated. It has many special properties. For example, it is skewed and usually its first 3 coefficients $a_d, a_{d-1}$ and $a_{d-2}$ are small compared to $m$ while the size of the rest coefficients is similar to or bigger than that of $m$. From this, the ratio $abs(a_{d-3}/a_{d-2})$ will bigger than $\sqrt[d]{a_0/a_d}$ while the ratio $abs(a_0/a_1)$ is smaller than $\sqrt[d]{a_0/a_d}$. Based on all these features and $CDS$ we can analyze the correlation between the number of real roots and the coefficients.

In degree 3, from the expression of $\Delta$, the sign of $\Delta$ should depend on the item $-4ac^3$ or $-27a^2d^2$, but not depend on $-4b^3d$ since $b$ is usually small. If the ratio $abs(d/c)$ is not big, the sign of $\Delta$ mainly be determined by $-4ac^3$. If $c$ is small enough, $\Delta > 0$, which means the polynomial $f(x)$ has 3 real roots. Similarly if the ratio $abs(d/c)$ is big, $\Delta < 0$, which means the polynomial $f(x)$ has only one real root. In Experiment 2, on about more than a half cases the polynomial has 1 real root and on less than a half cases the polynomial has 3 real roots, where the ratio $abs(d/c)$ is small and $c$ is negative and small enough.

In degree 4, from the expression of $D_4$, the exponents of $a_3, a_2, a_1$ are 4 and the exponent of $a_0$ is 3. If the polynomial is skewed, the coefficients $a_1, a_0$ or the ratio $abs(a_0/a_1)$ determine the sign of $D_4$. As the ratio $abs(a_0/a_1)$ is usually smaller than $\sqrt[4]{a_0/a_4}$, we have $abs(27a_4^2a_1^4) > abs(256a_4^3a_0^3)$ and $D_4 < 0$ with large chance. That is, in most case the polynomial has 2 real roots. To obtain 4 real roots, the coefficient $a_2$ should be negative and small enough and the absolute value of $a_1$ should be of similar size with that of $a_2$. In Experiment 2, on about 80 percent of cases the polynomial has 2 real roots and on about 20 percent of cases the polynomial has 4 real roots, where the absolute values of $a_2$ and $a_1$ are of similar size. The case with zero real roots should be avoided.

For degree =5, similarly from the expression of $D_5$, the items $256r^5$ and $3125s^4$ determine the sign of $D_5$. If $r$ is small enough the polynomial will have 3 real roots. It is hard to obtain 5 real roots. In order to avoid the case that there is only one real roots, to have 3 real roots is a good choice.

The analysis above in case of degree 3 should be useful in choosing polynomial in nonlinear method, where a polynomial with degree 3 is already enough for practical purpose.

**Experiment** 2:

(1) Generate polynomial as step 1 of experiment 1.
(2) Collect relation as step 2 of experiment 1. Denote the number of relation by $num_{rel}$.
(3) For each polynomial, there is a row corresponding to it. The row has

$num_{rel}$, the number of real roots $num_{root}$, and all coefficients as its items. We form a file now.

(4) Sort the above file in ascending order with $num_{root}$ as the key word. From the sorted file, we observe the correlation between $num_{root}$ and the polynomial coefficients. In case degree =3, if the coefficients of degree 1 is below some value, there will be 3 real roots for most cases. In case degree=4, if coefficient of degree 2 is below some value, there will be 4 real roots for most cases. In case degree=5, only a few polynomials have 5 real roots.

(5) Sort the file above in ascending order with $num_{rel}$ as the key word. From the sorted file, we observe the correlation between $num_{root}$ and $num_{rel}$. We can find $num_{root}$ is also in ascending order, but not strictly. In order to obtain an obvious impression, we divide the sorted file by rows into many length-equal parts, each of which contains equal number of rows and calculate the sum of the parameters $num_{root}$ in each part.

Table 1 lists the sum of $num_{root}$, where the parameters are the same as in experiment 1. From Table 1 we find that increasing the number of roots can increase the yield in degree 3. For degree 4 or 5, we get similar results, but not strong as the case in degree 3.

For polynomial generated as suggested by Kleinjung in [7], where the linear polynomial is nonmonic, the results is similar. As for the nonlinear polynomial, we don't do the experiments, but we conjecture results should be similar if the polynomials are skewed.

By the analysis above and the experiments, we have:

**Observation 2**: The number of real roots can be determined almost only by the last two or three coefficients of the polynomial.

**Remark 3**: Usually the number of real roots is left as random. However, based on Observation 2, we can adjust the value of the related coefficients in polynomial optimizing stage such that the polynomial have more real roots. This observation is useful because it was stated that increasing the number of real roots could increase the yield[18].

## 6 Conclusion

Studying the correlation between the yield of a polynomial and its coefficients is important because it take less computation if we can choose polynomial by checking its coefficients first. In this paper, we study the correlation between the yield of a polynomial and its coefficients. The theoretical analysis and

the experiments both show that the ending coefficient containing more small primes will increase the yield of the polynomial. As the ending coefficient is much bigger than the leading coefficient, the ending coefficient can contain more small primes in root optimization step. This is one advantage of ending coefficient over leading coefficient. And the fact that the number of real roots can be determined almost only by the last two or three coefficients of the polynomial is also a necessary consideration in choose polynomial as increasing the number of real roots can increase the yield of the polynomial pair.

## References


[1] J. P. Buhler, H.W. Lenstra, JR., C. Pomerance, Factoring Integers With The Number Field Sieve, in A. K. Lenstra and H. W. Lenstra, Jr. (eds.), The Development of the Number Field Sieve, LNCS 1554, 50-94, 1993.

[2] C. Pomerance, The Number Field Sieve, Proceedings of Symposia in Applied Mathematics, Vol.48, 465-480, 1994.

[3] P. L. Montgomery, A Block Lanczos Algorithm for Finding Dependencies over GF(2), Eurocrypt'95, LNCS921, 106-120, 1995.

[4] D. Coppersmith, Solving Homogeneous Linear Equations over GF(2) via Block Wiedemann Algorithm, Mathematics of Computation. 62, 333-350, 1994.

[5] P. Nguyen, A Montgomery-like Square Root for the Number Field Sieve, Proceedings ANTS III, Springer-Verlag, LNCS 1423,151-68, 1998.

[6] B. Murthy, Polynomial Selection for the Number Field Sieve Integer Factorisation Algorithm, Ph.D. thesis, The Australian National University, 1999.

[7] T. Kleinjung, On Polynomial Selection For The General Number Field Sieve, Mathematics of Computation, Vol.75, No.256, 2037-2047, 2006.

[8] P. L. Montgomery, Small Geometric Progressions Modulo n, manuscript (1995).

[9] N. Koo, G.H. Jo, and S. Kwon, On Nonlinear Polynomial Selection and Geometric Progression (mod N) for Number Field Sieve. https://eprint.iacr.org/2011/292.pdf

[10] T. Prest, P. Zimmermann, Non-linear Polynomial Selection For The Number Field Sieve, Journal of Symbolic Computation, Vol.47, Issue 4, 401-409, 2012.

[11] R. S. Williams, Cubic Polynomials in the Number Field Sieve, Master Thesis, Texas Tech University, 2010.

[12] Huanguo Zhang, Xiutao Feng, Zhongpin Qin, Yuzhen Liu, Research on Evolutionary Cryptosystems and Evolutionary DES, Journal of computer, Vol.26,No.12, 1678-1684, 2003.

[13] Qingshu Meng, Huanguo Zhang, Zhangyi Wang, Zhongpin Qin, Wenling Peng, Designing Bent Functions Using Evolving Method, Acta Electronica Sinica, Vol.32, No.11, 1901-1903, 2004.

[14] Min Yang, Qingshu Meng, Huanguo Zhang, Evolutionary Design of Trace Form Bent Functions in Cryptography, International Journal of Information and Computer Security, Vol.3, NO.1, 47-59, 2009.

[15] Huanguo Zhang, Qingshu Meng, Sequence Generator Based on Time-Varying Binary Combiner, Acta Electronica Sinica, Vol.32,No.4, 651-653, 2004.

[16] Huanguo Zhang, Chunlei Li, Ming Tang, Evolutionary Cryptography Against Multidimensional Linear Cryptanalysis, Science China: Information Science, Vol.54, No.12, 2565-2577, 2011.

[17] Huanguo Zhang, Chunlei Li, Ming Tang, Capability of Evolutionary Cryptosystem Against Differentil Cryptanalysis. Science China: Information Science, Vol. 54,No.10, 1991-2000, 2011.

[18] M. Elkenbracht-Huizing,An Implementation of the Number Field Sieve, Experimental Mathematics, Vol.5, No.3,231-251, 1996.

[19] J.E. Gower,Rotations and Translations of Number Field Sieve Polynomials, Advances in Cryptology - ASIACRYPT 2003, LNCS2894, 302-310, 2003.

[20] Shi Bai, Polynomial Selection for the Number Field Sieve, Ph.D thesis, the Australian National University,2011.

[21] Lu. YANG, Recent Advances on Determining the Number of Real Roots of Parametric Polynomials, Journal of Symbolic Computation, Vol. 28, 225-242, 1999.

[22] http://en.wikipedia.org/wiki/Cubic_function.