通信情報保護學會論文誌
第6卷 第3號, 1996. 9

Semi-bent 함수의 일반화와 구성 방법

박 상 우*, 지 성 택*, 김 광 조*

Generalization of Semi-bent functions and their Construction Method

Sangwoo Park*, Seongtaek Chee*, Kwangjo Kim*

요 약

참고문헌 [4, 12]에서 지성택외 2인은 새로운 암호 기본 논리로서 semi-bent 함수를 정의하였는데, semi-bent 함수는 우수한 암호학적 특성을 가지는 반면 홀수차 벡터 공간에만 존재하는 단점을 가지고 있다. 본 논문에서는, 홀수차 뿐만 아니라 짝수차에도 존재하는 generalized semi-bent 함수를 정의하고, 이를 생성하는 체계적인 방법을 제안하며, 암호학적 주요 특성을 분석한다. 또한, SUC를 만족하는 부울함수들을 홀수차뿐만 아니라 짝수차에서도 찾을 수 있음을 보인다.

Abstract

In [4, 12], Chee *et al.* proposed a new class of cryptographic primitive, "semi-bent functions", which exists on only odd dimensional vector spaces [4]. In this paper, we discuss new notion of *generalized semi-bent functions* which can be defined on any vector spaces. And we suggest systematic methods for constructing *generalized semi-bent functions* and analyse their cryptographic properties. In addition, we show that SUC fulfilling Boolean functions can be found on any dimensional vector spaces.

1. 서 론

안전한 블럭 암호 알고리즘, 스트림 암호 알고리즘, 해쉬함수들을 설계하기 위하여, 암호학적으로 우수한 특성을 가지는 부울함수(Boolean function)가 필요하다. 암호학에 이용되는 부울 함수(이하 부울 함수)가 가지는 주요한 특성으로는 균등성(balancedness), 비선형성(nonlinearity), 상관면역성(correlation immunity), PC(Propagation Criterion) 특성[7]

* 한국전자통신연구소

등이 있다. 또한, 암호학적으로 우수한 특성을 가지는 부울 함수의 설계 방법이 여러가지 제안되어왔다[3,4,9].

참고문헌 [4, 12]에서, 지성택외 2인은 semi-bent 함수(이하 유사 벤트 함수)라는 새로운 암호 기본 논리를 제안하였다. 그들이 제안한 유사 벤트 함수는 암호학적 특성이 우수한 반면 홀수차 벡터 공간에만 존재하는 단점을 가진다. 본 논문에서는 이러한 단점을 해결한, 즉, 모든 차수에서 정의되는 generalized semi-bent 함수(이하 범용 유사 벤트 함수)를 정의하고, 그 생성 방법을 제안한다. 참고 문헌 [4, 12]의 유사 벤트 함수에 대한 정의는 홀수차 범용 유사 벤트 함수를 생성하는 방법임을 보이고, 짝수차 범용 유사 벤트 함수를 생성하는 새로운 방법을 제안한다. 다음으로 범용 유사 벤트 함수의 암호학적 특성을 분석한다. 범용 유사 벤트 함수는 균등 함수이며, 비선형성이 우수하고, 선형 함수에 대해서 거의 균일한 상관값을 가지고, 우수한 PC 특성을 가진다. 마지막으로, 범용 유사 벤트 함수를 이용하면, 차수에 관계없이 SUC(Strict Uncorrelated Criterion)[4, 12]을 만족하는 부울 함수의 쌍을 찾을 수 있음을 보인다.

2장에서는 본 논문에서 사용하는 각종 기호와 부울 함수의 여러 가지 암호학적 특성, WHT(Walsh-Hadamard Transform)에 의해 얻어지는 주요 기본 정리들을 소개한다. 3장에서는 범용 유사 벤트 함수를 정의하고, 암호학적 특성을 분석하며, 생성 방법을 제안한다. 4장에서는 생성 방법에 따른 범용 유사 벤트 함수의 PC 특성을 증명하고, SUC을 만족하는 부울 함수의 쌍을 모든 차수에서 찾을 수 있음을 보인다.

2. 예비 사항

본 장에서는 본 논문에서 사용하는 기호, 부울 함수의 여러 가지 암호학적 특성, 그리고, WHT에 의해 얻어지는 주요 기본 정리들을 소개한다. Z_2^n을 $GF(2)$ 위의 n차 벡터 공간이라 하자. $\mathbf{x} = (x_1, \cdots, x_n)$과 $\mathbf{y} = (y_1, \cdots, y_n)$를 Z_2^n의 두 벡터라 하면, $\mathbf{x}$와 $\mathbf{y}$의 내적은 $(\mathbf{x}, \mathbf{y}) = x_1y_1 \oplus \cdots \oplus x_ny_n$이며, 여기서, 곱과 합은 $GF(2)$의 연산이다. 부울 함수 f는 Z_2^n을 정의역으로하고, 0 또는 1의 값을 가지는 함수이다. Z_2^n상에 정의된 모든 부울 함수의 집합을 일반적으로 $\mathcal{B}_n$으로 표시한다. $f(\mathbf{x}) = l_{\mathbf{w}}(\mathbf{x}) \oplus c = (\mathbf{x}, \mathbf{w}) \oplus c = x_1w_1 \oplus \cdots \oplus x_nw_n \oplus c$가 되는 벡터 $\mathbf{w} \in Z_2^n$와 상수 $c \in Z_2$가 존재하는 부울 함수 f를 아핀(affine) 함수라 하며, 특히, $c = 0$인 경우, f를 선형(linear) 함수라 한다.

Z_2^n상에 정의된 모든 아핀 함수와 선형 함수의 집합을 각각 $\mathcal{A}_n$과 $\mathcal{L}_n$으로 표시한다. 벡터 $\mathbf{x} \in Z_2^n$의 해밍 무게(Hamming weight)는 $\mathbf{x}$에서 '1'의 개수이며, $wt(\mathbf{x})$으로 표시한다. 그리고, 부울 함수 $f \in \mathcal{B}_n$의 해밍 무게는 $wt(f)$로 표시하며, f의 함수값들 중 '1'의 개수이다. 두 함수 f와 g의 해밍 거리 $d(f, g)$는 f와 g의 서로 다른 함수값의 개수이다. $f \oplus g$는 Z_2^n상의 함수로서, f와 g의 함수값들의 비트별 논리합으로 얻어지며, $f \| g$는 Z_2^{n+1}상의 함수로서 f와 g의 진리표의 연접으로 얻어진다. 즉,

$$(f \oplus g)(\mathbf{x}) = f(\mathbf{x}) \oplus g(\mathbf{x})$$

이고,

$$\begin{aligned}(f \| g)(\mathbf{x}^*) &= (f \| g)(\mathbf{x}, x_{n+1}) \\ &= (1 \oplus x_{n+1})f(\mathbf{x}) \oplus x_{n+1}g(\mathbf{x}), \\ &\quad \mathbf{x}^* \in Z_2^{n+1}\end{aligned}$$

이다. 다음은 WHT의 정의이다.

■ **정의 1** 부울 함수 $f \in \mathcal{B}_n$에 대해서, f의 WHT $\hat{f}_f : Z_2^n \to \mathcal{R}$은 다음으로 정의된다.

$$\hat{\mathcal{F}}_f(\mathbf{w}) = \sum_{\mathbf{x}\in Z_2^n} \hat{f}(\mathbf{x})\cdot(-1)^{\langle \mathbf{x},\, \mathbf{w}\rangle}.$$

여기서, $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$이며, $\mathcal{R}$은 실수 전체의 집합이다.

■ **정의 2** $|\{\mathbf{x} \in Z_2^n \mid f(\mathbf{x}) = 0\}| = |\{\mathbf{x} \in Z_2^n \mid f(\mathbf{x}) = 1\}|$이면, $f \in \mathcal{B}_n$는 균등 함수(*balanced function*)이다.

❖ **보조정리 1** $f \in \mathcal{B}_n$가 균등 함수라는 사실과 $\hat{\mathcal{F}}_f(\mathbf{0}) = 0$은 동치이다.

임의의 부울 함수의 비선형성은 부울 함수와 모든 아핀 함수와의 해밍 거리로 표시된다.

■ **정의 3** 임의의 부울 함수 $f \in \mathcal{B}_n$의 비선형치 $\mathcal{N}_f$는 다음으로 정의된다.

$$\mathcal{N}_f = \min_{\lambda_n \in \mathcal{A}_n} d(f, \lambda_n).$$

높은 비선형치는 DES(Data Encryption Standard) 구조의 블럭 암호 알고리즘 설계 시 고려해야 할 필수 요소인데, 이는 Matsui가 제안한 선형 해독법[5]에 의해 비교적 낮은 비선형치를 가지는 S-box를 사용한 블럭 암호 알고리즘인 DES와 FEAL(Fast data Encipherment ALgorithm)등이 공격되었다는 사실에 기인한다. S-box가 선형 해독법에 견디기 위해서는 S-box의 각 구성 함수들의 모든(0을 제외한) 선형 결합의 비선형치가 높아야 한다[10].

❖ **보조정리 2** 부울 함수 $f \in \mathcal{B}_n$에 대해서, $\mathcal{N}_f = 2^{n-1} - \frac{1}{2}\max_{\mathbf{w}\in Z_2^n}|\hat{\mathcal{F}}_f(\mathbf{w})|$이다.

스트림 암호 알고리즘에 사용될 경우에 일반적으로 부울 함수는 선형 궤환 레지스터(linear feedback shift register)의 출력 수열을 결합하는 논리로서 사용되는데, 이 경우 상관 공격(correlation attack)[11]에 강한 함수가 필요하다.

■ **정의 4** $1 \le wt(\mathbf{w}) \le m$인 모든 $\mathbf{w} \in Z_2^n$에 대해서,

$$d(f, l_{\mathbf{w}}) = 2^{n-1}$$

인 부울 함수 $f \in \mathcal{B}_n$를 m차 무상관 함수(m-th order correlation immune function)라 한다. 또한, f와 g의 무상관값은 다음과 같다.

$$c(f,g) = 1 - \frac{d(f,g)}{2^{n-1}}.$$

PC[7]는 SAC(Strict Avalanche Criterion)의 정의를 확장한 개념으로 우수한 PC 특성을 가져야 함은 블럭 암호 알고리즘이 입, 출력 변화 공격법[2]에 강하기 위한 필수 조건이다.

■ **정의 5** $\sum_{\mathbf{w}\in Z_2^n} f(\mathbf{x}) \oplus f(\mathbf{x}\oplus\alpha) = 2^{n-1}$인 부울 함수 $f \in \mathcal{B}_n$는 $\alpha \in Z_2^n$에 대해서 propagation criterion(PC)을 만족한다. 또한, $1 \le wt(\alpha) \le k$인 모든 $\alpha \in Z_2^n$에 대해서 PC를 만족하는 경우, f는 k차 PC를 만족한다고 하고, $PC(k)$로 표기한다.

■ **정의 6** 임의의 부울 함수 $f \in \mathcal{B}_n$의 자기 상관 함수(autocorrelation function) $\hat{\mathcal{A}}_f : Z_2^n \to \mathcal{R}$는 다음과 같다.

$$\hat{\mathcal{A}}_f(\mathbf{s}) = \sum_{\mathbf{x}\in Z_2^n} \hat{f}(\mathbf{x})\cdot\hat{f}(\mathbf{x}\oplus\mathbf{s}).$$

또한, 부울 함수 $f_0, f_1 \in \mathcal{B}_n$의 교차 상관 함수(crosscorrelation function) $\hat{C}_{f_0,f_1} : Z_2^n \to \mathcal{R}$는 다음과 같다.

$$\hat{C}_{f,f_1}(\mathbf{s}) = \sum_{\mathbf{x}\in Z_2^n} \hat{f}_0(\mathbf{x})\cdot\hat{f}_1(\mathbf{x}\oplus\mathbf{s}).$$

❖ 보조정리 3 [7] 부울 함수 f_0, $f_1 \in \mathcal{B}_n$에 대해서,

$$\hat{C}_{f_0,f_1}(\mathbf{s}) = \frac{1}{2^n}\sum_{\mathbf{w}\in Z_2^n} \hat{\mathcal{F}}_{f_0}(\mathbf{w})\cdot\hat{\mathcal{F}}_{f_1}(\mathbf{w})\cdot(-1)^{(\mathbf{s},\mathbf{w})}$$

이다.

❖ 보조정리 4 [7] 부울 함수 $f \in \mathcal{B}_n$에 대해서, f가 $PC(k)$를 만족하면 $1 \le wt(\mathbf{s}) \le k$인 모든 $\mathbf{s} \in Z_2^n$에 대해서

$$\hat{\mathcal{A}}_f(\mathbf{s}) = 0$$

이다. 또한, 역도 성립한다.

❖ 보조정리 5 [7] 임의의 부울 함수 $f \in \mathcal{B}_n$가 $PC(k)$를 만족하면 $1 \le wt(\mathbf{s}) \le k$인 모든 $\mathbf{s} \in Z_2^n$에 대해서,

$$\sum_{\mathbf{w}\in Z_2^n} \hat{\mathcal{F}}_f^2(\mathbf{w})\cdot(-1)^{(\mathbf{s},\mathbf{w})} = 0$$

이다. 또한, 역도 성립한다.

❖ 정리 1 (Parseval의 정리) 부울 함수 $f \in \mathcal{B}_n$에 대해서

$$\sum_{\mathbf{w}\in Z_2^n} \hat{\mathcal{F}}_f^2(\mathbf{w}) = 2^{2n}$$

이다.

■ 정의 7 모든 $\mathbf{w} \in Z_2^n$에 대해서

$$|\mathcal{F}_f(\mathbf{w})| = 2^{\frac{n}{2}},$$

인 부울 함수 $f \in \mathcal{B}_n$를 벤트 함수(bent function)라 한다.

벤트 함수는 짝수차 벡터 공간에만 존재하며, 균등 함수가 아니다. 벤트 함수 $f \in \mathcal{B}_n$는 $PC(n)$을 만족하며, 모든 선형 함수와 균일한 상관값을 가진다. 즉, 모든 $\mathbf{w} \in Z_2^n$에 대해서, 벤트 함수 f와 선형 함수 $l_\mathbf{w}$의 상관값은 $\pm 2^{-\frac{n}{2}}$이다. 그리고, 벤트 함수의 비선형치는 $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n}{2}-1}$이다. Propagation characteristic, 상관 면역성, 그리고, 비선형성 관점에서 벤트 함수는 우수한 암호학적 성질을 가진다. 그러나, 벤트 함수는 균등 함수가 아니며, 짝수차 벡터 공간에만 존재한다는 사실에 의해 알고리즘 설계 시에 직접적으로 응용되지는 않는다. 부울 함수 f의 WHT와 자기 상관 함수에 의해서, 아핀 변환에 의한 부울 함수의 암호학적 성질의 변화를 용이하게 분석할 수 있다[7].

❖ 정리 2 부울 함수 $f \in \mathcal{B}_n$와 $\mathbf{a}, \mathbf{b} \in Z_2^n$, $c \in Z_2$ 그리고 $n \times n$ 정칙 행렬 A에 대해서, $g \in \mathcal{B}_n$를 다음으로 정의하자.

$$g(\mathbf{x}) = f(A\mathbf{x}\oplus\mathbf{a}) \oplus l_\mathbf{b}(\mathbf{x}) \oplus c.$$

그러면,

$$\hat{\mathcal{F}}_g(\mathbf{w}) = (-1)^c(-1)^{(A^{-1}\mathbf{a},\mathbf{w}\oplus\mathbf{b})}\hat{\mathcal{F}}_f((A^{-1})^t(\mathbf{w}\oplus\mathbf{b}))$$

이고,

$$\hat{\mathcal{A}}_g(\mathbf{s}) = (-1)^{(\mathbf{s},(A^{-1})^t\mathbf{b})}\hat{\mathcal{A}}_f(A\mathbf{s})$$

이다.

❖ 정리 3 부울 함수 f_0, $f_1 \in \mathcal{B}_n$, $\mathbf{w}^*$, $\mathbf{s}^* \in Z_2^{n+1}$ 그리고 $\mathbf{w}$, $\mathbf{s} \in Z_2^n$에 대해서, $g = f_0 \| f_1$라 하자. 그러면

$$\hat{\mathcal{F}}_g(\mathbf{w}^*) = \hat{\mathcal{F}}_{f_0}(\mathbf{w}) + (-1)^{w_{n+1}}\hat{\mathcal{F}}_{f_1}(\mathbf{w})$$

이고

$$\hat{\mathcal{A}}_g(\mathbf{s}^*) = \begin{cases} \hat{\mathcal{A}}_{f_0}(\mathbf{s}) + \hat{\mathcal{A}}_{f_1}(\mathbf{s}) & \text{if } s_{n+1} = 0 \\ 2\cdot\hat{C}_{f_0,f_1}(\mathbf{s}) & \text{if } s_{n+1} = 1 \end{cases}$$

이다.

지성택외 2인은 참고 문헌 [4, 12]에서 유사 벤트 함수를 정의하고, 암호학적 특성을 분석하였다. 유사 벤트 함수는 우수한 암호학적 특성을 가지지만, 홀수차 벡터 공간에만 존재하는 단점이 있다.

■ **정의 8** (유사 벤트 함수) $f_0 \in \mathcal{B}_{2n}$가 벤트 함수이고, $\mathbf{a} \in Z_2^{2n}$, 그리고 A를 $2n \times 2n$ 정칙 행렬이라 하자. 다음으로 $f_1 \in \mathcal{B}_{2n}$과 $g \in \mathcal{B}_{2n+1}$를 정의하자.

$$f_1(\mathbf{x}) = f_0(A\mathbf{x} \oplus \mathbf{a}) \oplus 1,$$
$$g = f_0 \| f_1$$

그러면 $g \in \mathcal{B}_{2n+1}$는 유사 벤트 함수이다.

❖ **정리 4** 유사 벤트 함수 $g \in \mathcal{B}_{2n+1}$는 다음과 같은 암호학적 성질을 가진다.

1) g는 균등 함수이다.
2) $\mathcal{N}_g = 2^{2n} - 2^n$
3) 모든 $\mathbf{w}^* \in Z_2^{2n+1}$에 대해서, 유사 벤트 함수 g와 선형 함수 $l_{\mathbf{w}^*}$의 상관값은 0 또는 $\pm 2^{n}$이며,

$$|\{\mathbf{w}^* \in Z_2^{2n+1} \mid c(g, l_{\mathbf{w}^*}) = 0\}| = 2^{2n}$$
$$= |\{\mathbf{w}^* \in Z_2^{2n+1} \mid c(g, l_{\mathbf{w}^*}) = \pm 2^{n}\}|$$

이다.

4) g는 $s_{2n+1} = 0$이고 0이 아닌 모든 $\mathbf{s}^* \in Z_2^{2n+1}$에 대해서 PC를 만족한다.
5) A를 $2n \times 2n$ 단위 행렬이라 하면, g는 $\mathbf{s} \neq \mathbf{a}$이고 0이 아닌 모든 $\mathbf{s}^* \in Z_2^{2n+1}$에 대해서 PC를 만족한다.
6) A가 $2n \times 2n$ 단위 행렬이고, $a = (1, \cdots, 1)$이면, g는 $PC(2n)$을 만족한다.

■ **정의 9** 두 부울 함수 $f, g \in \mathcal{B}_n$ 그리고, $f \oplus g$가 모두 균형 함수이고, $PC(1)$을 만족하면, f와 g는 SUC을 만족한다.

❖ **정리 5** 부울 함수 g_1과 g_2를, $f_1 \oplus f_2$가 균등 함수이고, $PC(1)$을 만족하는 벤트 함수 f_1과 f_2에 의해 $2n \times 2n$ 대치 행렬(permutation matrix) A와 $wt(\mathbf{a}) = 1$인 $\mathbf{a} \in Z_2^{2n}$에 의해 정의 8에 의하여 생성된 Z_2^{2n+1} 상에 정의된 유사 벤트 함수라 하자. 그러면 g_1과 g_2는 SUC을 만족한다.

3. 범용 유사 벤트 함수

본 장에서는 범용 유사 벤트 함수를 정의하고, 균등성, 비선형성, 상관 무결성등과 같은 암호학적 특성을 분석하며 구체적인 생성 방법을 소개한다.

■ **정의 10** $|\hat{\chi}_f(\mathbf{w})| = 0$ 또는 $2^{\lfloor \frac{n}{2} \rfloor + 1}$이고, $\hat{\chi}_f(\mathbf{0}) = 0$인 부울 함수 $f \in \mathcal{B}_n$를 범용 유사 벤트 함수라 한다. 여기서, $\lfloor m \rfloor$는 m 보다 같거나 작은 정수 중 가장 큰 정수이다.

❖ **정리 6** 범용 유사 벤트 함수 $f \in \mathcal{B}_n$의 암호학적 성질은 다음과 같다.

1) f는 균등 함수이다.
2) $\mathcal{N}_f = 2^{n-1} - 2^{\lfloor \frac{n}{2} \rfloor}$
3) 모든 $\mathbf{w} \in Z_2^{2n}$에 대해서, f와 선형 함수 $l_{\mathbf{w}}$의 상관값은 0 또는 $\pm 2^{\frac{n-2+(n \bmod 2)}{2}}$이다. 그리고, $|\{\mathbf{w} \in Z_2^{2n} \mid c(f, l_{\mathbf{w}}) = \pm 2^{\frac{n-2+(n \bmod 2)}{2}}\}|$ $= 2^{n-2+(n \bmod 2)}$이다.

증 명.

1) 정의 10에 의해 자명하다.
2) 보조 정리 2에 의해서,

$$\mathcal{N}_f = \begin{cases} 2^{(2k+1)-1} - \frac{1}{2} \cdot 2^{k+1} = 2^{2k} - 2^k \\ \qquad\qquad\qquad\qquad if\ n = 2k+1 \\ 2^{(2k+2)-1} - \frac{1}{2} \cdot 2^{k+2} = 2^{2k+1} - 2^{k+1} \\ \qquad\qquad\qquad\qquad if\ n = 2k+2 \end{cases}$$

이다.

3) $n = 2k + 1$인 경우에, 모든 $\mathbf{w} \in Z_2^{2n}$에 대해서,

$$c(f, l_{\mathbf{w}}) = \frac{\hat{\mathcal{F}}_f(\mathbf{w})}{2^{2k+1}} = \frac{0 \text{ 또는 } \pm 2^{k+1}}{2^{2k+1}} = 0 \text{ 또는 } \pm 2^{-k}$$

이다. 그리고, N_1을 $c(f, l_{\mathbf{w}}) = \pm 2^{-k}$인 $\mathbf{w} \in Z_2^{2k+1}$의 개수라 하면, Parseval의 정리에 의해 $N_1 = 2^{2k}$이다.

또한, $n = 2k + 2$인 경우에, 모든 $\mathbf{w} \in Z_2^{2n}$에 대해서,

$$c(f, l_{\mathbf{w}}) = \frac{\hat{\mathcal{F}}_f(\mathbf{w})}{2^{2k+2}} = \frac{0 \text{ 또는 } \pm 2^{k+2}}{2^{2k+2}} = 0 \text{ 또는 } \pm 2^{-k}$$

이다. 그리고, N_2를 $c(f, l_{\mathbf{w}}) = \pm 2^{-k}$인 $\mathbf{w} \in Z_2^{2k+2}$의 개수라 하면, Parseval의 정리에 의해 $N_2 = 2^{2k}$이다. □

정리 6에 의하면 홀수차 벡터 공간상의 범용 유사 벤트 함수 $f \in \mathcal{B}_{2k+1}$의 비선형치는 $\mathcal{N}_f = 2^{2k} - 2^k$인데, 이 값은 Pieprzyk와 Finkelstein이 참고 문헌 [6]에서 $2k + 1$차 균등 부울 함수가 가지는 최대 비선형치로 주장한 바 있다. 그리고, $2k + 2$차 범용 유사 벤트 함수 $f \in \mathcal{B}_{2k+2}$의 비선형치는 $\mathcal{N}_f = 2^{2k+1} - 2^{k+1}$이며, 이 값 역시 $2k + 2$차 균형 부울 함수가 가지는 최대 비선형치로 알려져 있다[1]. 그리고 $2k + 1$차 범용 유사 벤트 함수는 모든 선형 함수의 반에 대해서 상관 면역이며, 나머지 반에 대해서 균일한 상관값을 가진다. 한편, $2k + 2$차 범용 유사 벤트 함수는 모든 선형 함수의 3/4에 대해서 상관 면역이며, 나머지 선형 함수에 대해서 균일한 상관값을 가진다.

다음으로 범용 유사 벤트 함수의 생성 방법을 소개한다. 먼저, 부울 함수 $g \in \mathcal{B}_n$를 정의 8에 의하여 생성된 유사 벤트 함수라 하자. 정리 2와 정리 3에 의해서,

$$\begin{aligned}|\hat{\mathcal{F}}_g(\mathbf{w}^*)| &= |\hat{\mathcal{F}}_{f_0}(\mathbf{w}) + (-1)^{w_{2k+1}} \hat{\mathcal{F}}_{f_1}(\mathbf{w})| \\ &= |\pm 2^k \mp (-1)^{((A^{-1})^t \mathbf{a}, \mathbf{w})} 2^k| \\ &= 0 \text{ 또는 } 2^{k+1} \\ &= 0 \text{ 또는 } 2^{\lfloor \frac{n}{2} \rfloor + 1}.\end{aligned}$$

이며, $\hat{\mathcal{F}}_g(\mathbf{0}) = 0$이다. 즉, 정의 8에 의해 생성된 유사 벤트 함수 g는 $2k + 1$차 범용 유사 벤트 함수이다.

■ **방법 1** $f_0 \in \mathcal{B}_{2k}$를 벤트 함수, $\mathbf{a} \in Z_2^{2k}$ 그리고 A를 $2k \times 2k$ 정칙 행렬이라 하자. 그리고, $f_1 \in Z_2^{2k}$과 $g \in \mathcal{B}^{2k+1}$를 다음으로 정의하자.

$$f_1(\mathbf{x}) = f_0(A\mathbf{x} \oplus \mathbf{a}) \oplus 1,$$
$$g = f_0 \| f_1$$

그러면 g는 Z_2^{2k+1} 상에 정의된 범용 유사 벤트 함수이다.

$g_0 \in \mathcal{B}_{2k+1}$는 방법 1에 의해 생성된 범용 유사 벤트 함수이고, $\mathbf{a}^* \in Z_2^{2k+1}$라 하자. $g_1 \in \mathcal{B}_{2k+1}$은 $g_1(\mathbf{x}^*) = g_0(\mathbf{x}^* \oplus \mathbf{a}^*) \oplus 1$, 이고, $h \in \mathcal{B}_{2k+2}$는 $h = g_0 \| g_1$이다. 그러면, 정리 2와 정리 3에 의해, 모든 $\mathbf{w}^{**} \in Z_2^{2k+2}$에 대해서,

$$\begin{aligned}\hat{\mathcal{F}}_h(\mathbf{w}^{**}) &= \hat{\mathcal{F}}_{g_0}(\mathbf{w}^*) + (-1)^{w_{2k+2}} \hat{\mathcal{F}}_{g_1}(\mathbf{w}^*) \\ &= \hat{\mathcal{F}}_{g_0}(\mathbf{w}^*) \\ &\quad + (-1)^{w_{2k+2}} \cdot (-1) \cdot (-1)^{(\mathbf{a}^*, \mathbf{w}^*)} \hat{\mathcal{F}}_{g_0}(\mathbf{w}^*)\end{aligned}$$

이며, $|\hat{\mathcal{F}}_{g_0}(\mathbf{w}^*)| = 0$ 또는 2^{k+1}이므로, $|\hat{\mathcal{F}}_h(\mathbf{w}^{**})| = 0$ 또는 $2^{k+2} = 0$ 또는 $2^{\lfloor \frac{n}{2} \rfloor} + 1$이며, $\hat{\mathcal{F}}_h(\mathbf{0}) = 0$이다. 따라서, h는 Z_2^{2k+2} 상에 정의된 범용 유사 벤트 함수이다.

■ **방법 2** $g_0 \in \mathcal{B}_{2k+1}$를 방법 1에 의해 생성된 범용 유사 벤트 함수라 하고, $\mathbf{a}^* \in Z_2^{2k+1}$라 하자. 그리고, $g_1 \in \mathcal{B}_{2k+1}$과 $h \in \mathcal{B}_{2k+2}$를 다음으로 정의하자.

$g_1(\mathbf{x}^*) = g_0(\mathbf{x}^* \oplus \mathbf{a}^*) \oplus 1,$

$h = g_0 \| g_1.$

그러면 h는 Z_2^{2k+2} 상에 정의된 범용 유사 벤트 함수이다.

4. PC 특성 및 SUC

본 장에서는 생성 방법에 따른 범용 유사 벤트 함수의 PC 특성을 분석한다. 그리고, SUC을 만족하는 범용 유사 벤트 함수의 쌍을 모든 차수에서 찾을 수 있음을 보이고, 그 실례를 제시한다.

우선 방법 1에 의하여 생성된 범용 유사 벤트 함수의 PC 특성을 알아보자. 정리 4의 4), 5), 6)에 의하여, 방법 1에 의하여 생성된 $2k + 1$차 범용 유사 벤트 함수의 PC 특성을 알 수 있다. $g \in \mathcal{B}_{2k+1}$를 방법 1에 의하여 생성된 범용 유사 벤트 함수라 하자. 그러면 g는 $s_{2k+1} = 0$이고 0이 아닌 모든 $\mathbf{s}^* \in Z_2^{2k+1}$에 대해서 PC를 만족한다. 그리고, 방법 1의 A가 $2k \times 2k$ 단위 행렬일 경우, g는 $\mathbf{s} \neq \mathbf{a}$인 0이 아닌 모든 $\mathbf{s}^* \in Z_2^{2k+1}$에 대해서 PC를 만족한다. 또한, A가 $2k \times 2k$ 단위 행렬이고, $\mathbf{a} = (1, \cdots, 1)$이면, g는 $PC(2k)$를 만족한다.

다음으로 방법 1에 의하여 생성된 범용 유사 벤트 함수의 PC 특성을 알아보자. $h \in \mathcal{B}_{2k+2}$를 방법 2에 의하여 생성된 범용 유사 벤트 함수라 하고, $\mathbf{s}^* = (\mathbf{s}^*, s_{2k+2}) = (\mathbf{s}, s_{2k+1}, s_{2k+2})$를 Z_2^{2k+2}의 0이 아닌 임의의 원소라 하자. $s_{2k+1} = s_{2k+2} = 0$이면, 정리 2와 3에 의해,

$$\begin{aligned}\mathcal{A}_h(\mathbf{s}^{**}) &= \mathcal{A}_{\tilde{g}_0}(\mathbf{s}^*) + \mathcal{A}_{\tilde{g}_1}(\mathbf{s}^*) \\ &= \mathcal{A}_{\tilde{g}_0}(\mathbf{s}^*) + (-1)^{(\mathbf{s}^*,0)}\mathcal{A}_{\tilde{g}_0}(\mathbf{s}^*)\end{aligned}$$

이다. $g_0 \in \mathcal{B}_{2k+1}$가 방법 1에 의해 생성된 $2k + 1$차 범용 유사 벤트 함수이므로, $\mathcal{A}_{\tilde{g}_0}(\mathbf{s}^*) = 0$이다. 따라서, $\mathcal{A}_h(\mathbf{s}^{**}) = 0$이다.

❖ **정리 7** 방법 2에 의해 생성된 범용 유사 벤트 함수 $h \in \mathcal{B}_{2k+2}$는 $s_{2k+1} = s_{2k+2} = 0$인 0이 아닌 모든 $\mathbf{s}^{**} \in Z_2^{2k+2}$에서 PC를 만족한다.

방법 2에서, $g_0 \in \mathcal{B}_{2k+2}$를 $2k \times 2k$ 단위 행렬 A에 의해 방법 1로 생성된 범용 유사 벤트 함수라 하자. $s_{2k+1} = 1$, $s_{2k+2} = 0$이면, 정리 4의 5)에 의하여, $\mathbf{s} \neq \mathbf{a}$인 0이 아닌 모든 $\mathbf{s}^* \in Z_2^{2k+1}$에 대해서, $\mathcal{A}_{\tilde{g}_0}(\mathbf{s}^*) = 0$이다. 즉, $s_{2k+1} = 1$, $s_{2k+2} = 0$이고, $\mathbf{s} \neq \mathbf{a}$인 모든 $\mathbf{s}^{**} \in Z_2^{2k+2}$에 대해서, $\mathcal{A}_h(\mathbf{s}^{**}) = 0$이다.

❖ **정리 8** $g_0 \in \mathcal{B}_{2k+2}$를 $2k \times 2k$ 단위 행렬 A에 의해방법 1로 생성된 범용 유사 벤트 함수라 하자. g_0에 의해 방법 2로 생성된 범용 유사 벤트 함수 $h \in \mathcal{B}_{2k+2}$는 $s_{2k+1} = 1$, $s_{2k+2} = 0$이고, $\mathbf{s} \neq \mathbf{a}$인 모든 $\mathbf{s}^{**} \in Z_2^{2k+2}$에 대해서, PC를 만족한다.

❖ **정리 9** 방법 2에 의해 생성된 범용 유사 벤트 함수 $h \in \mathcal{B}_{2k+2}$는 $s_{2k+2} = 1$이고 $\mathbf{s}^* \neq \mathbf{a}^*$인 모든 $\mathbf{s}^{**} \in Z_2^{2k+2}$에 대해서 PC를 만족한다.

증 명.

$\mathbf{s}^{**} = (\mathbf{s}^*, s_{2k+2})$를 $s_{2k+2} = 1$이고 $\mathbf{s}^* \neq \mathbf{a}^*$인 Z_2^{2k+2}의 원소라 하면, 정리 3에 의해 다음을 얻는다.

$$\begin{aligned}\mathcal{A}_h(\mathbf{s}^{**}) &= 2 \cdot \hat{C}_{\tilde{g}_0\tilde{g}_1}(\mathbf{s}^*) \\ &= 2 \cdot \frac{1}{2^{2k+1}} \sum_{\mathbf{w}^* \in Z_2^{2k+1}} \hat{\mathcal{F}}_{\tilde{g}_0}(\mathbf{s}^*) \cdot \hat{\mathcal{F}}_{\tilde{g}_1}(\mathbf{s}^*) \cdot (-1)^{(\mathbf{s}^*,\mathbf{w}^*)} \\ &= \frac{1}{2^{2k}} \sum_{\mathbf{w}^* \in Z_2^{2k+1}} \hat{\mathcal{F}}_{\tilde{g}_0}(\mathbf{w}^*) \cdot \{(-1) \cdot (-1)^{(\mathbf{a}^*,\mathbf{s}^*)} \\ &\quad \cdot \hat{\mathcal{F}}_{\tilde{g}_0}(\mathbf{s}^*)\} \cdot (-1)^{(\mathbf{s}^*,\mathbf{w}^*)} \\ &= -\frac{1}{2^{2k}} \sum_{\mathbf{w}^* \in Z_2^{2k+1}} \hat{\mathcal{F}}^2_{\tilde{g}_0}(\mathbf{s}^*) \cdot (-1)^{(\mathbf{a}^* \oplus \mathbf{s}^*,\mathbf{w}^*)} \\ &= 0.\end{aligned}$$

참고문헌 [4, 12]에서, 저자들은 SUC을 만족하는 $2k+1$차 유사 벤트 함수의 쌍을 발견하였다. 본 논문에서는 SUC을 만족하는 $2k+2$차 부울 함수의 쌍이 존재함을 보인다. 먼저, 다음 보조 정리를 증명한다.

❖ **보조정리 6** $g_0 \in \mathcal{B}_{2k+1}$는 범용 유사 벤트 함수이고, $h \in \mathcal{B}_{2k+2}$는 g_0와 $wt(\mathbf{a}^*) = 1$인 $\mathbf{a}^*$로서, 방법 2에 의해 생성된 범용 유사 벤트 함수라 하자. g_0가 $PC(1)$을 만족하면, h는 $PC(1)$을 만족한다.

증 명.

$\mathbf{s}^{**} = (\mathbf{s}^*, s_{2k+2})$를 Z_2^{2k+2}의 단위 원소(unit element)라 하자. $s_{2k+2} = 0$이면, $wt(\mathbf{s}^*) = 1$이다. g_0가 $PC(1)$을 만족하므로, 정리 2과 3에 의해

$$\hat{\mathcal{A}}_h(\mathbf{s}^{**}) = 0$$

을 얻는다. $s_{2k+1} = 1$이면 $\mathbf{s}^* = \mathbf{0}$이다. $wt(\mathbf{a}^*) = 1$이므로, 정리 2와 3 그리고 따름 정리 5에 의해,

$$\begin{aligned}\hat{\mathcal{A}}(\mathbf{s}^{**}) &= 2\cdot\hat{C}_{g_0,g_1}(\mathbf{0}) \\ &= 2\cdot\frac{1}{2^{2k+1}}\sum_{\mathbf{w}^*\in Z_2^{2k+1}}\hat{\mathcal{F}}_{g_0}(\mathbf{w}^*)\cdot\hat{\mathcal{F}}_{g_1}(\mathbf{w}^*)\cdot(-1)^{(\mathbf{0},\mathbf{w}^*)} \\ &= \frac{1}{2^{2k}}\sum_{\mathbf{w}^*\in Z_2^{2k+1}}\hat{\mathcal{F}}^2_{g_0}(\mathbf{w}^*)\cdot(-1)^{(\mathbf{a}^*,\mathbf{w}^*)} \\ &= 0\end{aligned}$$

이다. 즉, h는 $PC(1)$을 만족한다. □

❖ **정리 10** $g_0, g_1 \in \mathcal{B}_{2k+1}$을 SUC을 만족하는 범용 유사 벤트 함수의 쌍이라 하고, h_0와 h_1을 $wt(\mathbf{a}^*) = 1$로서 방법 2에 의해 각각 g_0와 g_1으로 부터 생성된 범용 유사 벤트 함수라 하면, h_0와 h_1은 SUC을 만족한다.

정리 5와 10에 의하여, $f_0 \oplus f_1$이 균형 함수이고 $PC(1)$을 만족하는 $2k$차 벤트 함수의 쌍 f_0와 f_1을 찾으면, 이들 벤트 함수의 쌍에 의하여 SUC을 만족하는 $2k+1$차 범용 유사 벤트 함수의 쌍 g_0와 g_1을 만들수 있다. 또한, 다시 이들을 이용하여 SUC을 만족하는 $2k+2$차 범용 유사 벤트 함수의 쌍 h_0와 h_1을 찾을 수 있다.

❖ **예 1** 다음의 두개의 4차 벤트 함수

$$f_1(x_1,x_2,x_3,x_4) = x_1x_3 \oplus x_1x_4 \oplus x_2x_4$$

와

$$f_2(x_1,x_2,x_3,x_4) = x_1 \oplus x_1x_2 \oplus x_1x_4 \oplus x_3x_4$$

는 $f_1 \oplus f_2$이 균형 함수이고 $PC(1)$을 만족한다. g_1과 g_2를 각각 f_1과 f_2에 의해, 4×4 단위 행렬 A와 $\mathbf{a} = (0,0,1,0) \in Z_2^4$로서, 정리 5에 의해 생성된 5차의 범용 유사 벤트 함수라 하자. 그러면

$$\begin{aligned}&g_1(x_1,x_2,x_3,x_4,x_5) \\ &\quad = x_1x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_5 \oplus x_3x_5 \oplus x_4x_5\end{aligned}$$

과

$$\begin{aligned}&g_2(x_1,x_2,x_3,x_4,x_5) \\ &\quad = x_1 \oplus x_1x_2 \oplus x_1x_4 \oplus x_3x_4 \oplus x_2x_5 \oplus x_4x_5\end{aligned}$$

는 SUC을 만족한다. 다음으로 h_1과 h_2를 각각 g_1과 g_2에 의해, $\mathbf{a} = (0,0,1,0,0) \in Z_2^5$로서, 정리 10에 의해 생성된 6차의 범용 유사 벤트 함수라 하자. 그러면

$$\begin{aligned}h_1(x_1,x_2,x_3,x_4,x_5,x_6) &= x_1x_3 \oplus x_1x_4 \oplus x_2x_4 \oplus x_5 \\ &\oplus x_3x_5 \oplus x_4x_5 \oplus x_6 \oplus x_1x_6 \oplus x_2x_6 \oplus x_5x_6\end{aligned}$$

과

$$\begin{aligned}h_2(x_1,x_2,x_3,x_4,x_5,x_6) &= x_1 \oplus x_1x_2 \oplus x_1x_4 \oplus x_3x_4 \\ &\oplus x_2x_5 \oplus x_4x_5 \oplus x_6 \oplus x_1x_6 \oplus x_3x_6 \oplus x_5x_6\end{aligned}$$

는 SUC을 만족한다. 즉 h_1, h_2, $h_1 \oplus h_2$은 모두 균형 함수이고, $PC(1)$을 만족한다.

5. 결 론

참고 문헌 [4, 12]에서 저자들은 유사 벤트 함수를 제안하였는데, 유사 벤트 함수는 균형 함수이며, 높은 비선형성을 가지고, 모든 선형 함수에 대해 거의 균일한 상관값을 가지고, 우수한 PC 특성을 가진다. 그러나, 유사 벤트 함수는 홀수차 벡터 공간에만 존재한다. 이러한 문제점을 해결하기 위하여, 본 논문에서는 유사 벤트 함수의 정의를 확장하여 모든 차수의 벡터 공간에 존재하는 범용 유사 벤트 함수를 정의하였다. 본 논문의 범용 유사 벤트 함수의 정의에 의하면, 기존의 유사 벤트 함수는 범용 유사 벤트 함수의 홀수 차 예가 된다. 그리고, 본 논문에서는 짝수차 벡터 공간에 존재하는 범용 유사 벤트 함수의 생성 방법을 소개하였다. 결과적으로 모든 차수의 벡터 공간에 존재하는 암호학적으로 우수한 특성을 가지는 범용 유사 벤트 함수를 생성할 수 있게 되었다. 범용 유사 벤트 함수는 유사 벤트 함수가 가지는 우수한 암호학적 특성을 모두 가진다. 또한, 본 논문에서는 모든 차수에서 SUC을 만족하는 부울 함수의 쌍을 발견할 수 있음을 증명하고, 그 실례를 제시하였다. 본 논문의 결과들로 인해, 차수에 관계없이 범용 유사 벤트 함수를 해쉬 함수, 스트림 암호, 블럭 암호 설계 시에 사용할 수 있다.

참 고 문 헌

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

[2] Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, 4(1):3-72, 1991.

[3] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In Joan Feigenbaum, editor, *Advances in Cryptology: CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 86-100. Springer-Verlag, Berlin, 1992.

[4] Seongtaek Chee, Sangjin Lee, and Kwangjo Kim. Semi-bent functions. In Josef Pieprzyk, editor, *Advances in Cryptology: ASIACRYPT '94*, volume 917 of *Lecture Notes in Computer Science*, pages 107-118. Springer-Verlag, Berlin, 1995.

[5] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology: EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 386-397. Springer-Verlag, Berlin, 1994.

[6] J. Pieprzyk and G. Finkelstein. Towards effective nonlinear cryptosystem design. *IEE Proceedings, Part E : Computers and Digital Techniques*, 135:325-335, 1988.

[7] Bart Preneel. *Analysis and Design of Cryptographic Hash Functions*. PhD thesis, Katholieke Universiteit Leuven, 1993.

[8] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory(A)*, 20:300-305, 1976.

[9] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. On constructions and nonlinearity of correlation immune functions. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 181-199. Springer-Verlag, Berlin, 1994.

[10] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Relationships among nonlinearity criteria(extended abstract). Im Alfredo De Santis, editor, *Advances in Cryptology: EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 376-388. Springer-Verlag, Berlin, 1995.

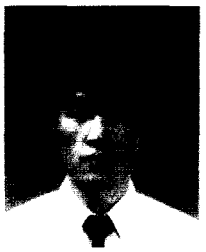
[11] T. Siegenthaler. Correlation immunity of non-linear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776-780, September 1984.

[12] 지성택, 이상진, 김광조, "확장 재생성된 부울 함수의 성질," 통신정보보호학회 논문지, 제5권, 제1호, pages 3-16, 1995.

□ 著者紹介

박 상 우

1985년 ~ 1989년 고려대학교 사범대학 수학교육과(이학사)
1989년 ~ 1991년 고려대학교 대학원 수학과(이학석사 : 응용수학 및 확률론)
1991년 ~ 현재 한국전자통신연구소 연구원



지 성 택

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

※ 관심 분야 : 암호학 및 응용 분야, M/W 통신