Regular paper | Journal of the KIECS. pp. 1181-1188 vol. 12, no. 6, Dec. 31 2017, t. 86, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2017.12.6.1181

효율적인 수체의 기본단수계 생성 알고리즘과 H/W 구현에 관한 연구

김용태*

On Efficient Algorithms for Generating Fundamental Units and their H/W Implementations over Number Fields

Yong-Tae Kim*

요 약

수체의 단수와 기본단수계는 RSA 암호계에서는 400자리 이상의 큰 수가 소수인지를 판별하는 소수판정법과 그 수를 소인수분해하는 데에 사용되는 다양한 수체선별법에 사용되며, 복소이차체를 기반으로 하는 암호계에서는 이데알의 곱셈과정과 류수(class number)를 계산하는 과정 등 다양한 암호계에서 사용되고 있다. 본 논문에서는 기본단수계를 이용하는 암호계의 구현시간과 공간을 줄이기 위하여, 수체의 기본단수계의 존재성을 증명한 Dirichlet의 정리와 몇 가지 기본단수계의 성질을 중심으로 우리가 제안하는 기본단수계의 생성 과정을 소개한다. 그리고 그에 따른 기본단수계의 H/W 구현의 시간과 공간을 최소화할 수 있는 효율적인 기본단수계의 생성알고리즘과 그 알고리즘을 H/W 상에서 구현한 결과를 제시한다.

ABSTRACT

The unit and fundamental units of number fields are important to number field sieves testing primality of more than 400 digits integers and number field seive factoring the number in RSA cryptosystem, and multiplication of ideals and counting class number of the number field in imaginary quadratic cryptosystem. To minimize the time and space in H/W implementation of cryptosystems using fundamental units, in this paper, we introduce the Dirichlet's unit Theorem and propose our process of generating the fundamental units of the number field. And then we present the algorithm generating our fundamental units of the number field to minimize the time and space in H/W implementation and implementation results using the algorithm over the number field..

키워드

Number Field, Unit, Dirchlet's Unit Theorem, Fundamental Units
수체, 단수, 디리끌레의 단수 정리, 기본 단수계,

* 교신저자: 광주교육대학교 수학교육과
• 접 수 일 : 2017. 10. 17
• 수정완료일 : 2017. 11. 15
• 게재확정일 : 2017. 12. 15
• Received : Oct 17, 2017, Revised : Nov 15, 2017, Accepted : Dec 15, 2017
• Corresponding Author : Yongtae Kim
Dept. of Mathematics Education, Gwangju National University of Education
Email : ytkim@gnue.ac.kr

Ⅰ. 서 론

주어진 큰 수의 소인수를 찾는 다양한 수체선별법(number field sieve) 알고리즘, 큰 수의 소인수분해 알고리즘 등의 RSA 암호계의 핵심이 되는 계산 알고리즘과 수체를 기반으로 하는 암호학의 여러 분야에 꼭 필요한 이데알의 곱셈 알고리즘 및 류수(class number)계산 등에 수체위에서의 기본단수계가 폭 넓게 응용되기 때문에 수체위에서의 기본단수계를 계산하는 일은 현재에도 꾸준히 주목을 받고 있다. 기본단수계의 존재성은 Dirichlet[1]에 의해서 처음 알려졌으며 그 후 Borevich 등[2]에 의하여 기본단수계의 구조가 좀 더 상세하게 밝혀지고, 대수적 정수론을 기반으로 하는 다양한 암호계가 제안되면서 기본단수계를 H/W상에서 구현하는 알고리즘이 모색[3]되기 시작하였다. 특히, 단수(unit)를 계산할 때에는 Pell 방정식의 성질[4]이 핵심적으로 이용되는데 그의 성질에 관한 연구가 계산적 정수론에서 매우 중요하기 때문에 현재에도 꾸준하게 연구[5]되고 있으며, 단수에 의해서 생성되는 수체의 order를 결정하는 H/W 구현방안이 최근에 제안[6]되어있다. 또한 수체를 기반으로 하는 암호학에서 수체의 특성을 결정하는 가장 중요한 성질 중의 하나인 수체의 류수를 계산하는 공식을 H/W상에서 효율적으로 구현하는 방안이 알려져 있으며 류수의 성질을 이용하여 기본단수계를 계산하는 방법[7]을 적용할 때, 류수의 수열의 성질에 따른 분류[8-9]에 관한 연구 결과를 활용하여 좀 더 효율적인 류수 계산이 가능하게 되었다. 모든 암호계의 공격과 방어의 핵심 요소는 H/W의 구현시간과 차지하는 공간을 줄이는 것이다. 따라서 암호계의 구현시간과 공간을 줄이기 위해서 수체의 기본단수계에 관한 연구 결과와 몇 가지 중요한 기본단수계의 특성을 기반으로, 본 논문의 Ⅱ장에서는 수체의 기본단수계의 정의와 그의 구조를 소개하고 본 논문에서 필요한 Dirichlet의 기본단수계 정리와 그와 연관된 내용을 소개한다. Ⅲ장에서는 주어진 수체의 기본단수계를 시간과 공간을 줄이면서 효율적으로 생성하는, 우리가 제안하는 과정과 그에 따른 계산알고리즘을 소개하고 Ⅳ장에서는 우리의 알고리즘을 H/W상에서 구현한 결과를 제시하기로 한다.

Ⅱ. 수체의 기본단수계

본 논문에서 사용하는 용어와 기호는 대부분 Pohst와 Zassenhaus[3]를 참조하였으며, 이장에서는 수체의 기본단수계의 구조와 그의 특성을 알아보기로 한다.

2.1 기본단수계의 구조

$f(x)$는 최고차항의 계수가 1(monic)이며 정수계수를 갖는 n차 기약다항식이고 α를 $f(x)$의 한 근이라고 하자. 또한 α에 의해서 생성되는 수체 $K=\mathbb{Q}(\alpha)$의 판별식을 d_K, 정환(ring of integers) O_K의 정수계수 기저를 $\{w_1,\cdots,w_n\}$, 쌍대기저를 $\{w_1^*,\cdots,w_n^*\}$이라고 하자. 또한 군론에서 잘 알려져 있으며 본 논문에서 필요한 다음 정의를 인용한다.

정의 1. 가환군 A의 모든 원소가 유한 위수(order)를 가질 때 A를 torsion(또는 periodic) 군이라고 부른다.

지금 이 장에서 중요한 Dirichlet의 정리를 현대적으로 정리한 Borevich와 Shafarevich[2]의 2장 4절의 정리 5를 증명 없이 인용하기로 한다

정리 1 (Dirichlet). R을 수체 K안에서 정수환 $\mathbb{Z}$의 정수적 폐포(integral closure)의 부분환, R의 $\mathbb{Z}$-위수는 n이고 K가 $\mathbb{Q}$에 대한 $s+2t$개의 공액체를 갖는다고 하자. $r=s+t-1$이라고 할 때 R의 단수군(unit group) $U(R)$은 단위근(root of unity) ζ로 생성되는 torsion 부분군과 r개의 무한군의 직적으로 다음과 같이 표현된다.

$$U(R)=<\zeta>\times<E_1>\times\cdots\times<E_r>. \quad (1)$$

정의 2. 식 (1)에서 $\{E_1,\cdots,E_r\}$을 수체 K 또는 정환 O_K의 기본단수계라고 한다.

이제 $n=r_1+2r_2, r=r_1+r_2-1$ 이고 $\{\eta_1,\cdots,\eta_r\}$을 수체 K의 기본단수계라고 하면 K의 단수군은

$$U(K)=TU(K)\times<\eta_1>\times\cdots\times<\eta_r> \quad (2)$$

이다. 단, $TU(K)$는 $U(K)$의 torsion 부분군이다. 또한 Pohst와 Zassenhaus[3]에 의하면, 수체 K의 r개의 0이 아닌 regulator를 갖는 단수들의 집합$\{\epsilon_1,\cdots,\epsilon_r\}$을 독립단수계라고 하며,
$U(K)$의 부분군

$$U(\epsilon)=TU(K)\times<\epsilon_1>\times\cdots\times<\epsilon_r> \quad (3)$$

의 $U(K)$안에서 군 위수(group index)를 I라고하면

$$I=[U(K):U(\epsilon)]=Reg(U(\epsilon))/Reg(U(K)). \quad (4)$$

2.2 독립단수계를 이용한 기본단수계의 생성

수체 K에서 임의의 독립단수계 $\{\epsilon_1,\cdots,\epsilon_r\}$를 이용하여 기본단수계를 생성해가는 과정을 알아보기로 한다. 우선 regulator의 하한 추정치에 의한 식 (4)의 I의 상한값은 다음 정리와 같다.

정리 2. ([3]의 5장 정리 5)

$$I\le \lfloor Reg(U(\epsilon))/Reg_{est} \rfloor = q\in\mathbb{Z}. \quad (5)$$

만일 $q=1$이면 $U(\epsilon)=U(K)$이므로, $\eta_i=\epsilon_i(1\le i\le r)$ 즉, 기본단수계는 독립단수계와 같다. 만일 $q\ge 2$이면 $U(\epsilon)$와 $U(K)$의 상등여부에 따라 다음의 정리가 성립한다.

정리 3. ([3]의 5장 정리 6)
$\{\eta_1,\cdots,\eta_k\}(0\le k<r)$이 정환 O_K의 기본단수계의 부분집합이라 할 때, $\eta_{k+1}\in U(K)$가 기본단수계에 속할 필요충분조건은 $\zeta\in TU(K), m,m_i\in\mathbb{Z}$ $(1\le i\le k), \omega\in O_K, |m|\ge 2$에 대하여 방정식

$$\eta_{k+1}=\zeta\eta_1^{m_1}\cdots\eta_k^{m_k}\omega^m \quad (6)$$

이 해를 갖지 않는 것이다.

정리 3의 결과로서 곧 바로 다음 정리를 얻을 수 있다.

정리 4. 만일 $\{\eta_1,\cdots,\eta_r\}$이 정환 O_K의 독립단수계이고, q이하인 모든 소수p와 정수 $0\le m_i\le p-1(1\le i\le r)$과 $TU(K)$의 모든 단수 ζ에 대하여 방정식

$$\omega^p=\zeta\eta_1^{m_1}\cdots\eta_r^{m_r} \quad (7)$$

이 O_K안에서 해가 없으면 $\{\eta_1,\cdots,\eta_r\}$이 정환 O_K의 기본단수계이다.

정리 4는 수체 K의 모든 order O_f에 적용된다.

III. 제안하는 기본단수계의 생성 알고리즘

이 장에서는 우리가 제안하는 기본단수계를 생성하는 알고리즘을 소개하기로 한다. 이 알고리즘의 핵심은 정리 4의 식 (7)에서 적당한 독립단수계의 원소 $\eta_i(1\le i\le r)$를 차례로 소거해가면서 η_i들의 지수인 $m_1,\cdots,m_r$을 줄여나가는 것이다.

3.1 초기치의 입력과 수정

초기치를 다음과 같이 치환한 후
$\eta_i\leftarrow\epsilon_i\ (1\le i\le r)$,
$Reg(U(K))\leftarrow Reg(U(\epsilon))$,
$q\leftarrow\lfloor Reg(U(K))/Reg_{est}\rfloor$
$I\leftarrow 1$,
q이하의 임의의 소수 p와 torsion 단수 $\zeta\in TU(K)$에 대하여 O_K안에서 다음 방정식의 해를 구한다.

$$\omega^p = \zeta\eta_1. \tag{8}$$

만일 식 (8)을 만족하는 해 ω가 존재하면 η_1은 기본단수가 아니다.

이 경우에는 식 (8)의 해 ω가 존재하면 다음과 같이 수정하여 치환한다.

$\eta_i \leftarrow \omega$,
$Reg(U(K)) \leftarrow Reg(U(K))/p$,
$q \leftarrow \lfloor Reg(U(K))/Reg_{est} \rfloor$
$I \leftarrow I * p$.

만일 $q=1$ 이면 ω가 기본단수이고 , $q \geq 2$이면 식 (8)을 반복 수행한다.

3.2 독립단수의 소거

식 (8)의 해가 존재하지 않으면, 다음의 판정과정을 거쳐 $\eta_i(1 \leq i \leq r)$를 차례로 소거한다.

먼저, $K(\eta_1^{1/p}) \supset K$이므로 다항식 $x^p - \eta_1$은 O_K안에서 기약이 된다. 그런데 Tschebotareff[10]에 의하면 판별식을 d_K로 갖지 않는 소 이데알(prime ideal) $\wp$가 존재하여 다항식 $x^p - \eta_1$은 $O_K/p[x]$안에서도 기약이 된다. 따라서 $p|(N(\wp)-1)$이다. 단, $N(\wp)$는 $\wp$의 norm이다. 또한 $(O_K/\wp)^*$는 순환군이므로 $p|\#(O_K/\wp)^* := kp$이고 η_1은 $(O_K/\wp)^*$안에서 어떤 수의 p 제곱으로 표현되지 않으므로 η_1의 위수는 p의 배수이다. 만일 $(O_K/\wp)^* = < g >$라고 한다면 $\eta_1 = y^p$이 성립하는 $(O_K/\wp)^*$의 원소 y가 존재하지 않으므로 η_1의 위수를 d라고 할 때 $\eta_1 = g^m$이 되면 $1 = \eta_1^d = g^{md}$이므로 $kp|md$ 즉, $p|d$이다. 또한 모든 단수 $\eta_i(2 \leq i \leq r)$에 대하여 꼭 하나의 정수 $v_i(0 \leq v_i < p)$가 존재하여 $\eta_1^{v_i}\eta_i$는 p를 법으로 $(O_K/\wp)^*$안에서 어떤 수의 p 제곱으로 표현된다. 이때 $\overline{\eta_i} = \eta_1^{v_i}\eta_i$로 치환하면

$$\begin{aligned} U(\epsilon) &= TU(K) \times < \eta_1 > \times \cdots \times < \eta_r > \\ &= TU(K) \times < \eta_1 > \times < \overline{\eta_2} > \times \cdots \times < \overline{\eta_r} > \end{aligned} \tag{9}$$

이고 $< \overline{\eta_2} > \times \cdots \times < \overline{\eta_r} >$의 모든 원소는 p를 법으로 어떤 수의 p 제곱으로 표현된다. 따라서 $U(\epsilon)$안에서 p의 거듭제곱으로 표현되는 원소가 존재한다면, $\omega \in O_K$, $\zeta \in TU(K)$와 $0 \leq m_i < p(1 \leq i \leq r)$에 대하여

$$\omega^p = \zeta\eta_1^{m_1}\overline{\eta_2^{m_2}} \cdots \overline{\eta_r^{m_r}}. \tag{10}$$

방정식 (10)은 p를 법으로 계산해도 참이다. 그러면 $\eta_1^{m_1}$은 p를 법으로 어떤 수의 p 제곱과 합동이다. 따라서 $\omega^p = \eta_1^{m_1}, \gcd(m_1, p) = 1$ 이므로 적당한 정수 x, y가 존재하여 $1 = m_1 x + py$로 표현되고, 따라서 $\eta_1 = \eta_1^{m_1 x + py} = (\omega^x \eta_1^y)^p$ 가 되므로 p의 존재성에 모순이다. 그러므로 η_1의 지수는 $m_1 = 0$이다. 즉,

$$\omega^p = TU(K) \times < \overline{\eta_2} > \times \cdots \times < \overline{\eta_r} > \tag{11}$$

이다. 이러한 과정을 반복 적용하여 오직 하나의 단수만을 남도록 하고 전 과정을 다음의 소수 p로 옮긴다.

3.3 우리의 알고리즘에 적합한 소수 p의 설정

다음 식을 만족하는 소수 P를 선택한다.

$$P \nmid d_K, \quad p|(P-1). \tag{12}$$

$P\mathbb{Z}[x]$를 법으로 생성함수 f를 인수분해 한다. 즉,

$$f(x) \equiv f_1(x) \cdots f_t(x) \bmod P\mathbb{Z}[x]. \tag{13}$$

그러면 $\wp_i := PO_K + f_i(\alpha)O_K (1 \leq i \leq t)$중에서 적당한 이데알 $\wp$가 있으므로 다항식 $x^p - \eta_1$ 이 $O_K/\wp_i[x]$를 법으로 기약이 되는지를 다음 정리를 이용하여 판정한다.

정리 5. 다음 세 조건은 동치이다.

(1) 다항식 $x^p - \eta_1$이 $O_K/O_K/\wp_i[x]$를 법으로 기약이 아니다.

(2) η_1이 $\wp_i$를 법으로 어떤 수의 p 제곱으로 표현된다.

(3) $\eta_1^{(N(p_i)-1)/p} \equiv 1 \bmod \wp_i$

(증명) (1) $\Rightarrow$ (2)는 자명하다.

(2) $\Rightarrow$ (3); $\eta_1 \equiv \omega^p \bmod \wp_i$ 이므로 $\omega \in O_K$인 경우에는 $N(p_i) = P^{\deg(f_i)}$이므로 $P\nmid(N(\wp_i)-1)$이고 따라서

$$\eta_1^{(N(p_i)-1)/p} = \omega^{N(p_i)-1} \equiv 1 \bmod \wp_i. \tag{14}$$

(3) $\Rightarrow$ (1)은 자명하다.

또한 torsion 단수의 처리방법은 다음과 같다. $<\zeta> \geqq TU(K)$라 하자. 만일 ζ가 어떤 수의 p 제곱으로 표현되지 않는다면 소 이데알 $\wp_i$가 존재하여 ζ는 $\wp_i$를 법으로 어떤 수의 p 제곱과 합동이 아니다. 따라서 지수 $v_i(1 \leq i \leq r)$이 존재하여 $\zeta^{v_i}\eta_i$는 $\wp_i$를 법으로 어떤 수의 p 제곱과 합동이 된다. 그러므로 η_i는 $\zeta^{v_i}\eta_i$로 치환된다. 그리고 수열에 관한 최근의 연구[11]가 소수 P를 효율적으로 선택하는 과정에서 도움이 된다.

3.4 방정식 $\omega^p = \eta$ 의 해

방정식 $\omega^p = \eta$의 해는 다음과 같은 과정으로 구한다.

(1) 만일 $\omega \in O_K$가 방정식의 해이면 ω를 정수계수 기저로 표현했을 때의 계수 $e_i(1 \leq i \leq r)$의 추정치는 다음과 같다.

$$\begin{aligned} |e_i| = |Tr(\omega\omega_i^*)| &= |\sum_{j=1}^{n} \omega^{(j)}\omega_i^{*(j)}| \\ &\leq \sum_{j=1}^{n} |\omega^{(j)}|\,|\omega_i^{*(j)}| \\ &= \sum_{j=1}^{n} |\eta^{(j)}|^{1/p}\,|\omega_i^{*(j)}| \\ &:= T_i (1 \leq i \leq n). \end{aligned} \tag{15}$$

(2) 다음 세 조건을 만족하는 첫 번째 소수 p를 택한다.

① $p > 2\max\{T_i | 1 \leq i \leq n\}$,

② $p \nmid d_K$,

③ $p | h_p := (O(K)/PO_K)^*$.

그러면 자연수 q가 존재하여 $pq \equiv 1 \bmod h_p$이고 $\eta^q = \omega^{pq} \equiv \omega \bmod PO_K$. 이러한 η^q을 계산하여 정수계수 $e_i(1 \leq i \leq r)$가 개구간 $(-P/2, P/2)$ 안에 해 ω가 존재하면 그 해가 방정식 $\omega^p = \eta$의 한 해이고, 존재하지 않으면 방정식의 해는 없는 것이다.

(3) h_p의 계산

생성함수 f를 $P\mathbb{Z}[x]$를 법으로 인수분해 하여

$$f(x) \equiv f_1(x) \cdots f_t(x) \bmod P\mathbb{Z}[x] \tag{16}$$

일 때, 이데알 $\wp_i := PO_K + f_1(\alpha)O_K (1 \leq i \leq t)$라고 놓으면

$$\begin{aligned} &N(\wp_i) := P^{\deg(f_i)} (1 \leq i \leq t), \\ &h_p = (O_K/PO_K)^* = \Pi_{i=1}^{t} (O_K/\wp_i)^* \\ &\quad = \Pi_{i=1}^{t} (P^{\deg(f_i)} - 1). \end{aligned} \tag{17}$$

우리가 제안하는 기본단수계의 생성 알고리즘을 요약하면 다음과 같다.

Algorithm

Step 1. 초기화

$\eta_i \leftarrow \epsilon_i \ (1 \leq i \leq r)$,
$Reg(U(K)) \leftarrow Reg(U(\epsilon))$,
$q \leftarrow \lfloor Reg(U(K))/Reg_{est} \rfloor$
$I \leftarrow 1$

Step 2. 다음 방정식의 해를 구한다.

$\omega^p = \zeta\eta_1$.

Step 3. 수정치환

방정식 $\omega^p = \zeta\eta_1$의 해가 존재하지 않으면 다음과 같이 수정하여 치환한다.

$\eta_i \leftarrow \omega$,
$Reg(U(K)) \leftarrow Reg(U(K))/p$,
$q \leftarrow \lfloor Reg(U(K))/Reg_{est} \rfloor$
$I \leftarrow I * p$

Step 4. 만일 $q=1$ 이면 ω가 기본단수이고 , $q \geq 2$이면 Step 2.를 반복 수행한다.

Step 5. 그 다음의 독립단수를 차례로 소거한다.

IV. 기본단수계의 H/W 구현 결과

Pentium 166 MHZ CPU에서 Mathematica 4.0[12]을 이용한 프로그램을 적용하여 제안하는 Algorithm을 따라 기본단수계를 H/W 구현한 결과는 다음과 같다. 단, fk,fp,fq는 각각 III장에서의 i,p,q이며, uuu는 fk번째 원소가 O_K안에서 fp번째 해가 존재하면 1이고 그렇지 않으면 0이다. 또한 PP는 $uuu=0$ 일 때 III장의 이데알 p이고 $ww1$은 이데알 p에 대하여 $\eta_{fk}^{k}=\eta_1$이 해를 가지면 1, 해를 가지지 않으면 0이다.

Generating polynomial
$f(x)=1-x-3x^2+x^3+x^4$,
Discriminant 725={{5,2},{29,1}},
$O_K=\mathbb{Z}[g]$, $f(g)=0$,
Independent units $\{g^3,1-2g+g^2,g^2+g^3\}$,
reg=4.950413087608543957,
lower bound=0.31517652749013484,

$\{g^3,1-2g+g^2,g^2+g^3\}$ fk 1 fp 2 fg 15
uuu 0
$PP=11O_K+(9+g)O_K$
11 2 kk 0 $ww1$ 1 fp 2
11 3 kk 0 $ww1$ 1 fp 2
$\{g^3,1-2g+g^2,g^2+g^3\}$ fk 3 fp 2 rq 15
uuu 1
$\{g^3,-1+g,g^2+g^3\}$ fk 2 fp 2 fq 7
uuu 0
$PP=3O_K+(1+2g+g^3+g^4)O_K$
11 3 kk 1 $ww1$ 0 fp 2
11 3 kk 1 $ww1$ 1 fp 2
$\{g^3,-1+g,-1+g+2g^2-g^3\}$ fk 3 fp 2 fq 7
uuu 0
$\{g^3,-1+g,-1+g+2g^2-g^3\}$ fk 1 fp 3 fq 7
uuu 1
$\{g,-1+g,-1+g+2g^2-g^3\}$ fk 1 fp 3 fq 2
uuu 0
$PP=7O_K+(2+2g+g^3)O_K$
11 2 kk 0 $ww1$ 0 fp 3
11 2 kk 1 $ww1$ 0 fp 3
11 2 kk 2 $ww1$ 1 fp 3
11 3 kk 0 $ww1$ 1 fp 3
$\{g,-g^2+g^3,-1+g+2g^2-g^3\}$ fk 2 fp 3 fq 2
uuu 0
$PP=13O_K+(11+5g+g^2)O_K$
11 3 kk 0 $ww1$ 1 fp 3
$\{g,-g^2+g^3,-1+g+2g^2-g^3\}$ fk 3 fp 3 fq 2
uuu 0
Fundamental units=$\{g,-g^2+g^3,-1+g+2g^2-g^3\}$
Regulator of fundamental units
=0.8260688478347573262
Lenstra-Lenstra-Lovaz Lattice reduction
algorithm=$\{g,-g^2+g^3,-1+g^2\}$
Other fundamental unit systems
(1) $\{g,-g^2+g^3,5-8g-11g^2+12g^3\}$
(2) $\{g,-1+g,1-g^2\}$
(3) $\{g,-1+g,1+g^2\}$

V. 결 론

수체의 기본단수계는 Dirichlet에 의해 대수적 정수론의 한 개념으로 소개된 후, 이데알의 곱셈이나 수체의 류수 계산 또는 Pell 방정식의 해를 구하기 위해서 다양한 연구가 이루어졌다. 그런데 암호학의 발전으로

수체를 기반으로 하는 RSA 암호계와 복소이차체를 기반으로 하는 암호계(IQC)가 상용화되면서, 주어진 큰 수의 소인수를 찾는 다양한 수체선별법 알고리즘, 큰 수의 소인수분해 알고리즘, 수체의 order O_f의 결정과 류수를 H/W 상에서 구현하는 데에 기본단수계가 중요한 역할을 하게 되어 이제는 기본단수계를 H/W 상에서 시간과 공간을 최소화할 수 있는 구현방법을 모색하는 데에 많은 노력을 하는 중이다. 이러한 기본단수계의 효율적인 구현 방안을 실행하기 위하여, 본 논문의 Ⅱ장에서는 수체의 기본단수계의 정의와 그의 구조를 소개하고 본 논문에서 필요한 Dirichlet의 기본단수계 정리와 그와 연관된 내용을 소개하였다. Ⅲ장에서는 주어진 수체의 기본단수계를 효율적으로 생성하는 우리가 제안하는 과정과 그에 따른 계산알고리즘을 소개하였으며 Ⅳ장에서는 우리의 알고리즘을 H/W상에서 구현한 결과를 제시하였다. RSA 암호계와 복소이차체를 기반으로 하는 암호계 등을 H/W상에서 실행할 때에 본 논문에서 제안한 기본단수계 생성 알고리즘을 적용하면 암호계의 전체 실행시간 또는 공격시간이 현저하게 감소할 것으로 예상된다.

감사의 글

본 논문은 2017년도 광주교육대학교 학술연구비 지원에 의한 것임

References

[1] P. Dirichlet, *Vorlesungen über Zahlentheorie.* Berlin: Springer Vieweg, 1894.

[2] Z. Borevich and I. Shafarevich, *Number Theory.* New York: Translated by Newcomb Greenleaf for Scripta Technica, Academic Press, 1966.

[3] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*. Cambridge: Cambridge University Press, 2002.

[4] É. Fouvry and J. Klüners, "On the negative Pell equation," *Annals of Mathematics,* vol. 172, no. 3, 2010, pp. 235-254.

[5] P. Stevenhagen, *Number rings.* Leiden,: Universiteit Leiden Press, 2017.

[6] J. Lee and S. Louboutinb, "Determination of the orders generated by a cyclic cubic unit that are Galois invariant," *J. of Number Theory,* vol. 148, no. 1, 2015, pp. 33-39.

[7] K. Wang, "Fundamental unit system and class number of real bicyclic biquadratic number fields," *Proc. of the Japan Academy, Ser. A, Mathematical Sciences,* Tokyo, Japan, vol. 77, no. 9, May, 2001, pp. 147-150.

[8] H. Kim, S. Cho, U. Choi, M. Kwon, and G. Kong, "Synthesis of Uniform CA and 90/150 Hybrid CA" *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 3, 2016, pp. 293-302.

[9] U. Choi, S. Cho, H. Kim, M. Kwon, and S. Kim, "Synthesis of 90/102(170)/150 linear CA using 90/150 linear CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 9, 2016, pp. 885-891.

[10] N. Tschebotareff, "Die Bestimmung der Dichtigkeit einer Menger von Primzahlen, welsche zu einer gegebenen Substitutions-klasse gehőren," *Mathematische Annalen,* vol. 95, no. 1, 1926, pp. 191-228.

[11] H. Kim, S. Cho, M. Kwon, and H. An, "A study on the cross sequences," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 7, no. 1, 2012, pp. 61-67.

[12] S. Wolfram, *Mathematica. 4th Ed..* New York: Wolfram Champaign Research, Inc., 1999.

저자 소개

김용태(Yong-tae Kim)

1976년 : 공주사범대학 수학교육과(이학사)

1986년 : 고려대학교 대학원 수학과 (이학석사)

1991년 : 고려대학교대학원 수학과(이학박사)

2000년 : 서울대학교 대학원 수학교육과(교육학석사)

2008년 : 서울대학교 대학원 수학교육과(박사과정수료)

1992년 ~ 현재 : 광주교육대학교 수학교육과 교수

※ 관심분야 : ECC, 정수론적 암호학, 공개키암호학