通信情報保護學會論文誌
第 6 卷 第 3 號, 1996. 9

상관면역 함수와 비선형치

성 수 학*, 지 성 택**, 이 상 진**, 김 광 조**

On the Correlation Immune Functions and their Nonlinearity

Soohak Sung*, Seongtaek Chee**,
Sangjin Lee**, Kwangjo Kim**

요 약

상관면역 함수는 스트림 암호의 여과함수, 비선형 결합 함수 뿐만 아니라 블럭 암호의 핵심 논리 설계에 많이 이용된다. 본 논문에서는 새로운 방식으로 상관면역 함수를 설계하는 방법을 제시한다. 본 고에서 제시하는 방법은 지금까지 알려진 다른 설계 방법에 비하여 간단할 뿐만 아니라, 균형성, 비선형치, 대수적 차수, 그리고 확산 특성을 명확히 밝힐 수 있다. 또한, 본 논문에서 제시한 방법에 의해서 생성되는 함수의 최대 비선형치와 상관면역도와의 관계를 규명한다.

Abstract

In this paper, we consider the relationship between the nonlinearity and correlation immunity of functions suggested in [1], [3]. For the analysis of such functions, we present a simple method of generating the same set of functions, which makes us possible to construct correlation immune functions with controllable correlation immunity and nonlinearity.

1. 서 론

암호학적으로 우수한 성질을 가지는 부울함수는 스트림 암호의 여과함수, 비선형 결합 함수 뿐만 아니라 블럭 암호에서도 핵심 비선형 논리를 설계하는데 많이 이용된다. 이러한 부울함수 중에서 특히 출력으로 부터 입력에 대한 정보가 노출되지 않는 상관면역 함수는

* 배재대학교 응용수학과
** 한국전자통신연구소

1984년 Siegenthaler[1]에 의해서 소개된 이후 새로운 설계 방법 및 이론이 많이 제시되었다[2,3,5,6]. 이렇듯 상관면역 함수가 활발히 연구된 이유 중의 하나는 지금까지 많은 암호시스템이 상관 공격에 의해서 해독되었기 때문이다.

상관면역 함수를 설계하는 Siegenthaler의 방법은 귀납적(recursive)인 방법으로 인하여 응용하는데 한계가 있으며, 부호이론을 이용하여 임의 차수의 상관면역 함수를 설계할 수 있는 Camion 등[1]의 방법은 다양한 형태의 함수를 설계하는데 어려움이 있다.

최근, Seberry 등[3]은 상관면역성과 다른 암호학적인 특성을 동시에 만족하는 부울함수 설계 방법을 제시하였다. 그들의 방법에 의하면 Camion 등의 방법에 의해서 생성된 부울함수를 모두 생성할 수 있으며, 특히 부울함수의 확산특성(propagation characteristic)을 명확히 할 수 있다. 그러나 그들은 상관면역 차수와 비선형치를 각기 독립적으로 취급하여 상관면역 함수 중 비선형치가 보다 높은 함수를 찾는 방법은 제시하지 않았으며, 비선형치를 계산하면서 정확한 값을 계산하지 않고 단지 하한값만 제시하였다.

본 논문에서는 Seberry 등의 설계방법을 변형하여, 비선형치가 우수한 상관면역 함수 설계 방법을 제안하고자 한다. 제안한 방법은 Seberry 등의 방법 보다 간단하기 때문에 제반 특성을 분석하기가 용이하며 생성도 쉽게 할 수 있다. 또한 생성된 상관면역 함수의 비선형치를 정확하게 계산할 수 있다는 장점 뿐만 아니라 균형성, 대수적 차수, 확산특성 등의 기본적인 특성도 모두 명확하게 밝힐 수 있고 특히, 비선형치와 상관면역도와의 관계도 밝힐 수 있다.

본 논문의 구성은 다음과 같다. 2절은 기본적인 용어에 대한 정의이며, 3절에서는 정의한 상관면역 함수에 대한 특성을 분석한다. 4절에서는 상관면역 함수 설계 방법을 소개하고, 구체적인 예를 제시한다. 5절에서는 제안된 방법으로 생성된 부울함수의 상관면역도와 비선형치 사이의 관계를 규명한다.

2. 기본적인 정의

n차원의 벡터공간 $\{0,1\}^n$ 상의 벡터를 $x = (x_1, \cdots, x_n)$, $y = (y_1, \cdots, y_n)$, $a = (a_1, \cdots, a_n)$, $b = (b_1, \cdots, b_n)$으로 쓰며, n개의 변수 $x_1, \cdots, x_n$을 갖는 부울함수를 $f(x_1, \cdots, x_n)$, $f(x)$, $f : \{0,1\}^n \rightarrow \{0,1\}$으로 쓰기로 한다. 또 두 벡터 $a = (a_1, \cdots, a_n)$, $b = (b_1, \cdots, b_n)$의 내적을 $a \cdot b$로 표시하며 $a \cdot b = a_1 b_1 \oplus \cdots \oplus a_n b_n$로 정의한다.

부울함수가 0과 1의 값을 가질 가능성이 같은, 즉 $\#\{x|f(x) = 0\} = \#\{x|f(x) = 1\}$인 함수를 균형(Balance)이라고 하며, $k(1 \le k \le n)$개의 변수 $x_{i_1}, \cdots, x_{i_k}(1 \le i_1 < \cdots < i_k \le n)$와 함수값이 독립일 때 f를 k차 상관면역(Correlation Immune)함수라고 한다. 또, 적당한 벡터 a에 대해 $f(x) \oplus f(x \oplus a)$가 균형일 때 f는 a에 대해서 PC(Propagation Criterion)를 만족한다고 한다. PC는 부울함수의 확산 정도가 얼마나 고르게 분포되는가를 나타내는 지표가 된다. 부울함수 $f(x)$를 대수적으로 정규화된 형태(Algebraic Normal Form)로 쓰면 다음과 같다.

$$\begin{aligned} f(x_1, \cdots, x_n) &= a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n \\ &\quad \oplus a_{12} x_1 x_2 \oplus \cdots \oplus a_{n-1,n} x_{n-1} x_n \\ &\quad \oplus a_{123} x_1 x_2 x_3 \oplus \cdots \oplus a_{n-2,n-1,n} x_{n-2} x_{n-1} x_n \\ &\quad \vdots \\ &\quad \oplus a_{12\cdots n} x_1 x_2 \cdots x_n. \end{aligned}$$

이때 계수가 1인 최대곱의 차수를 대수적 차수(Algebraic Degree)라고 하며 $deg(f)$로 표시한다. $deg(f) \le 1$인 부울함수, 즉 $f(x) = a_0$

$\oplus a_1x_1 \oplus \cdots \oplus a_nx_n$를 affine이라고 하며 특히 $a_0 = 0$일때 선형(Linear)이라고 한다. 두 부울함수 f와 g에 대해, 거리 $d(f, g)$는 $\#\{x|f(x) \neq g(x)\}$로 정의하며, 특히, f와 Affine 함수군과의 최소거리 즉, Affine 함수군 전체의 집합을 Λ라 할 때, $min_{\lambda\in\Lambda}d(f,\lambda)$를 f의 비선형치(Nonlinearity)라고 하며, N_f로 표시한다.

이제 부울함수의 균형성, 상관면역, 비선형치 정의가 Hadamard-Walsh 변환으로 정의될 수 있음을 살펴보자. Hadamard-Walsh 변환은 부울함수와 같은 정의역 상에서 정의되나 그 값은 실수값을 갖는 함수로 아래와 같이 정의한다.

■ **정의 2.1** 부울함수 f의 Hadamard-Walsh 변환을 $\hat{f}$로 표시하며 다음과 같이 정의한다.

$$\hat{f}(w) = \sum_x f(x)(-1)^{w\cdot x}.$$

균형함수에 대한 다음 동치 정의는 Hadamard-Walsh 변환의 정의로부터 바로 유도된다.

■ **정의 2.2** $\widehat{(-1)^f}(0) = 0$인 부울함수 f를 균형함수라고 한다. 여기서 $\widehat{(-1)^f}(x)$는 $1 - 2f(x) \in \{-1, 1\}$로 정의된 함수이다.

Hadamard-Walsh 변환을 이용하여 상관면역에 대한 동치 정의를 얻을 수 있다.

■ **정의 2.3** [6] Hamming 가중값이 1과 k사이인 임의의 벡터 a, 즉 $1 \leq wt(a) \leq k$에 대해서 $\widehat{(-1)^f}(a) = 0$인 함수 f를 k차 상관면역이라고 하며, k를 함수 f에 대한 상관면역도라 한다.

부울함수의 비선형치에 관한 정의도 아래와 같이 쉽게 Hadamard-Walsh 변환으로 쓸 수 있다.

■ **정의 2.4** f의 비선형치는 다음과 같이 정의한다.

$$N_f = 2^{n-1} - \frac{1}{2}\max_w|\widehat{(-1)^f}(w)|.$$

3. 상관면역 함수의 설계

여기서는 부울함수의 Hadamard Walsh 변환을 이용하여 균형, 비선형인 상관면역 함수의 설계방법을 제시한다. 또, 제시한 것 중 비선형치가 가장 우수한 것도 찾는다.

❖ **정리 3.1** 3개의 양수 $n, k, m(n \geq 4, 1 \leq k \leq n-3, 1 \leq m < n)$이 주어졌을 때, $\{0,1\}^m$ 상의 모든 벡터 y에 대해 Hamming 가중값이 $k+1$ 이상인 적당한 벡터 $A_y \in \{0,1\}^{n-m}$를 대응시키자.
또 임의의 벡터 $a \in \{0,1\}^{n-m}$에 대해 $t_a = \#\{y|A_y = a\}$, $t = \max_a t_a$라고 두자. 이때 부울함수 $f : \{0,1\}^n \to \{0,1\}$를 $f(y, x) = A_y \cdot x$ 로 정의한다. 단, $y = (y_1, \cdots, y_m) \in \{0,1\}^m$, $x = (x_1, \cdots, x_{n-m}) \in \{0,1\}^{n-m}$이다. 그러면 다음이 성립한다.

(i) f는 균형이다.

(ii) f는 k차 상관면역이다.

(iii) $N_f = 2^{n-1} - t2^{n-m-1}$이다.

(iv) 만일 적당한 $(1 \leq i \leq n-m)$에 대해 $\oplus_y A_y(i) = 1$이면 $deg(f) = m+1$이다.

(v) 만일 A_y들이 서로 다른 벡터(즉, $t = 1$)이면 f는 (β, α) (단, $\alpha \in \{0,1\}^{n-m}$, $0 \neq \beta \in \{0,1\}^m$)에 대해 PC를 만족한다.

[증 명]

(i) 정의 2.2에 의해서 $\widehat{(-1)^f}(0) = 0$임을 보이면 된다. $wt(A_y) \geq k+1$이므로 $A_y \neq 0$이다. 따라서 $\sum_x (-1)^{A_y \cdot x} = 0$이다. 그러므로

$$\widehat{(-1)^f}(0) = \sum_{y,x}(-1)^{f(y,x)} = \sum_{y,x}(-1)^{A_y \cdot x} = \sum_y \sum_x (-1)^{A_y \cdot x} = 0.$$

(ii) 정의 2.3에 의해서 Hamming 가중값이 1과 k 사이인 임의의 벡터 $(b, a) \in \{0,1\}^n$에 대해 $\widehat{(-1)^f}(b, a) = 0$임을 보이면 된다. 정의된 부울함수 f에 대해서 Hadamard Walsh 변환을 계산하면

$$\widehat{(-1)^f}(b,a) = \sum_{y,x}(-1)^{f(y,x)}(-1)^{(b,a)\cdot(y,x)} = \sum_{y,x}(-1)^{A_y \cdot x}(-1)^{b \cdot y \oplus a \cdot x} = \sum_y (-1)^{b \cdot y}\sum_x (-1)^{(A_y \oplus a)\cdot x} \quad (1)$$

이다. 만일 $1 \leq wt(b, a) \leq k$이면 $0 \leq wt(a) \leq k$이다. 그런데 $wt(A_y) \geq k+1$이므로 $a \oplus A_y \neq 0$이다. 따라서 $\sum_x (-1)^{(A_y \oplus a)\cdot x} = 0$이다. 그러므로 식 (1)에 의해서 $\widehat{(-1)^f}(b, a) = 0$이다.

(iii) 정의 2.4에 의해서 $\max_{b,a}|\widehat{(-1)^f}(b, a)| = t2^{n-m}$임을 보이면 된다. 식 (1)에 의해서

$$\widehat{(-1)^f}(b,a) = \sum_y (-1)^{b \cdot y}\sum_x (-1)^{(A_y \oplus a)\cdot x} = 2^{n-m}\sum_{\{y|A_y = a\}}(-1)^{b \cdot y} \quad (2)$$

이다. 따라서 $\max_{b,a}|\widehat{(-1)^f}(b, a)| \leq 2^{n-m}\max_a t_a = t2^{n-m}$이다. 한편 식 (2)에 $b = 0$을 대입하면

$$\widehat{(-1)^f}(0,a) = 2^{n-m}\#\{y|A_y = a\} = 2^{n-m}t_a$$

이므로 $\max_{b,a}|\widehat{(-1)^f}(b, a)| \geq \max_a|\widehat{(-1)^f}(0, a)| = 2^{n-m}\max_a t_a = t2^{n-m}$이다. 그러므로 $\max|\widehat{(-1)^f}(b, a)| = t2^{n-m}$이다.

(iv) $f(y, x) = A_y \cdot x$를 구체적으로 쓰면

$$f(y,x) = (y_1 \oplus 1)(y_2 \oplus 1)\cdots(y_m \oplus 1)A_0 \cdot x \oplus (y_1 \oplus 1)(y_2 \oplus 1)\cdots y_m A_1 \cdot x \oplus \vdots \oplus y_1 y_2 \cdots y_m A_{2^m-1} \cdot x$$

이다. 만일, $\oplus_y A_y(i) = 1$이면 위의 $f(y, x)$ 전개식에서 $y_1 y_2 \cdots y_m x_i$ 항은 소거되지 않는다. 따라서 $deg(f) = m + 1$이다.

(v) $f(y, x)$의 정의로 부터

$$\begin{aligned} &f(y,x) \oplus f((y,x) \oplus (\beta, \alpha)) \\ &= (A_y \cdot x) \oplus (A_{y \oplus \beta} \cdot (x \oplus \alpha)) \\ &= (A_y \cdot x) \oplus (A_{y \oplus \beta} \cdot x \oplus A_{y \oplus \beta} \cdot \alpha) \\ &= (A_y \oplus A_{y \oplus \beta}) \cdot x \oplus A_{y \oplus \beta} \cdot \alpha \end{aligned}$$

이다. 한편 A_y들이 서로 다른 벡터이므로 $\beta \neq 0$이면 $A_y \oplus A_{y \oplus \beta} \neq 0$이다. 따라서 (i)의 증명과 같은 방법으로 계산하면 $f(y, x) \oplus f((y, x) \oplus (\beta, \alpha))$는 균형이다. 즉, f는 $(\beta, \alpha)(\beta \neq 0)$에 대해 PC를 만족한다. □

Seberry 등[3]은 정리 3.1-(i)(ii)(iv),(v)를 다른 방법으로 증명하였으며, (iii)의 등식은 증명하지 않고 부등식 $N_f \geq 2^{n-1} - t2^{n-m-1}$을 증명하였다. 임의의 부울함수 $y : \{0,1)^n \rightarrow \{0,1\}$에 대하여 $f(y, x) = A_y \cdot x \oplus r(y)$로 정의해

도 정리 3.1-(i)(ii)(iv),(v)는 성립한다. 또한, 그들은 벡터 대신에 이것에 대응되는 부울함수 $y \cdot A_v$를 사용하여 정리 3.1보다 복잡하게 부울함수 f를 정의하였다.

아래의 정리는 정리 3.1과 같은 조건하에서 비선형치가 최대가 되는 조건을 찾는데 이용되는 것으로 본 논문에서 중요한 역할을 한다.

❖ **정리 3.2** 양의 정수 n, $k(n \geq 4,\ 1 \leq k \leq n-3)$가 주어졌을 때, 임의의 양의 정수 t에 대해

$$t\left\{\binom{l}{k+1}+\binom{l}{k+2}+\cdots+\binom{l}{l}\right\} \geq 2^{n-l}$$

을 만족하는 최소의 l을 l_t라고 하면 $2^{l_t} \leq t2^{l_t}$이다. 즉, $\min\{t2^{l_t} | t = 1, 2, \cdots\} = 2^{l_t}$이다.

정리 3.2를 증명하기 위해서 여러 개의 보조정리가 필요하다. 보조정리 3.1은 잘 알려진 결과이며 증명도 간단하므로 증명은 생략한다.

❖ **보조정리 3.1** 양의 정수 n, k에 대해 다음이 성립한다.

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

❖ **보조정리 3.2** 양의 정수 n, k에 대해 다음이 성립한다.

$$2\left\{\binom{n}{k+1}+\binom{n}{k+2}+\cdots+\binom{n}{n}\right\} \leq \binom{n+1}{k+1}+\binom{n+1}{k+2}+\cdots+\binom{n+1}{n+1}.$$

[증 명]

보조정리 3.1에 의해서

$$\begin{aligned}
&\binom{n+1}{k+1}+\binom{n+1}{k+2}+\cdots+\binom{n+1}{n+1} \\
&= \left\{\binom{n}{k+1}+\binom{n}{k}\right\} \\
&\quad + \left\{\binom{n}{k+2}+\binom{n}{k+1}\right\} + \cdots \\
&\quad + \left\{\binom{n}{n}+\binom{n}{n-1}\right\} + 1 \\
&= \left\{\binom{n}{k+1}+\binom{n}{k+2}+\cdots+\binom{n}{n}\right\} \\
&\quad + \left\{\binom{n}{k}+\binom{n}{k+1}+\cdots+\binom{n}{n-1}\right\} + 1 \\
&= 2\left\{\binom{n}{k+1}+\binom{n}{k+2}+\cdots+\binom{n}{n}\right\} \\
&\quad + \binom{n}{k}. \qquad \square
\end{aligned}$$

❖ **보조정리 3.3** 만일 $l \geq l_t$이면

$$t\left\{\binom{l}{k+1}+\binom{l}{k+2}+\cdots+\binom{l}{l}\right\} \geq 2^{n-l}$$

이다. 여기서 l_t는 정리 3.2에서 정의된 값이다.

[증 명]

l_t의 정의에 의해서

$$t\left\{\binom{l_t}{k+1}+\binom{l_t}{k+2}+\cdots+\binom{l_t}{l_t}\right\} \geq 2^{n-l_t}$$

이다. 그런데 $\geq$ 이므로

$$\begin{aligned}
&t\left\{\binom{l}{k+1}+\binom{l}{k+2}+\cdots+\binom{l}{l_t}+\cdots+\binom{l}{l}\right\} \\
&\geq t\left\{\binom{l_t}{k+1}+\binom{l_t}{k+2}+\cdots+\binom{l_t}{l_t}\right\} \\
&\geq 2^{n-l_t} \geq 2^{n-l}. \qquad \square
\end{aligned}$$

이제 위의 보조정리들을 이용하여 정리 3.2

를 증명해 보자.

[정리 3.2의 증명]

$t = 1$일 때는 $t2^{l_t} = 2^{l_1}$이므로, $t \geq 2$일 때 $t2^{l_t} \geq 2^{l_1}$임을 증명하면 된다. $t \geq 2$이면 $2^p \leq t < 2^{p+1}$인 $p(p \geq 1)$가 존재한다. 만일 $l_1 - p \leq l_t$이면

$$t2^{l_t} \geq t2^{l_1-p} \geq 2^p 2^{l_1-p} = 2^{l_1}$$

이다. 따라서 $l_1 - p \leq l_t$일 때는 증명이 가능하다. 반면에 다른 경우($l_t < l_1 - p$)는 일어나지 않는다. 이를 증명하기 위해 $l_t < l_1 - p$(즉, $l_t \leq l_1 - p - 1$)이라고 가정하여 모순점을 도출해 보자. $l_t \leq l_1 - p - 1$이면 보조정리 3.3에 의해서

$$t\left\{\binom{l_1-p-1}{k+1}+\binom{l_1-p-1}{k+2}+\cdots+\binom{l_1-p-1}{l_1-p-1}\right\} \geq 2^{n-(l_1-p-1)} \quad (3)$$

이다. 또, 보조정리 3.2에 의해서

$$t\left\{\binom{l_1-p-1}{k+1}+\binom{l_1-p-1}{k+2}+\cdots+\binom{l_1-p-1}{l_1-p-1}\right\}$$

$$\leq 2^{p+1}\left\{\binom{l_1-p-1}{k+1}+\binom{l_1-p-1}{k+2}+\cdots+\binom{l_1-p-1}{l_1-p-1}\right\}$$

$$\leq 2^{p}\left\{\binom{l_1-p-1}{k+1}+\binom{l_1-p-1}{k+2}+\cdots+\binom{l_1-p-1}{l_1-p-1}\right\}$$

이다. 보조정리 3.2를 위의 식에 계속 적용하면 다음 식을 얻을 수 있다.

$$t\left\{\binom{l_1-p-1}{k+1}+\binom{l_1-p-1}{k+2}+\cdots+\binom{l_1-p-1}{l_1-p-1}\right\}$$

$$\leq 2\left\{\binom{l_1-1}{k+1}+\binom{l_1-1}{k+2}+\cdots+\binom{l_1-1}{l_1-1}\right\}.$$

따라서 식 (3)에 의해서

$$2\left\{\binom{l_1-1}{k+1}+\binom{l_1-1}{k+2}+\cdots+\binom{l_1-1}{l_1-1}\right\} \geq 2^{n-(l_1-p-1)}.$$

이다. 그런데 $p \geq 1$이므로

$$\binom{l_1-1}{k+1}+\binom{l_1-1}{k+2}+\cdots+\binom{l_1-1}{l_1-1} \geq 2^{n-l_1+p} \geq 2^{n-(l_1-1)}$$

이다. 따라서 l_1의 정의에 의해서 $l_1 \leq l_1 - 1$이나 이 사실은 모순이다. 그러므로 $l_t \leq l_1 - p - 1$인 경우는 일어나지 않으므로 증명이 완성된다. □

아래의 정리는 본 논문의 핵심 결과이며 이것은 다음 절에 언급될 구성방법에 바로 이용된다.

❖ **정리 3.3** 부울함수 f가 정리 3.1과 같이 정의되었을 때, $m = n - l_1$, $t = 1$이면 f의 비선형치는 최대가 되며 $N_f = 2^{n-1} - 2^{l_1-1}$이다. 단, l_1은 정리 3.2에서 정의된 값이다.

[증 명]

벡터 A_y의 정의로 부터 t와 m은 아래의 관계식을 만족해야 한다.

$$t\left\{\binom{n-m}{k+1}+\binom{n-m}{k+2}+\cdots+\binom{n-m}{n-m}\right\} \geq 2^m. \quad (4)$$

식(4)에서 $n - m$을 l로 치환하면

$$t\left\{\binom{l}{k+1}+\binom{l}{k+2}+\cdots+\binom{l}{l}\right\} \geq 2^{n-l}. \quad (5)$$

이고, f의 비선형치는 정리 3.1-(iii)에 의해서 $N_f = 2^{n-1} - 2^{l-1}$이다. 따라서 각 $t(t = 1, 2, \cdots)$에 대해 비선형치가 최대인 것은 l이 식 (5)를 만족하는 최소값일 때다. 즉 $\max_m N_f = \max_l N_f = 2^{n-1} - t2^{l_1-1}$이다. 그러므로 정리 3.2에 의해서

$$\max_{m,t} N_f = \max_{l,t} N_f = 2^{n-1} - \min_t t2^{l_1-1}$$
$$= 2^{n-1} - 2^{l_1-1}$$

이다. □

4. 상관면역 함수 설계 방법

여기서는 정리 3.3을 이용하여 균형, 비선형인 상관면역 함수를 설계하는 방법을 제시한다. 이 방법은 균형이고 k차 상관면역 함수 중 비선형치가 우수한 것을 찾는데 그 목적이 있다.

[균형, $N_f = 2^{n-1} - 2^{l_1-1}$인 k차 상관면역 함수 설계 방법]

입력값 : ($n \geq 4$; 부울함수의 입력크기), $k(1 \leq k \leq n-3$; 상관면역 차수)

단계 1. $k+1 \leq l \leq n$에 대해

$$\binom{l}{k+1}+\binom{l}{k+2}+\cdots+\binom{l}{l}\} \geq 2^{n-l} \quad (6)$$

을 만족하는 최소값 l을찾는다. 이 값을 l_1이라고 두자.

단계 2. $\{0,1\}^h$상의 벡터 중 Hamming 가중값이 $k+1$ 이상인 것을 2^{n-l_1}개(모두 다른 벡터) 택하여 이를 $A_0, A_1, \cdots, A_{2^{n-l_1}-1}$로 표시한다. 즉, A_i는 서로 다른 $\{0,1\}^h$상의 벡터로 $wt(A_i) \geq k+1 (0 \leq i \leq 2^{n-l_1}-1)$이다.

단계 3. 부울함수 $f : \{0,1\}^n \rightarrow \{0,1\}$를 다음과 같이 정의한다.

$$f(y_1, \cdots, y_{n-l_1}, x_1, \cdots, x_{l_1}) = f(y, x)$$
$$= A_y \cdot x$$

위의 방법을 단계별로 검토해 보자. 첫째로 입력값에 대해 살펴보면 대수적 차수가 0인 부울함수는 상수함수이므로 균형이 아니며, 대수적 차수가 1차인 부울함수(즉, affine)는 비선형치 값이 0이다. 더군다나 부울함수 f의 상관면역 차수와 대수적 차수의 합은 n(n은 f의 입력 크기)이하이며[1], 특히 f가 균형이면 그 합은 $n-1$ 이하이다[4]. 즉, f가 균형일 때 k와 d를 각각 f의 상관면역 차수와 대수적 차수라고 하면 $k+d \leq n-1$이다. 따라서, 균형, 비선형이고 상관면역인 부울함수가 되기 위해서는 다음 관계식을 만족해야 한다.

$$k+d \leq n-1, \quad k \geq 1, \quad d \geq 2$$

위의 조건식을 만족하는 최소의 n은 4, k는 1과 $n-3$ 사이의 값($1 \leq k \leq n-1-d \leq n-3$)으로 이 값들이 입력값이다.

둘째로 단계 1이 가능한지 살펴보자. 입력값 n, k의 조건에 의해서 $k+2 \leq n-1$이다. 따라서

$$\binom{n-1}{k+1}+\binom{n-1}{k+2}+\cdots+\binom{n-1}{n-1}$$
$$\geq \binom{n-1}{k+1}+\binom{n-1}{k+2} \geq 2$$

이다. 그러므로 단계 1의 식 (6)을 만족하는 $l_1(l_1 \le n-1)$을 찾을 수 있다.

셋째로 단계 2가 가능한지 살펴보자. Hamming 가중값이 $k+1$ 이상인 $\{0,1\}^{l_1}$ 상의 벡터의 갯수는

$$\binom{l_1}{k+1}+\binom{l_1}{k+2}+\cdots+\binom{l_1}{l_1}$$

이며 이 합은 이미 단계 1에 의해서 2^{n-l_1} 이상을 보장해 준다. 따라서 Hamming 가중값이 $k+1$ 이상인 벡터를 2^{n-l_1}개 선택할 수 있다.

끝으로 단계 3에서 정의한 부울함수는 정리 3.3의 조건을 만족(정리 3.1의 조건도 만족: $t=1$, $m=n-l_1$)하므로 부울함수 f는 균형, k차 상관면역 그리고 비선형치는 $N_f = 2^{n-1} - 2^{l_1-1}$이다.

위 방법을 이용하여 구체적인 상관면역 함수의 예를 들어보자.

■ **예 4.1** 균형이고 1차 상관면역인 비선형 부울함수 : $\{0,1\}^7 \to \{0,1\}$를 찾아보자.

입력값 : $n=7$, $k=1$

단계 1 : $\binom{3}{2}+\binom{3}{3} \not\ge 2^{7-3}$이나

$\binom{4}{2}+\binom{4}{3}+\binom{4}{4} \ge 2^{7-4}$

이므로 $l_1=4$이다.

단계 2 : $\{0,1\}^4$ 상의 Hamming 가중값이 2 이상인 벡터를 8개 선택한다. 예를들어 8개의 그러한 벡터를 아래와 같이 택하자.

$A_0=(1,1,0,0)$ $A_1=(1,0,1,0)$
$A_2=(1,0,0,1)$ $A_3=(0,1,1,0)$
$A_4=(0,1,0,1)$ $A_5=(0,0,1,1)$
$A_6=(1,1,1,0)$ $A_7=(1,1,0,1)$

단계 3 : 부울함수 $f : \{0,1\}^7 \to \{0,1\}$를 다음과 같이 정의한다.

$$\begin{aligned}
&f(y_1,y_2,y_3,x_1,x_2,x_3,x_4)\\
&= f(y,x)\\
&= A_y \cdot x\\
&= (y_1\oplus 1)(y_2\oplus 1)(y_3\oplus 1)(x_1\oplus x_2)\\
&\quad \oplus (y_1\oplus 1)(y_2\oplus 1)y_3(x_1\oplus x_3)\\
&\quad \oplus (y_1\oplus 1)y_2(y_3\oplus 1)(x_1\oplus x_4)\\
&\quad \oplus (y_1\oplus 1)y_2y_3(x_2\oplus x_3)\\
&\quad \oplus y_1(y_2\oplus 1)(y_3\oplus 1)(x_2\oplus x_4)\\
&\quad \oplus y_1(y_2\oplus 1)y_3(x_3\oplus x_4)\\
&\quad \oplus y_1y_2(y_3\oplus 1)(x_1\oplus x_2\oplus x_3)\\
&\quad \oplus y_1y_2y_3(x_1\oplus x_2\oplus x_4)
\end{aligned}$$

위와 같이 정의한 부울함수 f는 균형, 1차 상관면역, $N_f = 2^6 - 2^3 = 56$이다. 또, $\oplus_y A_y(1)=1$, $\oplus_y A_y(2)=1$, $\oplus_y A_y(3)=0$, $\oplus_y A_y(4)=0$, 이므로 정리 3.1-(iv)에 의해서 $deg(f) = n - l_1 + 1 = 4$이다.

5. 비선형치와 상관면역도

본 절에서는 제시된 방법에 의해서 생성된 부울함수의 비선형치와 상관면역도와의 관계를 규명하기 위해, n에 따른 l_1의 하한 값을 계산하고 이로부터 상관면역도와 비선형치의 관계를 조사한다.

❖ **보조정리 5.1** 정수 n, k, l_1이 정리 3.2와 같이 정의되었을 때, $l_1 \ge [n/2]+1$이다.

[증 명]

l_1의 정의에 의해서

$$\binom{l_1}{k+1}+\binom{l_1}{k+2}+\cdots+\binom{l_1}{l_1} \geq 2^{n-l_1}$$

이다. 그러므로

$$2^{l_1}-2^{n-l_1} \geq \binom{l_1}{0}+\binom{l_1}{1}+\cdots+\binom{l_1}{k}. \tag{7}$$

식 (7)의 우변은 항상 0보다 크므로 $l_1 > n - l_1$이다. 결국 $l_1 \geq [n/2] + 1$이다. □

❖ **보조정리 5.2** 정수 n, x가 다음 식을 만족할 필요충분조건은 $x \leq \left[\frac{n+1}{2}\right]$이다.

$$\binom{n}{x+1}+\binom{n}{x+2}+\cdots+\binom{n}{n} \geq 2^{n-1}. \tag{8}$$

[증 명]

n이 짝수인 경우에는

$$\binom{n}{n/2}+\binom{n}{n/2+1}+\cdots+\binom{n}{n} > 2^{n-1},$$

$$\binom{n}{n/2+1}+\binom{n}{n/2+2}+\cdots+\binom{n}{n} < 2^{n-1}.$$

이므로 식 (8)이 성립할 조건은

$x \leq \left[\frac{n+1}{2}\right]$이다. 또, n이 홀수인 경우에는

$$\binom{n}{\frac{n+1}{2}}+\binom{n}{\frac{n+1}{2}+1}+\cdots+\binom{n}{n} > 2^{n-1}$$

이므로 식 (8)이 성립할조건은

$x \leq \left[\frac{n+1}{2}\right]$이다.

❖ **정리 5.1** 전 절에서 제안된 방법으로 구성할 수 있는 상관면역함수 f의 비선형치는 $N_f \leq 2^{n-1} - 2^{[n/2]}$이고, 등호가 성립하기 위한 k의 필요충분조건은 다음과 같다.

(i) n이 짝수일 때

$$\binom{n/2+1}{k+1}+\binom{n/2+1}{k+2}+\cdots+\binom{n/2+1}{n/2+1} \geq 2^{\frac{n}{2}-1}$$

(ii) n이 홀수일 때

$k \leq [n/4]$

[증 명]

보조정리 5.1에 의해서 $l_1 \geq [n/2] + 1$이므로,

$$N_f = 2^{n-1} - 2^{l_1-1} \leq 2^{n-1} - 2^{[n/2]}$$

이고, 등호는 $l_1 = [n/2] + 1$일 때 성립한다. 따라서 l_1의 정의에 의해

$$\binom{[n/2]+1}{k+1}+\binom{[n/2]+1}{k+2}+\cdots+\binom{[n/2]+1}{[n/2]+1} \geq 2^{n-([\frac{n}{2}]+1)}, \tag{9}$$

$$\binom{[n/2]}{k+1}+\binom{[n/2]}{k+2}+\cdots+\binom{[n/2]}{[n/2]} < 2^{n-[\frac{n}{2}]} \tag{10}$$

이 성립할 때, 등호가 성립한다. 한편 식 (10)은 항상 성립하므로 등호가 성립할 필요충분조건은 식 (9)가 성립하는 것이다. n이 홀수일 때는 식 (9)의 우편은 $2^{[n/2]}$이므로 보조정리 5.2에 의해서 식 (9)가 성립할 필요충분조건은

$$k+1 \leq \left[\frac{[n/2+1+1]}{2}\right] = \left[\frac{n-1}{4}\right] + 1 = [n/4] + 1$$

이다. 즉, $k \leq [n/4]$이다. □

위의 정리로부터 n이 홀수인 경우, 비선형치 $2^{n-1} - 2^{[n/2]}$를 갖고 상관면역도가 $[n/4]$인 부울함수를 설계할 수 있다.

이제 n이 짝수인 경우, 제안된 방법에 의해서 생성된 부울함수의 비선형치가 $2^{n-1} - 2^{[n/2]}$일 때 상관면역도 k의 상한을 구하자.

X가 $p = 1/2$인 이항확률분포를 갖는 확률변수일 때, 즉, $X \sim B(n, 1/2)$일 때,

$$P(X \geq x) = \sum_{k=x}^{n} \binom{n}{k} (1/2)^2$$

이다. 따라서, 정리 5.1 (i)의 식이 성립할 조건은

$$P(X \geq k+1) \geq 1/4,$$

즉, $P(X \geq k) \leq 3/4$이다. 이 때, $X \sim B(n/2 + 1, 1/2)$이고, $n/2 + 1$이 클 때[1], 다음이 성립한다.

$$P(X \leq k) \simeq P(Z \leq \frac{k - \frac{n/2+1}{2} + 1/2}{1/2\sqrt{n/2+1}}).$$

여기서, $Z \sim N(0, 1)$이다. 한편, $P(Z \leq 0.67) = 0.7486 \simeq 3/4$이므로

$$\frac{k - \frac{n/2+1}{2} + 1/2}{1/2\sqrt{n/2+1}} \leq 0.67.$$

즉, $k \leq n/4 + 0.335\sqrt{n/2 + 1}$이므로 다음을 얻는다.

$$k \leq [n/4 + 0.335\sqrt{n/2 + 1}]. \quad (11)$$

위의 결과로 부터 우리는 제안한 방식에 의해서 생성된 함수 중 최대 비선형치를 가지는 부울함수에 대한 상관면역의 범위를 구할 수 있다. 즉, n이 홀수인 경우에는 정리 5.1의 (ii)로 부터 상관면역도 k의 범위가 구해지며, n이 짝수인 경우에는 식 (11)로 부터 k의 범위를 구할 수 있다. 식 (11)는 근사식이므로 실제로는 더 큰 k값이 존재할 수 있지만 실험결과에 의하면 근사식은 매우 오차가 적다. 즉, n이 4 ~ 100인 짝수에 대하여 상관면역도 k값을 조사한 결과, $n = 38$인 경우를 제외하고[2] 식 (11)은 실제 범위와 같다.

6. 결 론

본 논문에서는 상관면역 함수 생성 방법을 제시하였다. 제안된 방식으로 상관면역함수를 설계하면 비선형치, 균형성, 대수적 차수, 확산특성 등 암호학적 특성을 명확하게 알 수 있고 특히, 상관면역도와 비선형치와의 상호 관계도 규명할 수 있으며 이에 대한 연구 결과는 국내외적으로 최초의 결과이다.

본 논문에서 제시된 방법에 의해서 생성된 상관면역 함수는 스트림 암호 설계시 여과함수나 비선형 결합 논리로 활용될 수 있으며 블럭 암호의 핵심 비선형 논리를 설계하는데 직접적으로 활용될 수 있다.

---

[1] 보통 $(\frac{n}{2} + 1)\frac{1}{2} > 5$, 즉, $\frac{n}{2} + 1 > 10$이라고 가정함.

[2] 이 경우, 식 (11)에 의하면 $k \leq 10$이지만, 실제로는 $k \leq 11$이다.

참 고 문 헌

[1] P. Camion, C. Carlet, P. Charpin and N. Spndrier, "*On correlation-immune functions*", Advances in Cryptology - CRYPTO '91, Springer-Verlag, pp. 87-100, 1992.

[2] W. Meier and O. Staffelbach, "*Nonlinearity criteria for cryptographic functions*", Advances in Cryptology - EUROCRYPT '89, Springer-Verlag, pp. 549-562, 1990.

[3] J. Seberry, X. M. Zhang and Y. Zheng, "*On constructions and nonlinearity of correlation immune functions*", Advances in Cryptology - EUROCRYPT '93, Springer-Verlag, pp. 181'199, 1994.

[4] T. Siegenthaler, "*Correlation immunity of non-linear combining functions for cryptographic applications*", IEEE Trans. on Inf. Th., **IT-30**, pp. 776-780, 1984.

[5] Y. Xian, "*Correlation-immunity of Boolean functions*", Electronics Letters **23**, pp. 1335-1336, 1987.

[6] G. Xiao and J. Massey, "*A spectral characterization of correlation-immune combining functions*", IEEE Trans. on Inf. Th., **IT-34**, pp. 569-571, 1988.

□ 著者紹介

성 수 학

1982년 경북대학교 수학과 학사
1985년 KAIST 응용수학과 석사
1988년 KAIST 응용수학과 박사
1988년 ~ 1991년 한국전자통신연구소 선임연구원
1991년 ~ 현재 배재대학교 응용수학과 조교수

지 성 택

1985년 서강대학교 이공대학 수학과(이학사)
1987년 서강대학교 대학원 수학과(이학석사)
1989년 ~ 현재 한국전자통신연구소 선임연구원

이 상 진

1987년 2월 고려대학교 이과대학 수학과(이학사)
1989년 2월 고려대학교 대학원 수학과(이학석사)
1994년 8월 고려대학교 대학원 수학과(이학박사)
1989년 10월 ~ 현재 한국전자통신연구소 선임연구원

김 광 조

1973년 ~ 1980년 연세대학교 전자공학과(학사)
1981년 ~ 1983년 연세대학교 대학원 전자공학과(석사)
1988년 ~ 1991년 요꼬하마 국립대학 대학원 전자정보공학과(박사)
현 한국전자통신연구소 실장,
본 학회 암호이론연구회 및 ISO/IEC JTC1 JSC-27 의장,
KIISC, IEICE, IEEE, IACR 각 회원

※ 주관심 분야 : 암호학 및 응용 분야, M/W 통신