通信情報保護學會論文誌
第5卷 第1號, 1995. 3

확장 재생성된 부울 함수의 성질

지 성 택*, 이 상 진**, 김 광 조***

On recursively extended Boolean functions

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

요 약

본 논문에서는 저차의 부울 함수를 연접시켜 고차의 부울 함수를 생성하는 방법을 소개하고, 이러한 방법으로 생성된 함수의 균등성, 비선형성, 무상관도 등의 제반 성질을 새롭게 규명한다. 또한, 두 함수 사이의 "uncorrelated" 개념을 확장하여 Differential Cryptanalysis에 강한 S-box가 가져야 할 필요조건으로 Strict Uncorrelated Criterion(SUC) 개념을 정의하고, 이를 만족하는 부울 함수를 제시하여 그 존재성을 밝히고 특히, 특수한 형태의 연접으로 생성한 함수가 이를 유지함을 보인다. 그리고, Walsh-Hadamard 변환을 이용하여 부울 함수의 상관관계 특성을 조사하여 이를 연접 방식으로 확장 재생성한 부울 함수에 적용, 이들 함수의 상관관계 특성을 규명한다. 더불어 bent 함수들의 연접으로 홀수차 벡터공간 위에서 semi-bent 함수를 정의하고 이 함수에 대한 상관관계 특성과 비선형치를 규명함과 동시에 SUC을 만족함을 증명하며 연접 방식에 의해서 확장 재생성된 다른 형태의 부울 함수와 비교하여 semi-bent 함수의 암호학적 우수성을 입증한다.

Abstract

In this paper, we deal with the cryptographic properties of Boolean functions generated by recursively extended methods from the points of balancedness, nonlinearity and correlation properties. First, we propose a new concept "Strict Uncorrelated Criterion(SUC)" for two Boolean functions as a necessary condition for constructing Boolean functions of S-box which can be guaranteed to be resistant against Differential cryptanalysis, then we show that the recurively extended Boolean functions with particular form preserve the SUC. We also examine the correlation properties of Boolean

* 한국전자통신연구소 선임연구원
** 한국전자통신연구소 선임연구원
*** 한국전자통신연구소 실장

functions using Walsh-Hadamard transformations and apply them to discuss nonlinearity, correlation properties and SUC of semi-bent function which is defined over odd dimensional vector space. Finally, we compare semi-bent function with Boolean functions which are generated by other similar recursive methods.

1. 서 론

부울 함수는 스위칭 이론, 오류 정정 부호 이론뿐만 아니라 암호학에서도 블럭 암호의 핵심 논리, 스트림 암호의 비선형 결합 논리 등으로 널리 응용된다[6]. 이러한 부울 함수가 암호에 응용되기 위해서는 균등성, 높은 비선형성, 입력과 출력간의 독립성, 입력의 변화에 대한 출력의 변화도 등 여러가지 특성을 가지고 있어야 한다(본 논문에서는 암호에 이용되는 부울 함수로 한정한다).

최근 암호학에서는 이러한 성질을 만족하는 부울 함수를 생성하는 연구가 활발히 진행되었고[12, 5, 3, 2, 10], 특히 이들 대부분의 방법은 모두 저차의 부울 함수를 연접하여 고차의 부울 함수를 생성하는 방법들이다.

예를들면, Sigenthaler는 n차원 벡터공간 Z_2^n 위에서 m차 무상관 부울 함수를 연접하여 $n+1$차원 벡터공간 Z_2^{n+1} 위의 m차 무상관 부울 함수 생성 방법을 제안하였고[12], Kim, Matsumoto, Imai(이하 KMI라 함)는 Strict Avalanche Criterion(SAC)을 만족하는 Z_2^n 위의 부울 함수를 이용하여 Z_2^{n+1} 위에서 SAC을 만족하는 부울 함수 생성 방법을 제안하였다[3], 그러나 Sigenthaler와 KMI의 방법은 확장된 부울 함수의 무상관도를 증가시키지 못하며, 특히 KMI의 방법은 최대 비선형치를 유지하지 않는 단점이 있다. 한편 KMI가 제안한 방법을 일반화시키면 Camion의 방법[2]을 유도할 수 있고, 또 이 방법은 Sigenthaler와 KMI의 방법과는 다르게 무상관도를 증가시키는 방법이지만 특정한 경우 이외에는 성립하지 않는다.

부울 함수가 일반적으로 블럭 암호에 이용되기 위해서는 부울 함수들 간의 상관관계 특성이 우수해야 한다. 최근 Seberry는 두 부울 함수 사이에 "uncorrelated"라는 개념을 정의하였으나[10], 이 개념으로는 DES 형태 블럭 암호의 공격 방법 중의 하나인 Differential Cryptanalysis(DC)[4]에 강한 부울 함수를 생성할 수 없기 때문에 좀더 엄격한 조건이 필요하다. 따라서 Strict Uncorrelated Criterion(SUC)이란 새로운 개념을 정의하고, KMI의 방법으로 생성된 부울 함수들이 SUC을 유지함을 증명한다. 본 논문에서 정의한 SUC을 n개의 부울 함수에 확장 적용하여 S-box(치환)를 생성할 수 있는 지는 현재까지 미해결 문제지만, 일반적으로 SUC을 만족하는 부울 함수들로 구성된 S-box는 DC 관점에서 강하기 때문에 매우 의미있는 개념이라 할 수 있다.

끝으로 상관관계 특성이 우수한 Z_2^{2n} 위의 bent 함수를 이용하여 Z_2^{2n+1} 위의 부울 함수를 생성하고(bent 함수를 이용하여 홀수차 벡터 공간 위의 부울 함수를 생성하는 방법은 본 논문과 다르게 [10]에 제안되어 있다), 이 방법에 의해서 생성된 부울 함수는 최대 비선형치를 갖고, bent 함수의 단점인 균등성 문제를 해결하고 bent 함수가 지닌 우수한 상관관계 특성을 유지함과 동시에 SUC을 만족함을 증명한다.

본 논문의 구성은 다음과 같다. 우선 2장에서는 기본적인 기호와 용어를 정의하고, 3장에서는 KMI의 방법을 소개하고 이 방법으로 생성된 부울 함수의 새로운 성질을 밝힌다. 4장에서는 Walsh-Hadamard 변환을 이용하여 부울 함수의 상관관계 특성을 규명하고 Camion의 방법에 의해서 생성된 부울 함수의 특성 및 Z_2^{2n+1} 위의 부울 함수를 생성하고 이 함수의 비선형성 및 상관관계 특성을 규명하고 SUC을 만족함을 증명한다. 5장에서는 4장에서 제시한 방법에 의해 생성한 부울 함수를 연접 방법에 의해서 생성된 다른 부울 함수와 균등성,

비선형성, SAC, 상관관계 특성, SUC 관점에서 비교한 결과를 제시하고 끝으로 결론을 맺는다.

2. 기호 및 용어 정의

본 논문에서 사용하는 기호는 다음과 같다.

- Z_2 : 2개의 원소로 구성된 갈로아 체(Galois field).
- R : 실수 전체의 집합.
- Z_2^n : Z_2 위의 n차원 벡터공간이고, 원소를 $\mathbf{x} = (x_1, \cdots, x_n)$로 표시.
- $(\mathbf{x},\mathbf{y}) = x_1y_1 \oplus \cdots \oplus x_ny_n$
- B_n : 부울 함수 $f : Z_2^n \rightarrow Z_2$들의 집합.
- $L_n = \{l_{\mathbf{w}} \in B_n \mid l_{\mathbf{w}}(\mathbf{x}) = x_1w_1 \oplus \cdots \oplus x_nw_n\}$: L_n의 원소를 선형(linear)이라 함.
- $\Lambda_n = \{\lambda \in B_n \mid \lambda(\mathbf{x}) = l_{\mathbf{w}}(\mathbf{x}) \oplus b,\ l_{\mathbf{w}} \in L_n,\ b \in Z_2\}$: Λ_n의 원소를 affine이라 함.
- $wt(\mathbf{x})$: $\mathbf{x}$의 해밍 weight.
- $wt(f) = \#\{\mathbf{x} \in Z_2^n \mid f(\mathbf{x}) = 1\}$.
- $d(f,g) = \#\{\mathbf{x} \in Z_2^n \mid f(\mathbf{x}) \neq g(\mathbf{x})\}$: 부울 함수 f와 g 사이의 거리(distance).
- $(f \oplus g)(\mathbf{x}) = f(\mathbf{x}) \oplus g(\mathbf{x})$.
- $(f \| g)(\mathbf{x},x_{n+1}) = (1 \oplus x_{n+1})f(\mathbf{x}) \oplus x_{n+1}g(\mathbf{x})$: 함수 $f,\ g \in B_n$의 연접(concatenation).

일반적으로 암호 논리는 비선형 함수, 즉 선형이나 affine이 아닌 함수를 사용하며, 부울 함수에 대한 비선형의 정도를 가늠하는 측도도 여러가지 제안되어 있다[5, 6, 7, 8]. 또한 암호 논리로 사용되기 위해서는 비선형성 이외에 필요한 특성이 여러가지 있으나 먼저 다음을 정의하기로 한다.

■ 정의 2.1 $f \in B_n$이라 하자.

- $\#\{\mathbf{x} \in Z_2^n \mid f(\mathbf{x}) = 0\} = \#\{\mathbf{x} \in Z_2^n \mid f(\mathbf{x}) = 1\}$일 때 균등(balanced)이라 함.
- $\mathcal{N}_f = min\{d(f,\lambda_n) \mid \lambda_n \in \Lambda_n\}$를 f의 비선형치(nonlinearity)라 함.
- $wt(\alpha) = 1$인 모든 $\alpha \in Z_2^n$에 대해서

$$\sum_{\mathbf{x} \in Z_2^n} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \alpha) = 2^{n-1}$$

이면 SAC(Strict Avalanche Criterion)을 만족한다고 함.

- $1 \leq wt(\mathbf{w}) \leq m$인 모든 $\mathbf{w} \in Z_2^n$에 대하여 $d(f,l_{\mathbf{w}}) = 2^{n-1}$이면 m차 무상관(m-th order correlation immune)함수라고 함.

균등성의 조건은 입력의 모든 변화에 대해 출력값이 0이나 1로 치중(bias)되지 않기 위한 필요조건이며, 암호 논리로 사용되는 대부분의 부울 함수가 균등함수이다. 그리고 무상관성은 스트림 암호의 분석 방법 중 상관관계 공격 방식에 대비하기 위한 필요조건이다.

3. 연접 부울 함수의 성질

본 장에서 KMI의 생성 방법[3] 및 특성을 소개하고 연접 부울 함수가 갖는 비선형치, 상관성 및 SUC과 관련된 새로운 성질을 고찰하고 증명한다.

3.1 KMI 방법

■ 정의 3.1 [3] 함수 $f \in B_n$과, $k \in \{1, 2, \cdots, n\}$, $b \in Z_2$에 대하여 변환된 함수 $t_b^k[f] : Z_2^n \rightarrow Z_2^n$를 다음과 같이 정의하자.

$$t_b^k[f](\mathbf{x}) = f(\mathbf{x} \oplus c_k^{(n)}) \oplus b$$

여기서,

$$c_k^{(n)} = \underbrace{(0, 0, \cdots, 0, \overset{k}{\hat{1}}, 0, \cdots, 0)}_{n}$$

을 의미한다. 이제 확장된 함수 $D_b^k[f] : Z_2^{n+1} \rightarrow Z_2$를 다음과 같이 정의한다.

$$\begin{cases} D_b^k[f](\mathbf{x},0) = f(\mathbf{x}) \\ D_b^k[f](\mathbf{x},1) = t_b^k[f](\mathbf{x}), \ \mathbf{x} \in Z_2^n. \end{cases}$$

※ 참고 3.1 $D_b^k[f]$는 f와 $t_b^k[f]$의 연접함수이다. 즉,

$$D_b^k[f] = f \parallel t_b^k[f]$$

특정한 조건을 만족하는 부울 함수들의 집합을 다음과 같이 표기한다.

- *BAL* : 균등함수들의 집합
- *NLIN* : 비선형 함수들의 집합
- *SAC* : SAC을 만족하는 함수들의 집합
- *CI*(m) : m차 무상관 함수들의 집합

특별히 B_n의 부분 집합임을 나타낼 때(Z_2^n 위에 정의된 부울 함수)는 첨자 n을 첨부하여 구별한다.

3.2 Strict Uncorrelated Criterion

우수한 부울 함수는 스트림 암호에서 그 단독으로 의미가 있지만, 블럭 암호에서는 부울 함수들 간의 상호 관계도 우수해야 함은 DC(Differential Cryptanalysis)[4]에 강하기 위한 필요조건이다. Seberry는 부울 함수를 이용하여 DC에 강한 S-box를 생성하기 위하여 S-box를 구성하는 부울 함수의 필요조건으로 다음과 같은 정의를 하였다.

■ 정의 3.2 [9] 두 부울 함수 f, g에 대하여 f, $g \in BAL \cap NLIN$이고 $f \oplus g \in BAL \cap NLIN$일 때, f와 g는 서로 uncorrelated되어 있다고 한다.

[1]에 의하여 두 부울 함수의 EXOR가 선형일 때, 두 부울 함수의 출력은 1의 확률로 상관관계가 존재하기 때문에 정의 3.2는 의미가 있지만 uncorrelated 되어 있는 두 부울 함수 사이에도 상관관계는 여전히 존재한다(1보다 작은 확률로). 정의 3.2에서 비선형성을 SAC으로 대체하면 부울 함수 사이의 상관관계는 존재하지 않기 때문에 (확률 $\frac{1}{2}$), uncorrelated를 강화한 새로운 개념을 정의하기로 한다.

■ 정의 3.3 두 함수 f, $g \in B_n$가 *SUC(Strict Uncorrelated Criterion)*을 만족한다 함은

1. f, $g \in BAL \cap SAC$이고
2. $f \oplus g \in BAL \cap SAC$

을 만족할 때이다. 이러한 경우에 (f, g) $\in$ *SUC*으로 표기한다.

정의 2.1에 의하면 정의 3.3을 만족하는 부울 함수들로 구성된 S-box의 EXOR Table은 균등하게 분포되어 DC에 강한 부울 함수의 필요조건이다.

예 3.1 다음은 Z_2^4 위에 정의된 *SUC*을 만족하는 부울 함수 쌍이다. 즉,

$$(f_i, f_j) \in SUC, \ 1 \le i, j \le 4, \ i \ne j.$$

- $f_1(x_1,x_2,x_3,x_4) = x_1x_3 \oplus x_2x_3 \oplus x_4 \oplus x_1x_4 \oplus x_2x_4$
- $f_2(x_1,x_2,x_3,x_4) = x_1x_2 \oplus x_3 \oplus x_1x_3 \oplus x_2x_4 \oplus x_3x_4$
- $f_3(x_1,x_2,x_3,x_4) = x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_4 \oplus x_2x_4$
- $f_4(x_1,x_2,x_3,x_4) = x_1 \oplus x_1x_2 \oplus x_3 \oplus x_1x_3 \oplus x_4 \oplus x_1x_4$

그러나 여기서 정의한 SUC을 만족하는 함수를 n개의 부울 함수에 확장 적용하여 S-box(치환)를 생성할 수 있는 지는 현재까지 미해결 문제지만, 일반적으로 SUC을 만족하는 부울 함수들로 구성된 S-box는 DC 관점에서 강하기 때문에 매우 의미있는 개념이라 할 수 있다. 다음의 S는 위의 4개의 부울 함수를 이용하여 구성한 Z_2^4 위의 S-box로($S = (f_4, f_3, f_2, f_1)$) 입,출력 상관관계 측면에서 매우 우수한 특성이 있을 뿐만아니라 DC 특성도 우수하다.

S : (0 1 2 3 4 5 6 7 8 9 a b c d e f)
→ (0 8 4 2 a 9 b 6 d c e 1 5 f 3 7)

3.3 KMI 방법에 의해서 생성된 부울 함수의 특성

본 절에서는 정의 3.1에서 제시된 함수의 특성을 조사하기로 한다.

❖ 정리 3.1 [3] $f \in B_n$이고, $k \in \{1, 2, \cdots, n\}$, $b \in Z_2$이라 하자. $f \in SAC_n$이면 $D_b^k[f] : Z_2^{n+1} \to Z_2 \in SAC_{n+1}$이다.

$D_b^k[f]$로 생성된 함수는 정리 3.1과 같은 SAC 이외에도 여러가지 성질들을 보존하는데, 이를 규명하기 이전에 다음의 보조정리들을 증명하자.

보조정리 3.1 임의의 $l_{\mathbf{w}^*} \in L_{n+1}$과 $k \in \{1, \cdots, n\}$에 대하여

$$D_b^k[l_{\mathbf{w}}] = l_{\mathbf{w}^*}$$

을 만족하는 적당한 $l_{\mathbf{w}} \in L_n$과 $b \in Z_2$가 존재한다.

(증 명) $\mathbf{w}^* = (w_1, \cdots, w_{n+1})$일 때 $\mathbf{w} = (w_1, \cdots, w_n) \in Z_2^n$이라 하면, 다음을 만족한다.

$$l_{\mathbf{w}}(\mathbf{x}) = l_{\mathbf{w}^*}(\mathbf{x},0),\ \mathbf{x} \in Z_2^n.$$

이제 $b = l_{\mathbf{w}^*}(c_{n+1}^{(n+1)}) \oplus l_{\mathbf{w}}(c_k^{(n)})$라 하면 $\mathbf{x} \in Z_2^n$에 대해 다음 식이 성립한다.

$$D_b^k[l_{\mathbf{w}}](\mathbf{x},0) = l_{\mathbf{w}}(\mathbf{x}) = l_{\mathbf{w}^*}(\mathbf{x},1). \quad (1)$$

또한,

$$\begin{aligned} D_b^k[l_{\mathbf{w}}](\mathbf{x},1) &= l_{\mathbf{w}}(\mathbf{x} \oplus c_k^{(n)}) \oplus b \\ &= l_{\mathbf{w}}(\mathbf{x} \oplus c_k^{(n)}) \oplus l_{\mathbf{w}^*}(c_{n+1}^{(n+1)}) \\ &\quad \oplus l_{\mathbf{w}}(c_k^{(n)}) \\ &= l_{\mathbf{w}}(\mathbf{x}) \oplus l_{\mathbf{w}^*}(c_{n+1}^{(n+1)}) \\ &= l_{\mathbf{w}^*}(\mathbf{x},0) \oplus l_{\mathbf{w}^*}(c_{n+1}^{(n+1)}) \\ &= l_{\mathbf{w}^*}(\mathbf{x},1),\ \mathbf{x} \in Z_2^n. \end{aligned} \quad (2)$$

식 (1)과 (2)에 의해서 $D_b^k[l_{\mathbf{w}}] = l_{\mathbf{w}^*}$. □

보조정리 3.1에서 선형인 경우를 affine으로 확장하면 다음을 얻는다.

보조정리 3.2 임의의 $\lambda^* \in \Lambda_{n+1}$와 $k \in \{1, \cdots, n\}$, $b \in Z_2$에 대하여

$$D_b^k[\lambda] = \lambda^*$$

을 만족하는 적당한 $\lambda \in \Lambda_n$이 존재한다.

(증 명) 보조정리 3.1의 증명에서 $l_{\mathbf{w}}$을 $l_{\mathbf{w}} + 1 \in \Lambda_n$으로 대치하면 된다. □

이제 $D_b^k[f]$의 비선형성 및 상관관계에 대한 성질을 조사하기로 한다.

보조정리 3.3 $f \in BAL_n$이면 모든 $k \in \{1, \cdots, n\}$, $b \in Z_2$에 대하여 $D_b^k[f] \in BAL_{n+1}$이다.

(증 명) $wt(t_b^k[f]) = wt(f)$이고 $f \in BAL_n$이므로 $D_b^k[f] \in BAL_{n+1}$. □

보조정리 3.4 $f \in B_n$, $k \in \{1, \cdots, n\}$라 하면 $wt(D_0^k[f]) = 2wt(f)$이다.

(증 명) $wt(t_b^k[f]) = wt(f)$이고 $wt(D_0^k[f]) = wt(f) + wt(t_b^k[f])$이므로 자명하다. □

보조정리 3.5 f, $g \in B_n$, $k \in \{1, \cdots, n\}$, $b \in Z_2$라 하면 다음이 성립한다.

$$D_b^k[f] \oplus D_b^k[g] = D_0^k[f \oplus g].$$

(증 명)

$$\begin{aligned} D_0^k[f\oplus g](\mathbf{x},0) &= (f\oplus g)(\mathbf{x}) = f(\mathbf{x})\oplus g(\mathbf{x}) \\ &= D_b^k[f](\mathbf{x},0)\oplus D_b^k[g](\mathbf{x},0) \\ &= (D_b^k[f]\oplus D_b^k[g])(\mathbf{x},0) \\ D_0^k[f\oplus g](\mathbf{x},1) &= (f\oplus g)\oplus(\mathbf{x}\oplus c_k^{(n)}) \\ &= f(\mathbf{x}\oplus c_k^{(n)})\oplus g(\mathbf{x}\oplus c_k^{(n)}) \\ &= (f(\mathbf{x}\oplus c_k^{(n)})\oplus b) \\ &\quad \oplus(g(\mathbf{x}\oplus c_k^{(n)})\oplus b) \\ &= D_b^k[f](\mathbf{x},1)\oplus D_b^k[g](\mathbf{x},1) \\ &= D_b^k[f]\oplus D_b^k[g](\mathbf{x},1). \quad \square \end{aligned}$$

즉, $D_b^k[f]$는 EXOR을 보존하는데 이 성질은 $D_b^k[f]$의 특성을 규명하는데 많이 이용된다.

보조정리 3.6 $f, g \in B_n$, $k \in \{1, \cdots, n\}$, $b \in Z_2$라 하면 $d(D_b^k[f], D_b^k[g]) = 2d(f, g)$이다.

(증 명)

$$\begin{aligned} d(D_b^k[f], D_b^k[g]) &= wt(D_b^k[f]\oplus D_b^k[g]) \\ &= wt(D_0^k[f\oplus g]) \\ &= 2wt(f\oplus g) \\ &= 2d(f, g). \quad \square \end{aligned}$$

이제 보조정리 3.2, 3.4, 3.5, 3.6을 이용하면 다음을 증명할 수 있다.

보조정리 3.7 $f \in B_n$, $k \in \{1, \cdots, n\}$, $b \in Z_2$이라 하면

$$\mathcal{N}_{D_b^k[f]} = 2\mathcal{N}_f.$$

(증 명) $\mathcal{N}_f$의 정의에 의해 적당한 $\lambda_0 \in \Lambda_n$가 존재하여

$$\mathcal{N}_f = d(f,\lambda_0)$$

보조정리 3.2에 의해서 $\lambda_0^* = D_b^k[\lambda_0] \in \Lambda_{n+1}$이고,

$$\begin{aligned} \mathcal{N}_{D_b^k[f]} &= min_{\lambda^*\in\Lambda_{n+1}} d(D_b^k[f],\lambda^*) \\ &\le d(D_b^k[f],\lambda_0^*) = d(D_b^k[f],D_b^k[\lambda_0]) \\ &= 2d(f,\lambda_0) = 2\mathcal{N}_f. \end{aligned} \quad (3)$$

한편 적당한 $\lambda_1^* \in \Lambda_{n+1}$이 존재하여 다음을 만족한다.

$$\mathcal{N}_{D_b^k[f]} = d(D_b^k[f],\lambda_1^*).$$

또한, 보조정리 3.2에 의하여

$$\lambda_1^* \in D_b^k[\lambda_1]$$

을 만족하는 적당한 $\lambda_1 \in \Lambda_n$이 존재한다. 따라서

$$\begin{aligned} \mathcal{N}_{D_b^k[f]} &= d(D_b^k[f],\lambda_1^*) = d(D_b^k[f],D_b^k[\lambda_1]) \\ &= 2d(f,\lambda_1) \ge 2min_{\lambda\in\Lambda_n} d(f,\lambda) \\ &= 2\mathcal{N}_f. \end{aligned} \quad (4)$$

식 (3)과 (4)에 의해서 $\mathcal{N}_{D_b^k[f]} = 2\mathcal{N}_f$. $\square$

즉, $D_b^k[f]$에 의해서 확장된 함수는 원래 함수의 비선형치보다 반드시 2배의 비선형치를 갖는다. 또한, $D_b^k[f]$는 상관관계에 관한 다음의 성질을 갖는다.

보조정리 3.8 $f \in CI(m)$이면 모든 $k \in \{1, \cdots, n\}$, $b \in Z_2$에 대해 $t_b^k[f] \in CI(m)$이다.

다음은 연접함수의 무상관도에 대한 잘 알려진 사실이다.

보조정리 3.9 [12] $f_1, f_2 \in CI(m)$이면 $f = f_1 \| f_2 \in CI(m)_{n+1}$이다.

이제 정리 3.1과 보조정리 3.3, 3.6, 3.8, 3.9를 이용하면 다음의 중요한 정리를 얻을 수 있다.

❖ 정리 3.2 함수 $f, g \in B_n$이라 하면 다음이 성립한다.

1) $f \in NLIN_n$이면 $D_b^k[f] \in NLIN_{n+1}$이고 $\mathcal{N}_{D_b^k(f)} = 2\mathcal{N}_f$이다.
2) $f \oplus g \in BAL_n$이면 $D_b^k[f] \oplus D_b^k[f] \in BAL_{n+1}$이다.
3) $f \oplus g \in SAC_n$이면 $D_b^k[f] \oplus D_b^k[f] \in SAC_{n+1}$이다.
4) $(f, g) \in SUC_n$이면 $(D_b^k[f], D_b^k[g]) \in SUC_{n+1}$이다.
5) $f \in CI(m)_n$이면 $D_b^k[f] \in CI(m)_{n+1}$이다.

위 정리에 의하면 함수 f에 대하여 $D_b^k[f]$는 f의 몇가지 암호학적인 성질을 보존한다. 즉, 비선형치는 2배로 증가시키고, SAC을 보존하며, SUC을 만족하는 두 함수를 SUC을 만족하는 함수로 확장하고 m차 무상관도를 유지하나 이 방법으로는 최대 비선형치를 유지하는 부울 함수는 생성할 수 없으며, 무상관도도 증가시키지 못한다.

4. 무상관 함수 및 semi-bent 함수

본 장에서는 m차 무상관 함수를 이용하여 $m+1$차 무상관 함수를 생성하는 Camion의 방법을 소개하고 이러한 방법은 특별한 경우밖에 없음을 밝힌다. 또한 Z_2^{2n} 위에 bent 함수를 이용하여 Z_2^{2n+1} 위의 함수를 정의하고 이 함수가 bent 함수와 유사한 특성이 있음과 동시에 SUC을 만족함을 보인다.

4.1 Walsh-Hadamard 변환의 성질

본 절에서는 먼저 부울 함수의 간단한 변형에 의해서 생성된 부울 함수에 대한 Walsh-Hadamard 변환을 구하기로 한다.

■ 정의 4.1 함수 $f \in B_n$에 대해 f의 *Walsh-Hadamard* 변환 $\mathcal{F} : Z_2^n \to R$은 다음과 같이 정의된다.

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

Walsh-Hadamard 변환은 편의상 $\hat{f}(\mathbf{x}) = (-1)^{f(\mathbf{x})}$에 대한 변환,

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

이 널리 이용된다.

❖ 정리 4.1 함수 $f \in B_n$에 대해 $f \in CI(m)$이기 위한 필요충분 조건은 $1 \le wt(\mathbf{w}) \le m$인 모든 $\mathbf{w} \in Z_2^n$에 대해 $\hat{\mathcal{F}}(\mathbf{w}) = 0$이 성립하는 것이다.

상관관계 특성을 살피기 위해 몇가지 사항을 조사한다.

보조정리 4.1 $f \in B_n$, *Walsh-Hadamard* 변환을 $\hat{\mathcal{F}}(\mathbf{w})$라 하면 $f \oplus 1$의 *Walsh-Hadamard* 변환은 $-\hat{\mathcal{F}}(\mathbf{w})$이다.

보조정리 4.2 $f \in B_n$, l_b, $b_0 \in Z_2$라 하자. 그리고, $g = f \oplus l_b \oplus b_0$라 하면

$$\hat{\mathcal{G}}(\mathbf{w}) = (-1)^{b_0} \hat{\mathcal{F}}(\mathbf{w} \oplus \mathbf{b})$$

이다.

보조정리 4.3 $f \in B_n$, $A : Z_2^n \to Z_2^n$를 일대일 함수라 하고 $g(\mathbf{x}) = f(A\mathbf{x} \oplus \mathbf{a})$라 하면

$$\hat{\mathcal{G}}(\mathbf{w}) = (-1)^{(A^{-1}\mathbf{a},\mathbf{w})} \hat{\mathcal{F}}((A^{-1})^t\mathbf{w})$$

이다.

보조정리 4.2와 4.3을 종합하면 다음을 얻는다.

❖ 정리 4.2 $g(\mathbf{x}) = f(A\mathbf{x} \oplus \mathbf{a}) \oplus l_b(\mathbf{x}) \oplus b_0$라 하면

$$\hat{\mathcal{G}}(\mathbf{w}) = (-1)^{b_0}(-1)^{(A^{-1}\mathbf{a},\mathbf{w}\oplus\mathbf{b})}\hat{\mathcal{F}}((A^{-1})^t(\mathbf{w}\oplus\mathbf{b}))$$

이다.

정리 4.2에서 A = I, $\mathbf{b}$ = 0으로 하면 다음을 얻는다.

따름정리 4.1 (dyadic shift와 complement에 의한 Walsh-Hadamard 변환)
$g(\mathbf{x}) = f(\mathbf{x} \oplus \mathbf{a}) \oplus b_0$라 하면

$$\hat{\mathcal{G}}(\mathbf{w}) = (-1)^{b_0}(-1)^{(\mathbf{a},\mathbf{w})}\hat{\mathcal{F}}(\mathbf{w})$$

이다.

즉, 부울 함수의 dyadic shift와 complement에 의한 Walsh-Hadamard 변환은 부호를 무시하면 값이 같다.

❖ 정리 4.3 (연접함수의 Walsh-Hadamard 변환)
$g_0, g_1 \in B_n$, $\mathbf{w}^* = (w_1, \cdots, w_{n+1}) \in Z_2^{n+1}$, $\mathbf{w} = (w_1, \cdots, w_n)$이라 하고 $f = g_0 \| g_1$이라 하면

$$\hat{\mathcal{F}}(\mathbf{w}^*) = \hat{\mathcal{G}}_0(\mathbf{w}) + (-1)^{w_{n+1}}\hat{\mathcal{G}}_1(\mathbf{w})$$

이다.

4.2 연접 부울 함수의 상관관계 특성

따름정리 4.1과 정리 4.3을 이용하면 보조정리 3.8과 3.9를 쉽게 유도할 수 있다.

이제 연접 부울 함수의 무상관도를 증가시키기 위한 Walsh-Hadamard 변환의 필요충분 조건을 알아본다.

❖ 정리 4.4 [6] $f_1, f_2 \in CI(m)_n$일 때 $f = f_1 \| f_2$라 하면

$$f \in CI(m+1)_{n+1} \text{ iff } \hat{\mathcal{F}}_1(\mathbf{w}) + \hat{\mathcal{F}}_1(\mathbf{w}) = 0, \quad \forall \mathbf{w} \in Z_2^n, \quad wt(\mathbf{w}) = m+1.$$

(증 명) 먼저 $wt(\mathbf{w}) = m+1$인 임의의 $\mathbf{w} \in Z_2^n$에 대해 $\mathbf{w}^* = (0,\mathbf{w}) \in Z_2^{n+1}$이라 하면

$$0 = \hat{\mathcal{F}}(\mathbf{w}^*) = \hat{\mathcal{F}}_1(\mathbf{w}) + \hat{\mathcal{F}}_2(\mathbf{w})$$

이 성립한다.

역으로, $1 \le wt(\mathbf{w}^*) \le m+1$인 $\mathbf{w}^* = (a, \mathbf{w}) \in Z_2^{n+1}$에 대해 다음이 성립한다.

경우 1 : $1 \le wt(\mathbf{w}) \le m$,

$$\hat{\mathcal{F}}(\mathbf{w}^*) = \hat{\mathcal{F}}_1(\mathbf{w}) + (-1)^a\hat{\mathcal{F}}_2(\mathbf{w}) = 0.$$

경우 2 : $wt(\mathbf{w}) = m+1$(a=1),

$$\hat{\mathcal{F}}(\mathbf{w}^*) = \hat{\mathcal{F}}_1(\mathbf{w}) + \hat{\mathcal{F}}_2(\mathbf{w}) = 0.$$

따라서 정리는 증명된다. □

4.3 Camion 방법에 의해서 생성된 부울 함수의 특성

함수 $D_b^k[f]$는 f의 무상관도(order of correlation immunity)를 그대로 보존하기 때문에 이 방법으로 무상관도가 큰 함수를 얻기에는 한계가 있다. Camion은 이러한 문제점을 해결하는 다음과 같은 방법을 제안하였다.

$\mathbf{v} \in Z_2^n$, $b \in Z_2$라 하면, 함수 $f \in B_n$에 대하여 함수 $T_b^{\mathbf{v}}[f] \in B_n$를 다음과 같이 정의하자.

$$T_b^{\mathbf{v}}[f](\mathbf{x}) = f(\mathbf{x} \oplus \mathbf{v}) \oplus b.$$

즉, $t_b^k[f]$에서 정수 k 대신에 벡터 $\mathbf{v}$로 확장한 함수이다.

$T_b^{\mathbf{v}}[f]$는 일반적으로 $D_b^k[f]$와 같이 무상관도를 보존한다.

보조정리 4.4 $f \in CI(m)$이면 $T_b^{\mathbf{v}}[f] \in CI(m)$이다.

(증 명) 따름정리 4.1에 의해서 자명하다. □

그러나 다음 정리에서와 같이 $T_b^v[f]$의 특별한 형태에 대해서는 무상관도를 증가시킨다.

❖ 정리 4.5 [2] $f \in CI(m)_n$에 대해 m이 짝수이고

경우 1 : $\mathbf{v} = (0, \cdots, 0)$, $b = 1$ 또는,
경우 2 : $\mathbf{v} = (1, \cdots, 1)$, $b = 0$

일 때, $g = f \| T_b^v[f] \in CI(m+1)_{n+1}$이다.

(증 명) $wt(\mathbf{w}) = m+1$인 임의의 $\mathbf{w} \in Z_2^n$에 대해서

$$\begin{aligned}\hat{G}(\mathbf{w}) &= \hat{\mathcal{F}}(\mathbf{w}) + (-1)^b(-1)^{(\mathbf{v},\mathbf{w})}\hat{\mathcal{F}}(\mathbf{w}) \\ &= \hat{\mathcal{F}}(\mathbf{w}) - \hat{\mathcal{F}}(\mathbf{w}) \\ &= 0\end{aligned}$$

이므로 정리 4.4에 의해
$g \in CI(m+1)_{n+1}$이다. □

따름정리 4.2 정리 4.5에서 m이 홀수인 경우에는 경우 2 대신에

경우 2′ : $\mathbf{v} = (1, \cdots, 1)$, $b = 1$

이어도 $g = f \| T_b^v[f] \in CI(m+1)_{n+1}$이다.

그러나 Camion의 방법은 다음의 따름정리에서와 같이 경우 1, 2(2′) 이외에는 성립하지 않기 때문에 일반적으로 널리 적용시키기에는 문제점이 있다.

따름정리 4.3 정리 4.5를 만족하는 $\mathbf{v}$, b는 오직 2가지 경우 뿐이다.

(증 명) $\mathbf{v} \neq (0, \cdots, 0), (1, \cdots, 1)$이라 하자. 그러면 $wt(\mathbf{w}) = m+1$인 경우 $(\mathbf{v},\mathbf{w})$는 0인 경우와 1인 경우가 모두 존재하므로 자명하다. □

4.4 semi-bent 함수

이제 정리 4.4를 bent 함수에 적용시켜 새로운 함수를 생성하기로 하자.

■ 정의 4.2 함수 $f \in B_{2n}$가 모든 $\mathbf{w} \in Z_2^{2n}$에 대하여 $|\hat{\mathcal{F}}(\mathbf{w})| = 2^n$이 성립하면, *bent* 함수라 한다.

정의 4.2에 의하면 bent 함수는 모든 선형함수에 대하여 균등한(부호는 무시) 상관관계를 가짐을 알 수 있다. 이러한 성질은 다음에 정의할 함수에 대해서도 유사하게 성립한다.

■ 정의 4.3 *bent* 함수 $g \in B_{2n}$에 대하여 함수 $f \in B_{2n+1}$를 다음과 같이 정의하고 *semi-bent* 함수라 부른다.

$$f = g \| T_1^0[g].$$

정의 4.3에서 정의한 semi-bent 함수는 실제로 다음과 같은 형태이다.

$$\begin{aligned}f(x_1,\cdots,x_{2n},x_{2n+1}) &= (1 \oplus x_{2n+1})g(x_1,\cdots,x_{2n}) \\ &\quad \oplus x_{2n+1}(g(x_1,\cdots,x_{2n}) \oplus 1) \\ &= g(x_1,\cdots,x_{2n}) \oplus x_{2n+1}.\end{aligned}$$

따라서 정리 4.3에 의하면 semi-bent 함수는 다음과 같은 성질을 지닌다.

따름정리 4.4 $f \in B_{2n+1}$가 *semi-bent* 함수이면

$$|\hat{\mathcal{F}}(\mathbf{w})| = 0 \text{ 또는 } 2^{n+1}.$$

즉, semi-bent 함수는 선형함수와의 상관관계가 bent 함수와 유사하게 균등한 상관관계를 갖는다. 또한, 따름정리 4.4에 의해 비선형치에 관한 다음의 사실을 알 수 있다.

따름정리 4.5 $f \in B_{2n+1}$가 *semi-bent* 함수이면

$$\mathcal{N}_f = 2^{2n} - 2^n.$$

※ 참고 4.1 $2n+1$차의 균등함수가 가질 수 있는 최대 비선형치는 다음과 같다[1].

$$\sum_{i=(n-1)}^{2n-2} 2^{i+1} = 2^{2n} - 2^n.$$

그러므로, 홀수차 위에서의 semi-bent 함수는 짝수차 위에서의 bent 함수와 같이 최대 비선형치를 갖는다.

보조정리 4.5 *semi-bent* 함수 $f : Z_2^{2n+1} \rightarrow Z_2$는 오직 한 점 $(x_1, \cdots, x_{2n}, x_{2n+1}) = (0, \cdots, 0, 1)$을 제외하고 *SAC*을 만족한다[1].

(증 명) semi-bent 함수의 정의에 의해

$$f(x_1, \cdots, x_{2n}, x_{2n+1}) = g(x_1, \cdots, x_{2n}) \oplus x_{2n+1}$$

을 만족하는 적당한 bent 함수 $g : Z_2^{2n} \rightarrow Z_2$가 존재하고, [8]에 의해 $g \in SAC_{2n}$이다. 한편 임의의 $(0, \cdots, 0, 1) \neq \alpha \in Z_2^{2n+1}$, $wt(\alpha) = 1$에 대해,

$$\alpha = (\alpha', \alpha_{2n+1}),\ wt(\alpha') = 1$$

을 만족하는 $\alpha' \in Z_2^{2n}$이 존재한다. 그러므로,

$$\begin{aligned}
&\sum_{x \in Z_2^{2n+1}} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \alpha) \\
&= \sum_{\substack{x' \in Z_2^{2n} \\ x_{2n+1}=0}} f(\mathbf{x}', x_{2n+1}) \oplus f(\mathbf{x}' \oplus \alpha', x_{2n+1} \oplus \alpha_{2n+1}) \\
&\quad + \sum_{\substack{x' \in Z_2^{2n} \\ x_{2n+1}=1}} f(\mathbf{x}', x_{2n+1}) \oplus f(\mathbf{x}' \oplus \alpha', x_{2n+1} \oplus \alpha_{2n+1}) \\
&= \sum_{x' \in Z_2^{2n}} g(\mathbf{x}') \oplus g(\mathbf{x}' \oplus \alpha') \\
&\quad + \sum_{x' \in Z_2^{2n}} g(\mathbf{x}') \oplus 1 \oplus g(\mathbf{x}' \oplus \alpha') \oplus 1 \\
&= 2^{2n-1} + 2^{2n-1} = 2^{2n}.
\end{aligned}$$

따라서, $f \in SAC_{2n+1}$이다. □

한편, Z_2^4 위에 정의된 896개의 모든 bent 함수 g_i 중에서 임의의 서로 다른 쌍은 ${}_{896}C_2 = 400{,}960$개 이고, 이 중에서

$$g_i \oplus g_j \in SAC \cap BAL,\ i \neq j \qquad (5)$$

을 만족하는 (g_i, g_j)는 59,904개 이다. 이 사실로부터 임의의 Z_2^{2n}에서도 식 (5)을 만족하는 bent 함수 쌍은 충분히 많이 존재하리라 예상된다(실제로 일반적인 bent 함수의 개수는 아직 알려져 있지 않다).

이제 semi-bent 함수를 구성하는 bent 함수가 식 (5)을 만족하면 SUC을 만족함을 보이자.

❖ 정리 4.6 g_1, g_2를 식 (5)을 만족하는 Z_2^{2n} 위에 정의된 bent 함수라 하고, f_1, f_2를 g_1, g_2로부터 생성한 semi-bent 함수라 하면

$$(f_1, f_2) \in SUC$$

이다.

(증 명) semi-bent 함수의 정의와 보조정리 4.5에 의해서

$$f_1, f_2 \in BAL \cap SAC \qquad (6)$$

이다. 한편, 임의의 x_{2n+1}에 대하여

$$\begin{aligned}
&f_1(x_1, \cdots, x_{2n}, x_{2n+1}) \oplus f_2(x_1, \cdots, x_{2n}, x_{2n+1}) \\
&\quad = g_1(x_1, \cdots, x_{2n}) \oplus g_2(x_1, \cdots, x_{2n})
\end{aligned}$$

이므로 $wt(f_1 \oplus f_2) = 2wt(g_1 \oplus g_2)$이고, 따라서

$$f_1 \oplus f_2 \in BAL \qquad (7)$$

이다. 또한, 보조정리 4.5의 증명과 같은 방법으로

[1] 한 점 이외에 SAC을 만족하는 함수는 편의상 SAC을 만족한다고 약속한다.

$$f_1 \oplus f_2 \in SAC \quad (8)$$

임을 증명할 수 있다[2]. 따라서 식 (7)와 (8)에 의해서

$$f_1 \oplus f_2 \in BAL \cap SAC \quad (9)$$

이고 식 (6)과 (9)에 의해서

$$(f_1, f_2) \in SUC$$

이다. □

5. 확장 재생성된 부울 함수의 비교

표 1은 semi-bent 함수를 Sigenthaler[12], KMI[3], Seberry[11], Camion[2]의 연접 방식에 의해 확장 생성된 부울 함수와 균등성, 최대 비선형치, SAC 그리고 SUC의 관점에서 비교한 결과이다.

표 1에서 나타내지 않은 상관관계에 대한 특성은 다음과 같다.

- Sigenthaler, KMI 방법 : 무상관도를 유지한다.
- Camion 방법 : 무상관도를 증가시킨다.
- Seberry 방법 : 무상관도를 보장한다.
- semi-bent 함수 : 균등한 상관 관계를 갖는다.

즉, 본 논문에서 생성한 semi-bent 함수는 암호학적 관점에서 매우 우수하며, 특히 SUC을 만족하기 때문에[3] DC에 강한 S-box를 생성하는데 이용될 수 있으리라 예상된다. 반면, 본 논문에서는 semi-bent 함수를 홀수 차원 벡터 공간 위에서만 생성하였으나 짝수 차원 벡터 공간위에서의 생성도 가능하며 이러한 함수에 대한 각종 특성은 추후 계속 연구할 예정이다.

6. 결 론

본 논문에서는 연접 방법에 의해서 확대 재생성된 부울 함수의 균등성, 비선형성 및 상관관계 특성을 조사하였다.

특히, Z_2^n 위에서 SAC을 만족하는 부울 함수를 이용하여 Z_2^{n+1} 위에서 SAC을 만족하는 부울 함수를 생성하는 KMI의 방법에 대해 비선형성과 무상관성의 유지 여부를 규명하였다. 즉, KMI의 방법에 의해서 생성된 부울 함수는 연접시킨 함수의 비선형치 보다 정확히 2배의 비선형치를 갖기 때문에 최대 비선형치를 갖지 못하며, 연접시킨 부

표 1: 확장 재성성된 부울 함수의 암호학적 특성 비교

○ : 만족함, × : 만족 못함

구 분	균등성	최대 비선형치	SAC	SUC
Sigenthaler 방법	○	×	×	×
KMI 방법	○	×	○	○
Seberry 방법	○	○	○	×
Camion 방법	○	×	×	×
semi-bent 함수	○	○	○	○

2 이 경우에도 한 점 x_{2n+1}은 제외한다.

3 KMI 방법은 SUC을 유지하고, semi-bent 함수는 SUC을 만족한다.

울 함수의 무상관도를 그대로 유지하기 때문에 계속 확장하면 비선형치와 무상관도가 낮아진다. 또한, 부울 함수들을 블럭 암호에 이용하기 필수적으로 필요한 부울 함수들 간의 상관관계 특성에 대한 기존의 개념을 보다 강화하여 SUC을 정의하였고, SUC을 만족하는 부울 함수의 예를 제시하였다. 특히, KMI의 생성 방법은 SUC을 유지함을 증명하였다. 그러나 본 논문에서 정의한 SUC을 n개의 부울 함수에 확장 적용하여 S-box(치환)를 생성할 수 있는 지는 현재까지 미해결 문제지만, 일반적으로 SUC을 만족하는 부울 함수들로 구성된 S-box는 DC 관점에서 강하기 때문에 매우 의미있는 개념이라 할 수 있다. 더불어, 무상관도를 증가시키는 방법으로 알려진 Camion의 방법에 대해 Walsh-Hadamard 변환 특성을 이용하여 이러한 방법은 특별한 형태 이외는 존재하지 않음을 규명하였다.

또, 상관관계 특성이 우수한 Z_2^{2n} 위의 bent 함수를 이용하여 Z_2^{2n+1} 위의 부울 함수를 생성하고, 이 방법에 의해서 생성된 부울 함수는 최대 비선형치인 $2^{2n} - 2^n$을 갖고, bent 함수의 단점인 균등성 문제를 해결함과 동시에 bent 함수가 지닌 우수한 상관관계 특성을 유지함과 동시에 SUC을 만족함을 보였다.

끝으로, 본 논문에서 제시한 semi-bent 함수를 연접 방법에 의해서 확장 생성된 다른 형태의 부울 함수와 비교하여 semi-bent 함수의 암호학적 우수성을 입증하였다.

참 고 문 헌

[1] C. Adams and S. Tavares, "*The structured design of cryptographically good S-boxes*", Journal of Cryptology **3**, no. 1, pp. 27-43, 1990.

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

[3] K. Kim, T. Matsumoto and H. Imai, "*A recursive construction method of S-boxes satisfying strict avalanche criterion*", Advances in Cryptology - CRYPTO '90, Springer-Verlag, pp. 564-573, 1991.

[4] M. Matsui, "*Linear cryptanalysis method for DES cipher*", Advances in Cryptology-EUROCRYPT '93, Springer-Verlag, pp. 386-397, 1994.

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

[6] B. Preneel, "*Analysis and design of cryptographic hash functions*", Ph.D. thesis, Katholieke Universiteit Leuven, 1993.

[7] B. Preneel, W. Van Leekwijck and L. Van Linden, "*Propagation characteristics of Boolean functions*", Advances in Cryptology - EUROCRYPT '90, Springer-Verlag, pp. 161-173, 1991.

[8] R.A. Rueppel, Stream Ciphers, IEEE Press, pp. 65-134, 1992.

[9] J. Seberry, X. M. Zhang and Y. Zheng, "*Systematic generation of*

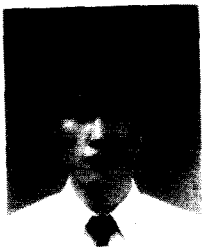
cryptographically robust S-boxes", In Proceedings of the first ACM Conference on Computer and Communications Security, pp. 172-182, 1993.

[10] 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.

[11] J. Seberry, X. M. Zhang and Y. Zheng, "*Nonlinearly balanced Boolean functions and their propagation characteristics*", Advances in Cryptology - CRYPTO '93, Springer-Verlag, pp. 49-60, 1994.

[12] T. Siegenthaler, "*Correlation immunity of non-linear combining functions for cryptographic applications*", IEEE Trans. Inform. Theory **IT-30**, pp. 776-780, 1984.

□ 著者紹介

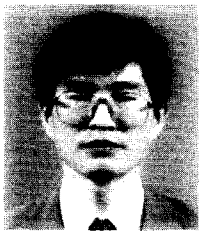


지 성 택(정회원)

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

이 상 진(정회원)

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



김 광 조(정회원)

1980년 연세대학교 전자공학과(학사)
1983년 연세대학교 대학원 전자공학과(석사)
1990년 요꼬하마 국립대학 대학원 전자 정보공학과(박사)
현 한국전자통신연구소 실장

※ 관심 분야 : 암호학 및 응용 분야, M/W 통신