通信情報保護學會誌
第6卷 第3號, 1996. 9

SUC의 확장 및 범용 유사 벤트 함수에 대한 고찰

A study on SUC and generalized semi-bent functions

박 상 우*, 지 성 택*, 김 광 조*

요 약

본 논문에서는 컴퓨터 조사를 통하여, 참고 문헌[15]에서 제안된 범용 유사 벤트 함수 설계 방법이 범용 유사 벤트 함수 모두를 설계하지 못함을 보인다. 다음으로, 본 논문의 주요 결과로서, 기존 SUC [7,16]의 정의에 대해, 고려되는 부울 함수의 개수와 PC 차수를 확장시킨, 확장된 SUC을 새로이 정의하고, 확장된 SUC을 만족하는 5차 범용 유사 벤트 함수들의 예를 제시한다.

1. 서 론

정보 인증(information authemtication)과 정보 암호(data encryption)등을 위하여 필요한 암호 기술에는 암호학적으로 우수한 특성을 가지는 부울 함수(Boolean function)가 많이 사용된다. 부울 함수가 가지는 주요한 특성으로는 균등성(balancedness), 비선형성(nonlinearity), 상관면역성(correlation immunity), PC(Propagation Criterion) 특성[11]등이 있으며, 또한, 암호학적으로 우수한 특성을 가지는 부울 함수의 설계 방법이 여러 가지 제안되어왔다[5,7,8].

참고문헌 [7,16]에서, 지성택외 2인은 유사 벤트 함수(semi-bent function)라는 새로운 암호 기본 논리를 제안하였다. 그러나, 그들이 제안한 유사 벤트 함수는 암호학적 특성이 우수한 반면 홀수차 벡터 공간에만 존재하는 단점을 가진다. 이를 해결하기 위해서, 참고 문헌 [15]에는 모든 차수에서 정의되는 범용 유사 벤트 함수(generalized semi-bent function)를 정의하고, 그 설계 방법을 제안하였다. 참고 문헌 [15]에 제안된 범용 유사 벤트 함수는 균등 함수이며, 비선형성이 우수하고, 선형 함수에 대해서 거의 균일한 상관값을 가지고, 우수한 PC 특성을 가진다. 또한, 범용 유사 벤트 함수를 이용하면, 차수에 관계없이 SUC(Strict Uncorrelated Criterion) [7,16]을 만족하는 부울 함수의 쌍을 찾을 수 있다. 그러나, SUC은 단지 두개의 부울 함수의 관계만을 고려하기 때문에 블록 알고리즘의 기본 논리로서 주로 사용되는 S(ubstitution)-box 설계시에 적용하기에는 매우 약한 개념이다. 왜냐

* 한국전자통신연구소

하면, S-box가 입·출력 변화 공격법(differential attack) [2,3,4]과 선형 공격법(linear attack) [8]에 강하기 위해서는 S-box의 성분 함수(component function)들의 모든 선형 결합(linear combination)들의 암호학적 특성이 우수하여야 한다.

본 논문에서는 우선 컴퓨터 조사를 통하여, 참고 문헌 [15]에 제안된 범용 유사 벤트 함수 설계 방법이 범용 유사 벤트 함수 모두를 설계하지 못함을 보인다. 다음으로, 본 논문의 주요 결과로서, 기존 SUC의 정의에 대해, 고려되는 부울 함수의 개수와 PC 차수를 확장시킨, 확장된 SUC을 새로이 정의하고, 확장된 SUC을 만족하는 5차 범용 유사 벤트 함수들의 예를 제시한다. 본 논문에서 새로이 제안하는 SUC은 입·출력 변화 공격법에 강한 S-box 설계 시에 응용될 수 있다.

2. 예비 사항

Z_2^n을 $GF(2)$위의 n차 벡터 공간이라 하자. $x = (x_1, \ldots, x_n)$과 $y = (y_1, \ldots, y_n)$를 Z_2^n의 두 벡터라 하면, x와 y의 내적은 $(x, y) = x_1y_1 \oplus \ldots \oplus x_ny_n$ 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 B_n으로 표시한다. $f(x) = lw(x) \oplus c = x_1w_1 \oplus \ldots \oplus x_nw_n \oplus c$가 되는 벡터 $w \in Z_2^n$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 $x \in Z_2^n$의 해밍 무게(Hamming weight)는 x에서 '1'의 개수이며, $wt(x)$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,

$$(f \oplus g)(x) = f(x) \oplus g(x)$$

이고,

$$(f \| g)(x^*) = (f \| g)(x, x_{n+1}) = (1 \oplus x_{n+1})f(x) \oplus x_{n+1}g(x),\ x^* \in Z_2^{n+1}$$

이다. 다음은 왈시-하다마드 변환(Walsh-Hadamard transform)의 정의이다.

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

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

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

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

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

$$\mathcal{N}_f = \min d(f, \lambda_n).$$

높은 비선형치는 DES(Data Encryption Standard) [9]형 블록 알고리즘 설계시 고려해야 할 필수 요소이며, S-box가 선형 공격법

[8]에 견디기 위해서는 S-box의 각 구성 함수들의 모든(0을 제외한) 선형 결합의 비선형치가 높아야 한다[13].

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

스트림 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) [14]에 강한 함수가 필요하다.

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

$$d(f, lw) = 2^{n-1}$$

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 [11]는 SAC(Strict Avalanche Criterion)의 정의를 확장한 개념으로 우수한 PC 특성을 가져야 함은 블록 암호 알고리즘이 입·출력 변화 공격법 [2,3,4]에 강하기 위한 필수 조건이다.

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

■ **정리 1** (Parseval의 정리)

부울 함수 $f \in \mathcal{B}_n$에 대해서

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

이다.

■ **정의 6** 모든 $w \in Z_2^n$에 대해서

$$|\hat{\mathcal{F}}_f(w)| = 2^{n/2}$$

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 $w \in Z_2^n$에 대해서, 벤트 함수 f와 선형 함수 lw의 상관값은 $\pm 2^{n/2}$이다. 그리고, 벤트 함수의 비선형치는 $\mathcal{N}_f = 2^{n-1} - 2^{\lfloor n/2 \rfloor}$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.

3. 범용 유사 벤트 함수

본 장에서는 범용 유사 벤트 함수의 정의와 균등성, 비선형성, 상관 무결성등과 같은 암호학적 특성을 소개한다[13].

■ **정의 7** $|\hat{\mathcal{F}}_f(w)| = 0$ 또는 $2^{\lfloor n/2 \rfloor + 1}$이고, $\hat{\mathcal{F}}_f(0) = 0$인 부울 함수 $f \in \mathcal{B}_n$를 범용 유사 벤트 함수라 한다. 여기서, $\lfloor m \rfloor$는 m보다 같거나 작은 정수 중 가장 큰 정수이다.

■ **정리 2** 범용 유사 벤트 함수 $f \in \mathcal{B}_n$의 암호학적 성질은 다음과 같다.

1) f는 균등 함수이다.
2) $\mathcal{N}_f = 2^{n-1} - 2^{\lfloor n/2 \rfloor}$

3) 모든 $w \in Z_2^n$에 대해서, f와 선형 함수 l_w의 상관값은 0 또는 $\pm 2^{\frac{n+2+(n \bmod 2)}{2}}$이다. 그리고, $\#\{w \in Z_2^n \mid c(f, l_w) = \pm 2^{\frac{n+2+(n \bmod 2)}{2}}\} = 2^{n-2+(n \bmod 2)}$이다.

◆ 증명

1) 정의 7에 의해 자명하다.

2) 보조 정리 2에 의해서,

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

이다.

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

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

$$= 0 \text{ 또는 } \pm 2^{-k}$$

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

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

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

$$= 0 \text{ 또는 } \pm 2^{-k}$$

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

정리 2에 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 [10]에서 $2k+1$차 균등 부울 함수가 가지는 최대 비선형치로 주장한 바 있다[1]. 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.

4. 범용 유사 벤트 함수의 개수

본 장에서는 범용 유사 벤트 함수의 설계 방법을 소개하고, 홀수차 범용 유사 벤트 함수 설계 방법이 5차인 경우에, 5차의 모든 범용 유사 벤트 함수를 설계하지 못함을 컴퓨터 조사를 통하여 밝힌다. 다음은 홀수차 범용 유사 벤트 함수 설계 방법이다.

방법 1 $f_0 \in \mathcal{B}_{2k}$를 벤트 함수, $a \in Z_2^{2k}$ 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.

$$f_1(x) = f_0(Ax \oplus a) \oplus 1,$$

$$g = f_0 \| f_1$$

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

다음은 짝수차 범용 유사 벤트 함수 설계 방법이다.

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

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

$$h = g_0 \| g_1.$$

그러면, h는 Z_2^{2k}상에 정의된 범용 유사 벤트 함수이다.

제안된 범용 유사 벤트 함수의 설계 방법이 실제로 모든 범용 유사 벤트 함수를 설계하는지를 확인하기 위하여, 5차인 경우를 예로 하여, 먼저, 4차 벤트 함수로부터 방법 1을 사용하여 설계할 수 있는 모든 범용 유사 벤트 함수의 수를 컴퓨터 조사를 통하여 직접 조사하였다. 다음으로, 5차의 부울 함수 중 정의 7을 만족하는 부울 함수의 수를 전수 조사하였다. 그 결과는 표 1과 같다.

표 1 5차 범용 유사 벤트 함수의 개수

전수조사	방법 1
$7,027,328 = 2^{22.75}$	$172,032 = 2^{17.39}$

표 1에 의하면, 방법 1에 의하여 설계된 5차 범용 유사 벤트 함수의 수는 전수 조사에 의하여 얻은 5차의 모든 범용 유사 벤트 함수의 수보다 적다. 따라서, 방법 1에 의하여 5차의 범용 유사 벤트 함수 모두를 설계할 수 없으며, 방법 2에 의하면, 5차의 범용 유사 벤트 함수로부터 6차의 범용 유사 벤트 함수를 설계하므로, 방법 2에 의하여, 모든 6차의 범용 유사 벤트 함수를 설계할 수 없게 된다. 즉, 보다 많은 또는 범용 유사 벤트 함수 모두를 설계할 수 있는 설계 방법이 필요하다.

5. Strict Uncorrelated Criterion의 확장

Biham과 Shamir는 DES 형 알고리즘에 대한 효과적인 공격방법으로, 입·출력 변화 공격법 [2,3,4]을 제안하였다. $F = (f_1, f_2, \ldots, f_m)$를 각 성분 함수가 $f_i \in \mathcal{B}_n$, $i = 1, 2, \ldots, m$, $m \geq 2$인 길이가 m인 벡터 부울 함수라 하자. F의 입·출력 변화 공격법에 대한 안전성을 분석하기 위하여, 집합

$$\mathcal{D}_F(a, b) = \{x \in Z_2^n \mid F(x \oplus a) \oplus F(x) = b\},$$
$$a \in Z_2^n - \{0\},\ b \in Z_2^m$$

에 대해,

$$\delta_F(a, b) = \#\mathcal{D}_F(a, b).$$

이 필요하며, 다음을 벡터 부울 함수 F의 입출력 변화 공격법에 대한 안전성의 척도(differential resistance)로 삼는다.

$$\Delta(F) = \max \delta_F(a, b)$$

벡터 부울 함수 F가 입·출력 변화 공격법에 대하여 안전하기 위해서는 $\Delta(F)$가 충분히 작아야 하며, 벡터 부울 함수 F의 $\Delta(F)$가 최소일 경우, F는 입·출력 변화 공격법에 대하여 내성을 가진다고 한다(differential resistant)[6]. F의 성분 함수의 모든 선형 결합이 균등 함수이고, PC(1)을 만족하면, $wt(a) = 1$인 a에 대한 $\delta_F(a, b)$는 최소화 될 수 있다. 그리고, F의 성분 함수의 모든 선형 결합이 균등 함수이고, 높은 차수의 PC를 만족하면, F의 각 성분 함수들의 선형 결합이 PC를 만족하는 모든 $a \in Z_2^n$에 대해서, $\delta_F(a, b)$가 최소화된다. 따라서, S-box를 설계할 때, S-box를 구성하는 성분 함수들의 모든 선형 결합에 대하여 암호학적 성질을 고려하여야 한다.

참고 문헌 [7]에서, 저자들은 두개의 부울 함수 사이의 암호학적 관계에 대한 개념으로 SUC을 제안하였는데, 이들이 제안한 SUC은 입력의 임의의 한 비트가 변화하였을 때 두개 부울 함수 사이의 출력 무상관성을 제공한다. 참고 문헌 [7]에 제안된 SUC의 정의는 다음과 같다.

부울 함수 f, g 그리고, $f \oplus g$가
모두 균등 함수이고, PC(1)을 만족하면,
f와 g는 SUC을 만족한다.

그러나, 이들이 제안한 SUC은 고려된 PC 차수가 1이고, 단지 두개의 부울 함수 사이의 관계만을 다루므로, S-box 설계 시에 적용하기에는 매우 약한 개념이다. 따라서, SUC을 S-box 설계 시 활용하며, 입·출력 변화 공격법에 대해 보다 강한 의미를 부여하기 위해서는 부울 함수의 수를 두개에서 가능한 많은 수로 늘리고, 고려되는 PC 차수 또한, 1에서 가능한 높게 하여야 한다. 그러나, n차 균등 부울 함수가 만족할 수 있는 PC 차수는 n에 의존하므로, PC 차수의 확장에는 한계가 있다. 이러한 사실을 바탕으로 SUC을 다음과 같이 확장한다.

■ **정의 8** $F = (f_1, f_2, \ldots, f_m)$를 각 성분 함수가 $f_i \in \mathcal{B}_n$, $i = 1, 2, \ldots, m$, $m \geq 2$인 m차 벡터 부울 함수라 하자. F의 모든 성분 함수 f_i의 모든 선형 결합이 균등 함수이고, 한 점을 제외하고 PC를 만족하면, F는 $SUC(n, m)$을 만족한다.

F가 $SUC(n, m)$을 만족하면, $\delta_F(a, b)$는 모든 $a \in Z_2^n - \{0\}$와 $b \in Z_2^m$에 대하여, 균등한 값을 가지게 된다. 따라서, $\Delta(F)$가 최소값에 가까워지게 된다. 컴퓨터 조사를 통하여, $n = m = 5$인 경우에 $SUC(5,5)$을 만족하는 F의 예를 찾았다.

예 1 5차 부울 함수 f_1, f_2, f_3, f_4, f_5를

$$f_1(x_1, x_2, x_3, x_4, x_5) = x_1 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1x_5$$

$$f_2(x_1, x_2, x_3, x_4, x_5) = x_1x_2 \oplus x_3 \oplus x_4 \oplus x_1x_4 \oplus x_5 \oplus x_4x_5$$

$$f_3(x_1, x_2, x_3, x_4, x_5) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_5 \oplus x_1x_5 \oplus x_3x_5 \oplus x_4x_5$$

$$f_4(x_1, x_2, x_3, x_4, x_5) = x_2 \oplus x_3 \oplus x_4 \oplus x_3x_4 \oplus x_5 \oplus x_1x_5 \oplus x_3x_5$$

$$f_5(x_1, x_2, x_3, x_4, x_5) = x_1x_3 \oplus x_2x_3 \oplus x_4 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1x_5 \oplus x_2x_5 \oplus x_3x_5 \oplus x_4x_5$$

라 하면, $F = (f_1, f_2, f_3, f_4, f_5)$는 $SUC(5,5)$를 만족하며, 각 $f_i \in \mathcal{B}_5$들은 범용 유사 벤트 함수이다. 또한, $\Delta(F)$는 2이며, 따라서, F는 입·출력 변화 공격법에 대하여 내성을 가진다.

n이 짝수인 경우에, $SUC(n, n)$을 만족하는 F를 찾는 것은 매우 어려운 일이다. 실제로, $m = n$이 짝수인 경우에, 최소 입·출력 변화 균등치는 알려져 있지 않으며, 이 경우에 입·출력 변화 균등치가 2인 이차 치환(quadratic permutation)은 존재하지 않는 것이 증명되어 있다[13]. 이러한 결과로 볼 때, 짝수 n에 대해서, $SUC(n, n)$을 만족하는 F를 찾는 것은 매우 어려운 일이다. 따라서, n이 짝수인 경우에는, $SUC(n, m)$에서 m이 n보다 작은 경우를 고려하여야 하는데, $m \leq n/2$인 경우를 고려하는 것이 바람직할 것이다.

6. 결 론

지금까지 본 논문에서는 컴퓨터 조사를 통하여, 참고 문헌 [15]에 제안된 범용 유사 벤트 함수 설계 방법이 범용 유사 벤트 함수 모두를 설계하지 못함을 보이고, 보다 많은 또는 범용 유사 벤트 함수 모두를 설계할 수 있는 설계 방법이 필요함을 지적하였다. 또한, 본 논문의 주요 결과로서, 기존 SUC의 정의에 대해, 고려되는 부울 함수의 개수와 PC 차수를 확장시킨, 확장된 SUC을 새로이 정의하고, 확장된 SUC을 만족하는 5차 범용 유사 벤트 함수들의 예를 제시하였다. 그리고, 예를 통하여,

본 논문에서 제안한 새로운 *SUC*은 입·출력 변화 공격법에 강한 S-box 설계 시에 응용될 수 있음을 보였다. 향후에는 *SUC*(n, m)을 만족하는 길이가 m인 범용 유사 벤트 함수들의 벡터 부울 함수의 최대 길이를 찾는 연구와, 모든 범용 유사 벤트 함수 설계 방법에 대한 연구를 수행할 것이다. 또한, 새로이 제안한 *SUC*이 선형 공격법에는 불충분하므로, 이를 보완할 수 있는 방안을 연구할 계획이다.

참 고 문 헌

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

[3] Eli Biham and Adi Shamir. Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. Technical Report CS91-18, Wiezmann Institute of Science, 1991.

[4] Eli Biham and Adi Shamir. Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer. In Joan Feigenbaum, editor, *Advances in Cryptology: CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 156-171. Springer-Verlag, Berlin, 1992.

[5] 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.

[6] Florent Chabaud and Serge Vaudenay. Links between differential and linear cryptanalysis. In Alfredo De Santis, editor, *Advances in Cryptology: EUROCRYPT'94*, volume 950 of *Lecture Notes in Computer Science*, pages 356-365. Springer-Verlag, Berlin, 1995.

[7] 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.

[8] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *Advances in Cryptology: EUROCRYPT'93*, volume 765 of *Lecture Notes in Computer Science*, pages 386-397. Springer-Verlag, Berlin, 1994.

[9] National Bureau of Standards. FIPS PUB} 46 : Data Encryption Standard, January 1977.

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

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

[12] Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. On constructions and nonlinearity of correlation immune functions. In Tor Helleseth, editor,

Advances in Cryptology - EUROCRYPT'93, volume 765 of *Lecture Notes in Computer Science*, pages 181-199. Springer-Verlag, Berlin, 1994.

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

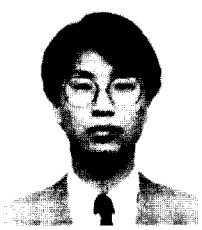
[14] T. Siegenthaler. Correlation immunity of non-linear combining functions for cryptographic applications. *IEEE Transactions on Information Theory*, IT-30(5):776-780, September 1984.

[15] 박상우, 지성택, 김광조. Semi-bent 함수의 일반화와 구성 방법. 통신정보보호학회 논문지, 투고중.

[16] 지성택, 이상진, 김광조. 확장 재생성된 부울 함수의 성질. 통신정보보호학회 논문지, 제 5 권, 제 1 호, pages 3-16, 1995.

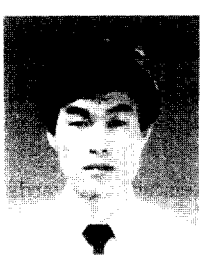
□ 著者紹介

박 상 우



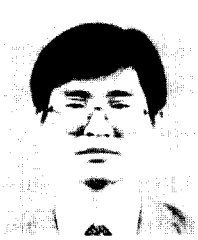
1985년 ~ 1989년 고려대학교 사범대학 수학교육과(이학사)
1989년 ~ 1991년 고려대학교 대학원 수학과(이학석사 : 응용수학 및 확률론)
1991년 ~ 현재 한국전자통신연구소 연구원

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