김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제12호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 12 JUCHE105(2016).

표수가 2인 유한체우에서 거꿀함수로부터 차분4－평등한 치환의 한가지 구성법

차성룡, 김률

론문에서는 부호 및 암호학의 중요한 연구대상으로 되고있는 표수가 2인 유한체우에서 차분4－평등한 치환의 한가지 새로운 구성법에 대하여 연구하였다.

지금 대칭암호계들에서는 핵심부인 S－통으로 확대차수가 짝수인 유한체우에서의 차동적균등성이 작고 비선형성과 대수적차수가 높은 치환함수들을 리용하고있다.

f를 유한체 $\mathbf{F}_{2^n}$우에서의 함수라고 할 때 방정식 $f(x+a)+f(x)=b$의 풀이 $x\in\mathbf{F}_{2^n}$의 개수를 $N(a,\ b)$로 표시한다. 여기서 $a,\ b\in\mathbf{F}_{2^n}$이다.

$\Delta_f=\max\{N(a,\ b)\,|\,a,\ b\in\mathbf{F}_{2^n},\ a\neq 0\}$이라고 할 때 $\Delta_f=k$이면 f는 차동적으로 k－균등하다고 말한다. 이때 $f(x+a)+f(x)=f((x+a)+a)+f(x+a)$이므로 Δ_f의 가능한 최소값은 2이다. 특히 $\Delta_f=2$일 때 f를 거의완전비선형(APN)함수라고 부른다.[2]

선행연구[1]에서는 함수 $x^{2^{2k}+2^k+1}$이 $\mathbf{F}_{2^{4k}}$(k：홀수)우에서 차분4－평등한 치환이라는것을 밝히고 선행연구[2]에서는 $\alpha x^{2^s+1}+\alpha^{2^k}x^{2^{-k}+2^{k+s}}$이 $s,\ k$에 대한 일정한 조건밑에서 $\mathbf{F}_{2^{3k}}$(k：짝수)우의 차분4－평등한 치환이라는것을 밝혔으며 선행연구[3]에서는 $\mathbf{F}_{2^{2m}}$의 어떤 부분체에서의 거꿀함수의 값들을 변화시켜 새로운 차분4－평등한 치환들을 얻었다.

k가 n의 약수라고 할 때 흔적넘기기 $\mathrm{Tr}_k^n:\mathbf{F}_{2^n}\to\mathbf{F}_{2^k}$을 아래와 같이 정의한다.[3]

$$\mathrm{Tr}_k^n(x):=x+x^2+x^{2^k}+\cdots+x^{2^{n-k}}$$

$f:\mathbf{F}_{2^n}\to\mathbf{F}_{2^n}$에 대하여 $f^w(a,\ b):=\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(ax+bf(x))}$, $a\in\mathbf{F}_{2^n}$, $b\in\mathbf{F}_{2^n}^*$로 정의되는 변환 $f^w:\mathbf{F}_{2^n}\times\mathbf{F}_{2^n}^*\to\boldsymbol{C}$를 f의 왈쉬변환, 모임 $W_f:=\{f^w(a,\ b)\,|\,a\in\mathbf{F}_{2^n},\ b\in\mathbf{F}_{2^n}^*\}$을 f의 왈쉬스펙트르, f에 대하여 $NL(f)=2^{n-1}-\frac{1}{2}\max_{w\in W_f}|w|$을 f의 비선형성이라고 부른다.[3]

$\mathbf{F}_{2^n}$우에서의 거꿀함수를 $f(x)=\begin{cases}x^{-1}, & x\neq 0\\ 0, & x=0\end{cases}$으로 정의한다.[3]

론문에서는 $\mathbf{F}_{2^{2m}}$의 어떤 부분모임에서의 거꿀함수의 값들을 변화시켜 차분4－평등한 새로운 치환들을 얻으려고 한다.

$n,\ s$는 $n>1$인 정의옹근수이고 $q=2^s$이며 ω는 유한체 $\mathbf{F}_q$의 대수적확대체에서 1의 원시3제곱뿌리라고 하자.

보조정리 1[3] s는 홀수, n은 짝수이고 $t\in\mathbf{F}_q^*$일 때 $a^{q-1}=\omega$ 혹은 $a^{q-1}=\omega^2$이 성립

되며 방정식

$$x^2+ax+a^2/(1+at)=0 \tag{1}$$

이 $\mathbf{F}_{q^n}\setminus\mathbf{F}_q$에서 두 풀이를 가지도록 하는 원소 $a\in\mathbf{F}_{q^n}^*\setminus\mathbf{F}_q$가 존재하기 위해서는 $s\geq 5$ 혹은 $s=1,\ 3$이고 $n/2$이 짝수일것이 필요하고 충분하다.

보조정리 2[3] $\mathbf{F}_{2^n}$ 우에서의 클루스터만합을 $K_s(\lambda):=\sum_{x\in\mathbf{F}_{2^n}}(-1)^{\mathrm{Tr}(\lambda x+x^{-1})}$, $\lambda\in\mathbf{F}_{2^n}$으로 정의하면 모임 $\{K_s(\lambda):\lambda\in\mathbf{F}_{2^n}\}$은 구간 $[-2^{s/2+1}+1,\ 2^{s/2+1}+1]$에서의 4의 배수들전부의 모임과 일치한다.

보조정리 3 $t\in\mathbf{F}_q^*$이고 i는 n의 정의약수이며 $a\notin\mathbf{F}_{q^i}$일 때 n/i이 홀수이면 방정식 (1)은 $\mathbf{F}_{q^i}$에서 풀이를 가지지 않는다.

i를 n의 정의약수라고 가정하고 다항식 $f(x)$를 아래와 같이 구성하자.

$$f(x)=x^{-1}+t(x^q+x)^{q^n-1}+t(x^{q^i}+x)^{q^n-1}+t=\begin{cases}x^{-1}+t, & x\in\mathbf{F}_q\\ x^{-1}, & x\in\mathbf{F}_{q^i}\setminus\mathbf{F}_q,\ t\in\mathbf{F}_q^*\\ x^{-1}+t, & x\notin\mathbf{F}_{q^i}\end{cases} \tag{2}$$

그러면 $f(x)$는 $\mathbf{F}_{q^n}$ 우에서 치환이다.

이제 다음의 방정식의 $\mathbf{F}_{q^n}$ 우에서의 풀이에 대하여 론의하자.

$$f(x+a)+f(x)=b,\ a\in\mathbf{F}_{q^n}^*,\ b\in\mathbf{F}_{q^n} \tag{3}$$

$b=0$인 경우 식 (3)은 풀이를 가지지 않으므로 $b\neq 0$으로 가정한다.

x를 방정식 (3)의 풀이이라고 가정하자.

$x=0,\ a$라고 하면 $b_0:=b=a^{-1}+t(a^q+a)^{q^n-1}+t(a^{q^i}+a)^{q^n-1}=\begin{cases}a^{-1}, & a\in\mathbf{F}_q\\ a^{-1}+t, & a\in\mathbf{F}_{q^i}\setminus\mathbf{F}_q\\ a^{-1}, & a\notin\mathbf{F}_{q^i}\end{cases}$ 이다.

$x\neq 0,\ a$일 때 아래와 같이 두가지 경우로 갈라서 풀이에 대하여 론의하자.

① $x,\ x+a\in\mathbf{F}_{q^i}\setminus\mathbf{F}_q$ 혹은 $x,\ x+a\notin\mathbf{F}_{q^i}\setminus\mathbf{F}_q$ 인 경우 방정식 (3)으로부터

$$bx^2+abx+a=0 \tag{4}$$

이 얻어지며 방정식 (4)는 기껏 2개의 풀이를 가진다.

② $x,\ x+a$ 중에서 꼭 하나만이 $\mathbf{F}_{q^i}\setminus\mathbf{F}_q$에 속하는 경우 방정식 (3)으로부터

$$(b+t)x^2+a(b+t)x+a=0 \tag{5}$$

이 얻어진다. $a\neq 0$이므로 방정식 (5)는 기껏 2개의 풀이를 가진다.

우의 두 경우를 종합하면 $b\neq b_0$인 경우 임의의 쌍 $(a,\ b)\in\mathbf{F}_{q^n}^*\times\mathbf{F}_{q^n}^*$에 대하여 방정식 (3)은 기껏 4개의 풀이를 가진다는것을 알수 있다.

다음으로 $b=b_0$일 때 우와 같이 두가지 경우로 갈라서 방정식 (3)의 풀이를 론의하여 함수 f의 차동적균등성을 구하자.

정리 1 s가 짝수이고 n/i이 홀수일 때 식 (2)에 의하여 얻어진 함수 f는 $\mathbf{F}_{q^n}$ 우에서 차분4－평등한 치환이다.

증명 $a\in\mathbf{F}_q$, $b=b_0=a^{-1}$일 때 첫 경우에는 방정식 (4)의 두 풀이 ωa, $\omega^2 a\in\mathbf{F}_q$를 가지며 둘째 경우에는 풀이를 가지지 않는다. 결국 방정식 (3)은 4개의 풀이 0, a, ωa, $\omega^2 a$를 가진다.

$a\in\mathbf{F}_{q^i}\setminus\mathbf{F}_q$, $b=b_0=a^{-1}+t$일 때 둘째 경우에 방정식 (5)의 두 풀이 ωa, $\omega^2 a$가 얻어진다. s가 짝수이므로 $q\equiv 1(\mathrm{mod}\ 3)$이고 따라서 ωa, $\omega^2 a\in\mathbf{F}_{q^i}\setminus\mathbf{F}_q$이므로 이 두 풀이는 둘째 경우의 풀이로 될수 없다. 따라서 방정식 (3)은 기껏 4개의 풀이를 가진다.

$a\notin\mathbf{F}_{q^i}$, $b=b_0=a^{-1}$일 때 첫 경우에 방정식 (4)의 두 풀이 ωa, $\omega^2 a\notin\mathbf{F}_{q^i}$를 가진다.

둘째 경우에 방정식 (5)로부터 식 (1)이 나오고 n/i이 홀수이므로 보조정리 3으로부터 방정식 (1)은 $\mathbf{F}_{q^i}$에서 풀이를 가지지 않으므로 방정식 (3)은 4개의 풀이 0, a, ωa, $\omega^2 a$를 가진다. 따라서 f는 $\mathbf{F}_{q^n}$ 우에서 차분4－평등한 치환이다.(증명끝)

정리 2 s가 홀수, n이 짝수, n/i이 홀수, i가 짝수일 때 $s=1, 3$이고 $n/2$이 홀수이면 식 (2)에 의하여 얻어진 함수 f는 $\mathbf{F}_{q^n}$ 우에서 차분4－평등한 치환이다.

정리 3 식 (2)에 의하여 얻어진 함수 f의 비선형성은 다음의 부등식을 만족시킨다.

$$NL(f)\geq 2^{sn-1}-2^{sn/2}-2^{si/2+1}-2^{s/2+1}$$

참 고 문 헌

[1] C. Bracken et al.; Finite Fields Appl., **16**, 4, 231, 2010.

[2] C. Bracken et al.; Finite Fields Appl., **18**, 3, 537, 2012.

[3] Z. Zha et al.; Finite Fields Appl., **25**, 64, 2014.

주체105(2016)년 8월 5일 원고접수

A Method of Constructing Differentially 4-Uniform Permutation Polynomials from the Inverse Function over Finite Fields with Characteristic 2

Cha Song Ryong, Kim Ryul

Many symmetric ciphers use the substitution boxes(*S*-boxes) to bring the confusion into the system. One would like these functions have low differential uniformity, high nonlinearity and high algebraic degree for resisting against linear cryptanalysis, differential cryptanalysis and other cryptanalysis. The inverse function over $\mathbf{F}_{2^8}$ is such a function and is used as the *S*-boxes of the advanced encryption standard (AES). We have some new differentially 4-uniform permutations over $\mathbf{F}_{2^{2m}}$ varying the values of the inverse function in some subset of $\mathbf{F}_{2^{2m}}$.

Key words: differentially uniformity, permutation polynomial