通信情報保護學會論文誌
第7卷 第2號, 1997. 6

상관면역 함수의 계수

지 성 택*, 이 상 진*, 박 춘 식*, 성 수 학**

Enumerating Correlation Immune Functions

Seongtaek Chee, Sangjin Lee, Choon-Sik Park, Soo Hak Sung

요 약

상관면역 함수는 스트림 암호의 여과 함수, 비선형 결합 함수 뿐만 아니라 블럭 암호의 핵심 논리 설계에 많이 이용된다. 본 논문에서는 새로운 방식으로 상관면역 함수를 설계하는 방법을 제시한다. 이 방법을 이용하여 상관면역 함수 개수의 하한값과 상한값을 구하였다. 이 값은 Mitchell(1990), Yang-Guo(1995)가 구한 하한값과 상한값을 크게 개선한다.

Abstract

Correlation immune functions can be used not only as filter functions or nonlinear combiners in stream ciphers but also as a primitive logic in block cipher. In this paper, we suggest a construction method of correlation immune functions. Using this method, we find lower and upper bound of the cardinality of the correlation immune functions. This result improves Mitchell's result and Yang-Guo's result.

1. 서 론

암호학적으로 우수한 성질을 가지는 부울함수는 스트림 암호와 블럭 암호의 핵심 논리로 사용될 수 있다. 어떤 성질이 좋은 부울함수를 판단하는 기준이라면 그러한 성질을 만족하는 부울함수는 충분히 많아야 한다. 따라서 암호학적으로 중요한 성질을 만족하는 부울함수가 얼마나 되는지를 아는 것은 중요하며 본 논문에서는 이러한 연구를 하고자 한다. 중요한 대

* 한국전자통신연구원
* * 배재대학교 응용수학과

표적인 성질로는 균형성(Balance), 비선형성(Nonlinearity), Nondegeneracy, 상관면역(Correlation Immune), 대칭성(Symmetry)등이 있다. 언급된 성질 중 상관면역을 제외하고는 그러한 성질을 만족하는 부울함수의 개수는 이미 잘 알려져 있다[2], [7]. 상관면역 성질을 만족하는 부울함수의 개수는 정확히 모르나 하한값과 상한값은 알려져 있다[2], [7]. 상관면역 함수는 Siegenthaler[4]에 의해서 소개된 이후 많은 사람들이 연구하였다[1], [3], [5], [6], [8]. 이렇듯 상관면역 함수가 활발히 연구된 이유 중의 하나는 지금까지 많은 암호 시스템이 상관공격에 의해서 해독되었기 때문이다.

상관면역 함수를 설계하는 방법은 크게 두 가지로 나눌 수 있다. Siegenthaler[4]의 방법처럼 상관면역 함수를 이용하여 새로운 상관면역 함수를 설계하는 귀납적(recusive)인 방법과, Camion 등[1]의 방법처럼 직접 상관면역 함수를 설계하는 방법이 있다. Mitchell과 Yang-Guo는 상관면역 함수를 직접 설계하는 방법으로 상관면역 함수 개수의 하한값과 상한값을 구하였다. Yang-Guo는 Mitchell이 구한 하한값을 개선하였으나, 두 하한값의 수렴 속도가 같으므로 많은 개선은 아니다.

본 논문에서는 상관면역 함수를 설계하는 새로운 귀납적인 방법을 이용하여 Yang-Guo가 얻은 하한값을 크게 개선하고자 한다. 이 귀납적인 설계 방법을 이용하여 n(부울함수의 정의역의 차원)이 5이하일 때는 상관면역 함수를 모두 찾을 수 있다. 또 Yang-Guo가 구한 상한값도 개선하고자 한다.

2. 기본적인 정의

n 차원의 벡터공간 $\{0, 1\}^n$을 V_n으로 쓰기로 하며, V_n 상의 벡터를 $x=(x_1, \cdots, x_n)$로 쓰며 n 개의 변수를 갖는 부울함수를 $f(x)=f(x_1, \cdots, x_n)$ 또는 $f:V_n \rightarrow V_1$로 쓰며 f를 V_n 상의 부울함수라고 부르기로 한다. 또 두 벡터 $x=(x_1, \cdots, x_n)$, $y=(y_1, \cdots, y_n)$의 내적을 $x \cdot y$로 표시하며 $x \cdot y = x_1 y_1 \oplus \cdots \oplus x_n y_n$으로 정의한다. $x_i=1$이고 $x_j=0 (j \neq i)$인 V_n 상의 벡터를 e_i^n으로 나타내기로 한다. 즉

$$e_i^n=(0, \cdots, 0,1,0, \cdots, 0),\ 1 \leq i \leq n$$

V_n 상의 벡터 x의 Hamming 가중치를 $wt(x)$로 쓴다. 부울함수 f의 n개의 변수 중 $k(1 \leq k \leq n)$개의 변수 $x_{i_1}, \cdots, x_{i_k} (1 \leq i_1 < \cdots < i_k \leq n)$와 함수값이 독립일 때를 k차 상관면역이라고 한다. 본 논문에서는 상관면역의 정의를 Hadamard-Walsh 변환으로 된 것을 사용하고자 한다. 이러한 정의는 이미 잘 알려져 있으나 본 논문에서 많이 사용되므로 다시 언급하고자 한다.

Hadamard-Walsh 변환은 부울함수와 같은 정의역 상에서 정의되나 그 값은 실수값을 갖는 함수로 아래와 같이 정의한다.

정의 2.1 부울함수 f의 Hadamard-Walsh 변환을 $\widehat{(-1)^f}$로 표시하며 다음과 같이 정의한다.

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

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

정의 2.2 Hamming 가중치가 1과 k 사이인 임의 벡터 α, 즉 $1 \leq wt(\alpha) \leq k$에 대해 $\widehat{(-1)^f}(\alpha)=0$인 함수 f를 k차 상관면역이라고 한다. 특히 $k=1$일 때는 간단히 상관면역이라고 부른다.

3. 새로운 부울함수의 설계

이 절에서는 귀납적인 방법으로 부울함수를 설계하는 새로운 방법을 제시한다. 즉 두 개의

부울함수를 이용하여 새로운 부울함수를 설계한다.

f와 g가 V_n 상의 부울함수일 때 V_{n+1} 상의 새로운 부울함수 h를 다음과 같이 정의한다.

$$h(x_1, \cdots, x_n, x_{n+1})=\begin{cases} f(x_1, x_3, \cdots, x_{n+1}), & x_1=0,\ x_2=0, \\ g(x_1, x_3, \cdots, x_{n+1}), & x_1=0,\ x_2=1, \\ g(x_1, x_3, \cdots, x_{n+1}), & x_1=1,\ x_2=0, \\ f(x_1, x_3, \cdots, x_{n+1}), & x_1=1,\ x_2=1, \end{cases}$$

즉,

$$\begin{aligned} h(x_1, \cdots, x_n, x_{n+1})=&(1\oplus x_1)(1\oplus x_2)f(x_1, x_3, \cdots, x_{n+1}) \\ &\oplus(1\oplus x_1)x_2g(x_1, x_3, \cdots, x_{n+1}) \\ &\oplus x_1(1\oplus x_2)g(x_1, x_3, \cdots, x_{n+1}) \\ &\oplus x_1x_2f(x_1, x_3, \cdots, x_{n+1}) \end{aligned} \quad (1)$$

이다. 이 때 h를 $<f, g>$로 쓰기로 한다.

[주] $<f, g>$는 V_{n+1} 상의 모든 부울함수를 생성한다. 즉 V_n 상의 모든 부울함수의 집합 Ω_n이라고 표시하면 다음과 같다.

$$\Omega_{n+1}=\{<f, g> \mid f, g \in \Omega_n\}$$

V_n 상의 부울함수를 이용하여 V_{n+1} 상의 모든 부울함수를 생성할 수 있기 때문에 $n+1$이 작을 때 ($n+1\leq 5$) V_{n+1} 상의 모든 상관면역 함수를 쉽게 찾을 수 있다(4절, 5절 참조).

Hadamard-Walsh 변환의 정의에 의해서 $h=<f, g>$의 Hadamard-Walsh 변환은 다음과 같이 쓸 수 있다.

$$\begin{aligned} &\widehat{(-1)^h}(w_1, \cdots, w_n, w_{n+1}) \\ &=\sum_{x_1=0,\ x_2=0}(-1)^{f(x_1, x_3, \cdots, x_{n+1})}(-1)^{w_1x_1\oplus w_3x_3\oplus\cdots\oplus w_{n+1}x_{n+1}} \\ &\quad -\sum_{x_1=0,\ x_2=1}(-1)^{g(x_1, x_3, \cdots, x_{n+1})}(-1)^{w_1x_1\oplus w_2x_2\oplus\cdots\oplus w_{n+1}x_{n+1}} \\ &\quad +\sum_{x_1=1,\ x_2=0}(-1)^{g(x_1, x_3, \cdots, x_{n+1})}(-1)^{w_1x_1\oplus w_3x_3\oplus\cdots\oplus w_{n+1}x_{n+1}} \\ &\quad -\sum_{x_1=1,\ x_2=1}(-1)^{f(x_1, x_3, \cdots, x_{n+1})}(-1)^{w_1x_1\oplus w_2x_2\oplus\cdots\oplus w_{n+1}x_{n+1}} \end{aligned} \quad (2)$$

여기서 $\sum_{x_1=a_1,\ x_2=a_2}$은 $x_1=a_1$, $x_2=a_2$인 V_{n+1} 상의 모든 벡터 $(x_1, \cdots, x_n, x_{n+1})$에 대해서 더하는 것을 나타낸다. $(-1)h$의 Hadamard-Walsh 변환의 값은 위와 같이 복잡하게 쓸 수 밖에 없으나 w의 성분 중 w_2가 0일 때는 아주 간단히 쓸 수 있다.

보조정리 3.1 $h=<f, g>$가 (1)과 같이 정의되었을 때 $w_2=0$인 w에 대한 $(-1)^h$의 Hadamard-Walsh 변환값은 다음과 같다.

$$\begin{aligned} &\widehat{(-1)^h}(w_1, 0, w_3, \cdots, w_{n+1}) \\ &=\widehat{(-1)^f}(w_1, w_3, \cdots, w_{n+1})+\widehat{(-1)^g}(w_1, w_3, \cdots, w_{n+1}) \end{aligned}$$

(증명) $w_2=0$일 때 식 (2)의 첫째식과 넷째식을 합하면

$$\begin{aligned} &\sum_{x_1=0,\ x_2=0}(-1)^{f(x_1, x_3, \cdots, x_{n+1})}(-1)^{w_1x_1\oplus w_3x_3\oplus\cdots\oplus w_{n+1}x_{n+1}} \\ &+\sum_{x_1=1,\ x_2=1}(-1)^{f(x_1, x_3, \cdots, x_{n+1})}(-1)^{w_1x_1\oplus w_3x_3\oplus\cdots\oplus w_{n+1}x_{n+1}} \\ &=\widehat{(-1)^f}(w_1, w_3, \cdots, w_{n+1}) \end{aligned}$$

이며, 같은 방법으로 $w_2=0$일 때 식 (2)의 둘째식과 셋째식을 합하면

$$\widehat{(-1)^g}(w_1, w_3, \cdots, w_{n+1})$$

이다. 따라서 증명이 완성된다.

$h=<f, g>$가 상관면역인지 비상관면역인지를 판정하기 위해서는 가중치가 1인 벡터 $w\in V_{n+1}$에 대해서만 $(-1)^h$의 Hadamard-Walsh 변환값을 구하면 된다. 기호를 간단히 쓰기 위해서 이미 제2절에서 언급하였드시 e_i^n은 i번째 성분은 1이고 나머지 성분은 0인 V_n 상의 벡터를 나타낸다.

보조정리 3.2 $h=<f, g>$가 (1)과 같이 정의되었을 때 Hamming 가중치가 1인 V_{n+1} 상의 벡터 $e_i^{n+1}(1\leq i\leq n+1)$에 대해 $(-1)^h$의 Hadamard-Walsh 변환값은 다음과 같다.

$$\begin{aligned} &\widehat{(-1)^h}(e_1^{n+1})=\widehat{(-1)^f}(e_1^n)+\widehat{(-1)^g}(e_1^n) \\ &\widehat{(-1)^h}(e_2^{n+1})=\widehat{(-1)^f}(e_1^n)+\widehat{(-1)^g}(e_1^n) \\ &\widehat{(-1)^h}(e_i^{n+1})=\widehat{(-1)^f}(e_{i-1}^n)+\widehat{(-1)^g}(e_{i-1}^n),\ 3\leq i\leq n+1 \end{aligned}$$

(증명) $e_i^{n+1}(1\leq i\leq n+1)$중 e_2^{n+1}를 제외한 나

머지 것들은 둘째 성분이 0인 벡터이다. 따라서 첫째식과 셋째식은 보조정리 3.1에 의해서 바로 유도된다. 이젠 둘째 식을 증명해 보자. 식 (2)에 의해서

$$\widehat{(-1)}^{f}(0,1,0,\cdots,0)=\sum_{x_1=0,x_2=0}(-1)^{f(x_1,x_3,\cdots,x_{n+1})}-\sum_{x_1=0,x_2=1}(-1)^{g(x_1,x_3,\cdots,x_{n+1})}+\sum_{x_1=0,x_2=1}(-1)^{g(x_1,x_3,\cdots,x_{n+1})}-\sum_{x_1=0,x_2=1}(-1)^{f(x_1,x_3,\cdots,x_{n+1})} \quad (3)$$

이다. (3)의 오른쪽의 첫째식과 넷째식을 더하면

$$\sum_{x_1,x_3,\cdots,x_{n+1}}(-1)^{f(x_1,x_3,\cdots,x_{n+1})}(-1)^{x_1}=\widehat{(-1)}^{f}(e_1^n)$$

이고 둘째식과 셋째식을 더하면 $-\widehat{(-1)}^{g}(e_1^n)$이므로

$$\widehat{(-1)}h(0,1,0,\cdots,0)=\widehat{(-1)}^{f}(e_1^n)-\widehat{(-1)}^{g}(e_1^n)$$

이다. 따라서 증명이 완성된다.

4. 상관면역 함수 개수의 하한값

상관면역 함수 개수의 하한값을 구하기 위해서 $h=<f, g>$가 상관면역 함수가 될 조건을 찾아보자.

정리 4.1 f와 g가 V_n 상에서 정의된 상관면역 함수이면 $h=<f, g>$도 V_{n+1} 상의 상관면역 함수이다.

(증명) h가 상관면역 함수임을 증명하기 위해서 V_{n+1} 상의 Hamming 가중치가 1인 벡터 $e_i^{n+1}(1\le i\le n+1)$에 대해 $(-1)^h$의 Hadamard-Walsh 변환값이 0임을 증명하면 된다. 만일 f와 g가 V_n 상에서 정의된 상관면역 함수이면 $\widehat{(-1)}^{f}(e_i^n)=0(1\le i\le n)$, $\widehat{(-1)}^{g}(e_i^n)=0(1\le i\le n)$

이다. 따라서 보조정리 3.2에 의해서 $\widehat{(-1)}^{h}(e_i^{n+1})=0(1\le i\le n+1)$이다. 즉 $h=<f, g>$도 V_{n+1} 상의 상관면역 함수이다.

[주] 정리 4.1은 귀납적인 방법으로 새로운 상관면역 함수를 설계하는 방법이다.

V_n 상의 상관면역 함수의 전체 집합을 A_n이라고 두자. 즉

$$A_n=\{f: V_n \rightarrow V_1 | f\text{는 상관면역 함수}\}$$

또 집합 S의 원소의 개수를 |S| 또는 #S로 표시한다.

정리 4.2 $|A_{n+1}|\ge|A_n|^2$이다.

(증명) 함수 $F: A_n\times A_n \rightarrow A_{n+1}$를 다음과 같이 정의한다.

$$F(f, g)=<f, g>$$

그러면 정리 4.1에 의해서 F는 잘 정의된다. 또한 F는 1-1 함수이다. 왜냐하면, 만일 $F(f, g)=F(f', g')$(즉 $<f, g>=<f', g'>$)이면 〈 , 〉의 정의에 의해서 $f=f'$이고 $g=g'$이기 때문이다. F가 1-1 함수이므로

$$|A_{n+1}|\le|A_n\times A_n|=|A_n|^2$$

이다. 따라서 증명이 완성된다.

따름정리 4.1 $|A_n|\ge|A_{n-k}|^{2^k}$이다.

(증명) A_n을 정리 4.2에 적용하면 $|A_n|\ge|A_{n-1}|^2$이고, 다시 A_{n-1}을 정리 4.2에 적용하면

$$|A_n|\ge|A_{n-1}|^2\ge|A_{n-2}|^{2^2}$$

이다. 정리 4.2를 계속 적용하면(총 k번) $|A_n|\ge|A_{n-k}|^{2^k}$을 얻을 수 있다.

제 3절에서 제안된 부울함수의 설계 방법을 이용하여 n이 5이하일 때 V_n 상의 모든 상관면역 함수를 쉽게 찾을 수 있다(좀 더 구체적인 방법은 5절에서 다시 언급함).

$|A_1|=2$, $|A_2|=4$, $|A_3|=18$, $|A_4|=648$, $|A_5|=3,140,062$

정리 4.3 $n \geq 6$일때 $|A_n|(3,140,062)^{2^{n-5}}$이다.

(증명) $|A_5|$=3,140,062이므로 따름정리 4.1에서 k대신 n-5를 대입하면 바로 증명된다.

[주] Mitchell(1990)은 $|A_n|$의 하한값이 $2^{2^{n-1}}$, Yang-Guo(1995)는 $2^{2^{n-1}}+2^n-2n+2^{2^{n-4}}-2^{2^{n-3}}$을 얻었으나, 우리가 얻은 하한값은 $(3,140,062)^{2^{n-5}}$이므로 우리가 구한 것이 훨씬 좋다(하한값은 클수록 좋고 상한값은 작을수록 좋다). Yang-Guo의 하한값은 Mitchell의 하한값을 개선한 것이지만 수렴 속도는 둘 다 $2^{2^{n-1}}=(65,536)^{2^{n-5}}$이므로 크게 개선한 것으로는 볼 수 없다. 정리 4.3에서는 $|A_5|$를 이용하여 $|A_n|$의 하한값을 구하였으며, $|A_6|$, $|A_7|$,등을 계산할 수 있으면 $|A_n|$의 하한값은 계속 개선할 수 있다.

5. 상관면역 함수 개수의 상한값

상관면역 함수 개수의 상한값을 구하기 위해서 먼저 $h=<f, g>$가 비상관면역함수가 될 조건을 찾아보자.

V_n 상의 부울함수 전체의 집합을 Ω_n, V_n 상의 상관면역 함수의 전체 집합을 A_n으로 사용한 것을 기억하자. 비상관 면역함수 전체집합을 다음과 같이 n개로 나누자.

$$B_{ni}=\{f:V_n \rightarrow V_1 | \widehat{(-1)}^f(e_j^n)=0(1\leq j\leq i\text{-}1), \widehat{(-1)}^f(e_j^n)\neq 0\},\ 1\leq i\leq n$$

그러면 $B_{ni}(1\leq i\leq n)$는 서로 소인 집합 ($B_{ni} \cap B_{nj}=\phi$, $i\neq j$)이며 A_n과도 서로 소이다. 따라서 다음 보조정리를 얻을 수 있다.

보조정리 5.1 $A_n, B_{n1}, \cdots, B_{nn}$은 서로 소인 집합이며 $\Omega_n=A_n \cup B_{n1} \cup \cdots \cup B_{nn}$이다.

다음 보조정리는 $h=<f, g>$가 비상관 면역함수가 될 조건을 제시한 것이다.

보조정리 5.1 $h=<f, g>$를 (1)과 같이 정의하였을 때 다음이 성립한다.

(i) $f\in A_n$, $g\in B_{ni}$ 또는 $f\in B_{ni}$, $g\in A_n$이면 <f, g>는 비상관 면역함수이다.

(ii) $f\in B_{n1}$ 또는 $g\in B_{n1}$이면 $<f, g>$는 비상관 면역함수이다.

(iii) $f\in B_{ni}$, $g\in B_{nj}(i\neq j)$이면 $<f, g>$는 비상관 면역함수이다.

(증명) (i). $f\in A_n$이면 $\widehat{(-1)}^f(e_i^n)=0(1\leq i\leq n)$이다. 따라서 보조정리 3.2에 의해서 $f\in A_n$일때

$$g\in A_n \Leftrightarrow h\in A_{n+1}$$

이다. 같은 방법으로 $g\in A_n$일때

$$f\in A_n \Leftrightarrow h\in A_{n+1}$$

이다. 따라서 (i)이 증명된다.

(ii). 대우를 증명하기 위해서 $h=<f, g>$가 상관 면역이라고 가정하자. 즉 $\widehat{(-1)}^h(e_i^{n+1})=0(1\leq i\leq n+1)$이라고 하자. 그러면 보조정리 3.2에 의해서

$$\widehat{(-1)}^f(e_1^n)=0,\ \widehat{(-1)}^g(e_1^n)=0,\ \widehat{(-1)}^f(e_{i-1}^n)+\widehat{(-1)}^g(e_{i-1}^n)=0\ (3\leq i\leq n+1)$$

이므로 $f\notin B_{n1}$, $g\notin B_{n1}$이다. 따라서 (ii)의 대우가 증명된다.

(iii). $f\in B_{ni}$, $g\in B_{nj}(i\neq j)$이라고 가정하자. 편의상 $i<j$라고 하자($i>j$일 때도 같은 방법으로 증명가능). $i=j$일 때는 (ii)에 의해서 $<f, g>$는 비상관 면역함수이다. 이젠 $i\geq 2$라고 가정하자. 그러면 $i+1\geq 3$이므로 보조정리 3.2에 의해서

$$\widehat{(-1)}^h(e_{i+1}^{n+1})=\widehat{(-1)}^f(e_1^n)+\widehat{(-1)}^g(e_1^n)$$

이다. 그런데 $f\in B_{ni}$이므로 $\widehat{(-1)}^f(e_i^n)\neq 0$이다.

반면에 $j>i$이고 $g\in B_{nj}$이므로 $\widehat{(-1)}^g(e_i^n)=0$이다. 따라서 $\widehat{(-1)}^h(e_{i+1}^{n+1})\neq 0$이므로 $h=<f, g>$는 비상관 면역함수이다.

이젠 보조정리 5.1과 5.2를 이용하여 $|A_n|$의 상한값을 구하여 보자.

정리 5.1 $h=<f, g>$를 (1)과 같이 정의하였을 때 다음이 성립한다.

(i). $A_{n+1} \subseteq \{<f, g> | f, g \in A_n\} \cup \cup_{i=2}^{n} \{<f, g> | f, g \in B_{ni}\}$

(ii). $|A_{n+1}| \le |A_n|^2 + \sum_{i=2}^{n} |B_{ni}|^2$

(증명) (i). V_{n+1} 상의 모든 부울함수는 $<f, g>$로 나타낼 수 있다. 즉 $\Omega_{n+1}=\{<f, g> | f, g \in \Omega_n\}$이므로 $A_{n+1}=\{<f, g> | <f, g>$: 상관면역 함수$\}$이다. 보조정리 5.1에 의해서

$$\begin{aligned} A_{n+1} = & \{<f, g> : \text{상관면역 함수} | f, g \in A_n\} \qquad (4) \\ & \cup \cup_i \{<f, g> : \text{상관면역 함수} | f \in A_n, g \in B_{ni}\} \\ & \cup \cup_i \{<f, g> : \text{상관면역 함수} | f \in B_{ni}, g \in A_n\} \\ & \cup \cup_{i,j} \{<f, g> : \text{상관면역 함수} | f \in B_{ni}, g \in B_{nj}\} \end{aligned}$$

이다. 그런데 보조정리 5.2에 의해서 (4)의 오른쪽의 둘째식과 셋째식은 공집합이며, 넷째식에서도 i와 j가 1이거나 $i \neq j$이면 공집합이다. 따라서 (4)의 넷째식은

$$\cup^{n}_{i=2} \{<f, g> : \text{상관면역 함수} | f, g \in B_{ni}\}$$

이다. 또 (4)의 첫째식은 정리 4.1에 의해서

$$\{<f, g> | f, g \in A_n\}$$

이다. 따라서 (i)이 증명된다.

(ii). (i)의 오른쪽 집합들은 서로 소이므로

$$|A_{n+1}| \le \#\{<f, g> | f, g \in A_n\} + \sum_{i=2}^{n} \#\{<f, g> | f, g \in B_{ni}\}$$

이다. 또 $\#\{<f, g> | f, g \in A_n\} = |A_n|^2$, $\#\{<f, g> | f, g \in B_{ni}\} = |B_{ni}|^2$이므로 (ii)의 결과도 증명된다.

[주] 정리 5.1에서 $|A_{n+1}|$의 상한을 구하였지만 이 값은 정확히 모른다. 왜냐하면, $|B_{n2}|$을 제외한 나머지 것들은 알 수 없다.

이제 $|A_{n+1}|$의 상한의 상한을 구하자. A_n, B_{n3}, $\cdots$, B_{nn}의 합집합을 C_n, 즉 $C_n=A_{ni} \cup \cup_{i=3}^{n} B_{ni}$이면 C_n은 다음과 같음을 알 수 있다.

$$C_n = \{f: V_n \to V_1 | \widehat{(-1)}^f(e_1^n)=0, \ \widehat{(-1)}^f(e_2^n)=0\}$$

정리 5.2 $h=<f, g>$를 (1)과 같이 정의하였을 때 다음이 성립한다.

(i) $A_{n+1} \subseteq \{<f, g> | f, g \in B_{n2}\} \cup <f, g> | f, g \in C_n\}$

(ii) $|A_{n+1}| \le |B_{n2}|^2 + |C_n|^2$

(iii) $|A_{n+1}| \le \{\binom{2^n}{2^{n-1}} - \binom{2^{n-1}}{2^{n-2}}^2\}^2 + \binom{2^{n-1}}{2^{n-2}}^4$

(증명) (i). $C_n=A_n \cup \cup_{i=3}^{n} B_{ni}$이므로 정리 5.1 (i)로부터 바로 나온다.

(ii). B_{n2}와 C_n은 서로 소인 집합이므로 (i)의 결과로부터 바로 나온다.

(iii). $C_n=\{f: V_n \to V_1 | \widehat{(-1)}^f(e_1^n)=0, \ \widehat{(-1)}^f(e_2^n)=0\}$이므로

$$\begin{aligned} |C_n| &= \sum_{a,b} \binom{2^{n-2}}{a}^2 \binom{2^{n-2}}{b}^2 \\ &= \sum_{a} \binom{2^{n-2}}{a}^2 \sum_{b} \binom{2^{n-2}}{a}^2 \\ &= \binom{2^{n-1}}{2^{n-2}}^2 \end{aligned}$$

이다. 한편 C_n, B_{n1}, B_{n2}는 서로 소인 집합이며 $C_n \cup B_{n1} \cup B_{n2} = \Omega_n$이므로

$$|B_{n2}| = |\Omega_n| - |B_{n1}| - |C_n|$$

이다. $B_{n1} = \Omega_n - \{f: V_n \to V_1 | \widehat{(-1)}^f(e_1^n)=0\}$이므로

$$\begin{aligned} |B_{n1}| &= 2^{2^n} - \#\{f: V_n \to V_1 | \widehat{(-1)}^f(e_1^n)=0\} \\ &= 2^{2^n} - \sum_{a} \binom{2^{n-2}}{a}^2 \\ &= 2^{2^n} - \binom{2^n}{2^{n-1}} \end{aligned}$$

이다. 따라서

$$\begin{aligned} |B_{n2}| &= 2^{2^n} - \left\{ 2^{2^n} - \binom{2^n}{2^{n-1}} \right\} - \binom{2^{n-1}}{2^{n-2}}^2 \\ &= \binom{2^n}{2^{n-1}}^2 - \binom{2^{n-1}}{2^{n-2}}^2 \end{aligned}$$

이다. 고로

$$|B_{n2}|^2+|C_n|^2=\left\{\binom{2^n}{2^{n-1}}-\binom{2^{n-1}}{2^{n-2}}^2\right\}^2+\binom{2^{n-1}}{2^{n-2}}^4$$

이므로 (ii)의 결과로부터 (iii)은 증명된다.

[주] 정리 5.2 (i)의 방법으로 상관면역 함수를 빨리 구할 수 있다. 즉 V_{n+1} 상의 상관면역 함수를 구할 때 모든 $f, g \in W_n$에 대해서 $<f, g>$가 상관면역인지를 조사할 필요없이 $f, g \in B_{n2}$이거나 $f, g \in C_n$인 것에 한해서 $<f, g>$가 상관면역인지를 조사하면 된다.

[주] $a>b$이면 $(a-b)^2<a^2-b^2$이므로 정리 5.2 (iii)으로부터 $|A_n|<\binom{2^{n-1}}{2^{n-2}}^2$이다. 이 상한값은 바로 Yang-Guo(1995)가 구한 값이므로 우리의 상한값이 그들의 것보다 좋다: n이 16이하일 때 두개의 상한값을 비교해 보면 다음 표와 같다.

n	Yang-Guo	우리의 것
3	36	20
4	4,900	2,452
5	1.65×10^{8}	8.75×10^{7}
6	3.61×10^{17}	2.17×10^{17}
7	3.35×10^{36}	2.29×10^{36}
8	5.73×10^{74}	4.35×10^{74}
9	3.32×10^{151}	2.73×10^{151}
10	2.23×10^{305}	1.94×10^{305}
12	3.24×10^{1229}	3.02×10^{1229}
14	9.24×10^{4927}	8.92×10^{4927}
15	3.89×10^{19723}	3.82×10^{19723}

표에서 알 수 있드시 우리의 상한값이 Yang-Guo의 것보다 작으므로 우리가 구한 상한값이 좋다고 말할 수 있으나 두 상한값의 수렴 속도는 거의 비슷하다. 앞으로 본 연구팀은 $|A_n|$의 상한값을 좀 더 개선시키고자 한다.

6. 결 론

본 논문에서는 상관면역 함수의 설계 방법을 제시하였다. 제시된 방법으로 정의역의 차수가 5이하일 때는 상관면역 함수를 모두 구할 수 있다. 또 정의역의 차수가 클 경우에는 상관면역 함수 개수의 하한값과 상한값을 구하였다. 하한값은 Mitchell, Yang-Guo의 것보다 훨씬 좋으며 상한값도 Yang-Guo의 것보다 훨씬 좋지는 않지만 비교적 좋다. 본 연구팀은 앞으로 Yang-Guo의 상한값보다 훨씬 좋은 상한값을 얻기 위해 이 분야의 연구를 계속 할 예정이다.

참 고 문 헌

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

[2] C.J. Mitchell, "Enumerating boolean functions of cryptographic significance", J. Cryptology, 2, pp. 155-170, 1990.

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

[4] T. Siegenthaler, "Correlation immunity of nonlinear 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.

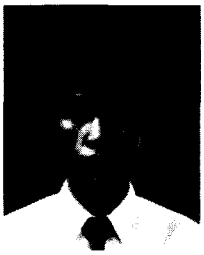
[6] G. Xiao and J. Massey, "A spectral

characterization of correlation-immune combining functions", IEEE Trans. on Inf. Th., IT-34, pp. 569-571, 1988.

[7] Y.X. Yang and B. Guo, "Further enumerating boolean functions of crtptographic significance", J. Cryptology, 8, pp. 115-122, 1995.

[8] 성수학, 지성택, 이상진, 김광조, "상관면역 함수와 비선형치", 한국통신정보보호학회 논문집 제6권 3호, pp. 11-22, 1996.

□ 著者紹介



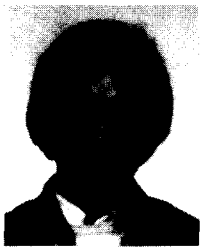
지 성 택

1985년 서강대학교 이공대학 수학과(이학사)
1987년 서강대학교 대학원 수학과(이학석사)
1989 ~ 현재 한국전자통신연구원 선임 연구원

이 상 진

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

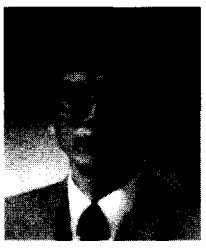
※ 주관심 분야 : 응용대수학 및 정수론, 암호론



박 춘 식

광운대학교 전자통신과 졸업(학사)
한양대학교 대학원 전자통신과 졸업(석사)
일본 동경공업대학 전기전자공학과 졸업(암호학 전공, 공학박사)
1989년 10월 ~ 1990년 9월 일본 동경공업대학 객원 연구원
1982년 ~ 현재 한국전자통신연구원 책임연구원

※ 주관심 분야 : 암호이론, 정보이론, 통신이론



성 수 학

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