한국수학사학회지 제19권 제3호(2006년 8월), 85-94

갈루아환 위의 DICKSON 다항식과 DICKSON 암호*

연세대학교 문리대학 수학과 **김경희**
khlkim@yonsei.ac.kr

갈루아환과 갈루아환 위의 순환다항식에 대하여 발전 과정을 따라 살펴보면서 갈루아환을 평문공간으로 하는 RSA형태의 공개키암호는 가능하지 않다는 결론을 얻었다.

주제어 : 갈루아환, 순환다항식, RSA암호, Dickson다항식

1. 서론

A가 B에게 비밀 메시지를 전하려고 할 때, 고전암호(대칭키 암호, 비밀키 암호)에서는 송신자와 수신자가 사용할 키를 사전에 약속하거나, 사동을 파견하여 상대방에게 알려주어야 했다. 어떤 시점에 사용될 키를 상대방에 알려서 그에 따라 정해지는 복호화함수를 사용할 수 있게 하는 것이다. 그런데, 이런 키의 전달 과정에서 여러 가지 문제가 발생하였다. 키의 관리의 문제, 즉, 보관되어 있던 키가 적에게 유출되거나 전달과정에서 사고가 발생하였다.

이런 키의 관리 및 전달의 문제를 해결하기 위하여 획기적으로 제안된 암호가 공개키 암호시스템이다. 1976년 Diffie와 Hellman이 "New Directions in Cryptography"라는 논문([2])에서 발표한 개념으로 암호화에 쓰이는 공개키와 복호화에 쓰이는 비밀키를 사용하면 키를 전달할 필요가 없다는 것이다. 암호화할 때는 수신자의 공개키를 사용하여 암호화하고 수신자가 복호화할 때는 수신자 자신이 비밀로 간직하고 있는 비밀키로 복호화하면 된다. 이는 제대로 관리되고 있는 우편함으로 비유할 수 있다. 우편함에는 소유자가 표시되어 있어 편지를 보내는 사람은 우편함 소유자의 이름을 보고 우편함에 편지를 넣을 수 있다. 우편물을 받아보려면 우편함 소유자의 열쇠가 필요하다. 여기서 우편함 소유자의 표시가 공개키에 해당하고 그의 우편함 열쇠가 비밀키에 해당하며 우편함속의 우편물이 암호문이라고 생각할 수 있다. 송신자는 원하

* 이 논문은 1996년도 연세학술연구비 지원에 의한 것입니다.

는 우편함을 찾아 우편물을 넣으면 되고 수신자는 자신의 열쇠로 우편함을 열어서 우편물을 꺼내면 된다. 따라서 송신자와 수신자 사이에 키를 교환할 필요가 없다.

그런데 Diffie와 Hellman은 공개키 암호시스템의 개념을 제시하였을 뿐 공개키 암호시스템의 암호알고리즘을 구체적으로 제시하지 못하였다. 1977년 최초의 공개키 암호가 Rivest, Shamir, Adleman에 의해서 만들어졌는데 그 세 사람의 이름의 첫글자를 따서 RSA암호라 부른다([10]). RSA는 소인수분해의 어려움에 근거한 것인데 순환다항식의 개념을 써서 설명하면 다음과 같다.

정의 1.1 곱셈에 대한 항등원(단위원, unity)를 가진 가환환 R위의 다항식 $f(x)$에 대하여 다항식 함수 $f: \begin{matrix} R \to R \\ s \mapsto f(s) \end{matrix}$가 전단사함수이면 $f(x)$를 R위의 순환다항식(Permutation Polynomial)이라고 한다.

정리 1.2 ([7]) n이 서로 다른 두 소수의 곱이라고 하자. 단항식 $f(x)=x^e$이 잉여류환 $Z/(n)$위의 순환다항식이 될 필요충분조건은 $\gcd(e, \phi(n))=1$인 것이다. 이 때, $de\equiv 1 \pmod{\phi(n)}$을 만족하는 d에 대하여 $g(x)=x^d \pmod{n}$은 f에 의해서 주어지는 함수의 역함수를 정의한다. (여기서, Z는 정수의 집합, n은 자연수이고, $\phi(n)$은 오일러 ϕ-함수의 n에서의 값을 나타내며, 앞으로도 계속 그렇다고 하자.)

RSA암호는 두 소수 p, q의 곱인 n과 $\gcd(e, \phi(n))=1$인 자연수 $e\ (1<e<\phi(n))$의 순서쌍 (n, e)를 공개키로 하고, 법 $\phi(n)$에 대한 e의 역원 $d\ (1<d<\phi(n))$를 비밀키로 한다. 암호화함수는

$$f: Z/(n) \to Z/(n)$$
$$x \mapsto f(x)=x^e \pmod{n}$$

이고, 복호화함수는 정리1.2에 의하여

$$g: Z/(n) \to Z/(n)$$
$$x \mapsto g(x)=x^d \pmod{n}$$

이다.

위에서 n의 소인수분해가 pq라는 것을 안다면 $\phi(n)=(p-1)(q-1)$이므로 정리 1.2에 의하여 역함수 g를 쉽게 구할 수 있다. 그러나, (n, e)를 공개해도 $n=pq$임을 모르면 $\phi(n)$을 쉽게 구할 수 없으므로 해독하는 제3자가 비밀키 d를 구하는 것은 거의 불가능하고 따라서 복호화함수를 알 수 없다는 것이다. n이 두 소수의 곱이라는 사실을 알 때, n을 소인수분해하는 것과 $\phi(n)$을 구하는 문제가 동치임을 쉽게 보일 수 있다. 또, n의 소인수분해와 비밀키 d를 구하는 문제가 (매우 높은 확률로) 동치

라는 것을 보일 수 있다. 그런데, n을 소인수분해하는 것은 능률적인 소인수분해 알고리즘이 아직 발견되지 못하여 어려운 문제로 인정을 받고 있다.(양자컴퓨터가 실용화 되면 소인수분해를 매우 쉽게 할 수 있게 될 것이다.) 따라서, 공개키 (n, e)에서 비밀키 d를 구하는 것은 거의 불가능하다. 특수한 상황에서 d를 구하지 않고 해독을 시도하는 공격들이 있었고 지금도 끊임없이 계속되고 있지만 RSA암호는 이런 공격들을 이겨내고 안전성을 인정받고 있다.

RSA암호가 잉여류환 $Z/(n)$에서 암호화함수 $x^e \pmod n$을 사용한다면 Dickson 암호는 암호화함수를 Dickson다항식 $g_d(x, \pm 1)$로 갖는 암호로서 RSA암호를 확장한 것으로 생각할 수 있다.

정의 1.3 R이 단위원을 가진 가환환이고, $a \in R$일 때, 다항식

$$g_k(x, a) = \sum_{t=0}^{[\frac{k}{2}]} \frac{k}{k-t}\binom{k-t}{t}(-a)^t x^{k-2t}$$

을 R위에서의 Dickson다항식이라고 한다. 여기서, $[k]$는 k를 넘지 않는 최대 정수를 나타낸다.

정리 1.4 ([9, p310]) $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$이 홀수일 때, Dickson다항식

$$g_k(x, \pm 1) = \sum_{i=0}^{[\frac{k}{2}]} \frac{k}{k-i}\binom{k-i}{i}(\mp 1)^i x^{k-2i}$$

가 $Z/(n)$위의 순환다항식일 필요충분조건은 $\gcd(k, \nu(n)) = 1$인 것이다.

이 때, p_i들은 서로 다른 소수이고, e_i들은 1이상인 정수이며,

$\nu(n) = lcm\left[p_1^{e_1-1}(p_1^2-1), \ldots, p_r^{e_r-1}(p_r^2-1)\right]$이다.

항등식 $g_k(y + \frac{a}{y}, a) = y^k + (\frac{a}{y})^k$을 이용하면

$$g_k(x, a^l) \circ g_l(x, a) = g_{kl}(x, a)$$

을 보일 수 있다. 정리 1.4에 의하면 $\nu(n)$에 대해서 $g_k(x, \pm 1)$가 $Z/(n)$에서 순환다항식이 되려면 $\gcd(k, \nu(n)) = 1$이어야 한다. $\nu(n)$은 항상 짝수이므로, $g_k(x, \pm 1)$이 순환다항식이면 k는 홀수이다. 따라서, $g_k(x, \pm 1)$가 순환다항식일 때는 위의 식에 의하여

$$g_k(x, \pm 1) \circ g_l(x, \pm 1) = g_{kl}(x, \pm 1)$$

임을 알 수 있다. 이는 $a=\pm 1$일 때 Dickson다항식이 교환법칙을 만족하여 Dickson다항식을 전자서명에도 이용할 수 있다는 것을 보인다.

정리 1.4에는 순환다항식 $g_k(x,\pm 1)$에 의해서 정의되는 함수 g의 역함수가 주어져 있지 않지만 1971년 Muller는 [7]에서 g의 역함수는 $kl\equiv 1(\mathrm{mod}\ \nu(n))$일 때 $g_l(x,\pm 1)$으로 주어진다는 것을 밝혔다.

홀수 n이 $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$로 소인수분해될 때($p_i$들은 서로 다른 소수), 각 i에 대하여 $\gcd(k, p_i^{e_i-1}(p_i^2-1))=1$ 인 자연수 k를 선택하자. 순서쌍 (n,k)를 공개키, $\nu(n)$에 대한 k의 역원 l을 비밀키로, 암호화함수는

$$f:\ Z/(n)\to Z/(n)$$
$$x\ \mapsto\ g_k(x,\pm 1)$$

복호화함수는

$$g:\ Z/(n)\to Z/(n)$$
$$x\ \mapsto\ g_l(x,\pm 1)$$

로 하는 암호를 Dickson암호라 한다. RSA암호와 마찬가지로 큰 수 n의 소인수분해가 어려우면 공개키에서 비밀키를 구하는 것이 거의 불가능하므로 공개키암호가 된다.

정의 1.3에서 $a=0$이면 Dickson 다항식 $g_k(x,a)=x^k$이고 n이 서로 다른 두 소수의 곱이어야 한다는 조건이 필요없으므로, Dickson암호는 RSA암호를 확장한 것이라고 할 수 있다. Dickson암호와 RSA암호는 잉여류환 $Z/(n)$을 평문공간으로 사용한다. 이에 대하여 평문공간을 갈루아환으로 확장한 Dickson암호 형태의 암호시스템이 가능한지 살펴보려고 한다. 우선 갈루아환과 갈루아환 위의 순환다항식에 대한 기존의 연구 결과들에 대해서 살펴보자.

2. 갈루아환

갈루아환과 갈루아환 위의 순환다항식에 대하여 알아보자.

정의 2.1 n, r이 양의 정수, p가 소수일 때, 소환(prime ring) $Z/(p^n)$의 r차 갈루아 확장(Galois extension)을 갈루아환(Galois ring)이라 하고 $GR(p^n, r)$로 나타낸다.

갈루아환의 존재와 그 구조는 1924년 Krull이 발견하였는데, 1966년 Janutz와 1969년 Raghavendran이 독립적으로 재발견하였다. 전통적으로 유한체 $GF(p^n)$과 소환

$Z/(p^n)$을 별개로 다루어 왔지만 McDonald는 이들을 갈루아환으로서 동시에 다루어야 한다고 주장하였다([6]). Mcdonald가 주장한대로 유한체나 잉여류환에 대한 대부분의 연구 결과들이 갈루아환에서도 성립하였다. 여기서, Dickson암호의 평문공간을 잉여류환에서 갈루아환으로 대체하는 문제를 생각해보는 것은 자연스러운 일임을 알 수 있다.

McDonald에 의하면 갈루아환 $GR(p^n, r)$은 잉여류환 $(Z/(p^n))[x]/(f)$와 동형이다([6], p308). f는 $(Z/(p^n))[x]$위의 r차의 최고차계수가 1인 기본 기약다항식(monic basic irreducible polynomial)이다. 기본기약다항식(basic irreducible polynomial)이란 법 p에 대하여 기약인 다항식이다. 따라서 갈루아환 $GR(p^n, r)$의 위수는 p^{nr}이다. $r=1$일 때, $GR(p^n, 1)=Z/(p^n)$이고, $n=1$일 때는 $GR(p, r)=GF(p^r)$이므로 위수 p^r인 유한체가 된다.

지금부터는 갈루아환 $GR(p^n, r)$을 R로 나타내기로 한다. R의 원소를 구체적으로 나타내보면 다음과 같다:

$\alpha=A_0+A_1\zeta+A_2\zeta^2+\ldots.+A_{r-1}\zeta^{r-1}$, 단, $A_i\in Z/(p^n)$이고, ζ는 r차의 monic basic irreducible polynomial $f(x)$에 대하여 $f(x)=0$의 근이다. 각 A_i는 A_{ij}가 $0\le A_{ij}<p$인 정수들일 때 $\sum_{j=0}^{k_i} A_{ij}p^j$로 나타낼 수 있으므로, α를 다음과 같이 나타낼 수 있다:

$$\alpha=\sum_{j=0}^{n-1}\alpha_j(\zeta)p^j, \quad (\text{단, } \alpha_j(\zeta)=\sum_{i=0}^{r-1}A_{ij}\zeta^i).$$

또한, R의 0아닌 원소는 up^t의 형태로 나타낼 수 있다. 여기서, u는 R의 단원(unit)이고, t는 $0\le t\le n-1$인 정수이며, u와 t는 유일하게 결정된다([5, p308]).

R은 유일한 극대아이디얼(maximal ideal) $M=pR$을 가지고 $R/M=GF(p^r)$이 된다. $\mu(a)=\overline{a}=a+M$에 의하여 결정되는 R에서 R/M으로의 준동형사상을 μ라 하자. $f(x)=\sum a_i x^i\in R[x]$에 대하여 $\overline{f}(x)$는 $\sum\mu(a_i)x^i=\sum\overline{a_i}x^i$이라 하자.

순환다항식에 대한 연구는 1860년대 C. Hermite가 유한소체(finite prime field)위의 순환다항식을 다루면서 시작되었다. 그 후 1900년대 초 Dickson이 임의의 유한체(finite field) 위의 순환다항식을 다루었으며 1970년대에 이르러 Laush와 Nobauer가 현대적 관점에서 그 때까지의 연구 결과를 정리하였다.([5], Chapter 7). 그 후 G. L. Mullen과 그의 제자들이 유한체 위의 순환다항식에 대한 연구를 발전시켜왔다.

한편, 1950년대에 Nobauer가 잉여류환 위의 순환다항식을 다루기 시작하여 Redei, Carlitz, S. D. Cohen등의 연구가 뒤를 이었다. 1990년경부터 G. L. Mullen, Priscilla S. Bremser, J. W. Brawley, Javier Gomez-Calderon 등이 갈루아환 위의 순환다항식

을 연구하였다. 그리하여 암호학에 응용할 수 있는 기반이 마련되었다. 다음 3절에서 갈루아환 위의 순환다항식을 암호학에 응용하는데 필요한 성질들에 대해서 살펴본다.

3. 갈루아환 위의 순환다항식

주어진 다항식이 순환다항식이라는 것을 쉽게 보일 수 있어도 그 역함수는 쉽게 구할 수 없는 경우가 많다. 공개키암호시스템에는 어떤 조건(이를 trapdoor라 한다)을 알면 역함수를 쉽게 구할 수 있는 순환다항식이 필요하다. RSA암호시스템에서는 순환하는 단항식 x^e을, Dickson암호시스템에서는 순환하는 Dickson다항식 $g_k(x, \pm 1)$을 암호화함수로 사용하였다. 잉여류환 위에서 x^e과 $g_k(x, \pm 1)$이 순환다항식일 때 어떤 조건을 알면 역함수를 쉽게 구할 수 있다는 것을 2절에서 살펴보았다.(정리 1.2, 정리 1.3 참조) 한편, Javier Gomez-Calderon과 G. L. Mullen([3])에 따르면 갈루아환 위의 순환다항식 x^e이나 $g_k(x, \pm 1)$도 어떤 조건을 알면 역함수를 쉽게 구할 수 있다.

우선, 어떤 다항식이 갈루아환 위의 순환다항식이 될 필요충분조건을 살펴보자.

정리 3.1 $f(x)$를 갈루아환 R 위의 다항식이라고 하자. $f(x)$가 R 위의 순환다항식이 될 필요충분조건은 $\overline{f}(x)$가 유한체 $GF(p^n)$ 위의 순환다항식이고 $GF(p^n)$의 각 원소 a에 대하여 $\overline{f'}(a) \neq 0$이 성립하는 것이다(여기서, f'은 f의 형식적 미분을 나타낸다).

이 정리는 McDonald([6, p269-272])가 증명한 일반적인 경우에서 직접 얻어진다. 다음 정리 3.2는 체가 아닌 갈루아환 위에서 단항식 x^d $(d>1)$은 순환다항식이 될 수 없음을 보인다. 지금부터 p는 홀수인 소수라고 하자.

정리 3.2([3], Corollary 15) $\gcd(d, p)=1$일 때, $f(x)=x^d$이 갈루아환 R 위에서 순환다항식이 될 필요충분조건은 $d=1$이거나 $n=1$이면서 $\gcd(d, p^r-1)=1$인 것이다.

증명. $d=1$이면 $f(x)$는 R에서 항등함수를 정의하므로 명백히 $f(x)$는 순환다항식이다. $n=1$이면 R은 위수가 p^r인 유한체이므로 정리 7.8([5])에 의하여 $\gcd(d, p^r-1)=1$이다(유한체 $GF(p^r)$에서 x^d이 순환다항식일 필요충분조건이

$\gcd(d, p^r-1)=1$인 것은 잘 알려져 있는 사실이다).

역으로, $f(x)$가 R에서 순환다항식이라고 하자. $d>1$일 때, $n=1$이고 $\gcd(d, p^r-1)=1$이 성립함을 보이면 된다. $n>1$이라 하면 R은 up형태의 0아닌 원소를 갖는다.

Case 1. $d \geq n>1$일 때: $d \geq n$이므로 $f(up)=(up)^d=0$. 그런데 명백히 $f(0)=0$이고 $up \neq 0$. 이는 $f(x)$가 순환다항식이라는 사실에 어긋난다.

Case 2. $1<d<n$일 때: $n=2$일 때는 $d=2$이므로 Case 1처럼 생각하면 된다. $n \geq 3$이라 하면 $\left|\frac{n}{d}\right|+1<n$이므로 $up^{\left|\frac{n}{d}\right|+1} \neq 0$.

그러나, $f(up)=(up^{\left|\frac{n}{d}\right|+1})^d=0$. 이는 $f(x)$가 순환다항식임에 어긋난다.

Case 1과 2에 의하여 n은 1이어야 한다는 것을 알 수 있다. $n=1$일 때 R은 위수 p^r인 유한체이므로 정리 7.8 ([5])에 의해서 $\gcd(d, p^r-1)=1$. (유한체 $GF(p^r)$에서 x^d이 순환다항식일 필요충분조건이 $\gcd(d, p^r-1)=1$인 것은 잘 알려져 있는 사실이다.) 따라서, $f(x)$가 순환다항식일 때 $d=1$이거나 $n=1$이면서 $\gcd(d, p^r-1)=1$이어야 한다. ■

정리 3.2에 언급된 정리 7.8 ([5])는 단항식 x^n이 위수가 q인 유한체 F_q위에서 순환다항식일 필요충분조건은 $\gcd(n, q-1)=1$이라는 것이다.

정리 3.1과 정리 3.2에 의하여 단항식 $f(x)=x^d$에 대하여 다음과 같은 사실을 알 수 있다:

1. $\gcd(d, p) \neq 1$이면 항등적으로 $f'=0$이므로, 정리 3.1에 의해서 차수 d가 p의 배수인 단항식 x^d은 갈루아환 $GR(p^n, r)$에서 순환다항식이 될 수 없다.
2. 차수가 1보다 큰 단항식 x^d은 체가 아닌 갈루아환, 즉, $n \neq 1$인 $GR(p^n, r)$ 위에서는 순환다항식이 될 수 없다.

위의 1,2에 의하면 체가 아닌 갈루아환에서 단항식 x^d이 단사함수가 되는 경우는 $d=1$인 경우밖에 없으므로 RSA암호에서는 평문공간을 체가 아닌 갈루아환으로 바꾸는 것이 불가능하다는 것을 알 수 있다. 이에 대하여 Dickson암호는 어떤지 알아보자.

정리 3.3 ([1], Theorem 3) R이 체가 아닌 갈루아환이고(즉, $n>1$) a가 R의 단원(unit)일 때, Dickson다항식 $g_k(x, a)$가 R 위의 순환다항식일 필요충분조건은

$\gcd(k, p^{2r}-1) = \gcd(k, p) = 1$인 것이다.

증명은 [1]을 참조하면 된다. 갈루아환 위의 단항식 x^d에 비하여 갈루아환을 순환시키는 Dickson 다항식이 풍부함을 알 수 있다. [3]에 의하면 $a=\pm 1$일 때만 순환다항식 $g_k(x, \pm 1)$과 $g_l(x, \pm 1)$의 합성함수가 순환다항식이 된다([3], Theorem 4). 또, [3]의 Theorem 13의 증명에서 다음을 얻는다.([3]의 Theorem 13을 여기에 제시하려면 새로운 개념과 용어들이 많이 필요하여 생략한다.)

정리 3.4 $g_k(x, \pm 1)$가 $GR(p^n, r)$ 위의 순환다항식일 때, 그 역함수는 $g_l(x, \pm 1)$, 단, $kl \equiv 1 \pmod{(p^{2r}-1)p^{n-1}}$로 주어진다.

Dickson암호에 사용된 잉여류환 $Z/(n)$ 위의 순환다항식 $g_k(x, \pm 1)$에 대하여 갈루아환 위의 순환하는 Dickson다항식도 그에 대응하는 성질을 갖는다는 것을 살펴보았다: 즉, $a=\pm 1$일 때 Dickson다항식의 합성함수가 Dickson다항식이 되고, 순환다항식이 될 필요충분조건은 $\gcd(k, p^{2r}-1) = (k, p) = 1$이며, 그 때의 역함수는 법 $(p^{2r}-1)p^{n-1}$에 대한 k의 역수를 알면 쉽게 구해진다는 것을 알아보았다.

4. 결론

RSA암호나 Dickson암호는 잉여류환 $Z/(n)$을 평문공간으로 사용하였고 trapdoor는 n의 소인수분해였다. n을 공개키로 사용하여 누구나 평문공간이 $Z/(n)$임을 알 수 있고 암호화함수를 계산할 수 있었다. 그러나, n의 소인수분해를 모르면 비밀키를 거의 구할 수 없으므로 공개키암호시스템이 성립되었다. 이에 반하여, 갈루아환 $GR(p^n, r)$을 평문공간으로 하면 p^n과 r이 알려질(또는 알려줄) 수밖에 없고 n을 몰라도 소수인 n제곱근 p를 구하는 것은 쉬운 문제이다. 여러 n에 대하여 소수인 n제곱근이 얻어질 때까지 n제곱근 구하기를 시도하면 된다. 얻어진 n제곱근이 소수인지를 판정하는 것은 어렵지 않게 할 수 있다(2002년 AKS 소수판정법이 발표되어 주어진 자연수가 소수인지를 다항식 시간 안에 결정할 수 있다). 암호화함수 $g_k(x, \pm 1)$의 역함수는 $g_l(x, \pm 1)$, $kl \equiv 1 \pmod{(p^{2r}-1)p^{n-1}}$이므로 소수 p를 알면 누구나 복호화함수를 구할 수 있다. n만 알면 계산이 가능한 $Z/(n)$과 달리 갈루아환 $GR(p^n, r)$에서는 p^n과 r을 알아야 계산을 할 수 있다. 따라서, $GR(p^n, r)$의 어떤 요소도 trapdoor의 역할을 할 수 없다는 것을 알 수 있다.

[3]에서 J. Gomez-Calderon과 G. L. Mullen은 m의 소인수분해가 $p_1^{e_1}p_2^{e_2}\ldots p_r^{e_r}$ 일 때 $m_i \geq 1$, $i=1,\ldots,r$에 대하여 $GR(p_i^{n_i}, m_i)$인 갈루아환을 생각하고, 그들의 직접곱(direct product)인 환 S를 사용할 것을 제안하였다(그들은 제안만하고 자세한 것은 생략한다고 하였는데 기대했던 결과가 분명하게 드러나지 않았기 때문인 듯하다.). RSA암호나 Dickson암호에서는 잉여류환 $Z/(n)$에서 n의 소인수분해를 모르더라도 암호를 계산할 수 있었지만, 이 경우는 $p_i^{n_i}$과 m_i를 알아야 암호를 계산할 수 있다. 적어도 암호화기계는 n의 소인수분해와 m_i를 알고 있어야 암호를 계산할 수 있다. 해독자는 암호기계를 어떤 형태로든 공격할 수 있으므로 m의 소인수분해는 trapdoor가 될 수 없다.

갈루아환 위의 Dickson다항식은 잉여류환 위의 단항식 x^d이나 Dickson다항식 $g_k(x, \pm 1)$과 마찬가지로 암호에 이용되는데 필요한 기본 성질을 만족하지만, 갈루아환 $GR(p^n, r)$에서의 계산은 p^n과 r이 알려져야 가능하므로 G. L. Mullen 등의 주장처럼 Dickson암호의 평문 공간을 갈루아환이나 그들의 직접곱 S로 확장하여 공개키암호를 얻는 것은 불가능해 보인다.

참고 문헌

1. Bresmer, P. S. and Gomez-Calderon, J., *Value sets of Dickson polynomials over Galois rings*, J. Number Theory 38(1991), 240-250.
2. Diffie, W. and Hellman, M., *New directions in cryptography*, IEEE Trans. Inform. Theory IT-22(1976), 644-654.
3. Gomez-Calderon, J. and Mullen, G. L., *Galois rings and algebraic cryptography*, ACTA ARITHMETICA LIX. 4, 1991.
4. Lausch, H., Nobauer W. and Schweiger F., *Polynompermutationen auf gruppen*, Monatsh. Math. 69(1965), 410-423.
5. Lidl, Rudolf and Niederreiter, Harald, *Finite Fields*, Cambridge, 1984.
6. McDonald, B. R., *Finite rings with identity*, Dekker, New York, 1974.
7. Muller, W. B., *Uber eine Klasse von durch Dickson-polynome dasestellen Gruppen*, Proc. of the Colloq. on rings, modules and radicals, 1971.
8. Muller, W. B. and Nobauer, R., *Cryptanalysis of the Dickson-scheme*, Proc. Eurocrypt 85, Lecture Notes in Computer Science, Vol. 219(1986), 50-61.
9. Nobauer, Rupert, *Cryptanalysis of a Public-key cryptosystem based on Dickson*

polynomials, Math. Slovaca 38, No. 4(1988), 309-323.

10. Rivest, R. L., Shamir, A. and Adleman, L., *A mehtod for obtaining digital signatures and public-key cryptosystems*, Comm. ACM 21(1978), 120-126.

Dickson polynomials on Galois rings and Dickson Schemes

Department of Mathematics, Yonsei University at Wonju **Kyung hee Kim**

We review Galois rings and permutation polynomials over Galois rings with emphasis on cryptological properties of Dickson polynomials and conclude that it is not plausible to obtain the Dickson scheme which has a Galois ring as a plaintext space.

Key words : Galois rings, Permutation Polynomials, RSA, Dickson Polynomials

2000 Mathematics Subject Classification : 11T71, 14G50, 94A60

ZDM Subject Classification : P20, F60

논문 접수 : 2006년 4월, 심사 완료 : 2006년 5월