通信情報保護學會論文誌
第 7 卷 第 4 號, 1997. 12

균형인 부울함수의 대역확산특성

성 수 학*, 천 정 희**, 지 성 택**, 김 광 조**

Global Avalanche Characteristics of Balanced Boolean Functions

Soo Hak Sung, Jung Hee Cheon, Seongtaek Chee, Kwangjo Kim

요 약

GAC(Global Avalanche Characteristics)은 부울함수가 확산특성 관점에서 얼마나 우수한지를 전체 경우에 대하여 나타내는 특성으로 Zhang-Zheng(1995)에 의해서 제안되었다. GAC 개념이 등장하기 이전에는 부분적인 확산특성에 대하여만 연구를 하였으나 다른 암호학적인 특성과 연관하여 생각하면 전체적인 확산특성이 의미가 있다. Zhang-Zheng은 GAC을 측정하는 두가지 기준을 제시하고 이 기준에 대한 하한과 상한을 구하였으며 선형함수와 벤트함수에 대하여 이러한 상한과 하한이 달성됨을 증명하였다. 그러나 암호학적으로 의미가 있는 균형인 함수의 두가지 기준에 대한 하한과 상한은 밝혀지지 않았다. 본 논문에서는 부울함수가 균형일 때 GAC을 측정하는 기준에 대한 하한을 제시한다. 이러한 하한은 아직까지 미해결 문제로 남아있는 균형인 부울 함수의 비선형치에 대한 상한을 구하는데 새로운 방향을 제시할 수 있다.

Abstract

GAC(Global Avalanche Characteristics) was introduced by Zhang-Zheng (1995) as a measure of cryptographic strength for Boolean functions. They proposed two indicators related to GAC, and they gave lower and upper bounds on the two indicators. In this paper, we give a lower bound on the one indicator for the balanced boolean functions.

1. 서 론

암호학에서 사용되는 부울 함수의 주요 요구조건으로는 균형성, 비선형성, 확산특성, 상관면역성 등이 있다[8][9]. 이 중에서 확산특성은 SAC(Strict Avalanche Criterion)과 PC(Propa-

* 배재대학교 응용수학과
* * 한국전자통신연구원 부호1실

gation Criterion)에 의하여 조사될 수 있으며, SAC과 PC에 대한 연구는 블럭 암호 알고리즘의 발전과 함께 1990년 이후로 많이 연구되어 왔다[3][4][5]. 그러나 PC와 SAC은 부울 함수의 국부적(local)인 확산특성을 측정하는 요소이기 때문에 확산 특성을 나타내는 지표로서 불충분하다. 즉, SAC은 Hamming 가중치가 1인 벡터에 대해서만 확산특성을 조사하는 것이고 PC는 어떤 특정한 벡터 α(α에 대해 PC를 만족할 경우) 또는 Hamming 가중치가 k 이하인 벡터(k차 PC를 만족하는 경우)에 대해서만 확산특성을 조사하는 것이기 때문이다.

1995년 Zhang-Zheng은 모든 벡터에 대해 확산특성을 측정하는 개념으로 대역확산 특성(GAC, Global Avalanche Characteristics)을 제안하였다. 이들은 PC 특성을 이용하여 부울함수 f의 σ_f와 Δ_f를 정의하고, 이 두값이 작을수록 대역 확산 특성이 우수하다고 하였다. 또한, 이들은 임의의 부울함수 f의 σ_f와 Δ_f에 대한 하한과 상한을 구하였으며, σ_f와 Δ_f의 하한에 대응되는 함수는 벤트(bent)함수이고 상한에 대응하는 함수는 선형 함수와 선형구조(linear structure)를 갖는 함수임을 증명하였다. 즉, 벤트함수가 대역확산특성 관점에서 가장 우수한 함수이다. 하지만 벤트함수는 균형이 아니라는 것이 잘 알려져 있다. 균형성은 부울함수가 암호 논리로 사용되기위한 최소의 필요조건이기 때문에, 대부분의 암호학적 특성 연구는 균형이면서 비선형성이 우수하거나, 균형이면서 SAC 및 PC 특성이 우수한 부울 함수를 설계하고 그 특성을 연구하는 방향으로 진행되어왔다.

본 본문의 목적은 균형인 부울 함수에 대한 대역확산특성을 연구하는 것이다. 즉, f가 균형일 때, σ_f의 하한을 구하고자 한다. 이러한 결과는 추후 균형인 부울 함수에 대한 비선형치의 상한[1]을 구하는데 이용할 수 있기 때문에 매우 의미있는 일이다.

2. 기본적인 정의

n 차원 벡터공간 $\{0, 1\}^n$ 상의 부울함수 f는 $\{0, 1\}^n \rightarrow \{0, 1\}$인 함수이다. 두 벡터 $x=(x_1, \ldots, x_n)$와 $y=(y_1, \ldots, x_n)$의 내적을 $x \cdot y$로 표시하며 $x \cdot y = x_1 y_1 \oplus \ldots x_n y_n$으로 정의한다. 또 두 벡터 x와 y의 XOR를 $x \oplus y$로 표시하며 $x \oplus y = (x_1 \oplus y_1, \ldots, x_n \oplus y_n)$으로 정의한다.

부울함수 f가 0과 1의 값을 가질 가능성이 같은, 즉 $\#\{x|f(x)=0\}=\#\{x|f(x)=1\}$인 부울함수를 균형(Balance)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[6]. 벡터 α에 대해 $f(x) \oplus f(x \oplus \alpha)$가 균형일 때 부울함수 f는 α에 대해 PC(Propagation Criterion)를 만족한다고 정의한다[1], [3]. Hamming 가중치가 k 이하인 모든 벡터에 대해 PC를 만족할 때 부울함수 f는 k차 PC를 만족한다고 정의한다. 1차 PC 조건이 바로 SAC이며, n차 PC를 만족하는 부울함수가 바로 완전비선형(Perfect Nonlinear)함수이다. 완전비선형 함수를 벤트(Bent)함수라고 부르기도 한다. SAC과 PC는 어떤 특정한 벡터에 대한 확산특성을 측정하므로 부울함수에 대한 전반적인 확산특성을 나타내지 못한다. 전반적인 확산특성을 측정할 수 있는 개념인 대역확산특성(GAC, Global Avalanche Characteristics)은 Zhang-Zheng[7]에 의해서 제안되었으며, 그들은 GAC를 측정하는 두 개의 기준을 제시하였다.

정의 2.1. 부울함수 $f:\{0, 1\}^n \rightarrow \{0, 1\}$에 대한

1 균형인 부울 함수의 정확한 상한을 구하는 문제는 아직 미해결 과제이다.

대역확산특성을 측정하는 두 개의 기준 σ_f와 Δ_f를 다음과 같이 정의한다.

$$\sigma_f = \sum_w \Delta_f^2 f(w)$$

$$\Delta_f = \max_{w \neq 0} |\Delta_f(w)|$$

여기서 $\Delta_f(w)=\sum_x (-1)f(x)(-1)^{f(x\oplus w)}$이다.

σ_f나 Δ_f가 작을수록 대역확산특성이 좋다고 말한다. Zhang-Zheng[7]은 σ_f와 Δ_f의 하한과 상한을 구하였다.

$$2^{2n} \leq \sigma_f \leq 2^{3n} \quad 0 \leq \Delta_f \leq 2^{2n}$$

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 좋은 부울함수이다. 하지만 벤트함수는 균형이 아니다. 그러면 균형인 부울함수 중에서 대역확산특성이 가장 좋은 것을 무엇인가? 이와 관련된 문제를 본 논문에서 연구하고자 하며 본격적인 논의는 다음 절에서 하기로 한다.

3. 균형인 부울함수에 대한 σ_f의 하한

부울함수 f가 균형일 때 σ_f의 하한을 계산해 보자. 먼저 일반적인 부울함수(균형일 필요 없음)에 대한 σ_f의 계산을 살펴보자. $\sigma_f=\sum_x \Delta_f^2 f(w)$로 정의되었음을 기억하기 바란다.

보조정리 3.1. 부울함수 f에 대해 다음식이 성립한다.

$$\sum_x \Delta_f^2(x) = \sum_x [2\#\{y|f(y)=f(x\oplus y)\}-2^n]^2$$

<증명> $\Delta_f(x)$의 정의에 의해서

$$\Delta_f(x) = \sum_y (-1)^{f(y)}(-1)^{f(x\oplus y)}$$

$$=\#\{y|f(y)=f(x\oplus y)\}-\#\{y|f(y)\neq f(x\backslash\oplus y)\}$$

$$=2\#\{y|f(y)=f(x\oplus y)\}-2^n$$

이다. 고로 증명이 완성된다.

부울함수가 균형일 때 $\#\{y|f(y)=f(x\oplus y)\}$의 합과 제곱합을 계산해 보자.

보조정리 3.2. 부울함수 f가 균형이면

$$\sum_x \#\{y|f(y)=f(x\oplus y)\}=2^{2n-1}$$

<증명> 균형인 부울 함수 f에 대하여 다음이 성립한다.

$$\sum_x \#\{y|f(y)=f(x\oplus y)\}$$

$$=\sum_y \#\{x|f(y)=f(x\oplus y)\}$$

$$=\sum_y \#\{z|f(y)=f(z)\}$$

$$=\sum_y 2^{n-1}=2^{2n-1}$$

고로 증명이 완성된다.

보조정리 3.3. 부울함수 f가 균형이면

$$\sum_x [\#\{y|f(y)=f(x\oplus y)\}]^2=4\sum_x [\sum_y f(y)f(x\oplus y)]^2$$

<증명> 임의의 x에 대해 다음이 성립한다.

$$\#\{y|f(y)=f(x\oplus y)\}=2f(y)f(x\oplus y)-f(y)-f(x\oplus y)+1$$

따라서

$$\sum_x [\#\{y|f(y)=f(x\oplus y)\}]^2$$

$$=\sum_x [\sum_y 2f(y)f(x\oplus y)-f(y)-f(x\oplus y)+1]^2$$

$$=\sum_x [2\sum_y f(y)f(x\oplus y)-\sum_y f(y)-\sum_y f(x\oplus y)+2^n]^2$$

$$=\sum_x [2\sum_y f(y)f(x\oplus y)-2^{n-1}-2^{n-1}+2^n]^2$$

$$=4\sum_x[\sum_y f(y)f(x\oplus y)]^2$$

이다. 따라서 증명이 완성된다.

보조정리 3.1, 3.2, 3.3을 이용하여 σ_f를 다음 정리와 같이 쓸 수 있다.

정리 3.4. 부울함수 f가 균형이면

$$\sum_x \Delta^2_f(x)=16\sum_x[\sum_y f(y)f(x\oplus y)]^2-2^{3n}$$

<증명> 보조정리 3.2와 보조정리 3.3을 보조정리 3.1에 적용하면

$$\sum_x \Delta^2_f(x)=4\sum_x[\#\{y|f(y)=f(x\oplus y)]^2-2^{n+2}\sum_x\#\{y|f(y)=f(x\oplus y)\}]+2^{3n}$$

$$=16\sum_x[\sum_y f(y)f(x\oplus y)]^2-2^{n+2}2^{2n-1}\}+2^{3n}\}$$

$$=16\sum_x[\sum_y f(y)f(x\oplus y)]^2-2^{3n}$$

이다. 따라서 증명이 완성된다.

이젠 부울함수 f가 균형일 때 $\sum_x[\sum_y f(y)f(x\oplus y)]^2$을 계산해 보자. 이를 위해 다음 보조정리가 필요하다. 이 결과는 잘 알려져 있기 때문에 여기서는 증명을 생략하기로 한다.

보조정리 3.5. $x_1, \ldots, x_n$의 합이 M, 즉 $\sum_{i=1}^n x_i=M$이라 하자. 이때, $\sum_{i=1}^n x_i^2$는 모든 $i(1\le 1\le n)$에 대해 $x_i=M/n$\$일 때 최소값 M^2/n을 갖는다.

보조정리 3.6. 부울함수 f가 균형이고 $f(0)=1$일 때

$$\sum_x[\sum_y f(y)f(x\oplus y)]^2\ge 2^{2n-2}+\min_{t_i}[\sum_{i=0}^{2^{n-1}} i^2t_i+\}\frac{1}{2^{n-1}}(\sum_{i=0}^{2^{n-1}}(2^{n-1}-i)t_i)^2]$$

이다. 여기서 t_i는 음이 아닌 정수로서 i가 홀수일 때 $t_i=0$이고 $\sum_{i=0}^{2^{n-1}} t_i=2^{n-1}-1$인 수열이다.

<증명>부울함수 f가 균형이므로 0에 대한 역상 $f^{-1}(0)$과 1에 대한 역상 $f^{-1}(1)$의 크기는 2^{n-1}로 같다. $f^{-1}(0)$을 집합 A로 나타내고 그 원소를 $a_1, \ldots, a_{2^{n-1}}$로 쓰기로 한다. 또 $f^{-1}(1)$을 집합 B로 나타내고 그 원소를 $b_1, \ldots, b_{2^{n-1}}$로 쓰기로 한다. 즉

$$A=f^{-1}(0)=\{a_1, \ldots, a_{2^{n-1}}\}$$
$$B=f^{-1}(1)=\{b_1, \ldots, b_{2^{n-1}}\}$$

$f(0)=1$이므로 $\{0, 1\}^n$ 상의 벡터 0은 B의 원소이며 편의상 B의 원소 b_1을 0벡터로 표시하자. 또 각 $x\in\{0, 1\}^n$에 대해 $x\oplus y\in B$인 y의 영역을 B_x로 표시하자.

$$B_x=\{y|x\oplus y\in B\}$$

그러면 $B_x=\{x\oplus b_i, 1\le i\le 2^{n-1}\}$이다. 집합 B_x의 원소 중 집합 A의 원소인 것의 수를 α_x, 집합 B_x의 원소 중 집합 B의 원소인 것의 수를 β_x로두자.

$$\alpha_x=\#B_x\cap A$$
$$\beta_x=\#B_x\cap B$$

그러면 $\sum_y f(y)f(x\oplus y)=\beta_x$이며

$$\sum_x\{\sum_y f(y)f(x\oplus y)\}^2=\sum_x\beta^2_x$$

이다. 한편 $\alpha_x+\beta_x=\#B_x$이므로 $\alpha_x+\beta_x=2^{n-1}$이다. $B_0=B$이므로 $\beta_{b_1}\}=2^{n-1}$이다(앞에서 $b_1=0$이라는 사실에 유의하기 바람). 또 B_x의 원소 $x\oplus b_i$가 B의 원소이면 $x\oplus b_i=b_j$로 쓸 수 있다. 그러면 $x\oplus b_j=b_i$이므로 $x\oplus b_j$는 B_x의 원소이며 동시에 B의 원소이다. 따라서 $\#B_x\cap B$의 원소 개수 β_x는 짝수이다. 한편 $\{0, 1\}^n=\{b_1, \ldots, b_{2^{n-1}}, a_1, \ldots, a_{2^{n-1}}\}$이므로 $\{0, 1\}$ 상의 벡터 x를 b_i 또는 a_i로 표시할 수 있다. $\beta_{b_2}, \ldots, \beta_{b_{2^{n-1}}}$ 중 i인 것의 개수를 $t_i(0\le i\le 2^{n-1})$라고 두자. 즉

$$t_i=\#\{j|\beta_{b_j}=i, 2\le j\le 2^{n-1}\}$$

그러면

$$\sum_{i=2}^{2^{n-1}} \beta^2_{b_i} = \sum_{i=0}^{2^{n-1}} i^2 t_i$$

이다. β_{b_j}가 짝수이므로 i가 홀수일 때 $t_i=0$이고, $t_0+t_2+\ldots+t_{2^{n-1}}=2^{n-1}-1$이다. 또 $\alpha_x+\beta_x=2^{n-1}$이므로 $\alpha_{b_2}, \ldots, \alpha_{b_{2^{n-1}}}$ 중 i인 것의 개수는 $t_{2^{n-1}-i}$이다.

한편

$$\alpha_{b_k}=\#B_{b_k}\cap A=\sum_{i=1}^{2^{n-1}}\sum_{j=1}^{2^{n-1}} I_{b_k\oplus b_i=a_j}$$

$$\beta_{a_k}=\#B_{a_k}\cap B=\sum_{i=1}^{2^{n-1}}\sum_{j=1}^{2^{n-1}} I_{a_k\oplus b_i=b_j}$$

이므로

$$\begin{aligned}\sum_{k=1}^{2^{n-1}} \beta_{a_k} &= \sum_{k=1}^{2^{n-1}}\sum_{i=1}^{2^{n-1}}\sum_{j=1}^{2^{n-1}} I_{a_k\oplus b_i=b_j}\\ &= \sum_{i=1}^{2^{n-1}}\sum_{j=1}^{2^{n-1}}\sum_{k=1}^{2^{n-1}} I_{b_i\oplus b_j=a_k}\\ &= \sum_{i=1}^{2^{n-1}} \alpha_{b_i} = \sum_{i=2}^{2^{n-1}} \alpha_{b_i}\\ &= \sum_{i=0}^{2^{n-1}} i t_{2^{n-1}-i} = \sum_{i=0}^{2^{n-1}} (2^{n-1}-i)t_i\end{aligned}$$

이다. 따라서 보조정리 3.5에 의해서

$$\sum_{k=1}^{2^{n-1}} \beta^2_{a_k} \ge \Big(\sum_{i=0}^{2^{n-1}} (2^{n-1}-i)t_i\Big)^2/2^{n-1}$$

이다. 고로

$$\begin{aligned}\sum_x \{\sum_y f(y)f(x\oplus y)\}^2 \& &= \sum_x \beta^2_x\\ &= \sum_{i=1}^{2^{n-1}} \beta^2_{b_i} + \sum_{i=1}^{2^{n-1}} \beta^2_{a_i}\\ &= \beta^2_{b_1} + \sum_{i=2}^{2^{n-1}} \beta^2_{b_i} + \sum_{i=1}^{2^{n-1}} \beta^2_{a_i}\\ &= 2^{2n-2} + \sum_{i=0}^{2^{n-1}} i^2 t_i + \sum_{i=1}^{2^{n-1}} \beta^2_{a_i}\\ &\ge 2^{2n-2} + \sum_{i=0}^{2^{n-1}} i^2 t_i + \frac{1}{2^{n-1}}\Big(\sum_{i=0}^{2^{n-1}} (2^{n-1}-i)t_i\Big)^2\end{aligned}$$

이다. 따라서 증명이 완성된다.

보조정리 3.6을 정리 3.4에 적용하면 아래의 결과를 얻을 수 있다.

정리 3.7. 부울함수 f가 균형일 때

$$\sigma_f = \sum_x \Delta^2_f(x) \ge 2^{2n+2} - 2^{3n} + 2^4 \min_{t_i} \Big[\sum_{i=0}^{2^{n-1}} i^2 t_i + \frac{1}{2^{n-1}}\Big(\sum_{i=0}^{2^{n-1}} (2^{n-1}-i)t_i\Big)^2\Big]$$

이다. 여기서 $\{t_i\}$는 음이 아닌 정수로서 i가 홀수일 때 $t_i=0$이고 $\sum_{i=0}^{2^{n-1}} t_i = 2^{n-1}-1$인 수열이다.

<증명> 부울함수 f가 균형이고 $f(0)=1$이면 위의 결과는 정리 3.4와 보조정리 3.6에 의해서 바로 증명된다. 만일 $f(0)=0$인 경우에는 $g(x)=f(x)\oplus 1$로 두면 g는 균형이고 $g(0)=1$이다. 따라서 g에 대해 정리가 성립한다. 그런데 $\Delta_f(x)=\Delta_g(x)$이므로 $f(0)=0$인 f에 대해서도 성립한다.

[주] 정리 3.7에서 $\min_{t_i}$을 취한 식은 부울함수 f에 무관하며 단지 수열 $\{t_i, 0\le i\le 2^{n-1}\}$에 의존한다.

이젠 정리 3.7에서 구한 σ_f의 하한을 $l(n)$이라고 두자. 즉

$$l(n) = 2^{2n+2} - 2^{3n} + 2^4 \min_{t_i} \Big[\sum_{i=0}^{2^{n-1}} i^2 t_i + \frac{1}{2^{n-1}}\Big(\sum_{i=0}^{2^{n-1}} (2^{n-1}-i)t_i\Big)^2\Big]$$

Zhang-Zheng[7]은 일반적인 부울함수(균형일 필요 없음)에 대해 σ_f의 하한이 2^{2n}임을 증명하였다. 부울함수가 균형일 때 본 논문에서 구한 σ_f의 하한과 Zhang-Zheng이 구한 것, 그리고 최적의 하한을 비교하면 다음 표와 같다.

n이 작을 때($n\le 5$) σ_f의 최적의 하한을 구할 수 있으나 n이 크면 구하기 어렵다. 위의 표에서 알 수 있듯이 우리의 하한은 Zheng-Zheng의 하한보다 크기 때문에 우리의 것이 그들의 것보다 좋은 하한이다. n이 2일 때 우리의 하

n	Zhang-Zheng의 결과	본 논문의 결과	최적의 하한
2	16	24	64
3	64	80	128
4	256	288	640
5	1024	1088	1664

한과 최적의 하한과는 2.67배, n=3일 때는 1.6배, n=4일 때는 2.22배, n=5일 때는 1.53배 차이가 나므로, n이 홀수로 증가하거나 짝수로 증가함에따라 그 비율이 감소함을 알 수 있다.

4. 결 론

본 논문에서는 부울함수가 균형일 때 대역 확산특성을 측정하는 기준인 σ_f의 하한을 구하였다. σ_f의 하한은 f의 비선형치의 상한을 구하는데 직접 이용되기 때문에 그 활용 범위 및 암호학에 미치는 파급 효과가 매우 큰 문제이다.

본 논문에서 제시한 하한은 $n \le 5$일 때 Zhang-Zheng(1995)의 것보다 우수하며, 최적은 아니지만 n이 홀수로 증가하거나 짝수로 증가함에 따라 최적의 하한에 접근함을 부분적으로 관찰하였다.

본 논문에서는 부울함수 f가 균형일 때 σ_f의 하한을 구하였지만 이 하한은 아주 복잡한 식으로 되어 있어 부울함수의 입력크기 n이 클 때($n \ge 6$) 정확한 값을 계산하기 어렵다. 따라서 앞으로 본 연구팀은 하한을 보다 간단한 식으로 표현할 수 있는지를 조사하여, 최적의 하한에 근접하게 하는 연구를 계속할 예정이다.

참 고 문 헌

[1] C. M. Adams and S. E. Tavares, "Generating and counting binary bent sequences", IEEE Transactions on Information Theory, IT-36 N0. 5, pp. 1170-1173, 1990.

[2] H. Dobbertin, "Construction of bent functions and balanced boolean functions with high nonlinearity", Fast Software Encryption, LNCS 1008, Springer-Verlag, pp. 61-74, 1995.

[3] B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle, "Propagation characteristics of boolean functionn", Eurocrypt'90, LNCS 437, pp. 155-165, 1991.

[4] J. Seberry and X. M. Zhang, "Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion", Auscrypt'92, LNCS 718, Springer-Verlag, pp.145-155, 1993.

[5] J. Seberry, X. M. Zhang, and Y. Zheng, "Nonlinearly balanced boolean functions and their propagation characteristics", Crypto'93, LNCS 773, Springer-Verlag, pp. 49-60, 1994.

[6] A. F. Webster and S. E. Tavares, "On the design of S-boxes", Crypto'85, LNCS 219, Springer-Verlag, pp. 523-534, 1986.

[7] X. M. Zhang and Y. Zheng, "GAC-the criterion for global avalanche characteristics of cryptographic functions", J. Universal Computer Science, 1, pp 320-337, 1995.

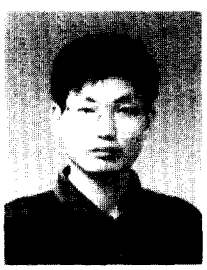
[8] 성수학, 지성택, 이상진, 김광조, "상관면역 함수와 비선형치", 통신정보보호학회 논문지, 제 6권, 3호, pp. 11- 22, 1996.

[9] 박상우, 지성택, 김광조, "Semi-bent 함수의 일반호와 구성 방법", 통신정보보호학회 논문지, 제 6권, 3호, pp. 31- 40, 1996.

□ 筆者紹介

성 수 학

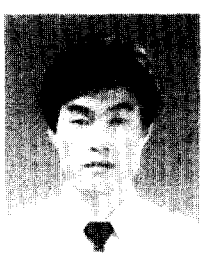
1982년 경북대학교 수학과 학사
1985년 KAIST 응용수학과 석사
1988년 KAIST 응용수학과 박사
1988년 ~ 1991년 한국전자통신연구소 선임연구원
1991년 ~ 현재 배재대학교 응용수학과 조교수



천 정 희

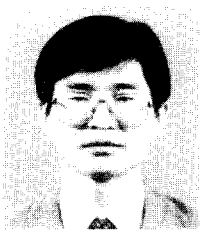
1991년 한국과학기술원 한국과학기술대학 수학과 학사
1993년 한국과학기술원 수학과 석사
1997년 한국과학기술원 수학과 박사
1997년 ~ 현재 한국전자통신연구원 선임연구원

※ 주관심 분야 : 정수론 및 그의 응용, 타원곡선 이론, 암호 이론



지 성 택

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



김 광 조

1973년 ~ 1980년 연세대학교 전자공학과(학사)
1981년 ~ 1983년 연세대학교 대학원 전자공학과(석사)
1988년 ~ 1991년 요꼬하마 국립대학 대학원 전자정보공학과(박사)
1979년 ~ 1997년 12월 한국전자통신연구원 부호1실장 재직
1997년 12월 ~ 현재 한국정보통신대학원 정보공학부 교수재직
본 학회 암호이론연구회 및 ISO/IEC JTC1 JSC-27 의장,
KIISC, IEICE, IEEE, IACR 각 회원

※ 주관심분야 : 암호학 및 응용 분야, M/W 통신