通信情報保護學會論文誌
第9卷 第1號, 1999. 3

최적 상관 무결 semi-bent 함수

지성택*, 박상우*, 김대호*, 임종인**

Optimum Correlation Immune Semi-bent Functions

Seongteak Chee*, Sangwoo Park*, Dae Ho Kim*, Jong-In Lim**

요 약

부울 함수는 정보 보호 기술 구현의 핵심 기본 논리로서 암호학적으로 우수한 특성을 가지는 부울 함수 설계 방법 및 부울 함수의 자체 특성에 관하여 많은 연구가 추진되고 있다. 본 논문은 참고 문헌[2,5]에서 제안된 균등 함수이며 2개의 상관값만을 가지는 semi-bent 함수의 상관 무결 특성에 관한 것으로 상관값이 0인 선형 함수를 결정할 수 있으며, 상관값이 0이 아닌 경우에는 상관값이 균일한 최적의 상관 특성을 가지는 semi-bent 함수 설계 방법을 제안하고, 제안 함수의 암호학적 특성을 분석한다.

Abstract

Boolean functions have an important role for designing block ciphers and hash functions. In this paper, we propose a method for designing optimum correlation immune functions. We also analyze their cryptographic properties - balancedness, nonlinearity, correlation value to the set of linear functions, correlation immunity, propagation characteristic, and algebraic degree. Such functions are special type of Semi-bent functions [2,5]

1. 서 론

부울 함수는 블록 알고리즘, 스트림 알고리즘, 해쉬 함수 등의 설계에서 중요한 비중을 차지하는 기본 논리로서, 부울 함수가 가지는 주요 특성으로는 균등성(balancedness), 비선형성(nonlinearity), 상관 무결성(correlation immunity)[10] PC(Propagation Criterion)[6] 특성 등이 있다. 이들 특성 중 상관 무결성에 대하여 우수한 상관 무결성을 가지는 부울 함수 설계 방법이 다수 제안되어 있다 [1,2,3,4,9,10]. 그러

* 한국전자통신연구원
** 고려대학교 수학과

나, 아무리 우수한 상관 무결 함수를 설계하여도 특정한 선형 함수와의 상관 관계는 반드시 존재하며, 특히, 이때 존재하는 상관값은 일반적으로 상관 무결도가 증가할수록 더욱 커진다. 따라서 전체적인 상관 관계 측면에서 보면 어떤 특정한 선형 함수와 높은 상관 관계를 가지는 상관 무결 함수보다는 모든 선형 함수와 유사한 상관 관계를 지니는 함수가 더 우수할 수 있다. 이러한 성질을 만족하는 함수가 바로 bent 함수이다 [7]. 그러나, bent 함수는 상관 관계 특성 면에서의 우수성 이외에 각종 비선형 특성이 다른 어느 함수보다도 우수하지만, 짝수차 벡터 공간 위에서만 존재한다는 점과 균형이 아니라는 단점으로 인하여 직접 활용이 불가능하다.

이러한 단점을 극복하기 위하여 도입된 함수가 semi-bent 함수[2,5]이다. Semi-bent 함수는 균등 함수(balanced function)이고 모든 벡터 공간 위에 존재하며, 비선형 특성이 우수하다. 또한, semi-bent 함수는 선형 함수와의 상관값을 오직 2개(0 또는 다른 하나의 값)만 갖기 때문에 상관 특성도 우수하다. 그러나, semi-bent 함수와의 상관값이 0인 선형 함수를 결정할 수 없기 때문에 일반적으로 상관 무결 함수가 아니다.

본 논문에서는 상관값이 0인 선형 함수를 결정할 수 있으며, 상관값이 0이 아닌 경우에는 상관값이 균일한 semi-bent 함수 설계 방법을 제안하고, 제안 함수의 암호학적 특성을 분석한다. 본 논문의 2장과 3장은 일반적인 부울 함수의 암호학적 특성 및 semi-bent 함수의 특성을 기술하며, 4장에서는 상관값을 조절 가능한 semi-bent 함수 설계 방법을 제안하고, 그 특성을 분석한다.

2. 예비 사항

Z_2^n은 길이가 n인 이진 벡터 $x=(x_1, x_2, \cdots, x_n)$을 원소로 하는 n차 벡터 공간이다. $x=(x_1, \cdots, x_n)$과 $y=(y_1, \cdots, y_n)$를 Z_2^n의 두 벡터라 하면, x와 y의 내적은 $x \cdot y = x_1y_1 \oplus \cdots \oplus x_ny_n$이며, 여기서, 곱과 합은 $GF(2)$의 연산이다. 부울 함수 f는 Z_2^n을 정의역으로 하고, 0 또는 1의 값을 가지는 함수이다. Z_2^n상에 정의된 모든 부울 함수의 집합을 B_n으로 표시한다. $f(x)=l_w(x) \oplus c = x \cdot w \oplus c = x_1w_1 \oplus \cdots \oplus x_nw_n \oplus c$ 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 A_n과 L_n으로 표시한다. 벡터 $x \in Z_2^n$의 해밍 무게(Hamming weight)는 x에서 '1'의 개수이며, $wt(x)$로 표시한다. 그리고, 부울 함수 $f \in B_n$의 해밍 무게는 $wt(f)$로 표시하며, f의 함수값들 중 '1'의 개수이다. 두 부울 함수 f와 g의 해밍 거리(Hamming distance)는 $d(f,g) = \#\{x|f(x) \neq g(g)\}$ 이다. 다음 정의들은 부울 함수의 기본 특성들이다.

정의 1. $\#\{x \in Z_2^n | f(x)=0\} = \#\{x \in Z_2^n | f(x)=1\}$이면, $f \in B_n$는 균등 함수이다.

정의 2. 임의의 부울 함수 f의 대수적 차수(*algebraic degree*)($deg(f)$로 표현)는부울 함수를 대수적 표준형(*algebraic normal form*)으로 표현하였을 때, 0이 아닌 계수를 가지는 항들 중에서 가장 높은 차수로 정의된다.

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

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

정의 4. $1 \leq wt(w) \leq m$인 모든 $w \in Z_2^n$에 대해서,

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

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

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

정의 5. $\sum_{x \in Z_2^n} f(x) \oplus f(x \oplus \alpha) = 2^{n-1}$인 부울 함수 $f \in B_n$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.

부울 함수의 특성을 분석할 때는 부울 함수 f 대신에 $\{-1,1\}$의 값을 가지는 $\hat{f}(x) = (-1)^{f(x)}$를 이용하는 것이 보편적이다. 다음은 $\hat{f}$의 *Walsh-Hadamard* 변환의 정의이다.

정의 6. 부울 함수 $f \in B_n$에 대해서, $\hat{f}$의 *Walsh-Hadamard* 변환 $\hat{\mathcal{F}}$: $Z_2^n \to \mathcal{R}$은 다음으로 정의된다.

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

여기서, $\mathcal{R}$은 실수 전체의 집합이다.

Walsh-Hadamard 변환을 사용하면, 부울 함수의 여러 가지 기본 특성들에 대한 다음 사실을 얻을 수 있다.

보조정리 1. f는 Z_2^n에 정의된 부울 함수이다. 그러면,

1. f는 균등 함수이다. $\Leftrightarrow \hat{\mathcal{F}}(0) = 0$.
2. f의 비선형치는 다음과 같다.

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_w |\hat{\mathcal{F}}(w)|.$$

3. f가 0이 아닌 $\alpha \in Z_2^n$에 대해서 PC를 만족한다는 사실과

$$\sum_{x \in Z_2^n} \hat{\mathcal{F}}^2(w) \cdot (-1)^{\alpha \cdot w} = 0$$

은 동치이다.

4. f가 m차 무상관 함수이면 $1 \le wt(w) \le k$인 모든 w에 대하여 $\hat{\mathcal{F}}(w) = 0$을 만족하며, 역 또한 성립한다. 그리고, Z_2^n상의 선형 함수 l_w에 대하여 $c(f, l_w) = \frac{\hat{\mathcal{F}}(w)}{2^n}$ 이다.

다음 정리는 부울 함수의 상관 특성 (correlation property)을 분석하기 위한 유용한 도구이다.

정리 1. [Parseval의 정리] 부울 함수 $f \in B_n$에 대해서

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

이다.

Parseval의 정리는 임의의 부울 함수의 모든 선형 함수에 대한 전반적인 상관 특성은 부울 함수 f와는 무관하며 즉, 임의의 점에서의 상관 특성을 좋게 하면, 어느 다음 점에서의 상관 특성이 나빠짐을 뜻한다.

3. Bent 함수와 Semi-bent 함수의 상관 특성

본 장에서는 bent 함수와 semi-bent 함수의 정의 및 상관 특성을 분석한다. 우선, bent 함수의 정의는 다음과 같다.

정의 7. [Bent 함수] Z_2^n상에 정의된 부울 함수 f에 대해 임의의 $w \in Z_2^n$에 대해

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

이면, f를 bent 함수라 한다.

즉, bent 함수는 부호를 고려하지 않으면 유일한 상관값을 가지며, 그 값은 $2^{-n/2}$ 이다. Bent 함수가 균등 함수가 아니고, 짝수차 벡터

공간에서만 정의되는 사실을 제외하면 bent 함수는 암호학적 관점에서 이상적인 특성을 가진다 [8].

참고 문헌 [2]에서 저자들은 짝수차 벤트 함수의 아핀 변환(affine transformation)을 이용하여 홀수차 벡터 공간에 정의되는 semi-bent 함수를 제안하였다. 다음으로, 참고 문헌 [5]에서 저자들은 [2]의 내용을 확장하여 홀수차 뿐만 아니라 짝수차 벡터 공간에서 정의되며, 모든 선형 함수에 대하여 2개의 상관값을 가지는 균형 함수로 semi-bent 함수를 재 정의하였다.

정의 8. (Semi-bent 함수). 임의의 부울 함수 $f \in \mathcal{B}_n$에 대해서, $\hat{\mathcal{F}} f(w) = 0$ 또는 $2^{\lfloor \frac{n+1}{2} \rfloor}$ 이고, $\hat{\mathcal{F}} f(0) = 0$ 인 부울 함수 f를 *semi-bent* 함수로 정의한다. 여기서, $\lfloor m \rfloor$은 m보다 같거나 작은 가장 작은 정수를 의미한다.

Semi-bent 함수가 가지는 2개의 상관값은 0과 $\pm 2^{\frac{n+2-(n \bmod 2)}{2}}$이다. 그러나, semi-bent 함수는 상관 무결성을 만족하지 않으며, Z_2^n상에 정의된 semi-bent 함수 f에 대하여 $1 \le wt(w) \le k$에 대해 $c(f, l_w) = 0$인 $w \in Z_2^n$를 결정하는 것은 매우 어려운 문제이다.

위에 언급한 $c(f, l_w) = 0$인 w $\in Z_2^n$를 결정할 수 있다면, 우리는 최적 상관 무결 함수(optimal correlation immune function)를 구성할 수 있다. 다음 장에서 최적 상관 무결 함수가 되는 semi-bent 함수 생성 방법을 제안한다.

4. 최적 상관 무결 semi-bent 함수

n은 4 보다 같거나 큰 정수이며, k는 $1 \le k \le n-3$인 정수이다. 또한, m은 $1 \le m < n-k$인 정수이다. $\phi : Z_2^m \to Z_2^{n-m}$ 는 모든 $y \in Z_2^m$ 에 대해서 $wt(\phi(y)) \ge k+1$ 인 단사 함수(injective function)이다. 마지막으로 r은 Z_2^m에 정의된 부울 함수이다.

그러면, $y \in Z_2^m$ 와 $x \in Z_2^{n-m}$ 에 대해서, 함수 $f : Z_2^n \to Z_2$를 다음으로 정의한다.

$$f(y,x) = \phi(y) \cdot x \oplus r(y). \qquad (1)$$

보조정리 2. 식 (1)의 부울 함수 $f \in B_n$ 과 $b \in Z_2^m$, $a \in Z_2^{n-m}$에 대해서 다음 사실이 성립한다.

$\hat{\mathcal{F}} f(b,a) = 0$ 또는 $\pm 2^{n-m}$.

증명.

$$\hat{\mathcal{F}} f(b,a) = \sum_{y,x} (-1)^{f(y,x)} \cdot (-1)^{(y,x)\cdot(b,a)}$$

$$= \sum_{y} (-1)^{b \cdot y \oplus r(y)} \sum_{x} (-1)^{(\phi(y) \oplus a) \cdot x}$$

$$= \begin{cases} 2^{n-m}(-1)^{b \cdot \phi^{-1}(a) \oplus r(\phi^{-1}(a))} \\ \quad \text{어떤 } y \in Z_2^m \text{에 대해 } a = \phi(y) \text{인 경우,} \\ 0 \qquad \text{그 외의 경우.} \end{cases}$$

□

보조 정리1과 2에 의해 다음 사실이 성립함을 알 수 있다.

정리 2. $f \in B_n$ 은 식 (1)의 부울 함수이다. 그러면,

1. f는 균등 함수이다.
2. $N_f = 2^{n-1} - 2^{n-m-1}$.
3. f는 단지 2개의 상관값을 가진다.
4. f는 k차 상관 무결 함수이다.
5. f는 $0 \ne \beta \in Z_2^m$, $\alpha \in Z_2^{n-m}$인 (β, α)에 대해서, PC를 만족한다.
6. $1 \le i \le n-m$인 i에 대해 $\oplus_y \phi(y)i = 1$ 이면, $deg(f) = m+1$ 이다. 여기서, $\phi(y)_i$는 $\phi(y)$의 i 번째 *component* 이다.

증명.

1. $wt(\phi(y)) \geq k+1$이므로 $\phi(y) \neq 0$ 이다. $\hat{\mathcal{F}}(0\}) = 0$ 이다.
2. $\max_{b,a}|\hat{\mathcal{F}}_f(b,a)| = 2^{n-m}$ 임으로, $\mathcal{N}_f = 2^{n-1} - 2^{n-m-1}$ 이다.
3. 임의의 $w \in Z_2^n$에 대해

$$|c(f, l_w)| = \frac{1}{2^n}|\hat{\mathcal{F}}_f(w)| = 2^{-m} \text{ 또는 } 0$$

이다.

4. $(b,a) \in Z_2^n$을 $1 \leq wt(b,a) \leq k$ 이라 하자. 임의의 $y \in Z_2^m$에 대해 $wt(\phi(y)) \geq k+1$이므로, $\phi(y) \neq a$ 이다. 따라서, $\hat{\mathcal{F}}(b,a) = 0$ 이다.
5. $0 \neq \beta \in Z_2^m$ 이고 $\alpha \in Z_2^{n-m}$ 인$(\beta, \alpha) \in Z_2^n$에 대해,

$$\sum_{b,a} \hat{\mathcal{F}}^2(b,a)(-1)^{(\beta,\alpha)\cdot(b,a)}$$

$$= 2^{2n-2m}\sum_{a\in im(\phi)}(-1)^{a\cdot\alpha}\sum_{b}(-1)^{b\cdot\beta} = 0 \text{ 이다.}$$

6. $\oplus_y \phi(y)i = 1$ 임으로, $deg(f) = m+1$ 이다.

□

정리 2에 의하여 식 (1)의 부울 함수 f는 균등 함수이고, 단지 2개의 상관값을 가지므로 semi-bent 함수이다.

정수 k에 대해서 m이 증가하면, 부울 함수 f의 비선형치와 대수적 차수 또한 증가한다. 그러나, ϕ는 단사 함수이고 모든 $y \in Z_2^m$ 에 대해 $wt(\phi(y)) \geq k+1$ 이어야 하므로 정수 m의 범위는 제한된다. 예를 들어, $n=4$, $m=2$, $k=1$ 이면 모든 $y \in Z_2^2$ 에 대해 $wt(\phi(y)) \geq 2$ 를 만족하는 함수 $\phi : Z_2^2 \rightarrow Z_2^2$가 존재하지 않는다. 다음 정리는 m을 결정하는 방법을 제시한다.

정리 3. 임의의 k에 대해, 모든 $y \in Z_2^m$에 대해 함수 ϕ가 $wt(\phi(y)) \geq k+1$를 만족하게 하는 가장 큰 정수 m은 다음 방정식을 만족하는 가장 큰 정수 m 이다.

$$\binom{n-m}{k+1} + \binom{n-m}{k+2} + \cdots + \binom{n-m}{n-m} \geq 2^m$$

따름정리 1. 함수 f의 m의 범위는 $m < [n/2]$ 이다.

$$2^{n-m} = \binom{n-m}{0} + \binom{n-m}{1} + \cdots + \binom{n-m}{k} + \binom{n-m}{k+1} +$$

$$\binom{n-m}{K+2} + \cdots + \binom{n-m}{n-m}$$

이므로, $2^{n-m} > 2^m$ 이다. 따라서, $m < [n/2]$ 이다.

ϕ가 전단사 함수(bijective function)이면 n은 짝수이고, $m = \frac{n}{2}$ 이다.

또한, $\mathcal{N}_f = 2^{n-1} - 2^{\frac{n}{2}-1}$ 이고 f은 모든 0이 아닌 점에 대해 PC를 만족한다. 즉, f는 bent 함수이며, 본 논문에서 제안한 부울 함수 설계 방법은 Maiorana의 설계 방법과 동일하다[8]. 본 논문에서 제안한 부울 함수는 다음의 성질을 만족한다.

정 리 4.

1. ζ를 $|c(f, l_w)| = 2^{-m}$인 w의 개수라 하자. 그러면, 정리 1에 의하여

$$2^{2n} = \sum_{w} \hat{\mathcal{F}}^2(w) = \zeta \cdot 2^{2n-2m}$$

이다. 따라서, $\zeta = 22^m$ 이다.

2. 부울 함수 f가 PC를 만족하는 점들의 개수는 적어도 $(2^m-1)2^{n-m} = 2^n - 2^{n-m}$ 보다 크다.

예 1. $n=4$, $k=1$, $m=1$, 그리고, 단사 함수 $\phi : Z_2 \rightarrow Z_2^3$가 by $\phi(0) = (1,1,0)$, $\phi(1) = (1,1,1)$ 이다. 그러면, 부울 함수

$$f(y,x) = \phi(y)\cdot x,\ y \in Z_2,\ x \in Z_2^3$$

은 $x_1 \oplus x_2 \oplus x_3\ y_1$ 이며, 다음 성질을 만족한다.

1. f는 균등 함수이다.
2. $N_f = 2^{4-1}-2^{4-1-1} = 4$.
3. f는 단지 2개의 상관값을 가진다.
4. f는 1차 상관 무결 함수이다.
5. f는 $(1,\alpha)$에 대해서 PC를 만족한다. 즉, 함수 f가 PC를 만족하는 점의 개수는 적어도 $2^3 = 8$ 이상이다.
6. $\oplus_y \phi(y)_3 = 1$ 임으로 $deg(f) = 2$ 이다.

5. 결 론

본 논문에서는 참고 문헌 [2,5]에서 제안된 균등 함수이며 2개의 상관값만을 가지는 semi-bent 함수에 대해서, 상관 무결의 범위를 결정할 수 있으며, 상관값이 0이 아닌 경우에도 균일한 상관값을 가지는 semi-bent 함수 설계 방법을 제안하였다. Parseval의 정리에 의하면 아무리 상관 무결 특성이 우수한 함수라 하여도 특정한 선형 함수와의 상관 관계는 반드시 존재하므로, 상관 무결이 아닌 부분에서 균일한 상관값을 가지는 부울 함수의 설계가 요구된다. 본 논문에서 제안한 방법에 의해 상관 무결 특성 관점에서 최적의 특성을 가지는 부울 함수를 설계할 수 있다.

참 고 문 헌

[1] P. Camion, C. Carlet, P. Charpin, and N. Semdroer. 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

[2] Seongtack 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

[3] Seongtaek Chee, Sangjin Lee, Kwangjo Kim, and Daeho Kim. Correlation immune functions With Controllable nonlinearity. ETRI Journal, 19(4):389-402, December 1977.

[4] Seongtaek Chee, Sangjin Lee, amd Soo Hak Sung. On the correlation immune functions and their nonlinearity. In Kwangjo Kim and Tsutomu Matsumoto, editors, editors, Advances in Cryptology : ASIA CRYPT' 96, volume 1163 of Lecture Notes in Computer science, pages 232-243. Springer-Verlag, Berlin, 1995.

[5] 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

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

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

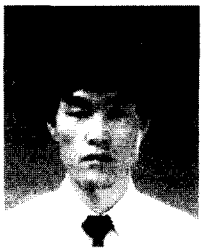
[8] Rainer A. Rueppel. Stream ciphers. In Gustavus J. Simmons, editor, Contemporary Cryptology : The Science of Information Integrity, chapter2, pages 65-134. IEEE Press, 1992.

[9] 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

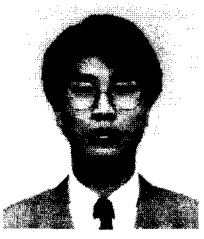
[10] T. Siegenthaler. Correlation immunity of non-linear combining functions for cryptographic applications. IEEE Transactions on Information Theory, IT-30(5): 776-780, September 1984.

□ 著者紹介



지 성 택

1985년 2월 서강대학교 이공대학 수학과(이학사)
1987년 2월 서강대학교 대학원 수학과(이학석사)
1999년 2월 고려대학교 대학원 수학과 (이학박사)
1989년 ~ 현재 한국전자통신연구원 선임연구원



박 상 우

1989년 2월 고려대학교 사범대학 수학교육학과(이학사)
1991년 2월 고려대학교 대학원 수학과(이학석사 : 응용수학 및 확률론)
1991년 ~ 현재 한국전자통신연구원 선임연구원

□ 著者紹介

김 대 호

1977년 2월 한양대학교 전자공학과(공학사)
1984년 2월 한양대학교 산업대학원 전자공학과(공학석사)
1993년 2월 Visiting Scholar(University of Maryland at College Park Dept. of Computer Science)
1977년 ~ 현재 한국전자통신연구원 책임연구원

※ 주관심분야 : 전송분야, 통신 및 컴퓨터 보안

임 종 인

1980년 2월 고려대학교 수학과 학사
1982년 2월 고려대학교 대학원수학과 석사
1986년 2월 고려대학교 대학원 수학과 이학박사
1986년 8월 ~ 현재 고려대학교 수학과 교수

※ 주관심분야 : 컴퓨터 · 네트워크 보안