情報保護學會論文誌
第15卷 第6號, 2005. 12

선형 다항식의 역원의 maximal 대수적 차수

이 동 훈
국가보안기술연구소

Maximal Algebraic Degree of the Inverse of Linearized Polynomial

Dong Hoon Lee
National Security Research Institute

요 약

유한체에서 정의된 선형 다항식의 역원은 함수 1/x의 일반화로 볼 수 있으므로, 암호학적 응용에서 유용한 부울 함수를 설계하는 데 좋은 후보가 될 수 있다. 특히, Crypto 2001에서는 선형 다항식 및 선형 부호를 이용하여 큰 대수적 차수를 가지는 resilient 함수를 설계하는 방법이 제안되었다. 그러나 Crypto 2001에서 대수적 차수를 분석한 결과에 오류가 있었으며, 본 논문에서 정확한 대수적 차수를 제시한다.

ABSTRACT

The linearized polynomial can be regarded as a generalization of the identity function, so that the inverse of the linearized polynomial is a generalization of the inverse function. Since the inverse function has so many good cryptographic properties, the inverse of the linearized polynomial is also a candidate of good Boolean functions. In particular, a construction method of vector resilient functions with high algebraic degree was proposed at Crypto 2001. But the analysis about the algebraic degree of the inverse of the linearized polynomial. Hence we correct the inexact result and give the exact maximal algebraic degree.

Keywords : *Boolean function, Algebraic degree, Linearized polynomial*

Ⅰ. 서 론

부울 함수는 블록 암호, 스트림 암호, 해쉬 함수 등의 암호 프리미티브에서 가장 기본적인 요소로 사용되는 중요한 함수이다. 일반적으로 암호학적 응용에 사용되기 위해서는 부울 함수는 몇 가지 성질들을 만족해야 한다. 예를 들면, 균형성(balancedness), 높은 대수적 차수(algebraic degree), 높은 대수적 면역성(algebraic immunity), 높은 비선형성(non-linearity), 높은 상관 면역성(correlation immunity) 등을 들 수 있다. 그러나 부울 함수는 이 모든 성질을 다 좋게 만들 수는 없다. 그러므로 부울 함수를 사용하는 응용에 따라서, 특정 성질을 좋게 하고 나머지 성질들은 최적으로 하는 부울 함수를 설계하는 것이 일반적이다.

부울 함수를 설계하는 방법으로 유한체에서 정의된 다항식을 활용하는 것이 있다. 유한체에서 정의된 다항식은 정해진 기저에 대하여 각 성분 함수는 부울 함수로 볼 수 있으며, 따라서 다항식을 벡터 부울 함수로 볼 수 있다. 이러한 방법에 의하면, 유한체에서 간단한 연산일지라도 부울 함수로 표현하는 경우 매우 복잡한 모양으로 나타나게 된다. 예를

접수일 : 2005년 9월 26일 ; 채택일 : 2005년 12월 6일
† 주저자, ‡ 교신저자 : dlee@etri.re.kr

들면, 1/x의 경우 간단한 대수적 연산이지만, 이것의 부울 함수의 대수적 특성은 매우 우수하다. 그러나 단항식을 제외하고는 일반적인 다항식의 경우 벡터 부울 함수로서 대수적 성질이 거의 알려진 바가 없다.

Crypto 2001에서는 대수적 차수가 큰 벡터 resilient 함수를 설계하는 새로운 방법으로 선형 다항식과 선형 부호이론을 사용하는 방법이 제안되었다[1]. 선형 다항식은 identity 함수인 f(x)=x를 일반화한 함수라고 볼 수 있으므로 선형 다항식의 역원은 f(x)=1/x를 일반화한 것으로 볼 수 있다. f(x)=1/x는 대수적인 성질이 매우 우수하며, 간단한 구조를 가지고 있으므로 AES의 S-box를 비롯한 여러 응용에서 많이 활용되는 벡터 부울 함수이다. 따라서 선형 다항식의 역원은 좋은 성질을 가지는 벡터 부울 함수를 설계하는데 활용할 수 있는 좋은 후보가 될 수 있다.

그러나 [1]에서 제시한 선형 다항식의 역원의 대수적 차수에 대한 분석 결과에 오류가 있어, 새로 제안된 벡터 resilient 함수의 대수적 차수에도 오류가 포함되었다. 본 논문에서는 선형 다항식의 역원의 정확한 대수적 차수를 제시하고자 한다. 본 논문의 구성은 다음과 같다. 우선 II절에서는 기호와 선형 다항식에 대한 정의 및 이후 증명에 필요한 성질들을 보인다. III절에서 실제로 대수적 차수를 구하고 IV절에서 결론을 내린다.

II. 선형 다항식

1. 기호 및 정의

F_{2^n}을 원소의 개수가 2^n개인 유한체라고 하고, F_2^n을 F_2위의 n차원 벡터 공간이라고 하자. 만일 임의로 F_{2^n}의 기저를 $\{\xi_0, \xi_1, \cdots, \xi_{n-1}\}$로 고정하면 두 집합사이에는 다음과 같은 자연스러운 동형사상 ϕ가 존재한다.

$$x=\sum_{i=0}^{n-1} x_i\xi_i \in F_{2^n} \langle - \rangle (x_0,\cdots,x_{n-1}) \in F_2^n$$

따라서 기저를 고정한 경우 필요에 따라서 F_{2^n}의 원소와 F_2^n의 원소를 서로 혼용해서 사용해도 무방하다. 본문에서 미지수 x는 유한체의 원소 혹은 벡터로서 $x=(x_0,x_1,\cdots,x_{n-1})$를 혼용해서 사용하도록 한다.

유한체 F_{2^n}에서 정의된 다항식 $f(x)$를 각 성분으로 나타내면, 위의 동형사상 ϕ를 통해서 다음과 같이 n개의 부울 함수 $(f_0, f_1, \cdots, f_{n-1})$로 표현할 수 있다.

$$f(x) = (f_0(x_0,\cdots,x_{n-1}), f_1(x_0,\cdots,x_{n-1}),, \cdots, f_{n-1}(x_0,\cdots,x_{n-1}))$$

따라서 유한체에서 정의된 다항식을 벡터 부울 함수로 간주할 수 있다. 여기서, 각 성분 부울 함수 f_i를 대수적 정규 형식(algebraic normal form)으로 표현했을 때, 항 중에서 가장 많은 변수의 개수를 f_i의 대수적 차수라고 부른다. 그러면 벡터 부울 함수의 대수적 차수는 다음과 같이 정의한다.

[정의 1] $f(x)$를 위와 같이 유한체 F_{2^n}에서 정의된 다항식이라고 하자. 그러면 maximal 대수적 차수는 각 성분 부울 함수 f_i에 대한 대수적 차수의 최대값으로 정의한다. 또한 minimal 대수적 차수는 각 성분 부울 함수 f_i들의 임의의 선형결합에 대한 대수적 차수의 최소값으로 정의한다.

Maximal 대수적 차수의 경우, 다항식을 이용하여 좋은 성질을 가지는 부울 함수를 설계하고자 할 때 유용하다. Almost bent 함수에 대하여 maximal 대수적 차수에 대한 상한에 대한 결과가 발표된 적도 있다[2]. S-box와 같은 벡터 부울 함수를 암호에 활용하는 경우라면, 공격자는 주어진 벡터 부울 함수에서 가장 공격하기 쉬운 것을 찾기만 하면 되므로 minimal 대수적 차수가 의미 있을 수도 있다.

Crypto 2001에서 선형 다항식의 역원에 대한 대수적 차수는 maximal 대수적 차수를 다루었으며, 본 논문에서도 우선 maximal 대수적 차수만을 다루도록 한다. 즉, 다른 언급이 없는 경우 벡터 부울 함수의 대수적 차수는 maximal 대수적 차수를 의미하는 것으로 하겠다. 그러면 선형 다항식은 다음과 같이 정의한다.

[정의 2] 유한체 F_{2^n}에서 정의된 선형 다항식(linearized polynomial) $R(x)$는 각 항의 x에 대한 지수가 모두 2의 거듭제곱만이 있는 다항식을 말한다. 즉, $R(x)$는 다음과 같이 표현된다[3].

$$R(x)=\sum_{i=0}^{h} c_i x^{2^i}, \ (c_i \in F_{2^n})$$

여기서, 유한체 F_{2^n}의 표수가 2이므로 모든 x^{2^i}는 선형 변환이다. 따라서 $R(x)$ 또한 선형 변환임을 알

수 있다. 그리고 $R(x)$의 kernel을 K_R이라고 하자. 즉, $K_R=\{x\in F_{2^n}|R(x)=0\}$이라고 하자. 그러면, $R(x)$가 선형이므로 $x,y\in K_R$이면, $x+y\in K_R$이 되므로 K_R은 F_2^n의 벡터 부분 공간이 된다. 역으로 V가 F_2^n의 부분 공간이라고 할 때, 다음의 다항식 또한 선형 다항식이다[3].

$$R(x)=\sum_{\zeta\in V}(x+\zeta)$$

이와 같이 벡터 공간 V에 대응하는 선형 다항식을 $R_V(x)$라고 표기하도록 한다.

이후부터 V를 w-차원의 벡터 부분 공간이라고 하고, $R(x)=R_V(x)$라고 하자. 이 때, w=0인 경우 $V=\{0\}$이고, w>0인 경우 V의 기저를 $\{\xi_0,\xi_1,\cdots,\xi_{w-1}\}$으로 선택한다. 그리고 $V_0=\{0\}$이라고 하고, V의 부분 공간 V_i를 $\{\xi_0,\xi_1,\cdots,\xi_{i-1}\}$로 생성되는 벡터 공간이라고 하자. 또한 각각의 V_i에 대응하는 선형 다항식 $R_{V_i}(x)$를 편의상 $R_i(x)$로 표기하도록 한다. 그러면, 쉽게 $R_0(x)=x$와 $R_{i+1}(x)=R_i(x)R_i(x+\xi_i)$가 성립함을 알 수 있다.

선형 다항식 $R(x)$의 역원 $R(x)^{-1}$을 $R(x)^{2^n-2}$로 정의한다. 즉, $R(x)=0$이면, $R(x)^{-1}=0$으로 정의하고, $R(x)\neq 0$이면 $R(x)^{-1}=1/R(x)$으로 정의한다. Crypto 2001에서는 $R(x)^{-1}$의 대수적 차수에 대해서 다음의 결과를 제시하였다.

[Crypto 2001] V와 $R(x)$를 위에서 정의한 바와 같이 각각 w-차원의 벡터 부분 공간과 그에 대응하는 선형 다항식이라고 하자. 그러면, $R(x)^{-1}$의 대수적 차수는 n-w-1이다[1].

그러나 증명과정에서 오류가 포함되어 실제 대수적 차수는 경우에 따라서 n-w가 될 수 있음을 본 논문의 [정리 6]에서 밝힌다.

2. 선형 다항식의 성질

[보조정리 3] $V^{(n-1)}$을 F_2^n의 (n-1)-차원의 부분 공간이라고 하고, $R^{(n-1)}(x)$를 대응하는 선형 다항식이라고 하자. 이 때,

$$R^{(n-1)}(x)=x^{2^{n-1}}+a_{n-2}x^{2^{n-2}}+\cdots+a_1x^2+a_0x$$

라고 하면, 모든 계수 $a_i\in F_{2^n}$은 0이 아니고, 다음과 같은 관계식이 성립한다.

$$R^{(n-1)}(x)=\begin{cases}0 & \text{if } x\in V^{(n-1)}\\ 1/a_0 & \text{if } x\notin V^{(n-1)}\end{cases}$$

(증명) 만일 특정한 i에 대해서 $a_i=0$이라고 가정하자. 그러면, $x^{2^n}=x$이므로 $R^{(n-1)}(x)^{2^{n-1-i}}$은 x에 관한 차수가 기껏해야 2^{n-2}이하가 된다. 그런데, 방정식 $R^{(n-1)}(x)=0$의 해집합(kernel)은 $V^{(n-1)}$이므로 원소의 개수가 2^{n-1}개이므로, 마찬가지로 방정식 $R^{(n-1)}(x)^{2^{n-1-i}}=0$의 해의 개수도 2^{n-1}개가 되어 모순이 생긴다. 따라서 모든 a_i는 0이 될 수 없다.

한편, $a_0^2R^{(n-1)}(x)^2$과 $a_0R^{(n-1)}(x)$를 비교해 보자.

$$a_0^2R^{(n-1)}(x)^2=a_0^2a_{n-2}^2x^{2^{n-1}}+\cdots+a_0^4x^2+a_0^2x$$
$$a_0R^{(n-1)}(x)=a_0x^{2^{n-1}}+\cdots+a_0a_1x^2+a_0^2x$$

두 식을 비교하면, x에 관하여 차수가 모두 2^{n-1}이고 x항의 계수가 서로 같다. 그런데, 두 식의 해집합은 서로 같으므로 두 식은 정확하게 서로 같을 수밖에 없다. 따라서 $R^{(n-1)}(x)=a_0R^{(n-1)}(x)^2$이므로 보조정리의 관계식이 성립한다.

[보조정리 3]에 따라서, 우리는 (n-1)-차원의 벡터 부분 공간에 대응하는 선형 다항식의 경우, 적당한 상수를 곱함으로써, 선형 다항식의 함수값이 (유한체의 원소로서) 0 또는 1로 만들 수 있다. 이후로 (n-1)-차원의 벡터 부분 공간에 대응하는 선형 다항식은 이러한 형태임을 가정한다.

[보조정리 4] $0\le i<k\le n$에 대해서, $V_i^{(n-1)}$를 k개의 (n-1)-차원의 부분 공간이라고 하자. 단, $\cap_{i=0}^{k-1}V_i^{(n-1)}$가 (n-k)-차원의 부분 공간이 된다고 가정한다. 그리고, $R_i^{(n-1)}(x)$를 $V_i^{(n-1)}$에 대응하는 선형 다항식이라고 하자. 그러면, $\Pi_{i=0}^{k-1}R_i^{(n-1)}(x)$의 대수적 차수는 k이다.

(증명) $V_i^{(n-1)}$가 (n-1)-차원의 부분 공간이므로, $x=(x_0,x_1,\cdots,x_{n-1})\in V_i^{(n-1)}$이면, 적당한 선형 부울 함수 f_i에 대하여 $f_i(x_0,x_1,\cdots,x_{n-1})=0$을 만족한다. 한편, $R_i^{(n-1)}(x)$는 $V_i^{(n-1)}$에 대응하는 선형 다항식이므로 정의에 따라서, $x\in V_i^{(n-1)}$이면, $R_i^{(n-1)}(x)=0$이고 $x\notin V_i^{(n-1)}$이면, $R_i^{(n-1)}(x)=1\in F_{2^n}$이

다. 그러면 $1 \in F_{2^n}$이 기저에 대하여 $1=\sum_{i=0}^{n-1} a_i\xi_i$로 표현된다고 할 때, $R_i^{(n-1)}(x)$는 $R_i^{(n-1)}(x)=(a_0 f_i(x), a_1 f_i(x),\cdots,a_{n-1}f_i(x))$과 같이 표현할 수 있음을 쉽게 알 수 있다. $\Pi_{i=0}^{k-1}R_i^{(n-1)}(x)$의 값은 x가 $V_i^{(n-1)}$중의 어느 하나의 원소라면, $R_i^{(n-1)}(x)=0$이므로 전체의 값이 0이다. $\Pi_{i=0}^{k-1}R_i^{(n-1)}(x)=1$인 경우는 x가 모든 $V_i^{(n-1)}$의 원소가 아닌 경우이고, 다시 말하면 모든 $f_i(x)$에 대하여 $f_i(x)=1$인 경우이다. 따라서 다음이 성립한다.

$$\Pi_{i=0}^{k-1}R_i^{(n-1)}(x)$$
$$=(a_0\Pi_{i=0}^{k-1}f_i(x),\ \cdots,a_{n-1}\Pi_{i=0}^{k-1}f_i(x))$$

만일 f_i가 선형 독립이 아니면, 이들을 곱하여도 대수적 차수가 증가하지 않을 수 있다. 그러므로 모든 f_i들이 선형 독립임을 보이면 보조정리가 증명된다. 이들이 독립이 아니라고 가정하자. 그러면, 적당한 공집합이 아닌 부분 집합 $I\subset\{0,1,\cdots,k-1\}$가 존재하여 $\sum_{i\in I}f_i=0$을 만족한다. 예를 들어 $0\in I$라고 가정해 보자. 그러면, $I^*=I-\{0\}$라고 하면, $f_0=\sum_{i\in I}f_i$이므로 다음이 성립한다.

$$\cap_{i\in I}V_i^{(n-1)}\subset V_0^{(n-1)}$$

그러므로 $\cap_{i=0}^{k-1}V_i^{(n-1)}=\cap_{i=1}^{k-1}V_i^{(n-1)}$가 성립하게 된다. 그러나 $\cap_{i=1}^{k-1}V_i^{(n-1)}$은 차원이 적어도 n-(k-1) 이상이 되므로 가정에 모순이다. 따라서 모든 f_i는 선형 독립이므로 보조정리가 증명된다.

Ⅲ. 선형 다항식의 역원의 대수적 차수

V_i와 $R_i(x)$는 Ⅱ절에서 정의한 바와 같다고 하자. 그러면, 새로운 다항식 $S_i(x)$를 다음과 같이 정의한다.

$$S_0(x)=x^{-1}$$

$$S_i(x)=\sum_{\zeta\in V_i}(x+\zeta)^{-1}x \quad \text{for } 1\le i\le w$$

그러면, 정의에 의해서
$S_{i+1}(x)=S_i(x)+S_i(x+\xi_i)$
가 성립한다. 그러면 $S_i(x)$와 $R_i(x)$는 다음과 같은 관계가 있다.

[보조정리]

$$S_i(x)=\begin{cases}\sum_{\zeta\in V_i}\zeta^{-1} & \text{if } x\in V_i\\ (\Pi_{j=0}^{i-1}R_j(\xi_j))R_i(x)^{-1} & \text{if } x\notin V_i\end{cases}$$

(증명) 만일 $x\in V_i$라면, V_i는 벡터 공간이므로 V_i와 $x+V_i$는 서로 같은 집합이다. 따라서 $S_i(x)=S_i(0)$이 성립하므로 첫 번째 식은 모든 i에 대해서 참이다.

두 번째 식은 i에 대한 귀납법으로 증명하도록 한다. 우선 $i=1$이면, $V_1=\{0,\xi_0\}$이므로 정의에 의해서

$R_1(x)=x(x+\xi_0)$.
$S_1(x)=x^{-1}+(x+\xi_0)^{-1}$

이 성립한다. $x\notin V_1$이면, $x(x+\xi_0)\neq 0$이므로 $S_1(x)$를 다음과 같이 쓸 수 있다.

$$S_1(x)=\frac{\xi_0}{x(x+\xi_0)}$$

따라서 $i=1$일 때 위의 보조정리가 성립함을 보였다. 이제, 위의 보조정리가 $i\le k$일 때 성립함을 가정한다. $x\notin V_{k+1}$일 때, $S_i(x)$의 정의와 가정으로부터 다음을 얻을 수 있다.

$$S_{k+1}(x)$$
$$=S_k(x)+S_k(x+\xi_k)$$
$$=\Pi_{j=0}^{k-1}R_j(\xi_j)(R_k(x)^{-1}+R(x+\xi_k)^{-1})$$

$x\notin V_{k+1}$이므로 $(x+\xi_k)\notin V_{k+1}$이다. 따라서 $R_k(x)\neq 0$이고 $R_k(x+\xi_k)\neq 0$이다. 그러면, 위 식은 다음과 같이 바꿀 수 있다.

$$S_{k+1}(x)=\Pi_{j=0}^{k-1}R_j(\xi_j)\left(\frac{R_k(\xi_k)}{R_k(x)R_k(x+\xi_k)}\right)$$
$$=(\Pi_{j=0}^{k}R_j(\xi_j))R_{k+1}(x)^{-1}$$

따라서 $i=k+1$인 경우에도 성립한다. 그러므로 수학적 귀납법에 의하여 위 보조정리가 증명된다. 그러면, 위의 보조정리들을 이용하여 다음의 정리를 보인다.

[정리 6] $R(x)$는 w-차원의 벡터 부분 공간 V에

대응하는 선형 다항식이라고 하자. 그러면, $R(x)^{-1}$의 대수적 차수는 다음과 같다.

$$\deg(R(x)^{-1}) = \begin{cases} n-w-1 & \text{if } \sum_{\zeta\in V}\zeta^{-1}=0 \\ n-w & otherwise \end{cases}$$

(증명) $R(x)^{2^n-1}$을 생각해보자. 0이 아닌 모든 $x \in F_{2^n}$에 대하여 $x^{2^n-1}=1$이므로 다음이 성립한다.

$$R(x)^{2^n-1} = \begin{cases} 0 & \text{if } x \in V \\ 1 & otherwise \end{cases}$$

한편, V의 차원이 w이므로 적당한 (n-w)개의 (n-1)-차원의 벡터 부분 공간 $V_i^{(n-1)}$이 존재하여 $V=\cap_{i=1}^{n-w} V_i^{(n-1)}$이 성립한다. 이 때, $R_i^{(n-1)}(x)$를 $V_i^{(n-1)}$에 대응하는 선형 다항식이라고 하자. 그러면, 다음이 성립함을 쉽게 알 수 있다.

$$\Pi_{i=1}^{n-w}(R_i^{(n-1)}(x)+1) = \begin{cases} 1 & \text{if } x \in V \\ 0 & otherwise \end{cases}$$

따라서

$$R(x)^{2^n-1} = \Pi_{i=1}^{n-w}(R_i^{(n-1)}(x)+1)+1$$

이 성립한다. [보조정리 4]에 따라서 $R(x)^{2^n-1}$의 대수적 차수는 n-w가 된다. 그런데, $R(x)^{2^n-1}$은 $R(x)^{2^n}$과 $R(x)^{-1}$의 곱으로 표현할 수 있고, $R(x)^{2^n}$는 역시 선형이므로

$$\deg(R(x)^{-1}) \geq n-w-1$$

임을 알 수 있다.

$w=0$이면, $S_0(x)=x^{-1}$이고 따라서 대수적 차수는 n-1이므로 위 정리가 성립한다[4]. 지금부터 $w>0$이라고 가정한다. [보조정리 5]로부터 다음과 같은 식을 얻을 수 있다.

$$(\Pi_{j=0}^{w-1}R_j(\xi_j))R(x)^{-1} = \begin{cases} S_w(x)+\sum_{\zeta\in V}\zeta^{-1} & \text{if } x \in V \\ S_w(x) & otherwise \end{cases}$$

즉, 위의 식과 조합하면 다음과 같은 식을 얻을 수 있다.

$$(\Pi_{j=0}^{w-1}R_j(\xi))R(x)^{-1} = S_w(x)+(\sum_{\zeta\in V}\zeta^{-1})\Pi_{i=1}^{n-w}(R_i^{(n-1)}(x)+1)$$

따라서 $\sum_{\zeta\in V}\zeta^{-1}\neq 0$이면, [보조정리 4]에 의하여 $\deg(R(x)^{-1})=n-w$이다. $\sum_{\zeta\in V}\zeta^{-1}=0$이면, $R(x)^{-1}$의 대수적 차수는 $S_w(x)$의 대수적 차수와 같다. $S_i(x)$의 정의로부터,

$$S_{i+1}(x) = S_i(x)+S_i(x+\xi_i)$$

이므로 $\deg(S_{i+1}(x)) < \deg(S_i(x))$이다. 따라서 $\deg(S_w(x)) \leq \deg(S_0(x))-w = n-1-w$이다. 이미 앞에서 $R(x)^{-1}$의 대수적 차수가 $n-w-1$이상임을 보였으므로 정리가 증명된다.

이제 언제 $\sum_{\zeta\in V}\zeta^{-1}=0$의 조건을 만족하는지 살펴보자. $V^*=V-\{0\}$이라고 하자. 정의에 의하여 $0^{-1}=0$이므로 다음과 같이 다시 쓸 수 있다.

$$\sum_{\zeta\in V}\zeta^{-1} = \sum_{\zeta\in V^*}\zeta^{-1} = \frac{\sum_{\xi\in V^*}(\Pi_{\zeta\in V^*-\{\xi\}}\zeta)}{\Pi_{\zeta\in V^*}\zeta}$$

위 식의 분모는 V^*의 원소의 곱이고, 분자는 V^*에서 한 원소를 제외한 나머지의 곱을 모두 합한 것이므로 $R(x)$를 전개하였을 때, 각각 x와 x^2의 계수임을 알 수 있다. 따라서 $\sum_{\zeta\in V}\zeta^{-1}=0$이라는 조건과 $R(x)$의 전개에서 x^2의 계수가 0인 것과는 동치이다.

[예제 7] V를 (n-1)-차원의 벡터 부분 공간이라고 하고, $R(x)$를 이에 대응하는 선형 다항식이라고 하자. 그러면 [보조정리 4]에 따라서 $R(x)$의 모든 계수는 0이 아니므로 $\sum_{\zeta\in V}\zeta^{-1}\neq 0$이다. 따라서 [정리 6]에 따르면, $R(x)^{-1}$의 대수적 차수는 n-(n-1) = 1로 선형이다. 실제로 [보조정리 3]에 따르면, $R(x)^2=a_{n-2}R(x)$이므로 $R(x)$의 임의의 거듭제곱도 $R(x)$의 적당한 상수배가 된다. 즉, $R(x)^{-1}=R(x)^{2^n-2}$로부터 $R(x)^{-1}$는 $R(x)$의 적당한 상수배가 되므로 선형이다.

[예제 8] $n=6$이라고 하고, α를 $x^6+x+1=0x$의 근일 때, V_1과 V_2를 각각 $\{1\}$과 $1,\alpha^3+\alpha^2+\alpha$

$\alpha^4+\alpha^2+\alpha$로 생성되는 1-차원과 3-차원의 벡터 부분 공간이라고 하자. 그러면, 여기에 대응되는 선형 다항식을 다음과 같이 구할 수 있다.

$$R_0(x)=x$$
$$R_1(x)=R_0(x)R_0(x+1)=x^2+x$$
$$R_2(x)=R_1(x)R_1(x+\alpha^3+\alpha^2+\alpha)$$
$$=x^4+(\alpha^4+\alpha^3)x^2+(\alpha^4+\alpha^3+1)x$$
$$R_3(x)=R_2(x)R_2(x+\alpha^4+\alpha^2+\alpha)=x^8+x$$

V_1와 V_2에 대응하는 선형 다항식은 각각 $R_1(x)$와 $R_2(x)$이다. $R_1(x)$의 x^2의 계수는 1이지만, $R_2(x)$의 x^2의 계수가 0이므로 [정리 6]에 따르면, $\deg(R_1(x)^{-1})=6-1=5$이고, $\deg(R_2(x)^{-1})=6-3-1=2$이다. 실제로 $R_1(x)^{-1}$와 $R_2(x)^{-1}$는 다음과 같다.

$$R_1(x)^{-1}=x^{62}+x^{61}+x^{59}+x^{55}+x^{47}+$$
(low-degree terms)
$$R_2(x)^{-1}=x^{24}+x^{17}+x^{10}+x^3$$

Ⅳ. 결 론

부울 함수는 암호 프리미티브에서 가장 기본적인 요소로 좋은 부울 함수를 설계하는 것은 매우 중요한 문제이다. 그러나 모든 조건을 다 충족시킬 수 있는 부울 함수를 설계하는 것은 불가능하고, 응용에 따라서 적절한 부울 함수를 설계하는 것이 필요하다. 그러한 방법의 하나로 유한체에서 정의된 다항식을 활용하여 부울 함수를 설계하는 것이 있으며, 예로 Crypto 2001에서는 선형 다항식을 이용하여 대수적 차수가 큰 벡터 resilient 함수를 설계한 경우가 있었다. 그러나 여기서 선형 다항식의 역원에 대한 대수적 차수의 분석에 오류가 있어서 본 논문에서는 선형 다항식의 성질을 좀 더 명확히 하고 이것을 이용하여 선형 다항식의 역원에 대하여 대수적 차수를 구하였다.

여기서 제시한 선형 다항식의 성질 및 선형 다항식의 변형 등을 통해서 좋은 부울 함수를 설계하는데 활용될 수 있을 것이다. 또한 선형 다항식의 역원에 대한 minimal 대수적 차수와 대수적 면역성(algebraic immunity)에 대한 연구가 보완되면 좀 더 많은 암호 프리미티브에 활용될 수 있을 것이라고 기대한다.

참 고 문 헌

[1] J.H. Cheon, "Nonlinear Vector Resilient Functions", *Advances in Cryptology - Crypto 2001*, LNCS 2139, pp. 458-469, 2001.

[2] C. Carlet, P. Charpin and V. Zinoviev, "Codes, Bent Functions and Permutations Suitable for DES-like Cryptosystems", *Designs, Codes and Cryptography*, vol.15(2), pp. 125-156, 1998.

[3] R. Lidle and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

[4] K. Nyberg, "Differentially Uniform Mappings for Cryptography", *Advances in Cryptology - Eurocrypt'93*, LNCS 765, pp. 55-64, 1993.

〈著者紹介〉

이 동 훈 (Dong Hoon Lee) 정회원

1994년 2월 : 서울대학교 수학교육과 학사
1996년 2월 : 한국과학기술원 수학과 석사
2000년 2월 : 한국과학기술원 수학과 박사
2000년 2월 ~ 2002년 3월 : (주)퓨쳐시스템 선임 연구원
2002년 4월 ~ 현재 : 국가보안기술연구소 선임연구원
〈관심분야〉 응용 정수론, 암호론, 인터넷 보안