情報保護學會論文誌
第13券 第5號, 2003. 10

종수 2인 초타원곡선을 이용한 균형상관면역함수의 생성에 관한 연구*

최 춘 수**, 이 민 섭**

On a construction of resilient functions using a hyperelliptic curve with genus 2

Chun-Soo Choi**, Min-Surp Rhee**

요 약

유한체 F_{2^n} 위에서 정의되는 다항식을 이용하여 암호학적으로 좋은 성질을 갖는 부울함수를 생성하는 방법으로 3차 다항식을 이용하여 균형상관면역함수를 생성하는 방법이 [3]에서 제안되었다. 이 논문에서는 $n \leq 14$일 때 5차 다항식을 이용하여 비선형치가 높은 균형상관면역함수를 생성하는 방법을 제안하고, 예를 제시한다.

ABSTRACT

In [3], J. H. Cheon and S. T. Chee proposed a method to generate boolean functions with good properties using a polynomials of degree 3 over a finite field F_{2^n}. In this paper, we propose a method generating resilient functions with high nonlinearity from polynomials of degree 5 over a finite field F_{2^n} ($n \leq 14$).

keyword :

Ⅰ. 서 론

안전한 블록 암호 알고리즘, 스트림암호 알고리즘 및 해쉬함수들을 설계하기 위하여 암호학적으로 좋은 특성을 갖는 부울함수가 가지는 주요한 특성으로 균등성(balancedness), 비선형치(nonlinearity), 상관면역도(correlation immunity), 확산판정(propagation criterion), 선형구조(linear structure) 등이 있다. 유한체 F_2위의 n차원 벡터공간에서 균형상관면역함수를 만드는 방법으로는 Seberry의 방법, Cheon의 방법 등이 있다.[3,15] 이 중에서 Cheon의 방법은 유한체 F_{2^n}위에서 정의되는 다항식을 이용하여 암호학적으로 좋은 성질을 갖는 부울함수를 생성하는 방법으로 3차 다항식을 이용하여 균형상관면역함수를 생성하는 방법을 제안하였다. 특히, Seberry는 변수가 적은 부울함수들을 이용하여 변수가 많은 즉, n이 큰 경우에 암호학적으로 좋은 상관면역도가 높은 함수를 설계하는 방법을 제안하였다.

본 논문에서는 $n \leq 14$일 때, 유한체 F_{2^n}위에서 정의되는 초타원곡선을 이용하여 위수가 1이고 비선형치가 좋은 균형상관면역함수를 생성하는 방법을 제안하고, 이를 구하는 알고리즘을 제시하였다.

제Ⅱ장에서는 부울함수에 관한 여러 가지 기본적인 정의 및 성질들을 소개한다. 제Ⅲ장에서는 선형화

* 본 논문은 2003년도 영남지부 학술대회 우수논문임.
** 단국대학교 첨단과학부(bleute@passmail.to, msrhee@dku.edu)

된 다항식을 정의하고, 선형화된 다항식과 부울함수의 관계를 설명한다. 제Ⅳ장에서는 초타원곡선을 이용하여 균형상관면역함수를 생성하는 알고리즘을 제안하고 제Ⅴ장에서 이 연구에서 제안한 방법에 의하여 생성된 부울함수는 비교적 높은 비선형치를 가짐을 설명하였다.

Ⅱ. 예비사항

유한체 F_2위의 n차원 벡터공간에서 정의되는 부울함수 f의 대수적 표준형은 다음과 같다.

$$f(x_1, x_2, \cdots, x_n) = a_0 + \sum a_i x_i + \cdots + a_{1\cdots n} x_1 \cdots x_n$$

단, $a_0, a_i, a_{ij}, \cdots, a_{12\cdots n}, x_1, x_2, \cdots, x_n \in F_2$이다. 한편, f의 대수적 차수는 대수적 표준형에서 변수들의 개수가 가장 많은 개수로 정의하고 $\deg(f)$로 표시한다. 함수 f의 대수적 차수가 1이면 함수 f를 아핀함수라고 한다. 즉, 임의의 $a_i \in F_2$에 대하여

$$f(x_1, x_2, \cdots, x_n) = a_0 + a_1 x_1 + \cdots + a_n x_n$$

이다. 특히, $a_0 = 0$인 f를 선형함수라고 한다.

함수 f의 함수값들 중 '1'의 개수를 함수 f의 무게라 하고 $wt(f)$로 표시한다. 함수 f의 무게가 2^{n-1}이면 함수 f는 균형이라 한다. 부울함수 f와 g의 해밍거리는 f와 g가 서로 다른 함수값을 가지는 정의역에 속한 원소의 개수이다. 즉,

$$d(f, g) = \#\{x \in F_{2^n} | f(x) \neq g(x)\}$$

이다. 부울함수 f와 g의 교차상관(cross correlation)은

$$c(f, g) = \frac{\#\{x \in F_{2^n} \mid f(x) = g(x)\}}{2^n} - \frac{\#\{x \in F_{2^n} \mid f(x) \neq g(x)\}}{2^n}$$

이다. 한편, F_{2^n} 위의 함수 f와 임의의 아핀함수의 거리 중에 최소값을 함수 f의 비선형치(nonliearity)라고 하고, N_f로 표시한다. 즉,

$$N_f = \min\{d(f, l) \mid l\text{은 아핀함수}\}$$

함수 f의 출력값이 k개 이하의 임의의 입력성분 $\{x_{i_1}, x_{i_2}, \cdots, x_{i_k}\}$과 독립일 때 함수 f를 위수 k인 상관면역함수(k-th correlation immune function)라고 한다. $(1 \leq k \leq n)$ 즉, 임의의 $i_1, i_2, \cdots, i_l$과 $a_1, a_2, \cdots, a_l \in F_{2^n}$에 대하여

$$P[f(x) = 1 \mid x_{i_1} = a_1, \cdots, x_{i_l} = a_l] = P[f(x) = 1]$$

이다. 단, $1 \leq i_1 < \cdots < i_l \leq n$, $1 \leq l \leq k$이고 $P[f(x) = 1]$는 $f(x) = 1$이 일어날 확률이다. 또한, 함수 f가 균형이면서 위수 k인 상관면역함수일 때 f를 위수 k인 균형상관면역함수라고 한다.

부울함수 f에 대하여 F_{2^n} 위에서 다음과 같이 정의되는 f의 실수값 함수를 f의 Walsh Hadamard 변환이라고 한다.

$$W_f(a) = \sum_{x \in F_{2^n}} (-1)^{f(x) + a \cdot x}$$

단, $a \cdot x$는 F_{2^n}위에서의 내적이다.

임의의 $\alpha \in F_{2^n}$에 대하여

$$Tr(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \cdots + \alpha^{2^{n-1}}$$

정의되는 함수 $Tr : F_{2^n} \rightarrow F_2$를 트레이스 함수(trace function)라고 한다. 또한 α의 상 $Tr(\alpha)$는 α의 트레이스라 한다. 즉, F_{2^n}위에서 α의 트레이스는 F_2에 관한 α의 공액원들의 합이다. 임의의 $\alpha, \beta \in F_{2^n}$와 $c \in F_2$에 대하여 다음이 성립한다.

(1) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.
(2) $Tr(c\alpha) = cTr(\alpha)$. 특히, $Tr(c) = nc$.
(3) $Tr(\alpha) = Tr(\alpha^2)$.

F_{2^n}위의 임의의 선형부울함수는 선택된 기저와 독립적으로 F_{2^n}에서 F_2로의 트레이스함수를 이용한 선형변환으로 표현할 수 있다. 즉, F_{2^n}에서 F_2로의 임의의 선형변환은 F_{2^n}에서 주어진 n개의 기저에 F_2의 임의의 원소를 대응함으로써 얻을 수 있으므로 2^n개의 서로 다른 선형변환이 존재한다.

정의 2.1 유한체 F_{2^n}의 기저 $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$와 $\{\beta_1, \beta_2, \cdots, \beta_n\}$에 대하여 $Tr(\alpha_i \beta_j) = \delta_{ij}$이면, 두 기

저는 쌍대(dual)라고 한다.

단, $\delta_{ij}=\begin{cases}0 & \text{for } i\neq j\\ 1 & \text{for } i=j\end{cases}$ 이다.

위의 정의로부터 F_{2^n}의 임의의 원소 x와 y를 각각 기저와 쌍대기저로 표현하면, $Tr(xy)=x\cdot y$이다.

Ⅲ. 선형화된 다항식

제Ⅱ장에서 선형부울함수를 적당한 $a\in F_{2^n}$에 대하여 $Tr(ax)$의 형태로 표현하였다. 이 장에서는 차수가 높은 부울함수의 성질을 일반화한다.

유한체 F_{2^n} 위에서 $a_i\in F_{2^n}$와 $x\in F_{2^n}$에 대하여 다음과 같이 정의되는 다항식 $L(x)$를 선형화된 다항식(linearized polynomial)이라고 한다.

$$L(x)=\sum_{i=0}^{n-1}a_ix^{2^i}$$

더욱이, d개의 변수를 갖는 선형화된 다항식 $L_d(x_1,x_2,\cdots,x_d)$는 임의의 $a_{i_1i_2\cdots i_d}\in F_{2^n}$과 변수 x_i에 대하여 다음과 같이 정의된다.

$$L_d(x_1,x_2,\cdots,x_d)=\sum_{i_1=0,\cdots,i_d=0}^{n-1}a_{i_1i_2\cdots i_d}x_1^{2^{i_1}}x_2^{2^{i_2}}\cdots x_d^{2^{i_d}}$$

성질 3.1[4] 부울함수 $f: F_{2^n}\rightarrow F_2$가 $d+1$차 라 하면,

$$f(x)=Tr(x_0L_d(x_1,x_2,\cdots,x_d))$$

를 만족하는 d개의 변수를 갖는 선형화된 다항식 L_d가 F_{2^n}위에 존재한다. 더욱이, 감소수열 $i_1,i_2,\cdots,i_d$에 대하여 그 계수가 $a_{i_1i_2\cdots i_d}=0$인 선형화된 다항식 L_d를 얻을 수 있다.

성질 3.2 양의 정수 d에 대하여 $f: F_{2^n}\rightarrow F_2$를 $d+1$차 함수라고 하면, $f(x)=Tr(xP_d(x))$ 를 만족하는 $2^{i_1}+2^{i_2}+\cdots+2^{i_d}$차 다항식

$$P_d(x)=\sum_{i_1=0,\cdots,i_d=0}^{n-1}a_{i_1i_2\cdots i_d}x^{2^{i_1}+2^{i_2}+\cdots+2^{i_d}}$$

이 존재한다($a_{i_1i_2\cdots i_d}\in F_2$). 더욱이 감소수열 $i_1,i_2,\cdots,i_d$에 대하여 그 계수가 $a_{i_1i_2\cdots i_d}=0$인 다항식 P_d를 얻을 수 있다.

〔표 3.1〕 f의 차수에 대한 $xP_d(x)$의 차수

f의 차수	$xP_d(x)$의 차수
1	1,2,4,8
2	3,6,12,9
	5,10
3	7,14,13,11

체 F_{2^n}를 유한체 F_2의 유한확대체라 하고 집합 $Z_N=\{0,1,2,\cdots,N-1\}$을 자연수 N을 법으로 한 잉여류의 집합이라고 하자. 자연수 N이 (2^n-1)의 약수이면 다음과 같이 정의되는 집합 C_i는 법 N에 관한 $i\in Z_N$를 포함하는 원분 잉여류(cyclotomic coset)라고 한다.

$$C_i=\{i,\ 2i,\ 2^2i,\ \cdots,\ 2^{n-1}i\ \}$$

이제, 법 N에 관한 i를 포함하는 원분 잉여류의 집합은 Z_N의 분할이다. 만약 $N=2^n-1$이면 법 N에 관한 i를 포함하는 원분 잉여류 C_i는 d차 부울함수를 생성하는 다항식 $xP_d(x)$의 차수들의 집합과 같다. 예를 들면 F_{2^4}에서 부울함수 f의 차수와 다항식 $xP_d(x)$의 차수의 관계는 표 3.1과 같다.

Ⅳ. 초타원곡선

이 장에서는 종수 2인 초타원곡선을 이용하여 균형상관면역함수를 생성하는 알고리즘을 제안한다.

정의 4.1 유한체 F_{2^n} 위에서 종수 g ($g\geq 1$)인 초타원곡선(hyperelliptic curve) C는 특이점을 갖지 않는 다음과 같이 정의된 방정식이다.

$$C:\ y^2+H(x)y=F(x)$$

단, $H(x)$는 최대 차수가 g인 다항식이고 $F(x)$는 차수가 $2g+1$인 모닉 다항식이다.

곡선 C위의 점 $(x,y)\in F_{2^n}\times F_{2^n}$을 C의 F_{2^n}-유리점이라고 하고, 무한원점 O와 식 C를 만족하는 모든 유리점 (x,y)의 집합을 기호 $C(F_{2^n})$으로 나타낸다. 한편, 무한 원점을 제외한 $C(F_{2^n})$의 개수를 $\#C(F_{2^n})$

로 표현한다.

유한체 F_{2^n} 위에서 다음과 같이 정의된 곡선

$$y^2+y=aF(x)+bx \tag{4.1}$$

을 $C_{a,b}$라고 하자. 단, $F(x)$는 F_{2^n}위에서의 다항식이다.

성질 4.2[3] $c(a\cdot F, b\cdot x)$을 $a\cdot F$와 $b\cdot x$의 교차상관이라고 하면,

$$c(a\cdot F, b\cdot x)=\frac{\#C_{a,b}(F_{2^n})}{2^n}-1$$

곡선 $C_{a,b}$의 점의 개수와 부울함수의 Walsh Hadamard 변환 사이의 관계는 다음과 같다.

성질 4.3[4] $f(x)=Tr(aF(x))$이라고 하면,

$$W_f(b)=\#C_{a,b}(F_{2^n})-2^n$$

이다. 단, $W_f(b)$는 f의 Walsh-Hadamard 변환이다. 즉, $W_f(b)=2^n c(a\cdot F, b\cdot x)$이다.

성질 4.4[13] 집합 $Z(L)$과 $Z(P)$는 각각 $x^{2^m}+x=0$와 $x^{2^m}+x=b$ ($b\in F_{2^n}$)의 모든 근들의 집합이라고 하자. 그러면, $x^{2^m}+x+b=0$가 F_{2^n}에서 근을 가질 필요충분조건은

$$Tr_{F_{2^d}}(b)=\sum_{i=0}^{k-1} b^{2^{im}}=0$$

이다. 단, $F_{2^d}\subseteq F_{2^n}$, $d=(n,m)$이고 $k=\frac{n}{d}$이다. 또한, 이러한 조건 아래 $Z(L)=F_{2^d}$이고, 임의의 $x_0\in Z(P)$에 대하여 $Z(P)=x_0+Z(L)$이다.

예 4.1 유한체 F_{2^n}위의 방정식

$$x^{16}+ax+b=0 \quad (a\neq 0) \tag{4.2}$$

에 대하여 다음이 성립한다.

(1) n이 홀수이면 (4.2)는 근을 갖지 않거나 2개의 근을 갖는다.

(2) n이 짝수이고 $\sqrt[15]{a}\in F_{2^n}$이면 $Tr_{F_q}\left(\frac{b}{\sqrt[15]{a^{16}}}\right)=0$일 때, (4.2)는 q개의 근을 갖고 $Tr_{F_q}\left(\frac{b}{\sqrt[15]{a^{16}}}\right)\neq 0$일 때는 근을 갖지 않는다. 단, $q=2^{(4,n)}$이다.

합성함수 $\phi\circ\psi$와 $\psi\circ\phi$ 가 각각 V_1과 V_2에서 항등함수인 동형 $\phi: V_1\to V_2$과 $\psi: V_2\to V_1$ (ϕ, ψ는 F_{2^n}위에서 정의된다) 가 존재하면 V_1과 V_2는 F_{2^n}위에서 동형(isomorphism)이라고 한다. $H(x)$는 F_{2^n}위에서 최대 차수가 g인 다항식이고 $F(x)$는 차수가 $2g+1$인 모닉다항식이라고 하면 F_{2^n}위에서 특이점을 갖지 않는 다음과 같이 정의된 방정식

$$H: y^2+H(x)y=F(x)$$

를 종수 g인 Weierstrass 방정식이라고 한다.

방정식 H에서 방정식 H'으로의 변수변환이 $(x,y)\to(a^2x+\beta, a^{2g+1}y+T(x))$인 F_{2^n}의 원소 $a(\neq 0)$, β와 $\deg(T(x))\leq g$인 다항식 $T(x)$가 존재하면 두 Weierstrass 방정식 H와 H'은 F_{2^n}위에서 동치(equivalent)라고 한다.

F_{2^n}위에서의 종수 g인 초타원곡선들의 집합을 H_g, F_{2^n}위에서 종수 g인 Weierstrass 방정식들의 집합을 M_g라고 하면, H_g의 초타원곡선의 동형류와 M_g의 Weierstrass방정식의 동치류는 일대일 대응이다.[10]

이제, 종수 $g=2$인 경우에 대하여 살펴보자.

성질 4.5[10] 유한체 F_{2^n}위에서의 다음과 같이 정의되는 종수 2인 초타원곡선을 E_1, E_2라고 하자.

$$\begin{aligned} E_1:\quad & y^2+(a_1x^2+a_3x+a_5)y \\ & =x^5+a_2x^4+a_4x^3+a_6x^2+a_8x+a_{10} \\ E_2:\quad & y^2+(\overline{a_1}x^2+\overline{a_3}x+\overline{a_5})y \\ & =x^5+\overline{a_2}x^4+\overline{a_4}x^3+\overline{a_6}x^2+\overline{a_8}x+\overline{a_{10}} \end{aligned}$$

그러면 E_1과 E_2는 F_{2^n}위에서 동형일 필요충분한 조건은 E_1을 E_2로 변환시키는 다음과 같은 변수변환 (4.3)

$$(x,y)\to(a^2x+\beta, a^5y+a^4\gamma x^2+a^2\delta x+\varepsilon)$$

을 만족하는 $a(\neq 0)$, β, γ, δ와 ε이 F_{2^n}에 존재한

다. 이 때 $E_1 \cong E_2$로 표시한다. 이때, E_1에서 E_2로의 변수변환 (4.3)은 다음과 같은 방정식으로 유도할 수 있다.

$$\begin{aligned}
&\alpha\overline{a_1} = a_1\\
&\alpha^3\overline{a_3} = a_3\\
&\alpha^5\overline{a_5} = a_5 + \beta a_3 + \beta^3 a_1\\
&\alpha^2\overline{a_2} = a_2 + \gamma a_1 + \gamma^2 + \beta\\
&\alpha^4\overline{a_4} = a_4 + \gamma a_3 + \delta a_1\\
&\alpha^6\overline{a_6} = a_6 + \gamma a_5 + \beta a_4 + (\delta + \beta\gamma)a_3\\
&\qquad + (\varepsilon + \beta^2\gamma)a_1 + \delta^2\\
&\alpha^8\overline{a_8} = a_8 + \delta a_5 + \beta^2 a_4 + (\varepsilon + \beta\delta)a_3\\
&\qquad + \beta^2\delta a_1 + \beta^4\\
&\alpha^{10}\overline{a_{10}} = a_{10} + \beta a_8 + \beta^2 a_6 + \varepsilon a_5 + \beta^3 a_4\\
&\qquad + \beta\varepsilon a_3 + \beta^4 a_2 + \beta^2\varepsilon a_1 + \varepsilon^2 + \beta^5
\end{aligned}$$

앞에서 (4.1)과 같은 형태의 곡선에 대한 교차상관과 부울함수의 Walsh-Hadamard에 대하여 알아보았다. 초타원곡선을 이용하여 부울함수를 생성하기 위하여 F_{2^n}위에서 다음과 같이 정의되는 종수 2인 초타원곡선을 분류하면 성질 4.6이 성립한다.

$$\begin{aligned}
&y^2 + a_5 y\\
&= x^5 + a_2 x^4 + a_4 x^3 + a_6 x^2 + a_8 x + a_{10}\\
&(a_5 \neq 0).
\end{aligned}$$

성질 4.6 E_1과 E_2를 F_{2^n}위에서 다음과 같이 정의되는 종수 2인 초타원곡선이라 하자.

$$\begin{aligned}
E_1 :\ & y^2 + a_5 y\\
&= x^5 + a_2 x^4 + a_4 x^3 + a_6 x^2 + a_8 x + a_{10}\\
E_2 :\ & y^2 + \overline{a_5} y = x^5 + \overline{a_4} x^3 + \overline{a_8} x + \overline{a_{10}}
\end{aligned}$$

그러면 E_1과 E_2는 동형이다(단, $a_5 \neq 0$, $\overline{a_5} \neq 0$).

증명 다음과 같은 변수변환

$$(x, y) \rightarrow (\alpha^2 x + \beta,\ \alpha^5 y + \alpha^4\gamma x^2 + \alpha^2\delta x + \varepsilon)$$

단, $\beta = \gamma^2 + a_2$이고 $\delta^2 = \beta a_4 + \gamma a_5 + a_6$이 존재하여 E_1은 E_2로 변환된다. 따라서 E_1과 E_2는 동형이다

성질 4.6에 의해 $a_5 \neq 0$일 때, 종수 2인 초타원곡선

$$\begin{aligned}
&y^2 + a_5 y\\
&= x^5 + a_2 x^4 + a_4 x^3 + a_6 x^2 + a_8 x + a_{10}
\end{aligned}$$

은 종수 2인 초타원곡선

$$E :\ y^2 + a_5 y = x^5 + a_4 x^3 + a_8 x + a_{10}$$

으로 표현할 수 있다. 또한, E_1과 E_2는 F_{2^n}위에서의 다음과 같이 정의되는 동형인 종수 2인 초타원곡선이라고 가정하면

$$\begin{aligned}
E_1 :\ & y^2 + a_5 y = x^5 + a_4 x^3 + a_8 x + a_{10}\\
E_2 :\ & y^2 + \overline{a_5} y = x^5 + \overline{a_4} x^3 + \overline{a_8} x + \overline{a_{10}}\\
& (a_5 \neq 0,\ \overline{a_5} \neq 0).
\end{aligned}$$

변수변환 (4.3)에 의하여 E_1을 E_2로 변환할 수 있다. 즉, 다음 조건을 만족하는 $\alpha(\neq 0)$, β, γ, δ 그리고 ε이 F_{2^n}에서 존재한다.

$$\begin{aligned}
&\alpha^5\overline{a_5} = a_5\\
&\alpha^4\overline{a_4} = a_4\\
&0 = \gamma^2 + \beta\\
&0 = \gamma a_5 + \beta a_4 + \delta^2\\
&0 = \alpha^8\overline{a_8} + a_8 + \delta a_5 + \beta^2 a_4 + \beta^4\\
&0 = \alpha^{10}\overline{a_{10}} + a_{10} + \beta a_8 + \varepsilon a_5 + \beta^3 a_4 + \varepsilon^2 + \beta^5
\end{aligned}$$

제Ⅲ장에서 3차 다항식과 5차 다항식은 모두 2차 부울함수를 생성함을 설명하였다.

이제, n이 짝수일 때 다음과 같이 정의되는 종수 2인 초타원곡선을 분류하면, 성질 4.7과 같다.

$$y^2 + a_5 y = x^5 + a_8 x + a_{10}\ (a_5 \neq 0) \qquad (4.4)$$

성질 4.7[5] $n \equiv 2 \bmod 4$이면 F_{2^n}위에서 정의된 종수 2인 초타원곡선 (4.4)는 다음 다섯 가지 곡선 중에 꼭 하나와 동형이다.

(1) $y^2 + y = x^5$
(2) $y^2 + y = x^5 + x$
(3) $y^2 + y = x^5 + \lambda x$

(4) $y^2+y=x^5+x+\mu$
(5) $y^2+y=x^5+\lambda x+\lambda$
단, $\lambda,\mu\in F_4\backslash\{0,1\}$이다.

성질 4.8[5] $n\equiv 0 \bmod 4$이고 $\sqrt[5]{a_5}\in F_{2^n}$이라고 하면 F_{2^n}위에서 정의된 종수 2인 초타원곡선 (4.4)는 다음 세 곡선 중에 꼭 하나와 동형이다.

(1) $y^2+y=x^5$
(2) $y^2+y=x^5+\mu$
(3) $y^2+y=x^5+\lambda x$
단, $Tr(\mu)=1$이고 임의의 $\lambda\in F_{16}\backslash\{0\}$에 대하여 $Tr_{F_{16}}(\lambda)\neq 0$이다.

이제, n이 짝수일 때 (4.4)와 같이 표현되는 초타원곡선의 F_{2^n}-유리점의 개수에 대하여 살펴보자.

성질 4.9[6] $n\equiv 2 \bmod 4$이면

$$\#\{(x,y)\mid y^2+y=x^5\}=2^n\pm 2^{\frac{n}{2}+1}.$$

다음 결과는 350 MHz Pentium Pro processor에서 MS Visual C++(version 6.0) 컴파일러를 이용하여 직접 구한 값이다.

정리 4.10 $n\equiv 2 \bmod 4 (n\leq 14)$이면

(1) $\#\{(x,y)\mid y^2+y=x^5+x\}=2^n\pm 2^{\frac{n}{2}}$
(2) $\#\{(x,y)\mid y^2+y=x^5+\lambda x\}=2^n$
(3) $\#\{(x,y)\mid y^2+y=x^5+x+\mu\}=2^n\pm 2^{\frac{n}{2}}$
(4) $\#\{(x,y)\mid y^2+y=x^5+\lambda x+\lambda\}=2^n$
단, $\lambda,\mu\in F_4\backslash\{0,1\}$이다.

정리 4.11 $n\equiv 0 \bmod 4$ $(4<n\leq 12)$이면

(1) $\#\{(x,y)\mid y^2+y=x^5\}=2^n\pm 2^{\frac{n}{2}+2}$
(2) $\#\{(x,y)\mid y^2+y=x^5+\mu\}=2^n\pm 2^{\frac{n}{2}+2}$
(3) $\#\{(x,y)\mid y^2+y=x^5+\lambda x\}=2^n$
단, $Tr(\mu)=1$이고 임의의 $\lambda\in F_{16}\backslash\{0\}$에 대하여 $Tr_{F_{16}}(\lambda)\neq 0$이다.

지금부터 (4.1)에서의 b를 w라 하고, x의 계수 a_8을 v라고 하면 다음과 같은 정리가 성립한다.

정리 4.12 $F(x)=x^5+vx$는 F_{2^n}위의 다항식이고 $\sqrt[5]{a}\in F_{2^n}$라고 하자(단, $n\leq 14$). 또한, F_{2^n}의 임의의 원소 x와 w는 각각 기저와 쌍대기저에 의하여 표현되었다고 가정하면 다음이 성립한다.

(1) $n\equiv 2 \bmod 4$이면

$$W_{a\cdot F}(w)=\begin{cases}0 & : Tr_{F_4}(\frac{av+w}{\sqrt[5]{a}})\notin\{0,1\}\\ \pm 2^{\frac{n}{2}+1} & : Tr_{F_4}(\frac{av+w}{\sqrt[5]{a}})=0\\ \pm 2^{\frac{n}{2}} & : Tr_{F_4}(\frac{av+w}{\sqrt[5]{a}})=1\end{cases}$$

(2) $n\equiv 0 \bmod 4$이면

$$W_{a\cdot F}(w)=\begin{cases}0 & : Tr_{F_{16}}(\frac{av+w}{\sqrt[5]{a}})\neq 0\\ \pm 2^{\frac{n}{2}+2} & : Tr_{F_{16}}(\frac{av+w}{\sqrt[5]{a}})=0\end{cases}$$

증명 $\sqrt[5]{a}\in F_{2^n}$이고 F_{2^n}위의 초타원곡선 E를 $y^2+y=a(x^5+vx)+wx$이라고 하자. 그러면 E는 선형변환 $(x,y)\rightarrow(\frac{x}{\sqrt[5]{a}},y)$에 의하여 다음과 같이 정의되는 곡선 E_1과 동형이다.

$$E_1: y^2+y=x^5+(\frac{av+w}{\sqrt[5]{a}})x$$

따라서 초타원곡선의 F_{2^n}-유리점의 개수에 관한 정리들에 의하여 이 정리는 성립한다.

정리 4.12에서의 $\sqrt[5]{a}$를 유한체 F_{2^n}의 임의의 원소 b라고 하면 다음 정리를 유도할 수 있다.

정리 4.13 유한체 F_{2^n} $(n\leq 14)$위의 다항식을 $F(x)=x^5+vx$ 라고 하자. 그리고 유한체 F_{2^n}의 임의의 원소 x와 w를 각각 F_{2^n}의 기저와 쌍대기저로 표현되었다고 가정하자. 그러면 $Tr(b^{-5}F(x))$가 위수가 1인 균형상관면역함수일 필요충분조건은 다음과 같다.

(1) $n\equiv 2 \bmod 4$ 이면,
(i) $w=0$ 일 때, $Tr_{F_4}(vb^{-4})\neq 0$이다.
(ii) 쌍대기저의 임의의 원소 w에 대하여

$$Tr_{F_4}(vb^{-4})=0,\quad Tr_{F_4}(wb)\notin\{0,1\}$$

(2) $n \equiv 0 \bmod 4$ 이면,

(i) $w = 0$ 일 때, $Tr_{F_{16}}(vb^{-4}) \neq 0$이다.

(ii) 쌍대기저의 임의의 원소 w에 대하여

$$Tr_{F_{16}}(wb) \neq Tr_{F_{16}}(vb^{-4})$$

증명 정리 4.12에 의하여, $W_{b^{5}\cdot F}(w) = 0$일 필요충분조건은 $Tr_{F_q}(wb + vb^{-4}) \neq 0$이다. 여기에서, $q = 2^{(4,n)}$이다. 따라서 $Tr(b^{-5}F(x))$는 위수 1인 균형상관면역함수일 필요충분조건은 다음과 같다.

$$Tr_{F_q}(wb) \neq Tr_{F_q}(vb^{-4})$$

정리 4.13을 이용하여 좀더 쉽게 균형상관면역함수를 생성하는 방법에 대하여 살펴보자.

정리 4.14 양의 정수 $n(\leq 14)$이 $n \equiv 0 \bmod 4$이고 $f(x) = Tr(x^5 + vx)$이라고 하자. 그리고 유한체 F_{2^n}의 임의의 원소 x와 w를 각각 F_{2^n}의 기저와 쌍대기저로 표현되었다고 가정하자. 그러면 $Tr_{F_{16}}(v) = 1$인 임의의 $v \in F_{2^n}$에 대하여 f는 위수 1인 균형상관면역함수이다. 더욱이 이러한 v의 개수는 2^{n-4}이다.

증명 $B = \{\theta, \theta^2, \cdots, \theta^{2^{n-1}}\}$을 유한체 F_{2^n}의 정규기저라 할 때, $x = \sum_{i=0}^{n-1} x_i \theta^{2^i}$ ($x_i \in F_2$)이면

$$Tr_{F_{16}}(x) = \sum_{i=0}^{n-1} X_i \theta^{2^i}$$

이다. 단, $Tr_{F_{16}}(x) = x + x^{16} + \cdots + x^{16^{n/4-1}}$이므로

$$X_i = \begin{cases} x_0 + x_4 + \cdots + x_{n-4} & : i \equiv 0 \bmod 4 \\ x_1 + x_5 + \cdots + x_{n-3} & : i \equiv 1 \bmod 4 \\ x_2 + x_6 + \cdots + x_{n-2} & : i \equiv 2 \bmod 4 \\ x_3 + x_7 + \cdots + x_{n-1} & : i \equiv 3 \bmod 4 \end{cases}$$

이다. $1 = \sum_{i=0}^{n-1} \theta^{2^i}$이므로 $Tr_{F_{16}}(w) = 1$일 필요충분조건은

$$\begin{cases} w_0 + w_4 + \cdots + w_{n-4} = 1 & : i \equiv 0 \bmod 4 \\ w_1 + w_5 + \cdots + w_{n-3} = 1 & : i \equiv 1 \bmod 4 \\ w_2 + w_6 + \cdots + w_{n-2} = 1 & : i \equiv 2 \bmod 4 \\ w_3 + w_7 + \cdots + w_{n-1} = 1 & : i \equiv 3 \bmod 4 \end{cases}$$

이다. 단, $w = (w_0, w_1, \cdots, w_{n-1})$이다. 따라서 해밍무게가 0 또는 1인 임의의 벡터는 $Tr_{F_{16}}(w) \neq 1$이다. 그러므로 $Tr_{F_{16}}(v) = 1$인 임의의 $v \in F_{2^n}$에 대하여 f는 위수 1인 균형상관면역함수이고 $Tr_{F_{16}}(v) = 1$인 F_{2^n}의 원소는 2^{n-4}개이다.

정수 n이 홀수인 경우에는 정리 4.13과 같은 성질을 만족하는 F_{2^n}의 원소 b는 0뿐이므로 균형상관면역함수가 존재하지 않는다. 따라서 짝수 n에 대하여 정리 4.13을 이용하여 좀더 쉽게 균형상관면역함수를 생성하는 알고리즘을 살펴본다.

먼저, $n \equiv 2 \bmod 4$일 때의 균형상관면역함수 생성알고리즘은 알고리즘 A와 같다.

알고리즘 A

1. 유한체 F_{2^n}의 기저 B를 선택한다.
2. 기저 B의 쌍대기저 $\hat{B}$를 구한다.
3. 집합 S를 계산한다.
   $S = \{ b \in F_{2^n} \mid$ 임의의 $w \in \hat{B}$에 대하여 $Tr_{F_1}(wb) \notin \{0, 1\}\}$
4. 각각의 $b \in S$에 대하여
   $Tr_{F_1}(v_b b^{-4}) = 0$를 만족하는 v_b를 구한다.
5. $f(x) = Tr(b^{-5}(x^5 + v_b x))$를 계산한다.

유한체 F_{2^n}의 기저가 $\{\alpha^0, \alpha^1, \cdots, \alpha^{n-1}\}$라고 할 때 유한체 F_{2^n}의 원소 $\sum_{i=0}^{n-1} a_i \alpha^i$를 $(a_0 a_1 \cdots a_{n-1})$로 표현한다.

예 4.2 F_2위의 기약 다항식 $x^6 + x + 1$의 한 근을 α라 하고 $B = \{1, \alpha, \alpha^2, \cdots, \alpha^5\}$를 유한체 F_{2^6}의 기저라고 하자. 그러면 B의 쌍대기저는 $\hat{B} = \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, 1 + \alpha^5\}$이다. 알고리즘 A를 이용하면 16개의 위수1인 균형상관면역함수를 얻을 수 있다. 그 중 몇 개는 다음과 같다.

$b = (111111)$이고 $v = (000000)$이면

$$f(x_1, \cdots, x_6) = x_1 + x_2 + x_4 + x_6 + x_1x_2 + x_1x_4 + x_3x_4 + x_1x_5 + x_2x_5 + x_4x_5 + x_1x_6 + x_3x_6 + x_4x_6 + x_5x_6.$$

$b = (111111)$이고 $v = (000011)$이면

$$f(x_1,\cdots,x_6) = x_1+x_2+x_3+x_1x_2+x_4+x_1x_4 + x_3x_4+x_1x_5+x_2x_5+x_4x_5 + x_1x_6+x_3x_6+x_4x_6+x_5x_6.$$

$b=(111111)$이고 $v=(000101)$이면

$$f(x_1,\cdots,x_6) = x_1+x_3+x_4+x_5+x_1x_2+x_1x_4 + x_3x_4+x_1x_5+x_2x_5+x_4x_5 + x_1x_6+x_3x_6+x_4x_6+x_5x_6.$$

유한체 F_{2^6}에서는 알고리즘 A에 의하여 위수 2인 균형상관면역함수는 생성되지 않음을 확인할 수 있다.

한편, $n\equiv 0 \bmod 4$일 때의 균형상관면역함수를 생성알고리즘은 알고리즘 B와 같다.

알고리즘 B

1. 유한체 F_{2^n}의 기저 B를 선택한다.
2. 기저 B의 쌍대기저 $\hat{B}$를 구한다.
3. 집합 S를 계산한다.
   $S=\{\ b\in F_{2^n} \mid$ 임의의 $w\in \hat{B}$에 대하여 $Tr_{F_4}(wb)\neq 1\}$
4. 각각의 $b\in S$에 대하여 $Tr_{F_4}(v_b b^{-4})=0$ 를 만족하는 v_b를 구한다.
5. $f(x)=Tr(b^{-5}(x^5+v_b x))$를 계산한다.

알고리즘 B에 관한 예는 다음과 같다.

예 4.3 F_2위의 기약 다항식 $x^8+x^4+x^3+x+1$의 한 근을 α라 하고 유한체 F_{2^8}의 기저를 $B=\{1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7\}$라고 하자. 그러면 B의 쌍대기저는

$$\hat{B}=\{1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^6+\alpha^7,\ \alpha^4+\alpha^5+\alpha^7,\alpha^3+\alpha^4+\alpha^6,1+\alpha^2,\ \alpha+\alpha^2+\alpha^5+\alpha^7,1+\alpha+\alpha^4+\alpha^6,\ \alpha^2+\alpha^5+\alpha^7,\alpha+\alpha^4+\alpha^6\}.$$

알고리즘 B를 이용하면 2416개의 위수 1인 균형상관면역함수를 얻을 수 있다. 그 중 몇 개는 다음과 같다. 변수가 $x=(x_1,x_2,\cdots,x_8)$이라 할 때,

$b=(00000001)$이고 $v=(00001001)$이면

$$f(x) = x_3+x_4+x_6+x_7+x_2x_3+x_2x_4 + x_3x_5+x_4x_5+x_3x_6+x_5x_6+x_3x_7 + x_4x_7+x_6x_7+x_5x_8+x_6x_8+x_7x_8.$$

$b=(00000101)$이고 $v=(00010001)$이면

$$f(x) = x_1+x_2+x_4+x_5+x_7+x_8+x_2x_3 + x_2x_4+x_3x_5+x_4x_5+x_3x_6+x_4x_6 + x_5x_6+x_3x_7+x_4x_7+x_6x_7+x_5x_8 + x_6x_8+x_7x_8.$$

$b=(00001101)$이고 $v=(00001011)$이면

$$f(x) = x_1+x_4+x_7+x_8+x_2x_3+x_2x_4 + x_3x_5+x_4x_5+x_3x_6+x_4x_6 + x_5x_6+x_3x_7+x_4x_7+x_6x_7 + x_5x_8+x_6x_8+x_7x_8.$$

또한, 이 중에 432개는 위수 2인 균형상관면역함수이다. 그 중 몇 개는 다음과 같다.

$b=(00000101)$이고 $v=(00010001)$이면

$$f(x) = x_1+x_2+x_4+x_5+x_7+x_2x_3+x_2x_4 + x_3x_5+x_4x_5+x_3x_6+x_4x_6+x_5x_6 + x_3x_7+x_4x_7+x_6x_7+x_8+x_5x_8 + x_6x_8+x_7x_8.$$

$b=(00000101)$이고 $v=(00110001)$이면

$$f(x) = x_1+x_2+x_4+x_5+x_6+x_7+x_2x_3 + x_2x_4+x_3x_5+x_4x_5+x_3x_6+x_4x_6 + x_5x_6+x_3x_7+x_4x_7+x_6x_7+x_5x_8 + x_6x_8+x_7x_8.$$

$b=(00000101)$이고 $v=(01000011)$이면

$$f(x) = x_1+x_4+x_2x_3+x_2x_4+x_3x_5+x_4x_5 + x_3x_6+x_4x_6+x_5x_6+x_3x_7+x_4x_7 + x_6x_7+x_5x_8+x_6x_8+x_7x_8.$$

이제 위의 알고리즘에 의하여 구한 균형상관면역함수 $f(x)=Tr(b^{-5}F(x))$의 비선형치를 구하여 보자.

정리 4.15 유한체 $F_{2^n}(n\leq 14)$ 위의 다항식을 $F(x)=x^5+vx$ 라고 하고 유한체 F_{2^n}의 임의의 원소 x와 w를 각각 F_{2^n}의 기저와 쌍대기저로 재표현되었다고 가정하면, $f(x)=Tr(b^{-5}F(x))$ 의 비선형치는 다음과 같다.

(1) $n\equiv 2 \bmod 4$ 이면, $N_f=2^{n-1}-2^{\frac{n}{2}}$.

(2) $n\equiv 0 \bmod 4$ 이면, $N_f=2^{n-1}-2^{\frac{n}{2}+1}$.

증명 정리 4.12에 의하여

$$N_f=2^{n-1}-\frac{1}{2}\max_{w\in F_{2^n}}|W_f(w)|$$

$$= \begin{cases} 2^{n-1} - \frac{1}{2}\left|2^{\frac{n}{2}+1}\right| & n \equiv 2 \bmod 4 \\ 2^{n-1} - \frac{1}{2}\left|2^{\frac{n}{2}+2}\right| & n \equiv 0 \bmod 4 \end{cases}$$

$$= \begin{cases} 2^{n-1} - 2^{\frac{n}{2}} & n \equiv 2 \bmod 4 \\ 2^{n-1} - 2^{\frac{n}{2}+1} & n \equiv 0 \bmod 4 \end{cases}.$$

예 4.4 예 4.2에서 생성한 균형상관면역함수의 비선형치는 $N_f = 24$이고 예 4.3에서 생성한 균형상관면역함수의 비선형치는 $N_f = 96$이다.

V. 결 론

제Ⅳ장의 n이 $4 < n \leq 14$인 짝수인 경우에 상관면역위수가 1인 균형부울함수를 생성하는 알고리즘 A와 알고리즘 B를 제안하였고 이들 알고리즘에 의하여 F_{2^6}와 F_{2^8}에서의 균형상관면역함수를 생성한 예를 보였다. 우리의 알고리즘에 의하여 생성된 부울함수의 비선형치는 정리 4.15와 같다.

한편, F_{2^n}에서 정의되는 부울함수의 최대 비선형치는 $2^{n-1} - 2^{\frac{n}{2}-1}$으로 널리 알려져 있다. 또한, n이 짝수이고 $k+1 \leq \frac{n}{2} - 1$인 경우, F_{2^n}에서의 위수 k인 상관면역함수의 최대 비선형치는

$$2^{n-1} - 2^{\frac{n}{2}-1} - 2^{k+1}$$

임이 증명되었다.[13]

n 차원 벡터공간 위에서 위수가 1인 균형상관면역함수의 가능한 최대 비선형치와 이 연구에서 제안한 방법에 의하여 생성된 균형상관면역함수의 비선형치의 차이는

$$\begin{cases} 2^{\frac{n}{2}-1} - 4 & : n \equiv 2 \bmod 4 \\ 3 \cdot 2^{\frac{n}{2}-1} - 4 & : n \equiv 0 \bmod 4 \end{cases}$$

이다(단, $n \leq 14$).

이 결과에 의하면, $n = 6$인 경우에 생성된 상관면역위수 1인 균형부울함수는 가능한 최대 비선형치를 가짐을 알 수 있고, 작은 정수 n에 대하여 생성된 균형부울함수의 비선형치도 상당히 좋은 값임을 알 수 있다.

실제로 n의 값이 큰 경우에 F_{2^n}위에서 균형이고 상관면역위수가 큰 부울함수는 n의 값이 작은 경우의 상관면역 위수가 1이고 비선형치가 비교적 큰 균형부울함수들을 이용하여 생성하는 방법이 Seberry 등에 의하여 잘 알려져 있다. 이 연구에서 구한 비선형치가 높고 상관면역위수 1인 균형 부울함수는 Seberry 등의 방법에 의하여 암호학적으로 바람직한 큰 n에 대한 부울함수를 생성하는데 이용될 수 있다.

참 고 문 헌

[1] S. T. Chee, S. J. Lee and K. J. Kim, "semi-bent functions", *Proc. of Asiacrypt'94,* pp.107～118, Springer-Verlag, 1995.

[2] J. H. Cheon, "Nonlinear Vector Resilient Function", *Advances in Cryptology-CRYPTO 2001,* LNCS. Vol. 2139, Springer-Verlag, pp.458～469, 2001.

[3] J. H. Cheon and S. T. Chee, "Elliptic Curves and Resilient Functions", *ICISC* 2000, LNCS 2015, pp. 64～72, Springer-Verlag, 2001.

[4] J. H. Cheon and J. H. Silverman, "An algebraic approach to boolean functions". http://www.kias.re.kr/conf/schedule.htm.

[5] C. S. Choi and M. S. Rhee, Isomorphism classes of hyperelliptic curves of genus 2 over F_{2^n} for even n, To be appeared in J. of Applied Math and Computing Vol.13 Sept 2003.

[6] T. M. Cusick and P. Stanica, "Fast Evaluation, Weights and Nonlinearity of Rotation-Symmetric Functions", ttp://citeseer.nj.nec.com/cache/papers/cs/12704/http;zSzzSzsciences.aum.eduzSz~stanpanzSzrotsymm1.pdf/cusick00fast.pdf

[7] R. Lidl and H. Niederreiter, Finite fields, Encyclopedia of Math. and its application, Vol.20, Addison-Wesley, 1983.

[8] A. Menezes, Applications of Finite Fields, Kluwer Academic Publishers, 1993.

[9] A. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1997.

[10] A. Menezes, L. Encinas and J. Masque, "Isomorphism Classes of Genus 2 Hyperelliptic Curves over Finite Fields", http://www.cacr.math.uwaterloo.ca/~ajmeneze/research.html

[11] A. Menezes, Y. Wu, and R. Zuccherato, An elem-

entary introduction to hyperelliptic curves, Technical Report CORR-96-19, CACR, University of Waterloo, 1996.

[12] G. Menichetti, "Roots of affine polynomial", Annals of Discrete Mathematics, vol.30, pp.303~310, 1986.

[13] P. Sarkar and S. Maitra, "Nonlinearity bounds and constructions of resilient boolean functions", Advances in Cryptology-Crypto 2000, LNCS. Vol.1880, Springer-Verlag, pp.515~532, 2000.

[14] J. Seberry, X. M. Zhang and Y. Zheng, "Highly nonlinear balanced Boolean functions satisfying high degree propagation criterion", Technical Report No. 93-1, Department of Computer Science, The University of Wollongong, Australia, 1993.

[15] J. Seberry, X. M. Zhang and Y. Zheng, "On constructions and nonlinearity of correlation immune functions", Advances in Cryptology-Eurocrypt'93, LNCS. Vol.765, pp.181~199. Springer-Verlag, 1994.

[16] J. Seberry, X. M. Zhang and Y. Zheng, "Nonlinearity and Propagation Characteristics of Balanced Boolean Functions", Information and Computation 119(1): pp.1~13, 1995.

[17] T. Siegenthaler, "Correlation immunity of nonlinear combining functions for cryptographic applications", IEEE Trans. Information Theory, Vol.30, pp.776~780, 1984.

〈著者紹介〉

최 춘 수 (Chun-Soo Choi)
1994년 2월 : 단국대학교 수학과 졸업
1996년 2월 : 단국대학교 대학원 수학과 졸업 이학석사
2002년 8월 : 단국대학교 대학원 수학과 졸업 이학박사
<관심분야> 대수학, 암호이론

이 민 섭 (Min-Surp Rhee) 종신회원
1976년 2월 : 서울대학교 사범대학 수학과 이학사
1979년 2월 : 서강대학교 대학원 수학과 이학석사
1987년 5월 : University of Alabama 대학원 수학과 이학박사
1992년12월~1994년2월 : Queensland 공과대학교 ISRC방문교수(호주)
현재 : 단국대학교 첨단과학부 응용수학전공 교수 한국정보보호학회 부회장
<관심분야> 대수학, 암호이론, 정보보호교육