通信情報保護學會論文誌
第 1 卷, 第 1 號, 1991. 12

유한환의 일향함수를 이용한 암호화에 대하여

김 철*

On the Enciphering by Using One-Way Function of the Finite Ring

Chul Kim

요 약

본 논문에서는 유한환(finite ring)의 이론으로 부터 하나의 일향함수(one-way function)를 만든다. 이때의 일향함수는 다른 방향은 계산적으로 어려운 일향함수라는 의미로 쓴다. 주어진 환(ring)에 대한 군의 작용(group action)을 이용하여 이 함수를 만들었으며 평문(plain text)의 암호화에 응용될 수 있음을 설명한다. 이 함수에 의한 암호문을 해독하는 것은, 이론적으로 불가능하지는 않으나, 소인수 분해(factoring)의 어려움에 근거한 암호 시스템, 예를 들면 RSA 암호 시스템과 같이, 계산이 어려운 문제이다.

Abstract

We construct one-way function based on a finite ring. One-way function in this paper means that to find the inverse of the function is hard computationally. We have used the extension of group action to construct this function and applied it to encipher the given plain text. To decipher the enciphered text generated by this function is considered a hard problem, but not impossible theoretically. However, a successful enciphering system, for example, RSA system which depends on the difficulty of factoring, need not have mathematically perfectness.

1. 개 요

본 논문에서는 유한환(finite ring)의 이론으로 부터 하나의 일향함수(one-way function)를 만든다. 이때의 일향함수는 다른 방향은 계산적으로 어려운 일향함수라는 의미로 쓴다. 둘째 절에서

* 광운대학교 수학과

군과 환의 기본적인 정리들 중, 본 논문의 전개에 필요한 용어와 정리들을 살펴본다. 셋째 절에서는 일향함수를 구축하기 위해, 환과 관련된 몇몇 계산적인 것들을 만든 후, 넷째 절에서 군의 작용(group action)을 이용하여 일향함수를 만든다. 마지막으로, 다섯째 절에서는 이 일향함수의 암호시스템으로서의 역할을 설명하고 본 논문을 맺는다.

2. 기본적인 용어와 정리

정리 2.1 A를 단위원을 가진 유한환(finite ring with identity)이라 하자. 그러면 A는 t개의 A_i들의 직합(direct sum)으로 나타낼 수 있다. 즉,

$$A \cong A_1 \oplus A_2 \oplus \cdots \oplus A_t$$

여기서, $|A_i| = p_i^{d_i}$이고, p_i들은 각기 다른 소수, d_i들은 양의 정수이다.

증명 [4]의 2페이지 참조■.

따라서, 유한환을 고려할 때에는 소수 p의 승으로, 그 위수(order)가 표현되는 환, 즉 p-환 (p-ring)을 살펴보아도 된다.

B가 A의 부분환(subring)일 때, 당연히

$B \cong \oplus(B \cap A_i)$이며, $A/B \cong \oplus(A_i/B \cap A_i)$이다.

정리 2.2 모든 유한 가환 p-군(finite Abelian p-group) G는 순환 부분군(cyclic subgroup)들의 직합(direct sum)이다.

증명 [6]의 103페이지 참조■.

따라서, G가 유한 가환 p-군(finite Abelian p-group)이라면, G는

$$Z/p^{d_1} \oplus Z/p^{d_2} \cdots \oplus Z/p^{d_k}$$

과 동형이며, $d_1, d_2, \cdots, d_k$는 재배열을 고려하면 유일하다.

환 A의 덧셈군(additive group)을 A^+라 놓자.

정의 2.3 A^+의 생성원(generator)들의 최소 집합을 A^+의 기저(base)라고 한다.

즉, A의 모든 원소 x는 다음과 같이 유일하게 표현될 수 있다.

$$x = c_1e_1 + c_2e_2 + \cdots + c_ke_k \text{ 여기서, } c_i \in Z/p^{d_i}$$

이때의 k를 A^+의 (따라서, A의) 계급 (rank)이라 한다.

정의 2.4 A^+의 기저를 $\{e_1, e_2, \cdots, e_k\}$라 하고, A^+의 원소 x, y를 다음과 같이 나타내자.

$$x = c_1e_1 + c_2e_2 + \cdots + c_ke_k \text{ 여기서, } c_i \in Z/p^{d_i}$$
$$y = d_1e_1 + d_2e_2 + \cdots + d_ke_k \text{ 여기서, } d_i \in Z/p^{d_i}$$

이때, x=y이기 위한 필요충분 조건은

모든 i=1, 2, …, k에 대하여, $c_i \equiv d_i \bmod p^{d_i}$

를 만족하는 것이다.

증명 $x = y$

$\Longleftrightarrow x - y = O_A$

$\Longleftrightarrow \Sigma(c_i - d_i)e_i = O_A, \quad i = 1, 2, \cdots, k$

$\Longleftrightarrow c_i \equiv d_i \bmod p^{d_i}, \quad i = 1, 2, \cdots, k$

$(\because \{e_1, e_2, \cdots, e_k\}$는 기저이다.)■

정의 2.5 A^+의 곱셈은 A^+ 위의 양 선형사상 $\pi : A^+ \times A^+ \to A^+$이며, π가 결합법칙을 만족한다는 것은, A^+의 a, b, c에 대해서

$$\pi(\pi(a, b), c) = \pi(a, \pi(b, c))$$

을 만족한다는 것이다.

예제 2.6 $A^+ = Z/p \oplus Z/p$이라면, 다음과 같이 정의되는 곱셈들은 결합법칙을 만족한다.

(1) $\pi((a_1, b_1), (a_2, b_2)) = (a_1a_2, b_2)$

(2) $\pi((a_1, b_1), (a_2, b_2)) = (a_1, b_2)$

군과 그 기저 간에는 곱셈에 관하여 다음과 같은 정리가 있다.

정리 2.7

1. 가환 군위에서 정의되는 모든 곱셈은 그 군의 한 기저위의 작용 (action)으로 볼 수 있다.

2. 역으로, 군의 기저위의 사상은 $o(\pi(a, b)) \leq \min\{o(a), o(b)\}$의 조건을 만족할때, 군위의 곱셈으로 확장 시킬 수 있다.

3. 군 위에서 곱셈이 교환(결합) 법칙을 만족하기 위한 필요충분 조건은 그 곱셈이 기저위에서 교환(결합) 법칙을 만족하는 것이다.

증명 [1] 참조■.

3. 환에 관한 계산 결과들

정의 3.1 A^+의 기저 $B=\{e_1, e_2, \cdots, e_k\}$에 관한 A^+의 곱셈표(multiplication table) T_π는

π	e_1	e_2	$\cdots$	e_k
e_1	$\pi(e_1, e_1)$	$\pi(e_1, e_2)$	$\cdots$	$\pi(e_1, e_k)$
e_2	$\pi(e_2, e_1)$	$\pi(e_2, e_2)$	$\cdots$	$\pi(e_2, e_k)$
$\cdots$	$\cdots$	$\cdots$		$\cdots$
e_k	$\pi(e_k, e_1)$	$\pi(e_k, e_2)$	$\cdots$	$\pi(e_k, e_k)$

이다.

예제 3.2 $A=GF(3^3)$이라 하면,
$A=Z_3[x]/(x^3+2x+1)$로 나타낼 수 있고, A^+의 기저는 $\{x^2, x, 1\}$이 된다. 따라서, 이 기저에 관한 곱셈표는,

π	x^2	x	1
x^2	x^2+2x	$x+2$	x^2
x	$x+2$	x^2	x
1	x^2	x	1

이다. 또한,
$A=Z_3[x]/(x^3+2x^2+1)$로도 나타낼 수 있고, 이때의 A^+의 기저도 $\{x^2, x, 1\}$이므로, 이 기저에 관한 다른 곱셈 π'의 곱셈표는

π'	x^2	x	1
x^2	x^2+2x+2	x^2+2	x^2
x	$x+2$	x^2	x
1	x^2	x	1

이다.

이 다른 두 곱셈은 "같은 수의 원소를 갖는 모든 체(field)는 서로 동형(isomorphic)이다."라는 것에 의해 동형인 곱셈으로 여겨진다.

A^+의 기저 $B=\{e_1, e_2, \cdots, e_k\}$는 좌표계로서 사용할 수 있으므로, A^+와 그 곱셈 π를 이용하여 이 기저에 관한 A에 있는 계수들을 블럭(block)의 형태로 모을 수 있다. 즉,

$\pi(e_i, e_j)=b_{ij}^1e_1+b_{ij}^2e_2+\cdots+b_{ij}^ke_k$를 만족하는 b_{ij}^n이 Z/p^{d_n}에 있다.

이 k개의 b_{ij}^n들이 벡터의 형태로 들어 있는 블럭을 B_{ij}라 하고, 이 블럭들의 행렬 형태의 모음을 $B=[B_{ij}]$라 하자. 그러면, B는 B_{ij}를 원소로 갖는 $k\times k$의 행렬이 되며, 각각의 B_{ij}는 k개의 b_{ij}^n들을 갖는 열(혹은 행) 벡터이다.

예제 3.3 $A^+=Z/2^4 \oplus Z/2^2$이라 하고,
$B_{11}=(1, 0)$, $B_{12}=(0, 1)$
$B_{21}=(0, 1)$, $B_{22}=(8, 1)$이라 하면, 곱셈표는

	(1, 0)	(0, 1)
(1, 0)	(1, 0)	(0, 1)
(0, 1)	(1, 0)	(8, 1)

이므로, A^+의 곱셈을 정의할 수 있다. 그러나, 다음과 같은 경우는 곱셈을 정의할 수 없다.

$B_{11}=(1, 0)$, $B_{12}=(0, 1)$
$B_{21}=(0, 1)$, $B_{22}=(2, 1)$이라 하면, 곱셈표는

	(1, 0)	(0, 1)
(1, 0)	(1, 0)	(0, 1)
(0, 1)	(1, 0)	(2, 1)

이므로, A^+의 곱셈으로 정의 할 수 없다.

다음 정리는 다음절에서 정의 하고자 하는 일향 함수의 일향성에 관한 근본을 제공하는 정리이다.

정리 3.4 A^+의 두 기저 $B_1=\{e_1, e_2, \cdots, e_k\}$와 $B_2=\{f_1, f_2, \cdots, f_k\}$에 대하여,

$$[e_1\ e_2\ \cdots\ e_k]\cdot M=[f_1\ f_2\ \cdots\ f_k]$$

를 만족하는 $GL(k, Z/p^d)$의 행렬 M이 존재한다. 여기서, $d=\max\{d_1, d_2, \cdots, d_k\}$이다.

증명 B_1은 기저이므로, 각 f_i들은 행렬 곱의 형태로 나타내어 질 수 있다. 즉,

$$[f_1\ f_2\ \cdots\ f_k]=[e_1\ e_2\ \cdots\ e_k]\cdot M$$

여기서, $M=[m_{ij}]$, m_{ij}는 k개의 식

$f_i=m_{1i}e_1+m_{2i}e_2+\cdots+m_{ki}e_k$

로 부터 계산된 수들이다. 비슷하게,

B_2는 기저이므로, 각 e_i들은 행렬 곱의 형태로 나타내어 질 수 있다.

$$[e_1\ e_2\ \cdots\ e_k]=[f_1\ f_2\ \cdots\ f_k]\cdot M'$$

따라서, $[f_1\ f_2\ \cdots\ f_k]=[f_1\ f_2\ \cdots\ f_k]\cdot M'\cdot M$

$\therefore M'\cdot M\equiv 1 \bmod p^d$.

$M\cdot(\mathrm{adj}\ M)=|M|\cdot I$이므로, M은 $GL(k, Z/p^d)$에 속한다■.

위 정리의 역은 항상 참이 아니다. 즉, 어떤 기저에 관한 $GL(k, Z/p^d)$의 원소가 다른 기저를 만들지는 못한다.

예제 3.5 A가 $Z/p^4 \oplus Z/p^2$이라 하고,

$$M=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\in GL(2, Z/p^4)$$라 하자.

이로 부터 얻는 집합 $\{e_1, e_1+e_2\}$는 기저가 아니다.

(왜냐하면, e_1+e_2의 차수는 p^4이지 p^2가 아니기 때문이다.)

참고 GL의 한 부분 집합을 이용할 때는 위 정리의 역도 성립한다. m_{ij}를 $p^{d_i-d_j}\mid m_{ij}$, $(d_i>d_j)$가 되도록 선택하여 만든 M은 또 다른 기저를 만들 수 있다.

정의 3.6 주어진 A^+의 모든 기저 변환 행렬들의 집합은, $C(d_i)$, i=1, 2, …, k로 표시되고, 다음과 같이 정의된다.

$$C(d_i)=\{M=[m_{ij}]\in GL(k, Z/p^d)\mid d=\max\{d_{ij}\},\ p^{d_{\sigma(i)}-d_{\sigma(j)}}\mid m_{\sigma(i)\sigma(j)}\}$$

여기서, σ는 k개의 원소의 대칭군이고, $d_{\sigma(i)}>d_{\sigma(j)}$이다.

정리 3. 7 A^+의 기저 $B=\{e_1, e_2, \cdots, e_k\}$에 대하여 $o(e_i)=p^{d_i}$이고, $d=\max\{d_1, d_2, \cdots, d_k\}$일때, [B]를 Z/p^d 위에서의 B_{ij}를 원소로 갖는 행렬이라 하자. 이 [B]가 기저 B 위에서 곱셈을 정의할 수 있기 위한 (결합법칙은 성립하지 않아도 되는) 필요충분 조건은 $\min\{p^{d_m}, p^{d_i}, p^{d_j}\}\cdot b_{ij}^m\equiv 0 \bmod p^{d_m}$이다.

증명 정리 2.7에 의하여 증명한다.

$o(\pi(e_i, e_j))\le\min\{o(e_i), o(e_j)\}$

$\Longleftrightarrow \min\{p^{d_i}, p^{d_j}\}\cdot(\pi(e_i, e_j))=O_R$

$\Longleftrightarrow \min\{p^{d_m}, p^{d_i}, p^{d_j}\}\cdot b_{ij}\equiv 0 \bmod p^{d_m}$,

m=1, 2, …, k이므로 정리 2.7에 의하여 성립한다■.

4. 일향 함수의 구축

B를 다음과 같이 정의되는 집합이라 하자.

$B=\{[B]=[b_{ij}^m]\mid b_{ij}^m\in Z/p^d,$

여기서 i, j, m=1, 2, …, k$\}$

참고 mod Z/p^d에 관한 덧셈과 곱셈을 하면, 이 B는 환으로서, 혹은 Z/p^d-모듀율(module)로서 $[Z/p^d]^k\times[Z/p^d]^k\times[Z/p^d]^k$과 동형임을 알 수 있다.

정의 4.1 $M=[m_{ij}]\in GL(k, Z/p^d)$과

$M^{-1}=[m_{ij}']$에 대하여

$F_A : B \to B$를 다음과 같이 정의한다.

$$[F_A([B])]_{ij}^{n}=\sum_{r=1}^{k}\sum_{s=1}^{k}\sum_{t=1}^{k} m_{ri}m_{sj}m_{nt}'b_{rs}^{t}$$

이 사상 F_A는

$F_A([B_1]+[B_2])=F_A([B_1])+F_A([B_2])$

$F_A(c\cdot[B])=c\cdot F_A([B]),\ C\in Z/p^d$

이므로, 선형 준동형 사상(linear homomorphism)이고, 따라서, B의 기저에 대해 행렬로 표현될 수 있다.

다음 정리는 GL(k, Z/p^d)가 B 위에서의 군의 작용(group action)임을 보이는 정리이다.

정리 4.2 M, $M'\in GL(k,\ Z/p^d)$와 $[B]\in B$에 대하여,

$$F_{M\cdot M'}([B])=F_{M'}\cdot(F_M([B]))$$

이다.

증명 정의 4.1과 Σ의 첨자들의 재배열로 증명할 수 있다■.

참고 [B]가 가환이라면, $F_A([B])$도 그러하다. 따라서, 불변 부분공간(invarant subspace)이 있음을 알 수 있고, F_A는 변형들의 직접으로 나타낼 수 있음을 알 수 있다.

정의 3.6을 이용하여, 곱셈표들의 집합 T 위의 군의 작용을 살필 수 있다.

정의 4.3 $C(d_i)$의 한 원소 D와 기저 $\{e_1, e_2, \cdots, e_k\}$에 대하여, 이 기저에 관한 곱셈 π의 표를 T라 하자. 사상 $D(\cdot) : T\to T$를 다음과 같이 정의 한다.

$$D(T)=D^t * T * D$$

이때, D(T)는 새로운 기저

$$\{\sum_{i=1}^{k} d_{i1}e_i,\ \sum_{i=1}^{k} d_{i2}e_i,\ \cdots,\ \sum_{i=1}^{k} d_{ik}e_i\}$$

에 관한 곱셈표, 즉 T의 원소가 된다.

참고 이때, 곱셈표 T 대신 [B]를 써서도 같은 방법으로 D([B])를 정의 할 수 있다.

정리 4.4 $C(d_i)$의 한 원소 D와 기저 $\beta=\{e_1, e_2, \cdots, e_k\}$, 그리고, 이 기저에 관한 곱셈 π의 표를 T, 계수 블럭 행렬을 $[B]_\beta$라 하자. 그렇다면,
기저

$$\beta'=\{\sum_{i=1}^{k} d_{i1}e_i,\ \sum_{i=1}^{k} d_{i2}e_i,\ \cdots,\ \sum_{i=1}^{k} d_{ik}e_i\}$$에 대하여,

$$F_D([B]_\beta)=[D[B]_\beta)]_{\beta'}$$ 이다.

증명 다음 등식이 증명 과정의 중심이 된다.

$$[D([B]_\beta)]_{ij}^{m}=\sum_{r=1}^{k}\sum_{s=1}^{k} d_{ri}\ d_{sj}\ b_{rs}^{m}$$

$$[[D([B]_\beta)]_\beta]_{ij}^{m}=\sum_{r=1}^{k}\sum_{s=1}^{k}\sum_{t=1}^{k} d_{ri}\ d_{sj}\ d_{mt}'\ b_{rs}^{t}$$

■.

정리 4.5 A^+의 두 곱셈 π′와 π, 기저 $\beta=\{e_1, e_2, \cdots, e_k\}$, 그리고, 이 기저에 관한 계수 블럭 행렬을 [B]과 [B′]라 하자. 또, A^+와 곱셈 π에 의하여 만들어지는 환을 A, A^+와 곱셈 π′에 의하여 만들어지는 환을 A′이라 하자. 그러면,

$A\cong A'$이기 위한 필요충분조건은 $F_D([B])=[B']$을 만족하는 $C(d_i)$의 행렬 D가 존재하는 것이다.

증명 정리 4. 4에 의하여 자명하다■.

5. 결 론

계수 블럭 행렬 [B]를 평문(plain text)으로 하고, 기저 변환 행렬 집합인, $C(d_i)$의 D를 암호화 행렬로 하면, $F_D([B])$는 암호문(ciphered text)이 된다. 이 함수에 의한 암호문을 해독하는 것은, 이론적으로는 불가능하지 않으나, 소인수 분해의 어려움

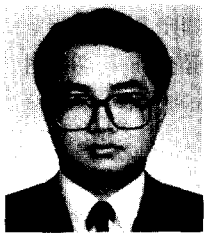
에 근거한 암호 시스템, 예를 들면 RSA 공개키 암호 시스템과 같이, 계산이 어려운 문제이다. 이 일향 함수를 적용하였을때 고려하여야 할 사항으로는 암호문의 크기가 평문의 크기의 세제곱의 비로 확대된다는 것이다.

D를 쉽게 찾을 수 있는 선형 분할 방법(linear subdividing method)이 없으므로, $F_D([B])$로부터 평문 [B]를 찾는 것은 어려운(hard) 문제이다. 물론 계급(rank)이 작은 환의 경우는 그 선형화(linearization)의 필요 연산이 많지 않으나, 일반적으로, k개의 [B]를 암호화한, k^3개의 $F_D[B]$를 풀기 위한 연산의 수는 "$k^n+f(k)$, deg f < n"이므로 계산이 어렵다.

참 고 문 헌

1. Fuchs, L., Infinite Aberian Groups, Vol. I, II, Academic Press, 1973.
2. Jacobson, N., The Structure of Rings, AMS Colloquium Pub., Vol 37, 1964.
3. Kim, C., A Classification of the Finite Rings with Unity by computable Means, Ph. D. Thesis, NCSU, USA, 1989.
4. McDonald, B. R., Finite Ring with Identity, Marcel Dekker inc, 1974.
5. Meyer, C. H. and Mattyas, S.M., Cryptography : A New Dimension in Computer Data Security, John Wiley & Sons, 1982.
6. 김응태 박승안 공저, 현대대수학, 제 3 판, 경문사, 1991.

□ 著者紹介



金　　鐵(正會員)

연세대학교 이과대학 수학과 졸업(이학사)
미국 North Carolina 주립대 대학원 수학과 졸업(이학 석사·박사)
미국 North Carolina 주립대 수학과 시간강사
미국 Shaw University 전임강사
미국 University of South Dakota 수학과 조교수
현 : 광운대학교 이과대학 수학과 조교수

연구 관심분야 : 추상 대수학의 응용, 암호학의 수학적 이론, DB의 보안, Chaos의 암호학에의 응용등임.