유한체 상에서 정의된 p진 Bent 함수

준회원 김 영 식, 장 지 웅, 종신회원 노 종 선*

On p-ary Bent Functions Defined on Finite Fields

Young-Sik Kim, Ji-woong Jang *Associate Members*, Jong-Seon No* *Life Member*

요 약

Bent 함수가 DES나 많은 블록 암호 시스템에서 차분 암호분석법이 어렵도록 만들어 주는 완전 비선형 함수와 상응관계가 있다는 것이 알려져 있다. 본 논문에서는 홀수인 소수 p에 대해서 유한체에서 정의된 2차 p진 bent 함수가 최적의 상관 특성을 갖는 p진 시퀀스의 군으로부터 주어졌다. 그리고 이차 p진 bent 함수, 즉 유한체 F_{p^m}에서 소수체 F_p로의 완전 비선형 함수가 trace 함수를 사용해서 생성되었다.

ABSTRACT

It is known that a bent function corresponds to a perfect nonlinear function, which makes it difficult to do the differential cryptanalysis in DES and in many other block ciphers. In this paper, for an odd prime p, quadratic p-ary bent functions defined on finite fields are given from the families of p-ary sequences with optimal correlation property. And quadratic p-ary bent functions, that is, perfect nonlinear functions from the finite field F_{p^m} to its prime field F_p are constructed by using the trace functions.

Key Words : Bent functions, bent sequences, perfect nonlinear function.

Ⅰ. 서 론

Rothaus는 m-tuple 이진 벡터 공간에서 $\{0,1\}$로의 bent 함수를 도입하였다[14]. m-tuple 이진 벡터 공간상에서 정의된 부울 함수는 푸리에 계수들이 $+1$과 -1 값만을 취할 경우에 bent 함수가 된다. 그리고 bent 함수는 선형 부울 함수로부터 Hamming 거리가 최대가 되는 함수이다. 좋은 푸리에 변환의 성질로부터 bent 함수들은 암호학, 최적의 상관 특성을 갖는[13] 이진 시퀀스의 군의 생성, 그리고 오류 정정부호와 같은 많은 분야에서 사용되어 왔다.

$a \in F_{q^m}^*$, $b \in F_q$에 대해서 $f(x+a)-f(x)=b$의 해 $x \in F_{q^m}$의 개수가 정확히 q^{m-1}일 때, F_{q^m}에서 F_q로의 함수를 완전 비선형 함수(perfect nonlinear function)라 부른다. Dembowski와 Ostrom은 평면 다항식(planar polynomial)을 생성하는 Dembowski-Ostrom 다항식을 제안하였다[2][3]. Nyberg는[11] DES와 다른 블록 암호 시스템에서의 차분 암호해석에 있어서 중요한 성질인 차분적 k-균등성(differential k-uniformity)을 갖는 사상(mapping)을 도입하였다. 그는 또한 완전 비선형 함

* 서울대학교 전기컴퓨터공학부 부호 및 암호 연구실(jsno@snu.ac.kr)
※ 본 연구는 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.
논문번호 : 030243-0609, 접수일자 : 2003년 6월 1일

수가 bent라는 것을 증명하였다[11]. Helleseth는 낮은 차분 균등성(differential uniformity)을[5][6] 갖는 몇 가지 멱 사상(power mapping)들을 도입하였고, 많은 다른 고도의 비선형 사상(highly nonlinear mapping)들이 Carlet과 Ding에 의해서 도입되었다[1].

이 논문에서는 홀수인 소수 p에 대해서 유한체에서 정의된 이차인 p진 bent 함수가 최적의 상관 특성을 갖는 p진 시퀀스의 군으로부터 주어졌다. 그리고 이차의 p진 bent 함수, 즉 유한체 F_{p^m}에서 소수체 F_p로의 완전 비선형 함수가 trace 함수를 이용해서 생성되었다.

Ⅱ. 예비지식

z가 정수이고 V_z^m이 z를 밑으로 하는 정수의 집합 J_z상에서의 m-차원 벡터 공간이라고 하자. 그리고 $\omega = e^{j\frac{2\pi}{z}}$, $j=\sqrt{-1}$이라고 하자. $f(x)$가 V_z^m에서 J_z로의 함수라 할 때 $f(x)$의 푸리에 변환과 푸리에 역변환이 다음과 같이 정의된다.

$$F(\underline{\lambda}) = \frac{1}{\sqrt{z^m}} \sum_{x\in V_z^m} \omega^{f(x)-\underline{\lambda}\cdot x^T}, \quad \text{all } \underline{\lambda}\in V_z^m$$

$$\omega^{f(x)} = \frac{1}{\sqrt{z^m}} \sum_{\underline{\lambda}\in V_z^m} F(\underline{\lambda})\omega^{\underline{\lambda}\cdot x^T}, \quad \text{all } x\in V_z^m$$

여기에서 x^T는 x를 전치시킨 것이다. 그러면 일반화된 bent 함수는 다음과 같이 정의된다.

정의 **1**. [Kumar, Scholtz, and Welch[8]]: V_z^m에서 J_z로의 함수 $f(x)$에서 이 함수의 푸리에 계수가 임의의 $\underline{\lambda}\in V_z^m$에 대해서 크기가 항상 1이 될 때 이 함수를 일반화된 bent 함수라 부른다. □

이 논문에서는 정수 z가 홀수인 소수 p일 때만 고려하였다. 그래서 V_p^m은 p개의 원소를 갖는 유한체 F_p상에서의 m-차원 벡터 공간이고 $f(x)$는 V_p^m에서 F_p로의 함수이다. 이 논문에서는 V_p^m에서 F_p로의 함수를 일반화된 bent 함수 대신에 p진 bent 함수라 부를 것이다.

F_{p^m}이 p^m개의 원소를 갖는 유한체라 하자. 임의의 양의 정수 e와 k에 대해서 $m=ek>1$라 하자. 그러면 $\mathrm{tr}_k^m(x)=\sum_{i=0}^{e-1} x^{p^{ki}}$로 정의되는 trace 함수 $\mathrm{tr}_k^m(\cdot)$는 F_{p^m}에서 부분체 F_{p^k}로의 사상이다. 여기에서 x는 F_{p^m}의 원소이다.

Olsen, Scholtz, 그리고 Welch는[13] F_{2^m}에서 F_2로의 함수에 대한 trace 변환을 도입하였다. 그러면 유한체 F_{p^m}에서 F_p로의 함수에 대한 trace 변환은 다음과 같이 일반화될 수 있다.

정의 **2**. [Olsen, Scholtz, and Welch[13]]: $f(x)$가 F_{p^m}에서 F_p로의 함수라 하자. 그러면 $f(x)$의 trace 변환과 역변환은 다음과 같이 정의된다.

$$F(\lambda) = \frac{1}{\sqrt{p^m}} \sum_{x\in F_{p^m}} \omega^{f(x)-\mathrm{tr}_1^m(\lambda\cdot x)}, \quad \text{all } \lambda\in F_{p^m}$$

$$\omega^{f(x)} = \frac{1}{\sqrt{p^m}} \sum_{\lambda\in F_{p^m}} F(\lambda)\omega^{\mathrm{tr}_m^k(\lambda\cdot x)}, \quad \text{all } x\in F_{p^m}$$

□

Nyberg는[12] $f(x+a)-f(x)=b$의 해 (단, 여기서 $a\in F_q^*$, $b\in F_q$) $x\in F_q$의 최대 개수가 k일 때 그 함수를 차분적 k-균등(differentially k-uniform)으로 정의했다. Nyberg는 Meier와 Staffelbach가 도입한 완전 비선형 함수를 다음과 같이 일반화하였다.

정의 **3**. [Nyberg[11]]: V_z^m에서 J_z로의 함수 $f(x)$는 모든 $\underline{\omega}\in V_z^m$, $\underline{\omega}\neq 0$에 대해서 그리고 $k\in J_z$에 대해서

$$f(x) = f(x+\underline{\omega}) + k$$

가 정확하게 z^{m-1}개의 $x\in V_z^m$에 대해서 만족할 경우에 완전 비선형이라 한다. □

그래서 완전 비선형 함수는 차분적 q^{m-1}-균등이다. Nyberg는 또한 완전 비선형 함수와 bent 함수 사이의 관계를 다음과 같이 증명하였다.

정리 1. [Nyberg[11]]: V_z^m에서 J_z로의 완전 비선형 함수는 bent이다. 역은 z가 소수인 경우에만 성립한다. □

다음절에서 우리는 F_{p^m}에서 F_p로의 p진 벤트 함수를 도입할 것이다. 이 함수는 차분적 p^{m-1}-균등 함수, 즉 완전 비선형 함수에 해당한다. 완전 비선형성은 DES와 많은 블록 암호 시스템에서 차분적 암호 분석에 있어서 중요한 성질로 여겨진다.

Ⅲ. 유한체에서 정의된 p진 Bent 함수의 생성

α가 유한체 F_{p^m}의 원시 원소라 하자. F_{p^m}에서의 x를 α^t로 치환하면, $F^*_{p^m}$에서 F_p로의 함수 $f(\alpha^t)$는 주기가 p^m-1인 p진 시퀀스로 여길 수 있다.

Welch의 상호상관 값들에 대한 하한으로부터[16], 주기가 p^m-1인 두 개의 p진 시퀀스의 상호상관 값들의 최대 값들은 $p^{m/2}+1$로 하한이 되고 이 때 p진 시퀀스가 최적의 상관 특성을 갖는다고 말한다.

Sidelnikov가 제안한 p진 시퀀스로부터, 우리는 다음과 같이 F_{p^m}에서 정의된 p진 bent 함수를 얻을 수 있다. 임의의 $b\in F^*_{p^m}$에 대해서,

$$f_b(x)=\mathrm{tr}_1^{\mathrm{m}}(bx^2)$$

Kumar와 Moreno는 최적 상관특성을 갖는 p진 시퀀스를 도입하였다. 이 시퀀스는 다음과 같이 F_{p^m}에서 정의된 p진 bent 함수를 생성한다. 임의의 $b\in F^*_{p^m}$에 대해서,

$$f_b(x)=\mathrm{tr}_1^{\mathrm{m}}(bx^{p^{kr}+1})$$

여기에서 e가 홀수인 정수일 때, $m=ek$이고 r은 $1\le r\le e-1$, $\gcd(r,e)=1$를 만족하는 정수이다. 또한 p진 Kasami 시퀀스는 다음과 같이 주어지는 F_{p^m}에서 정의된 p진 bent 함수를 생성한다. 임의의 $b\in F^*_{p^m}$에 대해서,

$$f_b(x)=\mathrm{tr}_1^{\mathrm{k}}(bx^T)$$

여기에서 $m=2k$이고 $T=p^k+1$이다. 더 나아가서, 다음 정리에서처럼 F_{p^m}에서 정의된 p진 bent 함수를 생성하는 것이 가능하다.

정리 2. $m=2k$ 또는 $2k+1$일 때, $a_i\in F_p$라 하자. F_{p^m}에서 F_p로의 이차 p진 함수

$$f(x)=\mathrm{tr}_1^{\mathrm{m}}\left(\sum_{i=0}^{k}a_ix^{1+p^i}\right) \tag{1}$$

는 다음과 같은 조건을 만족할 때 bent 함수, 즉 완전 비선형 함수이다. 모든 l, $0\le l\le m-1$에 대해서

$$\sum_{i=0}^{k}a_i(\varepsilon^{il}+\varepsilon^{il})\neq 0 \tag{2}$$

여기서 $\varepsilon=e^{j\frac{2\pi}{m}}$은 m-차 단위근이다. □

증명) 우리는 다음과 같은 trace 변환이 모든 $\lambda\in F_{p^m}$에 대해서 크기가 1을 가짐을 보여야 한다.

$$F(\lambda)=\frac{1}{\sqrt{p^m}}\sum_{x\in F_{p^m}}\omega^{\sum_{i=0}^{k}\mathrm{tr}_1^{\mathrm{m}}(a_ix^{1+p^i})-\mathrm{tr}_1^{\mathrm{m}}(\lambda x)}$$

$y_l=x^{p^l-1}$라 하자. 그러면

$$\begin{aligned}\sum_{i=o}^{k}\mathrm{tr}_1^{\mathrm{m}}(a_ix^{1+p^i}) &= \sum_{i=0}^{k}a_i\mathrm{tr}_1^{\mathrm{m}}(x^{1+p^i})\\ &=\sum_{i=0}^{k}a_i\sum_{l=1}^{m}(x^{1+p^i})^{p^l-1}\\ &=\sum_{i=0}^{k}a_i\sum_{l=1}^{m}x^{p^l-1+p^{l+i}-1}\\ &=\sum_{i=0}^{k}a_i\sum_{l=1}^{m}y_iy_{l+1}\\ &=G(y_1,y_2,\cdots,y_m)\end{aligned}$$

이다. 여기에서 $G(y_1,y_2,\cdots,y_m)$는 $V^m_{p^m}$에서의 이차 함수이다. [7]에서의 증명과 유사한 방법으로, $\{\mu_1,\mu_2,\cdots,\mu_m\}$와 $\{\gamma_1,\gamma_2,\cdots,\gamma_m\}$가 F_p상에서 F_{p^m}의 한 쌍의 쌍대기저(dual basis)라 하자. 즉

$$\mathrm{tr}_1^m(\gamma_i\mu_l)=\begin{cases}1, & \text{if } i=l\\ 0, & \text{otherwise}\end{cases}$$

이다. 그리고 기저 $\{\mu_1,\mu_2,\cdots,\mu_m\}$를 사용해서

$x=\sum_{i=1}^{m}x_i\mu_i \in F_{p^m}$일 때면 언제나

$\underline{x}=(x_1,x_2,\cdots,x_m)^T$

가 성립하고 쌍대기저로부터

$$x_i=\mathrm{tr}_1^m(x\gamma_i),\ 1\le i\le m$$

가 된다. 그러면 우리는 다음과 같은 관계식을 얻게 된다.

$$\underline{x}=A\underline{y},\ \underline{y}=B\underline{x}$$

여기서

$$A=\begin{bmatrix}\gamma_1 & \gamma_1^p & \gamma_1^{p^2} & \cdots & \gamma_1^{p^{m-1}}\\ \gamma_2 & \gamma_2^p & \gamma_2^{p^2} & \cdots & \gamma_2^{p^{m-1}}\\ & & \cdots & & \\ \gamma_m & \gamma_m^p & \gamma_m^{p^2} & \cdots & \gamma_m^{p^2}\end{bmatrix}$$

$$B=\begin{bmatrix}\mu_1 & \mu_2 & \mu_3 & \cdots & \mu_m\\ \mu_1^p & \mu_2^p & \mu_3^p & \cdots & \mu_m^p\\ & & \cdots & & \\ \mu_1^{p^{m-1}} & \mu_2^{p^{m-1}} & \mu_3^{p^{m-1}} & \cdots & \mu_m^{p^{m-1}}\end{bmatrix}$$

식 (1)에서 x를 $\sum_{i=1}^{m}x_i\mu_i$로 치환하면, V_p^m에서 정의된 이차 함수는 다음과 같이 주어진다.

$$H(\underline{x})=f(\sum_{i=1}^{m}x_i\mu_i)$$

그러면 다음 식이 성립한다.

$$G(\underline{y})=G(B\underline{x})=H(\underline{x})$$

만일 모든 l에 대해서 식 $\frac{\partial H(x_1,\cdots,x_m)}{\partial x_l}=0$의 집합에 0이 아닌 공통 해가 존재한다면, $H(x_1,x_2,\cdots,x_m)$는 특이성(singular)을 갖는다고 말한다.

Deligne의 정리[4]로부터, 만일 $H(\underline{x})$가 비특이적이라면(non-singular)

$$\left|\sum_{x\in V_p^m}\omega^{H(x)+L(x)}\right|\le p^{\frac{m}{2}}$$

가 성립한다. 여기서 $L(\underline{x})$는 V_p^m에서의 임의의 선형 함수이다. Parseval의 정리로부터 다음이 성립한다.

$$\left|\sum_{x\in V_p^m}\omega^{H(x)+L(x)}\right|=p^{\frac{m}{2}}$$

이것은 $F(\lambda)$가 모든 $\lambda\in F_{p^m}$에서 크기가 1이 된다는 것을 의미한다.

이제 $H(\underline{x})$의 비특이성(non-singularity)을 보여야 한다.

$$\frac{\partial H}{\partial \underline{x}}=\begin{bmatrix}\frac{\partial H}{\partial x_1}\\ \frac{\partial H}{\partial x_2}\\ \vdots\\ \frac{\partial H}{\partial x_m}\end{bmatrix}=B^T\frac{\partial G}{\partial \underline{y}}$$

가 성립하기 때문에 $G(\underline{y})$의 비특이성을 보이는 것으로 충분하다. $G(\cdot)$를 미분하면,

$$\frac{\partial G(y_1,\cdots,y_m)}{\partial y_1}=\sum_{i=0}^{k}a_i(y_{l+i}+y_{l-i})$$

만일 모든 l에 대해서, 식 $\frac{\partial G(y_1,\cdots,y_m)}{\partial y_l}=0$의 집합이 공통의 0이 아닌 해가 존재한다면, 즉 모든 l에 대해서 $\sum_{i=0}^{k}a_i(y_{l+i}+y_{l-i})\neq 0$가 성립한다면 $G(y_1,y_2,\cdots,y_m)$는 비특이성을 갖는다.

그래서 $G(y_1,y_2,\cdots,y_m)$이 비특이성을 갖기 위해서는 $m=2k+1$에 대해서 F_p상에서의 다음과 같이 주어지는 순환 행렬(circulant matrix)가 최대 계수(full rank)를 갖거나,

$$\begin{bmatrix} 2a_0 & a_1 & \cdots & a_k & a_k & a_{k-1} & \cdots & a_1 \\ a_1 & 2a_0 & \cdots & a_{k-1} & a_k & a_k & \cdots & a_2 \\ a_2 & a_1 & \cdots & a_{k-2} & a_{k-1} & a_k & \cdots & a_3 \\ & & \cdots & & & & \cdots & \\ a_2 & a_3 & \cdots & a_{k-1} & a_{k-2} & a_{k-3} & \cdots & a_1 \\ a_1 & a_2 & \cdots & a_k & a_{k-1} & a_{k-2} & \cdots & 2a_0 \end{bmatrix}$$

또는 $m=2k$에 대해서 주어지는 F_p상에서의 순환 행렬

$$\begin{bmatrix} 2a_0 & a_1 & \cdots & 2a_k & a_{k-1} & a_{k-2} & \cdots & a_1 \\ a_1 & 2a_0 & \cdots & a_{k-1} & 2a_k & a_{k-1} & \cdots & a_2 \\ a_2 & a_1 & \cdots & a_{k-2} & a_{k-1} & 2a_k & \cdots & a_3 \\ & & \cdots & & & & \cdots & \\ a_2 & a_3 & \cdots & a_{k-2} & a_{k-3} & a_{k-4} & \cdots & a_1 \\ a_1 & a_2 & \cdots & a_{k-1} & a_{k-2} & a_{k-3} & \cdots & 2a_0 \end{bmatrix}$$

가 최대 rank를 가져야만 한다.

순환 행렬 $C=[c_0, c_1, \cdots, c_{m-1}]$의 행렬식이 다음과 같이 주어진다는 것이 알려져 있다[9].

$$D=\prod_{l=0}^{m-1} h(\varepsilon^l)$$

여기에서 $h(x)=\sum_{i=0}^{m-1} c_i \cdot x_i$이고 ε은 m-차 단위근이다. □

정리2를 사용해서 다음과 같은 이차 p진 bent 함수들을 찾을 수 있다.

따름정리 1: I가 $\gcd(p,|I|)=1$을 만족하는 첨수의 집합(index set)이라고 하자. 그리고 m은 $\gcd(m,|I|)=1$을 만족하는 양의 정수이다. 그러면 F_{p^m}에서 F_p로의 이차 p진 함수

$$f(x)=\sum_{i\in I} \mathrm{tr}_1^m (x^{p^i+1})$$

는 bent이다. □

증명) x가 집합 $E=\left\{e^{j\frac{2\pi l}{m}} \mid 0\le l\le m-1\right\}$의 한 원소라 하자. 그러면 식 (2)에서의 조건은 다음과 같이 쓸 수 있다. 모든 $\delta\in E$에 대해서

$$\sum_{i\in I}(\delta^i+\delta^{-i})\neq 0 \qquad (3)$$

$\gcd(p,|I|)=1$과 $\gcd(m,|I|)=1$로부터, 식 (3)이 만족하는 것을 보이는 것을 쉽게 확인할 수 있다. □

정리2의 결과를 사용해서, p진 bent 함수는 다음과 같이 Kumar와 Moreno가 제시한 bent 함수들과 유사함을 발견할 수 있다.

따름정리 2: e가 홀수, k가 양수이고, $m=ek$라 하자. r이 $1\le r\le e-1$, $\gcd(r,e)=1$를 만족하는 정수라 하자. 그러면 F_{p^m}에서의 함수

$$f(x)=\mathrm{tr}_1^m (x^{p^{\frac{me}{2}-kr}+1})$$

는 bent이다. □

$k=0$일 때, $f(x)$는 p진 Kasami 시퀀스로부터의 bent 함수가 된다.

이제 $q=p^m$이라 하자. Dembowski 와 Ostrom은 F_q상에서의 Dembowski-Ostrom 다항식[2][3]

$$f(x)=\sum_{i=0}^{m-1}\sum_{l=0}^{m-1} a_{i,l} x^{p^i+p^l} \qquad (4)$$

를 소개하였다. 여기서 $a_{i,l}\in F_q$이다. $a\in F_q^*$에 대해서 다음 식이 성립한다.

$$f(x+a)-f(x)=\sum_{i=0}^{m-1}\sum_{l=0}^{m-1}\left(a_{i,l}(x^{p^i}a^{p^l}+x^{p^l}a^{p^i})+a_{i,l}a^{p^i+p^l}\right)$$

p-다항식이 순열 다항식이 될 필요충분조건은 p-다항식이 0을 유일한 해로 갖는 것이라는 사실이 알려져 있다[10]. 분명히

$$\sum_{i=0}^{m-1}\sum_{l=0}^{m-1} a_{i,l}(x^{p^i}a^{p^l}+x^{p^l}a^{p^i})$$

는 p-다항식이고 그래서 $f(x)$는 임의의 $a \in F_q^*$에 대해서 다음 조건을 만족하면 평면 다항식(planar polynomial)이 된다. 모든 $x \in F_q^*$에 대해서

$$\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{i,j}(x^{p^i}a^{p^j} + x^{p^j}a^{p^i}) \neq 0 \qquad (5)$$

Dembowski-Ostrom 다항식을 사용해서 다음과 같이 F_{p^m}상에서 정의된 p진 bent 함수를 만들 수 있다.

정리 3: $f(x)$가 (4)에서 정의된 (5)를 만족하는 Dembowski-Ostrom 다항식이라고 하자. 그러면 F_{p^m}에서 F_p로의 함수 $\mathrm{tr}_1^m(f(x))$는 bent이다. □

시뮬레이션 결과로부터, 정리3의 역은 성립하지 않는다는 것을 보였다.

참 고 문 헌

[1] C. Carlet and C. Ding, "Highly nonlinear mappings," Preprint, 2002.

[2] R. Coulter and R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," Designs, Codes and Cryptography, vol. 10, pp. 167-184, 1997.

[3] P. Dembowski and T. G. Ostrom, "Planes of order n with collineation groups of order n^2," Math. Z. 103, pp. 239-258, 1968.

[4] L. E. Dickson, Linear groups with exposition of the Galois field theory, New York, Dover Publications, 1958.

[5] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," IEEE Trans. Inform. Theory, vol. 45, no. 2, pp. 475-485, Mar. 1999.

[6] T. Helleseth and D. Sandberg, "Some power mappings with low differential uniformity," Applicable Algebra in Engineering, Communication and Computing, vol. 8, pp. 363-370, 1997.

[7] P. V. Kumar and O. Moreno, "Prime-phase sequences with periodic correlation properties better than binary sequences," IEEE Trans. Inform. Theory, vol. 37, pp. 603-616, May 1991.

[8] P.V. Kumar, R.A. Scholtz, and L.R. Welch, "Generalized bent functions and their properties," J. Combinatorial Theory, Series A. vol. 40, pp. 90-107, 1985.

[9] P. Lancaster and M. Tismenetsky, The Theory of Matrices with Applications, 2nd ed., 1985.

[10] R. Lidl and H. Niederreiter, Finite Fields, vol. 20 of Encyclopedia of Mathematics and Its Applications, Reading, MA: Addison-Wesley, 1983.

[11] K. Nyberg, "Constructions of bent functions and difference sets," Lecture Notes in Computer Science 473, Springer-Verlag, pp. 151-160, 1991.

[12] K. Nyberg, "Differentially uniform mappings for cryptography," Lecture Notes in Computer Science 765, Springer-Verlag, pp. 55-64, 1994.

[13] J. D. Olsen, R. A. Scholtz, and L.R. Welch, "Bent-function sequences," IEEE Trans. Inform. Theory, vol. 28, pp. 858-864, Nov. 1982.

[14] O. S. Rothaus, "On bent functions," J. Combinatorial Theory, Series A. vol. 20, pp. 300-305, 1976.

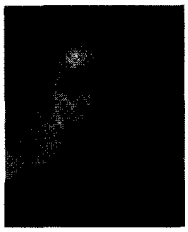
[15] G. Seroussi and A. Lempel, "Factorization of symmetric matrices and trace-orthogonal bases in finite fields," SIAM J. Comput., vol. 9, no. 4, pp. 758-767, Nov. 1980.

[16] L. R. Welch, "Lower bounds on the maximal cross correlation of signals," IEEE Trans. Inform. Theory, vol. 20, pp. 396-399, May 1976.

[17] Young-Sik Kim, Ji-Woong Jang, Jong-Seon No, and Tor Helleseth, "On p-ary bent function defined on finite field," Mathematical Properties of Sequences and Other Combinatorial Structures, The Kluwer International Series in Engineering and Computer Science, Kluwer Academic

Publishers, pp. 65-76, 2003.

김 영 식(Young-Sik Kim) 준회원



2001년 2월 : 서울대학교 전기공학부 공학사
2003년 2월 : 서울대학교 전기컴퓨터공학부 석사
2003년 3월~현재 : 서울대학교 전기컴퓨터공학부 박사과정

<관심분야> 시퀀스, 오류정정부호, 디지털통신

장 지 웅(Ji-Woong Jang) 준회원

2000년 2월 : 서울대학교 전기공학부 공학사
2002년 2월 : 서울대학교 전기컴퓨터공학부 석사
2002년 3월~현재 : 서울대학교 전기컴퓨터공학부 박사과정

<관심분야> 시퀀스, 오류정정부호, 디지털 통신

노 종 선(Jong-Seon No) 종신회원

1981년 2월 : 서울대학교 전자공학과 공학사
1984년 2월 : 서울대학교 대학원 전자공학과 석사
1988년 5월 : University of Southern California, 전기공학과 공학박사
1988년 2월~1990년 7월 : Hughes Network Systems, Senior MTS
1990년 9월~1999년 7월 : 건국대학교 전자공학과 부교수
1999년 8월~현재 : 서울대학교 전기컴퓨터공학부 교수

<관심분야> 시퀀스, 시공간부호, LDPC 부호, OFDM, 이동통신, 암호학