韓國 컴퓨터情報學會 論文誌
第9卷 第3號, 2004. 9.

2004-9-3-3-2

LUC 암호시스템의 효율적인 복호화

박 택 진*, 원 동 호**

Efficient Decryption of LUC cryptosystem

Taek-jin Park*, Dong-ho Won**

요 약

본 논문은 간략화된 Lehmer totient 함수로 LUC 암호시스템을 효율적으로 복호화 할 수 있음을 제안한다. 기존 LUC 암호시스템 에 비하여 복호화된 메시지의 모호성과 중국인의 나머지정리 이용을 줄일 수 있다.

Abstract

In this paper, we proposed LUC cryptosystem of the methods of decryption by reduced Lehmer totient fuction in Eisenstein field. it is more efficient than original LUC crytosystem. Futhermore, use of Chinese Reminder Theorem and ambiguity problem in decrypted message can be eliminate.

▸ Keyword : LUC 암호시스템,Lucas 함수, Lehmer totient 함수

• 제1저자 : 박택진
• 접수일 : 2004.05.10, 심사완료일 : 2004.08.21
* 강릉영동대학 전자정보과 조교수
** 성균관대 정보통신공학부 교수

Ⅰ. 서 론

LUC 공개키 알고리즘은 1993년 Perter Smith가 Lucas 수열을 이용하여 RSA 알고리즘을 변형해서 제안한 암호시스템이다. LUC 암호시스템은 Lucas 수열의 점화식과 소인수분해의 어려움을 기반으로 하는 공개키 암호시스템이며, RSA 암호시스템에서 사용하는 지수 연산을 대신해서 Lucas 수열을 이용한 고차선형 점화식을 사용한다.

LUC 암호시스템은 RSA 암호시스템의 단점중의 하나인 막대한 지수 계산량을 Lucas 수열에 의한 지수 승 계산에 의해 반으로 줄일 수 있어 계산상 효율적이며, 준 동형(homomorphic) 공격도 불가능하다[1]. 그러나 기존 LUC 암호시스템은 Lehmer totient 함수를 이용 하므로써, 메시지 P에 따라 복호화 키 d가 달라지는 문제점이 있다. 즉 P에 따라 Lehmer totient 함수 $r(n)=(p-(\frac{D}{p})(q-(\frac{D}{q})$의 값이 4가지 중의 하나가 생성된다. 주어진 암호문 E에 대하여 4가지 가능한 P_i를 얻으므로 $V_e(P_i)=E$가 되는 P_i를 선택하여 복호화 한다. 따라서 메시지의 4:1의 모호성을 가지는 단점이 있다[2]. 이 문제를 해결 하기위해 메시지 P를 선택 할 때 $(\frac{D}{n})=1$ 되도록 하면 $(\frac{D}{p})=(\frac{D}{q})$가 같아지므로 2가지로 줄일 수 있으나 $(\frac{D}{n})=1$인 P를 선택하는 일은 서로 다른 소수의 곱 $n=pq$ 를 알아야 하므로 어려운 문제이다. 그러나 본 논문에서는 LUC 암호시스템을 Eisenstein 체로 확장하여 $p\equiv q\equiv 1(\mathrm{mod}\ 3)$인 서로 다른 소수임을 증명하고 Lemer totient 함수가 2가지 값으로 줄일 수 있음을 보였다. 그 결과 복호화된 메시지의 4:1모호성을 2:1로 줄일 수 있고, 이차잉여 문제 계산을 줄일 수 있어 복호화 과정에서 연산의 효율성을 증대시킬 수 있다.

Ⅱ. LUC 암호

Lucas 수열의 점화식과 소인수 분해의 어려움을 이용한 공개키 암호시스템이다.

2.1 Lucas 함수

Lucas 함수는 고차선형 점화식 중의 하나이다. $P_1,P_2,\ldots,P_m$이 정수라 하면, 수열 $\{T_n : P_1T_{n-1} + P_2T_{n-2} + \ldots + P_mT_{n-m}\}$을 정의 할 수 있으며 위의 방정식을 m차 선형 점화식이라 한다.

[정의 1.1] 2차 선형 점화식

P, Q가 정수 일 때,
수열$\{\ T_n : PT_{n-1} + QT_{n-2}\}$
을 2차 선형 점화식이라 한다.
P와 Q가 서로소 일 때,
$T_n = PT_{n-1} - QT_{n-2}$
으로 나타낸다.
$P=-Q=1$ 이고 $T_0=1$과 $T_1=1$로 고정하면 수열 T_n은 Fibonacci 수열이다.

2차 선형 점화식의 일반해를 구하기 위하여 다음 과정을 고찰한다.

특성 방정식 $x^2-Px+Q=0$ 의 근 을 α,β 라 하자.

c_1가 c_2 실수 일 때 수열 $T_n=\{\ c_1\alpha^n + c_2\beta^n\}$은 다음과 같은 성질을 만족한다.

$$P(c_1\alpha^{n-1} + c_2\beta^{n-1}) - Q(c_1\alpha^{n-2} + c_2\beta^{n-2})$$
$$= c_1\alpha^{n-1}(P\alpha - Q) + c_2\beta^{n-2}(P\beta - Q)$$
$$= c_1\alpha^{n-2}(\alpha^2) + c_2\beta^{n-2}(\beta^2)$$
$$= c_1(\alpha^n) + c_2(\beta^n)$$

따라서 $T_n = PT_{n-1} - QT_{n-2}$을 만족하는 수열 $\{\ T_n\}$은

$T_0 = c_1 + c_2$이고, $T_1 = c_1\alpha + c_2\beta$ 일 때

$T_n = c_1\alpha^n + c_2\beta^n$ 이라 할 수 있다.

상수 c_1, c_2 에 대한 일반해를

$c_1 = \frac{1}{\alpha-\beta} = -c_2$ 일 때, $U_n = \frac{\alpha^n - \beta^n}{\alpha-\beta}$

$c_1 = 1 = c_2$ 일 때, $V_n = \alpha^n \beta^n$

이라 정의하면 이들 수열은 $U_n = U_n(P,Q)$와 $V_n = V_n(P,Q)$로 표기하고 이를 P 와 Q의 Lucas 함수라 한다.

2.2 Lehmer totient 함수

이차방정식 $x^2 - Px + Q = 0$의 두 근을 α,β라 할 때 자연수 n에 대하여 Lemer totient함수를 정의 할 수 있다.

[정의 2.1] 자연수 $n = p_1^{t_1}, p_2^{t_2}, \ldots\ldots, p_m^{t_m}$,

$D = P^2 - 4Q = (\alpha-\beta)^2$라 하자.

자연수 n의 D에 대한 Lehmer totient 함수 $r(n)$은

$r(n) = \Pi_{p^{e^i} | n} p^{e^i - 1}(p - (\frac{D}{p}))$

으로 정의한다. 단, $\frac{D}{p}$는 Jacobi 기호이고 $D = p^2 - 4Q = (\alpha-\beta)^2$이며 $p^{e^i} \mid n$ 의 지수 e^i는 n을 나누는 p의 최대 멱승이다.

Lehmer totient 함수의 값은 n에 의해 결정된다.

즉, $n = p$가 소수이면 $r(n) = p - \frac{D}{p}$이고,

$n = pq$의 합성수이면 Lehmer totient 함수는 $r(n) = (p - (\frac{D}{p}))(q - (\frac{D}{q}))$로 된다. 그러므로

$(\frac{D}{p}) = 1$ $(\frac{D}{q}) = -1$, $(\frac{D}{p}) = -1$ $(\frac{D}{q}) = 1$에 따라 4가지 값을 가진다.

2.3 Eisenstein 체

본 절에서는 $p \equiv q \equiv 1 \pmod 3$인 소수임을 증명하기 위해 Eisenstein 체의 몇 가지 특성을 살펴본다.

Z는 모든 유리정수(rational integer)의 집합이라 하고, ρ는 단위 원시삼승근(primitive cube root of unity)이라 하자. 즉 $\rho^2 + \rho + 1 = 0$인 이차체 $K = Q(\rho)$는 Eisenstein체라 한다. ρ의

최소 다항식은 $x^2 + x + 1$이고, ρ의 공액은 ρ^2이다.

O_k는 다음과 같이 표시한다.

$O_k = \{ a + b\rho \mid a, b \in Z \}$

여기서 O_k는 K에서 모든 대수적 정수들의 집합니다.

만약 $\pi \in O_k$,이고 $\overline{\pi} = a + b\rho^2$이면

π 의 노옴(norm)은 $N(\pi) = a^2 - ab + b^2$이다.

여기서 $\overline{\pi}$는 π 의 켤레수이다.

O_k의 원소 중 소수는 다음과 같이 주어진다.

① $1 - \rho$

② $a + b\rho$, 여기서 $a \equiv -1 \pmod 3, 3 \mid b$,

$N(a + b\rho) = p$, 여기서 p는 Z에서 소수이고

$p \equiv 1 \pmod 3$ 이다.

[정리 3.1] 만약 $p = N(\pi) = \pi\overline{\pi}$인 소수이면

$p \equiv 1 \pmod 3$이다. 여기서 π는 O_k에서 소수이다.

• 증 명

$(\frac{-3}{p}) = (\frac{-1}{p})$ $(\frac{3}{p}) = (-1)^{(p-1)/2}$

$(\frac{p}{3})(-1)^{((p-1)/2)((3-1)/2)} = (\frac{-p}{3}) = (\frac{1}{3}) = 1$

[정의 3.2] π가 $N(\pi) \neq 3$이고 O_k에서 소수라 하자. 만약 π / α라면, 삼차잉여류기호(cubic residue symbol) $(\alpha/\pi)_3$는 ρ^m으로 정의한다. 여기서 $\alpha^{(N\pi-1)/3} \equiv \rho^m (\pi)$이고, $m = 0, 1, 2$인 유일한 정수이다.

[정리 3.3]

① $(\alpha\beta/\pi)_3 = (\alpha/\pi)_3 (\beta/\pi)_3$이고,

② 만약 $\alpha \equiv \beta (\pi)$이면,

$(\alpha/\pi)_3 \equiv (\beta/\pi)_3$이다.

• 증명 ① : $(\alpha\beta/\pi)_3 \equiv (\alpha\beta)^{(N\pi-1)/3}$

$\equiv (\alpha)^{(N\pi-1)/3} (\beta)^{(N\pi-1)/3}$

$\equiv (\alpha/\pi)_3 (\beta/\pi)_3 (\pi)$.

② : 만약 $\alpha \equiv \beta(\pi)$이면,

$(\alpha/\pi)_3 \equiv (\alpha)^{(N\pi-1)/3}$

$\equiv \beta^{(N\pi-1)/3} \equiv (\beta/\pi)_3(\pi)$.

[정의 3.4] $O_k/\pi O_k$는 $N(\pi)$의 원소를 가진 유한체이다.

[정리 3.5] 만약 π가 O_k의 소수이고, $\pi \nmid \alpha$ 라면,

$\alpha^{(N(\pi)-1)} \equiv 1 (\mathrm{mod}\,\pi)$이다.

• 증명 : [정의 3.4]에 의해, $O_k/\pi O_k$의 곱셈군의 위수는 $N(\pi)-1$ 이다. 따라서 Fermat의 소 정리에 의해 성립한다.

[정의 3.6] 만약 π가 O_k의 소수이고, $\pi \equiv 2 (\mathrm{mod}\,3)$ 이면 π는 원시적(primary)이 라고 한다.

III. LUC 암호시스템의 Eisestein 체 확장

3.1 시스템 설정

[1 단계]

$N(\pi_1)=p, N(\pi_2)=q$이고, $p \equiv q \equiv 1 (\mathrm{mod}\ 3)$인 서로 다른 소수를 구하고, $n = pq$인수를 계산하여 n은 공개한다. 여기서 π_1, π_2는 Q_k의 소수이다.

[2 단계]

주어진 p, q를 이용하여 e를 구한다.

즉, $gcd((r(n)), e) = 1$

여기서 $r(n) = (p-(\frac{D}{p}))(q-(\frac{D}{q}))$이다.

[3 단계]

유클리드 호제법을 이용하여 e의 역수 d 를 구한다. 즉, $de \equiv 1 (\mathrm{mod}\, r(n))$ 여기서 d는 비밀키이다.

[4 단계]

주어진 메시지 P에 대하여 n, e와 Lucas 함수를 이용하여 $E \equiv V_e(P,1) (\mathrm{mod}\, n)$ 을 계산하여 암호화한다.

[5 단계]

메시지 P에 대하여 비밀 키 d를 이용하여 $V_d(E,1) \equiv P (\mathrm{mod}\ n)$을 구하여 복호화 한다.

3.2 간략화 된 Lehmer totient 함수

본 논문에서 제안한 Lehmer totient 함수의 값이 두 가지로 줄 이기위해 $p \equiv q \equiv 1 (\mathrm{mod}\,3)$가 Eisenstein체에서 서로 다른 소수임을 아래 정리에서 증명한다.

[정리 3.7] $p \equiv q \equiv 1 (\mathrm{mod}\,3)$이 Z에서 서로 다른 소수이고, $n = pq$이고, π_1, π_2가 O_k의 소수 라 두면 $N(\pi_1)=p, N(\pi_2)=q$이다.

• 증명 : $r_1 = \overline{\pi_1}$, $r_2 = \overline{\pi_2}$ 라 두자.

따라서 γ_1, γ_2은 원시적이고, $p_1 = \pi_1\gamma_1$ 이고 $p_2 = \pi_2\gamma_2$이다. $g(\chi_{r_1})^3 = p_1 r_1$ 로 부터,

$(N(\pi_2)-1)/3 = (p-1)/3$ 의 멱승에 $\mathrm{mod}\,\pi_2$을 취하면. $\chi_{r_1}(p_2^2) = \chi_{\pi_1}(p_1 r_1)$이다.

여기서 $g(\chi)$는 Gauss 합이고, χ는 표수이다. 유사하게

$g(\chi_{\pi_2})^3 = p_1 r_1$로부터,

$(p_1-1)/3$ 의 멱승에 $\mathrm{mod}\,\pi_1$을 취하면,

$\chi_{\pi_1}(p_2^2) = \chi_{\pi_1}(p_2\pi_2)$이다.

또한, $r_1 = \overline{\pi_1}$, $p_2 = \overline{p_2}$이기 때문에,

$\chi_{r_1}(\pi_2)(p_2^2) = \chi_{\pi_1}(p_2)$이다.

$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1)$

$= \chi_{\pi_1}(\pi_2)(p_2^2) = \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2)$

$= \chi_{\pi_1}(p_2\pi_2)$

$= \chi_{\pi_2}(p_1^2) = \chi_{\pi_2}(p_1\pi_1\gamma_1)$

$= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1)$

따라서 $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$ 이다.

기존 Lehmer totient 함수

$r(n) = (p-(\frac{D}{p})(q-(\frac{D}{q}))$로부터

$p \equiv q \equiv 1 \pmod 3$ 이므로

$r(n) = p - \frac{D}{p}$

$$(\frac{D}{p}) = (\frac{D}{q}) = 1$$

$$(\frac{D}{p}) = 1, \quad (\frac{D}{q}) = 1$$

따라서 $r(n)$은 2가지 값만 가진다.

Eisenstein체로 확장 할 경우 π를 $N(\pi) = \pi\bar{\pi} \equiv 1 \pmod 3$인 복소소수(complex prime)이라 하자. $O_k/\pi O_k$는 표수 p의 유한체이기 때문에, $O_k/\pi O_k$와 Z/pZ는 모두 p개의 원소를 갖는다. 따라서 두 체는 항등성을 갖고 있다. 이 항등성은 Z/pZ에 있는 n의 잉여류 집합(coset)을 $O_k/\pi O_k$에 있는 n의 잉여류 집합으로 보냄으로서 명백히 주어진다[3]. 더구나 $p \equiv q \equiv 1 \pmod 3$에서 n이 소수인 경우 인수 분해는 더욱 어려운 것으로 알려져 있으며,[4] $p \equiv q \equiv 1 \pmod 3$을 찾는 알고리즘은 단지 $O(\log n)$연산만 수행한다[5][6].

IV. 결 론

본 논문에서는 LUC암호시스템을 Eisenstein 체로 확장하여, $p \equiv q \equiv 1 \pmod 3$를 만족하는 소수 p, q 를 선정하여 복호화 과정에서 Lehmer totient 함수 $r(n)$값이 두 가지로 줄일 수 있음을 보였다. 따라서 키 생성과정에서 $p \equiv q \equiv 1 \pmod 3$인 소수 p, q를 선택하면, 복호화 과정에서 복호화된 메시지의 모호성을 2:1로 줄일 수 있고, 이차잉여 문제 계산을 한번만 하므로, 기존 LUC 암호시스템 보다 쉽게 복호화 할 수 있고 Lucas 함수 계산의 효율성을 20%이상 증대시킬 수 있다.

참고문헌

[1] P.Smith, LUC public-key encryption, Dr. Dobb′ s Jurnal(1993), no.1,44-49.

[2] Marc Joye, Security Analysis of RSA-type Cryptosystem Ph.D. thesis, 1997, UCL. Crypto Group, http//www.dice.ucl.ac.be/crypto/joye

[3] Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory 2nd ed. Springer.

[4] Peter Wilker, An effecient algorithmic solution of the diophantine equation u2 +5v2 =m, Math. Com. 35(1980), 1347 - 1352.

[5] H.C. Williams, An M3 public-key Encryption Scheme. Proc.of CRYPTO′ 85, LNCS 218 (1986).

[6] Guang gong, Lein Harn, Public-key Cryptosystems Based on Cubic Finite Extensions. IEEE Transactions on Information Theory, VOL,45, NO.7, NOV.,1999.

저 자 소 개

박 택 진(Taek-jin Park)

1985년 2월 서울산업대학교 전자공학과(학사)
1990년 2월 한양대학교 전자공학과(석사)
1987 ~ 1993 한국통신기술(주) 기술과장
1998년 2월 KAIST/성균관대학교 전기전자 및 컴퓨터공학과 박사과정 수료
1993년 ~ 현재 강릉영동대학 전자정보과 조교수

원 동 호 (Dong-ho Won)

성균관대학교 전자공학과 졸업 (학사, 석사, 박사)
1978년 ~ 1980년 한국전자통신연구원 전임연구원
1985년 ~ 1986년 일본 동경공업대 객원연구원
1988년 ~ 1999년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장 정보통신기술연구 소장
1996년 ~ 1998년 국무총리실 정보화추진위원회 자문위원
2002년 ~ 2003년 한국정보보호학회장
현 재 성균관대학교 정보통신공학부 교수, 정통부 지정 정보보호 인증기술 연구센터장, 성균관대학교 연구처장