通信情報保護學會論文誌
第 8 卷 第 3 號. 1998. 9

대역확산특성이 우수한 균형인 부울함수 설계

지 성택*, 이 상진*, 박 춘식*, 성 수학**

Constructing Balanced Boolean Functions with Good GAC

Seongtaek Chee*, Sangjin Lee*, Choonsik Park*, Soo-Hak Sung**

요 약

GAC(Global Avalanche Characteristics)은 부울함수가 전파특성 관점에서 얼마나 우수한지를 전체적인 관점에서 나타내는 특성으로 Zhang-Zheng(1995)에 의해서 제안되었다. GAC을 측정하는 기준으로는 σ_f와 Δ_f가 있으며, 두 기준값이 작을수록 부울함수는 보다 우수한 전파특성을 갖는다. Zhang-Zheng은 GAC이 우수한 균형인 부울함수를 설계하는 두 가지 방법을 제시하였으며, 균형인 부울함수 f의 대수적 차수가 3 이상일 때 Δ_f의 하한이 $2^{n/2+1}$이라고 추측하였다. 본 논문에서는 Zhang-Zheng의 방법보다 우수한 새로운 설계방법을 제시하며, 이를 이용하여 그들의 추측에 대한 반례를 제시한다.

Abstract

GAC(Global Avalanche Characteristics) was introduced by Zhang and Zheng as a measure of cryptographic strength of Boolean functions. Two indicators σ_f and Δ_f related to GAC are introduced. They conjectured that $\Delta_f \geq 2^{n/2+1}$ if f is balanced and $\deg(f) \geq 3$. In this paper, we give two constructing methods of balanced Boolean functions with good GAC. Also, we give a counter example to Zhang-Zheng's conjecture.

1. 서 론

암호에 사용되는 부울함수의 주요 요구조건으로는 균형성 (Balance), 비선형성 (Nonlinearity), 전파특성 (Propagation Characteristics), 대수적 차수 (Algebraic Degree), 상관면역(Correlation Immune) 등이 있다[2, 7]. 이 중에서 전파특성은 SAC(Strict

* 한국전자통신연구원
** 배재대학교 응용수학과

Avalanche Criterion)과 PC(Propagation Criterion)에 의해 조사될 수 있으나, 이들은 부울함수의 국부적(local)인 전파특성을 측정하는 것이다. 반면에 대역확산특성(GAC, Global Avalanche Characteristics)은 모든 벡터에 대한 전파특성을 측정하는 개념으로 Zhang-Zheng에 의해서 제안되었으며[6], 대역확산특성을 측정하는 기준으로는 σ_f와 Δ_f가 있다. 이 기준값이 작을수록 부울함수는 보다 우수한 대역확산특성을 지닌다고 말한다. Zhang-Zheng은 임의의 부울함수 f의 σ_f와 Δ_f에 대한 하한과 상한을 구하였으며, σ_f와 Δ_f의 하한에 대응되는 함수는 벤트(bent)함수임을 증명하였다.

암호논리로 사용될 수 있는 부울함수는 전파특성과 비선형성이 우수해야 하며 랜덤성을 보장하기 위해 균형이어야 한다. 따라서 부울함수 f가 균형일 때, σ_f와 Δ_f의 하한을 구하는 것과 하한값에 접근하는 대역확산특성을 갖는 부울함수를 설계하는 것은 중요한 일이며, 이런 연구는 일부 이루어졌다[4, 6, 8].

Zhang-Zheng은 GAC이 우수한 균형인 부울함수를 설계하는 두 개의 방법을 제시하였으며, 균형인 부울함수 f의 대수적 차수가 3이상일 때 Δ_f의 하한이 $2^{\frac{1}{2}(n-1)}$이라고 추측하였다. 본 논문에서는 Zhang-Zheng의 방법보다 우수한 새로운 설계방법을 제시하며, 그들의 추측에 대한 반례를 제시한다.

2. 기본적인 정의

n차원 벡터공간 Z_2^n상의 부울함수 f는 $Z_2^n \rightarrow Z_2$인 함수이다. 두 벡터 $x=(x_1, \cdots, x_n)$와 $y=(y_1, \cdots, x_n)$의 내적을 $x \cdot y$로 표시하며 $x \cdot y = x_1y_1 \oplus \cdots x_ny_n$으로 정의한다. 또 두 벡터 x와 y의 XOR를 $x \oplus y$로 표시하며 $x \oplus y = (x_1 \oplus y_1, \cdots, x_n \oplus y_n)$으로 정의한다.

부울함수 f가 0과 1의 값을 가질 가능성이 같은, 즉 $\#\{x|f(x)=0\} = \#\{x|\ f(x)=1\}$인 부울함수를 균형(balanced)이라고 한다.

Hamming 가중치가 1인 임의의 벡터 α에 대해 $f(x) \oplus f(x \oplus \alpha)$가 균형일 때 부울함수 f는 SAC(Strict Avalanche Criterion)을 만족한다고 정의한다[5]. 벡터 α에 대해 $f(x) \oplus f(x \oplus \alpha)$가 균형일때 부울함수 f는 α에 대해 PC (Propagation Criterion)를 만족한다고 정의한다[1, 3]. Hamming 가중치가 k이하인 모든 벡터에 대해 PC를 만족할 때 부울함수 f는 k차 PC를 만족한다고 정의한다. 1차 PC조건이 바로 SAC이며, n차 PC를 만족하는 부울함수가 바로 완전비선형(Perfect Nonlinear)함수이다. 완전비선형 함수를 벤트(bent)함수라고 부르기도 한다. 부울 함수의 비선형치는 보통 아핀함수와의 최소거리(Hamming 거리)로 정의된다. SAC과 PC는 어떤 특정한 벡터에 대한 전파특성을 측정하므로 부울함수에 대한 전반적인 전파특성을 나타내지는 못한다. 전반적인 전파특성을 측정할 수 있는 개념인 대역확산특성(GAC, Global Avalanche Characteristics)이 Zhang-Zhengcite[6]에 의해서 제안되었으며, 그들은 GAC를 측정하는 두 개의 기준을 제시하였다.

정의 1. 부울함수 $f: Z_2^n \rightarrow Z_2$에 대한 대역확산특성을 측정하는 두 개의 기준 σ_f와 Δ_f를 다음과 같이 정의한다.

$$\sigma_f = \sum_{\omega} \Delta_f^2(\omega)$$
$$\Delta_f = \max_{\omega \neq 0} |\Delta_f(\omega)|$$

여기서 $\Delta_f(\omega) = (-1)^f \otimes (-1)^f(\omega) = \Sigma_x (-1)^{f(x)} (-1)^{f(x \oplus \omega)}$는 $(-1)^f$의 자기상관함수(autocorrelation function)이며 편의상 $C[f]$로나타내기로 한다.

자기상관함수와 더불어 많이 사용되는 것은 Walsh-Hadamard 변환이다. 부울함수 f의 Walsh-Hadamard 변환은 $F[f](\omega) = \Sigma_x (-1)^{f(x) \oplus}$

$\omega \cdot x$로 정의되며 Z_2^n상에 정의된 f의 비선형치를 다음과 같이 표시할 수 있다.

$$N_f = 2^{n-1} - \frac{1}{2} \max_{\omega} |F[f](\omega)|.$$

일반적으로 σ_f나 Δ_f가 작을수록 대역확산특성이 우수하다고 말하며 Zhang-Zheng[6]은 σ_f와 Δ_f의 하한과 상한을 다음과 같이 구하였다.

$$2^{2n} \le \sigma_f \le 2^{3n},\ 0 \le \Delta_f \le 2^{2n}$$

σ_f가 하한을 가질 때, 즉 $\sigma_f = 2^{2n}$일 때 대응되는 부울함수는 벤트함수이며, Δ_f가 하한을 갖는 경우 역시 대응되는 부울함수는 벤트함수이다. 따라서 벤트함수는 대역확산특성이 가장 우수한 부울함수이다. 하지만 벤트함수는 균형이 아니다. 부울함수 f가 균형일 때 $\sigma_f \ge 2^{2n} + 2^{n+3}$이나[4], 이 하한값을 갖는 균형인 부울함수를 찾는 것은 쉽지 않다. 다음 절에서 대역확산특성이 우수한 균형인 부울함수의 설계방법을 제시하고자 한다.

3. GAC이 우수한 균형인 부울함수 설계

부울함수 $f: Z_2^n \rightarrow Z_2$가 균형이면서 대역확산특성이 우수한 것을 찾아보자. Z_2^n 상에서 정의된 균형인 부울함수의 개수는 $\binom{2^n}{2^{n-1}}$으로 부울함수의 입력 개수 n이 크면 균형인 부울함수는 너무 많아 대역확산특성이 가장 우수한 것을 찾는 것은 불가능하다. 반면에 n이 작을($n \le 5$)때는 대역확산특성이 가장 우수한 균형인 부울함수를 찾을 수 있다.

입력 개수가 1인 균형인 부울함수는 모두 affine 함수이므로 $\sigma_f = 2^{3n} = 8$이다. 입력 개수가 2인 균형인 부울함수도 모두 affine함수이므로 $\sigma_f = 2^{3n} = 64$이다. 입력 개수가 3인 균형인 부울함수의 개수는 $\binom{2^3}{2^2} = 70$이며, 이 중에서 σ_f의 최소값은 128이다. 최소값을 갖는 부울함수의 예는 다음과 같다.

$$f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3x_1$$

입력 개수가 4인 균형인 부울함수의 개수는 $\binom{2^4}{2^3} = 12{,}870$이며, 이 중에서 σ_f의 최소값은 640이다. 최소값을 갖는 부울함수의 예는 다음과 같다.

$$f(x_1, x_2, x_3, x_4) = 1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2x_4 \oplus x_1x_2x_4$$

입력 개수가 5인 균형인 부울함수의 개수는 $\binom{2^5}{2^4} = 601{,}080{,}390$이며, 이 중에서 σ_f의 최소값은 1,664이다. 최소값을 갖는 부울함수의 예는 다음과 같다.

$$\begin{aligned} f(x_1, x_2, x_3, x_4, x_5) = {} & x_1x_3 \oplus x_1x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_4x_5 \\ & \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_4x_5 \\ & \oplus x_1x_2x_3x_4 \oplus x_1x_2x_4x_5 \end{aligned}$$

입력 개수가 6 이상이면 균형인 부울함수는 너무 많아, 그 중에서 σ_f를 일일이 계산하여 최소값을 찾는것은 불가능하다.

이젠 $n(n = 2k+1)$이 7 이상인 홀수일 때 Z_2^{2k+1}상의 대역확산특성이 우수한 균형인 부울함수를 설계하는 방법을 살펴보자.

정리 1. $n = 2k+1$, $m(2 \le m < n)$은 짝수, f는 Z_2^m상의 벤트함수 그리고 g는 Z_2^{n-m}상의 균형인 부울함수일 때 Z_2^{2k+1} 상의 부울함수 h를 다음과 같이 정의하자.

$$h(y, x) = f(y) \oplus g(x)$$

그러면 다음이 성립한다.

(1) $F[h](b,a) = \pm 2^{\frac{m}{2}} \cdot F[g](a)$

(2) $C[h](b,a) = \begin{cases} 2^m \cdot C[g](a) & ,b=0 \\ 0 & ,b \neq 0 \end{cases}$

(3) h는 균형이다.

(4) $N_h = 2^{n-1} - 2^{n-1-\frac{m}{2}} + 2^{\frac{m}{2}} N_g$

(5) $\sigma_h = 2^{2m}\sigma_g$

(6) h가 PC를 만족하는 벡터 집합은 다음과 같다.

$$PC = \{(b,a) | \ b \neq 0\} \cup (0,a) | C[g](a) = 0\}$$

정리 1의 (1)과 (2)로부터 (3),(4),(5),(6)은 쉽게 증명할 수 있다. 정리 1의 상세한 증명은 생략하기로 한다. 정리 1의 설계방법에서 g를 Z_2^5상의 균형인 부울함수로 σ_g가 1,664인 것을 선택하면 대역확산특성이 우수한 h를 설계할 수 있다. 만일 g를 Z_2^7상의 균형인 부울함수로 σ_g가 최소인 것을 선택하면 대역확산특성이 보다 우수한 h를 설계할 수 있으나 현재로는 그런 g를 찾을 수 없다.

Z_2^{2k+1} 상의 균형인 부울함수로 σ_g가 1,664인 g를 이용하여 대역확산특성이 우수한 Z_2^{2k+1}상의 균형인 부울함수 h를 설계하는 예를 살펴보자.

예 1. g를 Z_2^5상의 균형인 부울함수로 $\sigma_g = 1{,}664$인 것을 선택하자.

$$\begin{aligned} g(x_1,x_2,x_3,x_4,x_5) = {} & x_1x_3 \oplus x_1x_5 \oplus x_2x_3 \oplus x_2x_4 \oplus x_4x_5 \\ & \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_4x_5 \\ & \oplus x_1x_2x_3x_4 \oplus x_1x_2x_4x_5 \end{aligned}$$

f를 다음과 같이 Z_2^{2k-4}상의 벤트함수로 정의하자.

$$f(y_1,y_2, \cdots, y_{2k-4}) = y_1y_{k-1} \oplus y_2y_k \oplus \cdots \oplus y_{k-2}y_{2k-4}$$

마지막으로 Z_2^{2k+1}상의 부울함수 h를 다음과 같이 설계하자.

$$\begin{aligned} & h(y_1, \cdots, y_{2k-4}, x_1, x_2, x_3, x_4, x_5) \\ & = y_1y_{k-1} \oplus y_2y_k \oplus \cdots \oplus y_{k-2}y_{2k-4} \oplus x_1x_3 \oplus x_1x_5 \oplus x_2x_3 \\ & \quad \oplus x_2x_4 \oplus x_4x_5 \oplus x_1x_2x_3 \oplus x_1x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_4x_5 \oplus \\ & \quad x_1x_2x_3x_4 \oplus x_1x_2x_4x_5 \end{aligned}$$

그러면 h는 균형이고 $\sigma_h = 6.5 \cdot 2^{4k}$이다. 한편 $N_g = 2^{5-1} - \frac{1}{2} \cdot 2^3$이므로 $N_h = 2^{2k} - 2^k$이다.

참고 1. Zhang-Zheng[6]은 $n = 2k+1$일 때 $\sigma_h = 8 \cdot 2^{4k}$인균형인 부울함수 h를 설계하였다. 따라서 위의 예에서 설계한 부울함수 h의 σ_h가 작으므로 본 논문에서 제시한 균형인 부울함수 h가 Zhang-Zheng이 제시한 함수보다 대역확산특성이 우수하다.

이제 $n(n=2k)$이 6이상인 짝수일 때 Z_2^{2k}상의 대역확산특성이 우수한 균형인 부울함수를 설계하는 방법을 살펴보자.

정리 2. $n=2k$, g는 Z_2^k상의 균형함수, f는 Z_2^{2k}상의 부울함수로 $f(y,x) = \phi(y) \cdot x$일 때 Z_2^{2k}상의 부울함수 h를 다음과 같이 정의하자.

$$h(y, x) = \begin{cases} g(x) & ,y=0 \\ f(y, x) & ,y \neq 0 \end{cases}$$

여기서 $\phi(y)$는 Z_2^k상의 $\phi(0)=0$인 치환(전단사 함수)이다. 그러면 다음이 성립한다.

(1) $F[h](b,a) = \begin{cases} 0 & ,a=0 \\ F[g](a) + (-1)^{b \cdot \phi^{-1}(a)} 2^k & ,a \neq 0 \end{cases}$

(2) $C[h](b,a)=\begin{cases} 2^{2k} & ,b=0,\ a=0 \\ C[g](a)-2^{k} & ,b=0,\ a\neq 0 \\ 2(-1)^{\phi(b)\cdot a}F[g](\phi(b)) & ,b\neq 0 \end{cases}$

(3) h는 균형이다.

(4) $N_h=2^{2k-1}-2^k+N_g$

(5) $\sigma_h=2^{4k}+5\cdot 2^{3k}+\sigma_g$

(6) h가 PC를 만족하는 벡터 집합은 다음과 같다.

$\{(b,a)\mid b\neq 0,\ F[g](\phi(b))=0\}\cup\{(0,a)\mid a\neq 0,\ C[g](a)=2^k\}$

정리 2의 (1)과 (2)로부터 (3),(4),(5)은 쉽게 증명할 수 있다. 정리2의 상세한 증명은 생략하기로 한다.

정리2의 설계 방법으로 k가 짝수이면 h를 설계한 방법과 같이 다시 g를 설계한다. 만일 k가 홀수이면 정리 1에서 h를 설계한 방법과 같이 다시 g를 설계한다. 이런 과정을 계속 사용하여 최종적으로 h를 선택하면 대역확산특성이 우수한 균형인 부울함수를 얻을 수 있다. 좀 더 구체적으로 살펴보자. n은 짝수이므로 $n=2^s u$(단, u는 홀수)로 쓸 수 있으며, $Z_2^{2^s u}$상에서 균형인 부울함수를 g_i를 설계하는 방법과 다음과 같다.

(i) $u=1$일때 : $i=1,\cdots,s-3$에 대해 $Z_2^{2^{s-i}}$상의 부울함수 g_i를 정리 2의 방법으로 설계하며, $Z_2^{2^2}$상의 부울함수 g_{s-2}는 $\sigma_{g_{s-2}}=640$인 균형인 부울함수로 설계한다.

(ii) $u\geq 3$인 홀수일때 : $i=1,\cdots,s-1$에 대해 $Z_2^{2^{s-i}u}$상의 부울함수 g_i를 정리 2의 방법으로 설계한다. Z_2^u상의 부울함수 g_i는 다시 $u=3$, $u=5$, $u\geq 7$인 경우로 나누어, $u=3$일 때는 $\sigma_{g_s}=128$인 균형인 부울함수로, $u\geq 7$일때는 정리 1의 방법으로 g_s를 설계한다.

예를 들어 $n=2^4$, $\phi(y)=y$그리고 $g_{s-2}(y_1,y_2,y_3,y_4)=1\oplus y_1y_2\oplus y_1y_3\oplus y_2y_3\oplus y_2y_4\oplus y_3y_2y_4$일 때 h를 설계하는 방법을 살펴보자. $n=2^4$이므로 $u=1$, $s=4$이다.

$$h(x_1,\cdots,x_{16})=\begin{cases} g_1(x_9,\cdots,x_{16}), & (x_1,\cdots,x_8)=0 \\ x_1x_9\oplus\cdots\oplus x_8x_{16}, & (x_1,\cdots,x_8)\neq 0 \end{cases}$$

그리고

$$g_1(x_9,\cdots,x_{16})=\begin{cases} g_2(x_9,\cdots,x_{16}), & (x_9,\cdots,x_{12})=0 \\ x_9x_{13}\oplus\cdots\oplus x_{12}x_{16}, & (x_9,\cdots,x_{12})\neq 0 \end{cases}$$

이다. 따라서 h의 구체적인 형태는 다음과 같다.

$$h(x_1,\cdots,x_{16})=\begin{cases} 1\oplus x_{13}x_{14}\oplus x_{13}x_{15} \\ \oplus x_{14}x_{15}\oplus x_{14}x_{16}\oplus x_{13}x_{14}x_{16}, (x_1,\cdots,x_{12})=0 \\ x_9x_{13}\oplus\cdots\oplus x_{12}x_{16}, (x_1,\cdots,x_8)=0, \\ (x_9,\cdots,x_{12})\neq 0 \\ x_1x_9\oplus\cdots\oplus x_8x_{16}, (x_1,\cdots,x_8)\neq 0 \end{cases}$$

이 경우 $\max_w|F[h](w)|=280$

$$\max_{w\neq 0}|C[h](q)|=280.$$

$\#PC=3,840$이다. 일반적으로 $n=2^s$일때 위의 방법으로 설계한 h의 특성을 살펴보자. 먼저 g_{s-2}의 특성을 살펴보자. $F[g_{s-2}]$는 다음과 같다.

$F[g_{s-2}](0)=0$ $\quad F[g_{s-2}](1)=0$

$F[g_{s-2}](2)=-4$ $\quad F[g_{s-2}](3)=-4$

$F[g_{s-2}](4)=-8$ $\quad F[g_{s-2}](5)=0$

$F[g_{s-2}](6)=-4$ $\quad F[g_{s-2}](7)=4$

$F[g_{s-2}](8)=-8$ $F[g_{s-2}](9)=0$
$F[g_{s-2}](10)=4$ $F[g_{s-2}](11)=-4$
$F[g_{s-2}](12)=0$ $F[g_{s-2}](13)=0$
$F[g_{s-2}](14)=4$ $F[g_{s-2}](15)=4$

그리고 $C[g_{s-2}]$는 다음과 같다.

$C[g_{s-2}](0)=16$ $C[g_{s-2}](1)=8$
$C[g_{s-2}](2)=0$ $C[g_{s-2}](3)=8$
$C[g_{s-2}](4)=0$ $C[g_{s-2}](5)=0$
$C[g_{s-2}](6)=0$ $C[g_{s-2}](7)=0$
$C[g_{s-2}](8)=0$ $C[g_{s-2}](9)=0$
$C[g_{s-2}](10)=0$ $C[g_{s-2}](11)=0$
$C[g_{s-2}](12)=-8$ $C[g_{s-2}](13)=-8$
$C[g_{s-2}](14)=-8$ $C[g_{s-2}](15)=-8$

g_1은 0벡터를 제외하고는 선형구조(Linear Structure)를 가지지 않으므로 정리 2(6)에 의해서

$$PC=\{(b,a)|b\neq 0,\ F[g_1](b)=0\}$$

이다. 정리 2(1)에 의해서

$$F[g_1](b_1,b_2)=\begin{cases}0, & b_2=0\\ F[g_2](b_2)+(-1)^{b_1\cdot b_2}2^{2^{s-2}}, & b_2\neq 0\end{cases}$$

이다. g_2도 0벡터를 제외하고는 선형구조를 가지지 않으므로 $F[g_1](b_1,b_2)=0$일 필요충분조건은 $b_2=0$이다. 따라서 $PC=\{(b_1,0,a_1,a_2)|b_1\neq 0\}$이며 $\#PC=2^{3\cdot 2^{s-2}}-2^{2^{s-1}}$이다.

이젠 h의 비선형치를 구해보자. 정리 2(4)에 의해서

$$\begin{aligned}N_h&=2^{2^s-1}-2^{2^{s-1}}+N_{g_1}\\&=2^{2^s-1}-2^{2^{s-1}}+2^{2^{s-1}-1}-2^{2^{s-2}}+N_{g_2}\\&=2^{2^s-1}-2^{2^{s-1}-1}-2^{2^{s-2}}+N_{g_2}\end{aligned}$$

이다. 이 방법을 계속 사용하면

$$N_h=2^{2^{s-1}}-2^{2^{s-1}-1}-\cdots-2^{2^3-1}-2^{2^2}+N_{g_{s-2}}$$

이다. 한편

$$N_{g_{s-2}}=2^{2^{2-1}}-\tfrac{1}{2}\max_w|F[g_{s-2}](w)|=2^{2^{2-1}}-4$$

이므로

$$N_h=2^{2^s-1}-2^{2^{s-1}-1}-\cdots-2^{2^3-1}-2^{2^2-1}-4$$

이다. 이젠 σ_h를 구해보자. 정리 2(5)에 의해서

$$\begin{aligned}\sigma_h&=2^{2\cdot 2^s}+5\cdot 2^{\frac{3}{2}\cdot 2^s}+\sigma_{g_1}\\&=2^{2\cdot 2^s}+2^{2\cdot 2^{s-1}}+5\cdot 2^{\frac{3}{2}\cdot 2^s}+5\cdot 2^{\frac{3}{2}\cdot 2^{s-1}}+\sigma_{g_2}\end{aligned}$$

이다. 이 방법을 계속 사용하면

$$\sigma_h=\{2^{2\cdot 2^s}+2^{2\cdot 2^{s-1}}+\cdots+2^{2\cdot 2^3}\}+\{5\cdot 2^{\frac{3}{2}\cdot 2^s}+5\cdot 2^{\frac{3}{2}\cdot 2^{s-1}}+\cdots+5\cdot 2^{\frac{3}{2}\cdot 2^3}\}+\sigma_{g_{s-2}}$$

이다. 한편 $\sigma_{g_{s-2}}=640$이므로

$$\sigma_h=\{2^{2^{s+1}}+2^{2^s}+\cdots+2^{2^4}\}+5\{2^{3\cdot 2^{s-1}}+2^{3\cdot 2^{s-2}}+\cdots+2^{3\cdot 2^2}\}+640$$

이다. 이젠 Δ_h를 구해보자. 정리 2(2)에 의해서

$$\begin{aligned}\Delta_h&=\max_{(b,a)\neq(0,0)}|C[h](b,a)|\\&=\max\{\max_{a\neq 0}|C[g_1](a)-2^{2^{s-1}}|,2\max_{b\neq 0}|F[g_1](b)|\}\end{aligned}$$

이며, 다시 정리 2(2)를 적용하면

$$\begin{aligned}&\max_{a\neq 0}|C[g_1](a)-2^{2^{s-1}}|\\&=\max\{\max_{a\neq 0}|C[g_2](a)-2^{2^{s-2}}-2^{2^{s-1}}|,\\&2\max_{b\neq 0}|F[g_2](b)|+2^{2^{s-1}}\}\end{aligned}$$

이다. 한편 정리 2(1)에 의해서

$$2\max_{b\neq 0}|F[g_1](b)| = 2\{\max_{a\neq 0}|F[g_2](a)| + 2^{2^{s-2}}\} < 2\max_{a\neq 0}|F[g_2](a)| + 2^{2^{s-1}}$$

이므로

$$\Delta_h = \max\{\max_{a\neq 0}|C[g_2](a) - 2^{2^{s-2}} - 2^{2^{s-1}}|, \; 2\max_{a\neq 0}|F[g_2](a)| + 2^{2^{s-1}}\}$$

이다. 이 방법을 계속 사용하면

$$\Delta_h = \max\{\max_{a\neq 0}|C[g_{s-2}](a) - 2^{2^2} - 2^{2^3} - \cdots - 2^{2^{s-1}}|, \; 2\max_{a\neq 0}|F[g_{s-2}](a)| + 2^{2^3} + 2^{2^4} + \cdots + 2^{2^{s-1}}\}$$

이다. 한편 $C[g_{s-2}](12) = -8$이고

$$\max_{a\neq 0}|F[g_{s-2}](a)| = 8$$이므로

$\Delta_h = 2^{2^{s-1}} + 2^{2^{s-2}} + \cdots + 2^{2^2} + 8$이다. 마지막으로 h의 대수적 차수를 살펴보자. $deg(g_{s-2}) = 3$이므로 $deg(h) \geq 3$이다.

$n = 2^s$일 때 위에서 설계한 균형인 부울함수 h의 특성을 요약하면 다음과 같다.

$$\#PC = 2^{3\cdot 2^{s-2}} - 2^{2^{s-1}}$$
$$N_h = 2^{2^{s-1}} - 2^{2^{s-1}-1} - \cdots - 2^{2^3-1} - 2^{2^2-1} - 4$$
$$\sigma_h = \{2^{2^{s+1}} + 2^{2^s} + \cdots + 2^{2^4}\} + 5\{2^{3\cdot 2^{s-1}} + 2^{4\cdot 2^{s-2}} + \cdots + 2^{4\cdot 2^2}\} + 640$$
$$\Delta_h = 2^{2^{s-1}} + 2^{2^{s-2}} + \cdots + 2^{2^2} + 8$$

Zhang-Zheng[6]은 $n = 2k$일 때 대역확산특성이 우수한 균형인 부울함수 h를 설계하였다. 그들이 설계한 h의 특성은 다음과 같다.

$$\#PC = 2^{2k} - 2^{k+1} + 2^{k-1} - 1$$
$$N_h = 2^{2k-1} - 2^k$$
$$\sigma_h = 2^{4k} + 6\cdot 2^{3k}$$
$$\Delta_h = 2^{k+1}$$

$n = 2^3$, 2^4, 2^5일 때 본 논문에서 설계한 균형인 부울함수와 Zhang-Zheng이 설계한 균형인 부울함수의 특성을 비교해 보자(표 1참조). 표 1에 의하면 본 논문에서 설계한 부울함수의 비선형치가 크며, σ_h와 Δ_h는 작다. 따라서 본 논문에서 설계한 부울함수는 모든 면에서 Zhang-Zheng의 것보다 우수하다. PC의 개수를 비교해 보면, 본 논문에서 설계한 것보다 Zhang-Zheng이 설계한 부울함수가 더 많은 PC 개수를 갖는다. 이런 사실로부터 PC를만족하는 벡터 개수는 부울함수의 암호학적 특성을 나타내는 중요한 요소이지만, 부울함수가 균형일 때 PC를 만족하는 벡터의 개수가 많다고 해서 반드시 우수한 부울함수가 될 수 없음을 알 수 있다. 또한 Zhang-Zheng은 Z_{2^n}상의 균형인 부울함수 h의 대수적 차수가 3 이상일 때 Δ_h의 하한이 $2^{\frac{1}{2}(n+1)}$이라고 추측하였다. $n = 2^4, 2^5$일 때 $2^{\frac{1}{2}(n+1)}$은 362.04, 92, 681.90이다. 표1에 의하면 $n = 2^4$일 때 본 논문에서 설계한 부울함수 h의 $\Delta_h = 280$, $n = 25$일 때 $\Delta_h = 65,816$이다. 또한 h의 대수적 차수도 3 이상이므로, Zhang-Zheng의 추측이 틀린다는 것을 알 수 있다.

표1: Zhang-Zheng의 설계방법과 본 논문의 설계방법 비교

n	$\#PC$	N_h	σ_h	Δ_h
2^3	231 48	112 116	90112 86,656	32 24
2^4	65,151 3,840	32,512 32,628	4,395,630,592 4,378,940,032	512 280
2^5	4,294,868,991 16,711,680	2,147,418,112 2,147,450,740	$1.84484\cdot 10^{19}$ $1.84481\cdot 10^{19}$	131,072 65,816

윗줄은 Zhang-Zheng이 설계한 부울함수의 특성값이고, 아랫줄은 본 논문에서 설계한 부울함수의 특성값이다.

4. 결 론

대 역 확 산 특 성 (Global Avalanche Characteristics)은 부울함수의 전반적인 전파특성을 측정하는 개념으로 두 개의 기준 σ_f와 Δ_f가 있다. σ_f와 Δ_f가 작을수록 부울함수는 우수한 전파특성을 지닌다고 말한다. Zhang-Zheng[6]은 대역확산특성이 우수한 균형인 부울함수의 설계방법을 제시하였으며, 균형인 부울함수의 대수적 차수가 3 이상일 때 Δ_f의 하한이 $2^{\frac{1}{2}(n+1)}$이라고 추측하였다. 본 논문에서는 대역확산특성이 우수한 균형인 부울함수의 설계방법을 제시하였다. 이 방법은 Zhang-Zheng의 것보다 우수하다. 또 설계방법으로부터 Zhang-Zheng의 추측이 옳지 않다는 것을 발견하였다.

참고문헌

[1] Carlisle M. Adams and Stafford E. Tavares. The structured design of cryptographically good S-boxes. Journal of Cryptology, 3(1):27-41, 1990.

[2] Sangwoo Park, Seongtaek Chee, and Kwangjo Kim. Semi-bent functions and strict uncorrelated criterion revisited. In International Computer Symposium -ICS' 96, pages 110-117, 1996.

[3] Bart Preneel, W.Van Leekwijck, and L.Van Linden. Propagation characteristics of boolean functions. In Advances in Cryptology - EUROCRYPT' 90, pages 161-173, 1991.

[4] JungJae Son, JongIn Lim, Seongtaek Chee, and SooHak Sung. Global avalanche characteristics and nonlinearity of balanced boolean functions. Information Processing Letter, 65: 139-144, 1998.

[5] A.F. Webster and Stafford E. Tavares. On the design of S-boxes. In Hugh C. Williams, editor, Advances in Cryptology: CRYPTO' 85, volume 218 of Lecture Notes in Computer Science, pages 523-534. Springer-Verlag, New York, 1986.

[6] Xian-Mo Zhang and Yuliang Zheng. GAC - the criterion for global avalanche characteristics of crpytographic functions. Journal of Universal Computer Science, 1(5):320-337, 1995.

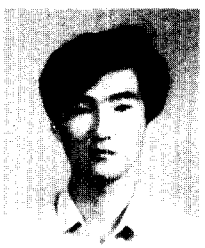
[7] 성수학, 지성택, 이상진, 김광조. 상관면역 함수와 비선형치. 통신정보보호학회 논문지, 제 7권 3호: 11-22, 1996.

[8] 성수학, 천정희, 지성택, 김광조. 균형인 부울함수의 대역확산 특성. 통신정보보호학회 논문지, 제 7권 4호: 51-58, 1997.

□ 著者紹介

지 성 택

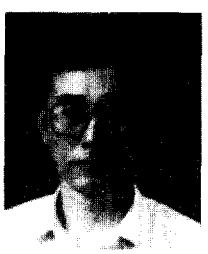
1985년 2월 서강대학교 이공대학 수학과(이학사)
1987년 2월 서강대학교 대학원 수학과(이학석사)
1989년 - 현재 한국전자통신연구원 선임 연구원



이 상 진

1987년 2월 고려대학교 이과대학 수학과(이학사)
1989년 2월 고려대학교 대학원 수학과(이학석사)
1994년 2월 고려대학교 대학원 수학과(이학박사)
1989년 - 현재 한국전자통신연구원 선임 연구원

※ 주관심분야 : 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
1989년 - 현재 한국전자통신연구원 책임연구원

※ 주관심분야 : 암호이론, 정보이론, 통신이론

성 수 학

1982년 2월 경북대학교 수학과(학사)
1985년 2월 KAIST 응용수학과(석사)
1988년 2월 KAIST 응용수학과(박사)
1988년 ~ 1991년 한국전자통신연구원 선임 연구원
1991년 - 현재 배재대학교 응용수학과 조교수