APN 함수를 이용한 부호계열 발생 알고리즘 설계 및 분석

Design and Analysis of Code Sequence Generating Algorithms using Almost Perfect Nonlinear Functions

이정재*
Jeong-Jae Lee*

요 약

암호화 시스템에서 대부분의 선형시스템은 쉽게 해석될 수 있기 때문에 비선형성은 매우 중요하다. 비선형 함수인 bent함수와 유사한 특성을 갖고 C.Bracken, Z.Zha 등에 의하여 제안된 APN(Almost Perfect Nonlinear) 함수를 이용하여 두 종류의 새로운 부호계열 발생 알고리즘을 제안하였다. 이를 이용하여 $GF(2)$상에서 발생된 부호계열의 자기상관함수 $R_{ii}(\tau)$, $\tau \neq 0$와 상호상관함수 $R_{ik}(\tau)$의 값은 $\{-1, -1-2^{n/2}, -1+2^{n/2}\}$을 가진다. 이 개념을 확장한 $GF(p)$, $p \geq 3$상에서 발생된 비이원부호계열의 자기상관함수 $R_{p,ii}(\tau)$, $\tau \neq 0$와 상호상관함수 $R_{p,ik}(\tau)$의 값은 $\{-1+p^{n-1}, -1-p^{(n-1)/2}+p^{n-1}, -1+p^{(n-1)/2}+p^{n-1}\}$로 역시 3종류 값을 가짐을 보였다. 이 분석결과로부터 발생된 부호계열의 상관함수가 Gold 부호계열과 유사한 특성을 가짐을 확인하였다.

Abstract

For cryptographic systems, nonlinearity is crucial since most linear systems are easily decipherable. C.Bracken, Z.Zha etc., propose the APN(Almost Perfect Nonlinear) functions with the properties similar to those of the bent functions with perfect nonlinearity. We design two kinds of new code sequence generating algorithms using the above APN functions. And we find that the out of phase $\tau \neq 0$, autocorrelation functions, $R_{ii}(\tau)$ and the crosscorrelation functions, $R_{ik}(\tau)$ of the binary code sequences generated by two new algorithms over GF(2), have three values of $\{-1, -1-2^{n/2}, -1+2^{n/2}\}$. We also find that the out of phase $\tau \neq 0$, autocorrelation functions, $R_{p,ii}(\tau)$ and the crosscorrelation functions, $R_{p,ik}(\tau)$ of the nonbinary code sequences generated by the modified algorithms over GF(p), $p \geq 3$, have also three values of $\{-1+p^{n-1}, -1-p^{(n-1)/2}+p^{n-1}, -1+p^{(n-1)/2}+p^{n-1}\}$. We show that these code sequences have the characteristics of the correlation functions similar to those of Gold code sequences.

Keywords: APN, nonlinear function, bent function, code sequence, correlation function, trace transform

Ⅰ. 서 론

정보데이터의 송신과 수신 과정에서 허용되지 않은 접속으로 인하여 중요한 정보의 노출과 손실과 같은 민감한 위험을 초래할 수 있기 때문에 이를 방지하고 정보를 보호하려는 암호화 기술이 요구된다. 과거에는 군용이나 외교와 관련된 분야에 국한되어 암호화에 대한 기술이 이용되었으나 최근에는 상업용이나 개인정보의 송수신에도 암호화 기술이 적용되고 있다. 기본적인 암호화 기술은 혼돈과 확산이며 특히 혼돈은 암호변환을 이루는 부울함수의 비선형성에 의하여 이루어진다. 이와 관련된 비선형함수는 bent 함수[1-2]가 있으며 비슷한 특성을 갖는 semi-bent 함수에 대한 연구도 K. Khoo와 G.Gong [3] 등에 의하여 진행되고 있다. C.Bracken과 Z.Zha [4] 등은 거의 완전한 비선형함수인 APN(Almost Perfect Nonlinear) 함수에 대한 연구를 계속하고 있다.

본 논문에서는 C.Bracken 등에 의하여 알려진 두 종류의 APN 함수를 이용하여 새로운 부호계열 발생 알고리즘을 설계하고 그 특성을 분석한다. 이를 위하여 제 II장에서는 비선형함수와 APN 함수에 대하여 살펴보고 제 III장에서는 두 종류의 APN 함수를 이용하여 새로운 부호계열 발생알고리즘을 설계한다. 제 IV장에서는 이를 이용하여 두 개의 원 {0,1}로 이루어지는 유한장(Galois field) GF(2)상의 부호

*동의대학교
투고 일자 : 2009. 12. 24 수정완료일자 : 2010. 1. 28
게재확정일자 : 2010. 1. 29
* 이 논문은 2008학년도 동의대학교 교내연구비에 의하여 연구되었음(2008AA172)

계열을 발생시키고 발생된 부호계열간의 상관함수 특성을 분석한다. 제 V장에서는 p개의 원 {0,1,..p-1}로 이루어지는 유한장 GF(p), $p \geq 3$상에서 비이원 부호계열을 발생시키고 상관함수 특성을 분석한다. 마지막으로 제 VI장에서는 결론을 맺는다.

II. 비선형함수

함수 f(x)의 Trace 변환과 Trace 역변환은 각각 다음 식 (1)과 식 (2)와 같이 정의된다[5].

$$\hat{f}(\lambda) = \frac{1}{2^{n/2}} \sum_{x \in GF(2^n)} f(x)(-1)^{Tr(\lambda x)} \tag{1}$$

$$f(x) = \frac{1}{2^{n/2}} \sum_{\lambda \in GF(2^n)} \hat{f}(x)(-1)^{Tr(\lambda x)} \tag{2}$$

여기서 Trace 함수는 다음 식 (3)과 같이 정의된다.

$$\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i} \tag{3}$$

그리고 $GF(2^n)$은 2^n개의 원으로 이루어지는 유한장이며 만약 $\hat{f}(\lambda) = \pm 1$의 값을 갖게 되면 f(x)는 bent 함수가 되며 완전한 비선형이다[1]. 한편 APN 함수는 다음과 같이 정의된다. 유한장 L= GF(2^n)에서 만약 식 (4)와 같은 다항식

$$f(x+a)-f(x)=b \tag{4}$$

에서 모든 $a,b \in GF(2^n)$, $a \neq 0$에 대하여 L안에서 단지 두 개 이하의 근을 가지면 임의의 함수 f: $L \rightarrow L$를 APN 함수라 부른다. 이와 관련하여 C.Bracken 등은 다음 식 (5)와 식 (6)과 같은 APN 함수를 제안하였다[4].

$$f(x) = bx^{2^s+1} + b^{2^k} x^{2^{k+s}+2^k} + cx^{2^{k+s}+2^s} + \sum_{i=0}^{k-1} r_i x^{2^{i+k}+2^i} \tag{5}$$

여기서 k와 s는 서로 소인 홀수 정수결레, $b,c \in GF(2^{2k})$, $c \notin GF(2^k)$ 그리고 모든 i에 대하여 $r_i \in GF(2^k)$이다.

$$f(x) = bx^{2^s+1} + (bx^{2^s+1})^{2^k} + cx^{2^k+1} \tag{6}$$

여기서 k와 s는 서로 소인 홀수정수, $b,c \in GF(2^{2k})$, $c \notin GF(2^k)$이고 b는 $GF(2^{2k})$의 원시원이다.

그리고 함수 f(x)의 Trace 함수 F(x)= Tr(f(x))의 Trace 변환은 식 (7)로 표현되며 $\hat{F}(\lambda)$가 두 값 ± 1로 제한되면 함수 F(x)도 bent 함수가 된다.

$$\hat{F}(\lambda) = \frac{1}{2^k} \sum_{x \in K} F(x)(-1)^{Tr(\lambda x)} \tag{7}$$

III. 부호계열발생 알고리즘

APN 함수 식 (5)와 관련하여 다음 식 (8)과 같은 부호계열 발생알고리즘을 설계하였다.

$$\begin{aligned} s_{1i}(t) &= Tr(v_i \alpha^t) + Tr[f(\alpha^t)] \\ &= Tr(v_i \alpha^t) + Tr[b(\alpha^t)^{2^s+1}] + Tr[b^{2^k}(\alpha^t)^{2^{k+s}+2^k}] \\ &\quad + Tr[c(\alpha^t)^{2^{k+s}+2^s}] + Tr[\sum_{j=0}^{k-1} r_j (\alpha^t)^{2^{j+k}+2^j}] \end{aligned} \tag{8}$$

여기서 α는 $GF(2^{2k})$에서 원시원, k와 s는 서로 소인 홀수정수, $v_i \in GF(2^{2k}), 1 \leq i \leq 2^{2k}$, $b,c \in GF(2^{2k})$, $c \notin GF(2^k)$ 그리고 $r_j \in GF(2^k)$를 만족하여야 한다.

한편 식 (6)과 관련하여 다음 식 (9)와 같은 발생 알고리즘을 설계하였다.

$$\begin{aligned} s_{2i}(t) &= Tr(v_i \alpha^t) + Tr[f(\alpha^t)] \\ &= Tr(v_i \alpha^t) + Tr[\alpha(\alpha^t)^{2^s+1}] \\ &\quad + Tr[\alpha^{2^k}(\alpha^t)^{2^{k+s}+2^k}] + Tr[c(\alpha^t)^{2^k+1}] \end{aligned} \tag{9}$$

여기서 α는 $GF(2^{2k})$에서 원시원, k와 s는 서로 소인 정수, $v_i \in GF(2^{2k})$, $1 \leq i \leq 2^{2k}$,$c \in GF(2^{2k})$, $c \notin GF(2^k)$이다.

식 (8)로부터 발생되는 부호계열 군 $\{s_{1n}^{(i)}\}$, $i=1,..,2^{2k}$의 자기상관함수 (autocorrelation function) $R_{ii}(\tau)$는 식 (10)과 같이 정의된다.

$$R_{ii}(\tau) = \sum_{t=0}^{N-1} \hat{s}_{1n}^{(i)} \hat{s}_{1(n+\tau)}^{(i)} \tag{10}$$

여기서 $\hat{s}_{1n}^{(i)} = (-1)^{s_{1n}^{(i)}}$, $s_{1n}^{(i)} \in \{0,1\}$이다. 그리고 두 부호계열 $s_{1n}^{(i)}$와 $s_{1n}^{(k)}$의 상호상관함수(crosscorrelation function) $R_{ik}(\tau)$는 다음 식 (11)과 같이 정의된다.

$$R_{ik}(\tau) = \sum_{t=0}^{N-1} \hat{s}_{1n}^{(i)} \hat{s}_{1(n+\tau)}^{(k)} \tag{11}$$

여기서 $\hat{s}_{1n}^{(k)} = (-1)^{s_{1n}^{(k)}}$, $s_{1n}^{(k)} \in \{0,1\}$이다. 정규화한 자기상관함수와 상호상관함수는 각각 $R_{ii}(\tau)$/N과 $R_{ik}(\tau)$/N으로 정의되며 $N=2^n-1$은 부호계열의 주기다. 그리고 식 (9)로부터 발생되는 부호계열 군 $\{s_{2n}^{(i)}\}$, $i=1,..,2^{2k}$에 대해서도 식 (10)과 식 (11)의 자기상관함수와 상호상관함수 정의식이 각각 적용된다.

IV. 이원부호계열발생 및 상관함수특성

식 (8)과 식 (9)의 두 발생알고리즘에 대한 발생 예로서 n=6, k=3 그리고 s=5, $b,c \in GF(2^6)$, $c \notin GF(2^3)$, 그리고 $r_i \in GF(2^3)$를 택하였다. 이를 위한 원시다항식은 x^6+x+1이 되며 이로부터 0을 제외한 $GF(2^6)$의 모든 원을 발생시킬 수 있는 발생기는 그림 1과 같이 구성된다. 여기서 $\oplus$은 MOD2 합(E-XOR)을 의미한다.

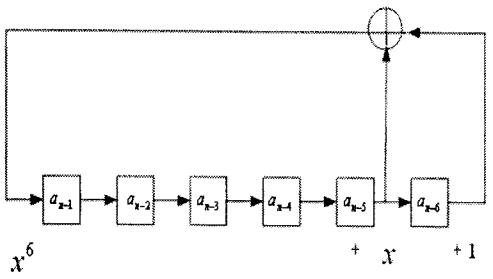

그림 1. x^6+x+1에 대응한 발생기.

Fig.1. Generator corresponding to x^6+x+1.

$GF(2^6)$에서 식 (9)와 식 (10)의 두 발생알고리즘은 각각 다음 식 (12)와 식 (13)과 같이 표현할 수 있다.

$$s_{1i}(t)=Tr(v_i\alpha^t)+Tr[b(\alpha^{33t})]+Tr[b^8(\alpha^{264t})] + Tr[c(\alpha^{288t})]+Tr[\sum_{j=0}^{2} r_j(\alpha^t)^{2^{j+3}+2^j}] \quad (12)$$

$$s_{2i}(t)=Tr(v_i\alpha^t)+Tr[\alpha(\alpha^t)^{2^s+1}] + Tr[\alpha^8(\alpha^{264t})]+Tr[c(\alpha^{9t})] \quad (13)$$

먼저 식 (12)를 이용하여 임의의 두 부호계열을 발생하고 상관함수 특성을 분석한다. 발생알고리즘 $s_{1i}(t)$에 의하여 $v_1=\alpha^0$일 때 발생된 부호계열 $s_{1n}^{(1)}$는 다음과 같으며 주기 $N=2^6-1=63$으로 된다.

$s_{1n}^{(1)}$=[0111111010 0010110100 1101001010
0100000101 1110101101 0100001000 100]

그리고 $v_{21}=\alpha^{20}$일때 발생된 부호계열 $s_{1n}^{(21)}$도 역시 주기 N=63이며 다음과 같다.

$s_{1n}^{(21)}$=[0000000100 1101110001 0000001010
0000110010 1111101101 1110001011 101]

임의의 두 부호계열 $s_{1n}^{(1)}$와 $s_{1n}^{(21)}$를 이용하여 상관함수 특성을 고찰해보자. 부호계열 $s_{1n}^{(1)}$의 자기상관함수 $R_{1,1,1}(\tau)$는 다음과 같다.

$R_{1,1,1}(\tau)$=[63 -9 7 7 -9 7 -9 -1 -9 7 -9 7 -9 -9 -1
-9 7 -9 7 7 7 -1 -9 7 7 7 7 7 -1 7 -9 -9 -9 -9
7 -1 7 7 7 7 7 -9 -1 7 7 7 -9 7 -9 -1 -9 -9 7
-9 7 -9 -1 -9 7 -9 7 7 -9]

그리고 부호계열 $s_{1n}^{(1)}$와 $s_{1n}^{(21)}$의 상호상관함수 $R_{1,1,21}(\tau)$는 다음과 같다.

$R_{1,1,21}(\tau)$=[7 -9 7 7 -9 7 -1 7 -9 7 7 7 7 -1 7 -9
-9 -9 7 -9 -1 7 -9 7 -9 -9 7 -1 -9 7 7 7 7 7
-1 7 7 7 7 7 -9 -1 7 -9 -9 7 -9 7 -1 -9 7 -9
-9 -9 7 -1 7 7 7 7 -9 7 -1]

한편 식 (13)의 발생알고리즘 $s_{2i}(t)$에 의하여 $v_1=\alpha^0$일때 발생된 주기 N=63인 부호계열 $s_{2n}^{(1)}$은 다음과 같다.

$s_{2n}^{(1)}$=[1001110000 0011010110 0100110000
0111100001 0101110000 1101100010 011]

그리고 $v_{21}=\alpha^{20}$일때 발생된 부호계열 $s_{2n}^{(21)}$ 역시 주기 N=63으로 다음과 같다.

$s_{2n}^{(21)}$=[0111110010 0010110100 1101001010
0100000101 1110101101 0100001000 100]

식 (10)으로 정의되는 부호계열 $s_{2n}^{(1)}$의 자기상관함수 $R_{2,1,1}(\tau)$는 다음과 같은 값을 갖는다.

$R_{2,1,1}(\tau)$=[63 7 -9 -9 -9 -9 -9 -1 7 7 7 -9 7 7 -1
-9 -9 7 7 7 7 -1 7 -9 -9 -9 7 7 -1 7 7 -9 -9 7
7 -1 7 7 -9 -9 -9 7 -1 7 7 7 7 -9 -9 -1 7 7 -9
7 7 7 -1 -9 -9 -9 -9 -9 7]

그리고 부호계열 $s_{2n}^{(1)}$와 $s_{2n}^{(21)}$의 상호상관함수 $R_{2,1,21}(\tau)$는 다음과 같은 결과를 갖는다.

$R_{2,1,21}(\tau)$=[-1 -9 7 7 -9 7 7 -1 7 -9 7 -9 -9 7 -1
7 7 7 -9 -9 -9 -1 7 7 7 7 7 7 -1 -9 -9 -9 7 7
7 -1 7 -9 -9 7 -9 7 -1 7 7 -9 7 7 -9 -1 7 7 7
7 -9 -9 -1 -9 -9 7 7 7 7]

이 상관함수 결과로 부터 자기상관함수 $R_{1,1,1}(\tau)$와 $R_{2,1,1}(\tau)$, 상호상관함수 $R_{1,1,21}(\tau)$과 $R_{2,1,21}(\tau)$를 각각 다음과 같이 정리하여 표현할 수 있다.

$$R_{1,1,1}(\tau)=R_{2,1,1}(\tau)=\begin{cases}-1-2^{6/2}=-9\\-1+2^{6/2}=7\\-1\\2^6-1=63, & \tau=0\end{cases}$$

$$R_{1,1,21}(\tau)=R_{2,1,21}=\begin{cases}-1-2^{6/2}=-9\\-1+2^{6/2}=7\\-1\end{cases}$$

이로부터 6을 n으로 바꿈으로서 자기상관함수 $R_{i,i}(\tau)$와 상호상관함수 $R_{i,k}(\tau)$를 각각 다음 식 (14a)와 식 (14b)와 같이 일반화하여 표현할 수 있다.

$$R_{i,i}(\tau)=\begin{cases}-1-2^{n/2}\\-1+2^{n/2}\\-1\\2^n-1, & \tau=0\end{cases} \quad (14a)$$

$$R_{i,k}(\tau)=\begin{cases}-1-2^{n/2}\\-1+2^{n/2}\\-1\end{cases} \quad (14b)$$

그림 2는 $R_{1,1,1}(\tau)$를 주기 N으로 정규화한 자기상관함수 특성을 표현한 것이며 그림 3은 부호계열 $R_{1,1,21}(\tau)$를 주기 N으로 정규화한 상호상관함수특성을 보여준다.

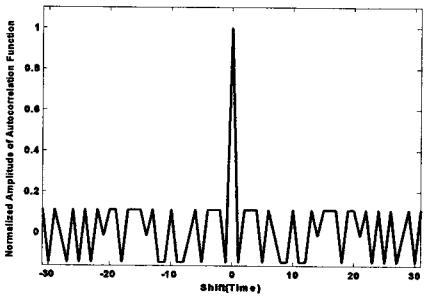

그림 2. 부호계열 $s_{1n}^{(1)}$의 정규자기상관함수.
Fig.2. Normalized autocorrelation function of the code sequence $s_{1n}^{(1)}$.

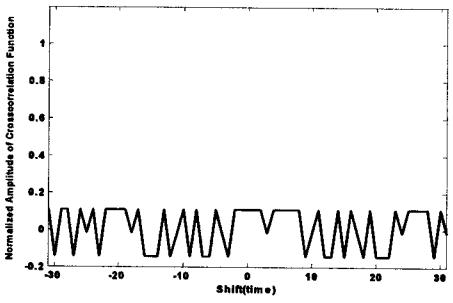

그림 3. 부호계열 $s_{1n}^{(1)}$와 $s_{1n}^{(21)}$의 정규상호상관함수.
Fig.3. Normalized crosscorrelation function between code sequence $s_{1n}^{(1)}$ and $s_{1n}^{(21)}$.

그리고 그림 4와 그림 5는 각각 $R_{2,1,1}(\tau)$와 $R_{2,1,21}(\tau)$를 주기 N으로 정규화한 특성을 보여준다. 그림 2와 그림 4에서 알 수 있는 바와 같이 $\tau=0$을 제외한 자기상관함수가 3종류의 값을 가짐을 알 수 있다. 또한 그림 3과 그림 5에서 알 수 있는 바와 같이 상호상관함수 역시 3종류의 값을 가진다. 이 결과는 주기 $N=2^n-1$인 Gold 부호계열[6]의 최대상관함수 $R_{\max}=1+2^{(n+1)/2}$,n이 홀수, $R_{\max}=1+2^{(n+2)/2}$, n=2 MOD4일 때와 유사한 상관함수 특성임을 확인할 수 있다.

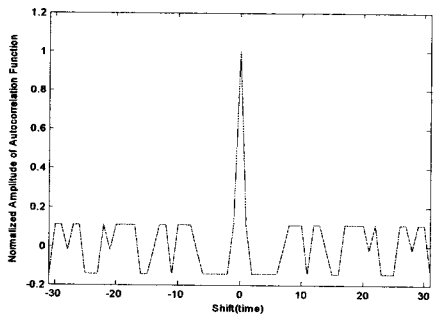

그림 4. 부호계열 $s_{2n}^{(1)}$의 정규자기상관함수.
Fig.4. Normalized autocorrelation function of the code sequence $s_{2n}^{(1)}$.

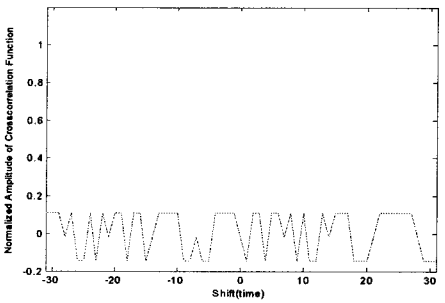

그림 5. 부호계열 $s_{2n}^{(1)}$와 $s_{2n}^{(21)}$의 정규상호상관함수.
Fig.5. Normalized crosscorrelation function between code sequence $s_{2n}^{(1)}$ and $s_{2n}^{(21)}$.

V. 비이원부호계열발생 및 상관함수특성

발생부호계열을 GF(2)에서 GF(p), $p\geq 3$로 확장하여 부호계열을 발생시키기 위하여 식 (8)의 부호계열발생 알고리즘에서 n이 홀수일 때 k=(n+1)/2, $v_i\in GF(p^n)$에 속하는 원소 $1\leq i\leq p^n$, b,c$\in GF(p^n)$, $c\notin GF(p^k)$ 그리고 $r_j\in GF(p^k)$를 만족하도록 설정하였다. 동일한 방법이 식 (9)의 발생알고리즘에 대하여 적용할 수 있으나 여기서는 식 (8)의 부호계열에 대해서만 검토 한다. 그리고 비이원 부호계열 $\{a_n\}$과 $\{b_n\}$의 자기상관함수와 상호상관함수는 각각 다음 식 (15a)와 (15b)와 같이 정의한다.

$$R_{aa}(\tau)=\sum_{n=0}^{N-1}a_n\bigcirc a_{n+\tau} \tag{15a}$$

$$R_{ab}(\tau)=\sum_{n=0}^{N-1}a_n\bigcirc b_{n+\tau} \tag{15b}$$

여기서

$$a_n\bigcirc a_{n+\tau}=\begin{cases}0, a_n\neq a_{n+\tau}\\ 1, a_n=a_{n+\tau}\end{cases}$$

로 정의된다. 그리고 $N=p^n-1$은 부호계열의 주기다.

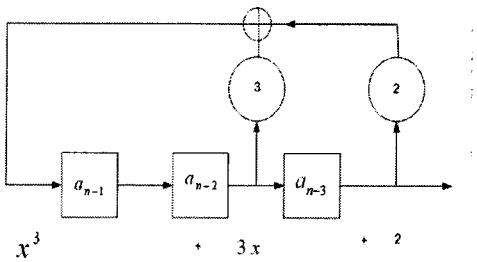

그림 6. x^3+3x+2에 대응한 발생기.
Fig.6. Generator corresponding to x^3+3x+2.

비이원부호계열의 발생 예로서 n=3, p=5로 하면 원시원 α에 대응하는 원시다항식은 x^3+3x+2이다. 이를 이용하여 0을 제외한 $GF(5^3)$의 모든 원을 발생 시킬 수 있는 발생기는 그

림 6과 같이 구성될 수 있다. 여기서 ⊕은 MOD5 합을 의미한다. 발생 예로서 s=1, $v_i \in GF(5^3)$에 속하는 원소 $1 \le i \le 5^3$, b, $c \in GF(5^3)$, $c \notin GF(5^2)$ 그리고 $r_j \in GF(5^2)$를 만족하도록 설정하였다. 이를 이용하여 $GF(5^3)$에서 $v_1 = \alpha^0$일 때 발생된 주기 $N=5^3-1=124$인 부호계열 $s_{5,n}^{(1)}$와 $v_6 = \alpha^5$일 때 부호계열 $s_{5,n}^{(6)}$는 각각 다음과 같이 발생된다.

$s_{5,n}^{(1)}$=[2331441140 0412412303 3013024123
2400313131 4240021142 0223143113
1444444304 4340311032 4434413240
2140332103 2134212334 1432420331
3300]

$s_{5,n}^{(6)}$=[0123112402 2132401330 2434331421
2033010144 3011302234 1044302102
3304240330 3210122420 2210234302
0420233314 2332303440 4122210323
4123]

그리고 식 (15a)를 이용한 부호계열 $s_{5,n}^{(1)}$의 자기상관함수 $R_{5,1,1}(\tau)$는 다음과 같다.

$R_{5,1,1}(\tau)$=
[124 24 19 29 29 19 24 19 29 29 19 29 24 19 19 29 19 29 29 29
24 29 29 29 24 29 29 24 19 24 24 19 19 24 29 24 29 19 19 29
29 29 19 19 29 29 24 19 29 24 29 29 29 19 29 29 19 19 29 29
19 29 24 29 19 29 29 19 19 29 29 19 29 29 29 24 29 19 24 29
29 19 19 29 29 29 19 19 29 24 29 24 19 19 24 24 19 24 29 29
24 29 29 29 24 29 29 29 19 29 19 19 24 29 19 29 29 19 24 19
29 29 19 24]

식 (15b)를 이용한 부호계열 $s_{5,n}^{(1)}$와 $s_{5n}^{(6)}$의 상호상관함수 $R_{5,1,6}(\tau)$는 다음과 같이 구해진다.

$R_{5,1,6}(\tau)$=
[19 29 29 19 19 24 19 29 19 19 29 24 19 24 19 29 29 19 24 19
29 19 29 29 29 24 24 24 29 24 29 29 19 19 29 29 24 29 24 29
24 24 19 29 24 24 24 29 29 24 24 29 19 19 19 24 19 19 19 29
24 19 29 19 29 29 29 29 29 19 29 24 19 24 24 29 24 24 24 19
19 29 29 29 29 24 24 19 19 29 29 19 29 29 19 19 29 19 29 29
29 29 19 29 24 29 24 29 24 29 19 19 29 29 29 19 19 24 29 19
29 29 29 29]

이 결과를 이용하여 자기상관함수 $R_{5,1,1}(\tau)$와 상호상관함수 $R_{5,1,6}(\tau)$특성을 각각 다음과 같이 표현할 수 있다.

$$R_{5,1,1}(\tau)=\begin{cases}-1-5^{(3-1)/2}+5^{3-1}=19\\-1+5^{3-1}=24\\-1+5^{(3-1)/2}+5^{3-1}=29\\5^3-1=124, & \tau=0\end{cases}$$

$$R_{5,1,6}(\tau)=\begin{cases}-1-5^{(3-1)/2}+5^{3-1}=19\\-1+5^{3-1}=24\\-1+5^{(3-1)/2}+5^{3-1}=29\end{cases}$$

3을 n으로 5를 p로 바꾸면 비이원부호계열의 일반화한 상관함수 특성은 (16a)와 (16b)로 표현할 수 있다.

$$R_{5,0,0}(\tau)=\begin{cases}-1-p^{(n-1)/2}+p^{n-1}\\-1+p^{n-1}\\-1+p^{(n-1)/2}+p^{n-1}\\p^n-1, & \tau=0\end{cases} \quad (16a)$$

$$R_{5,0,1}(\tau)=\begin{cases}-1-p^{(n-1)/2}+p^{n-1}\\-1+p^{n-1}\\-1+p^{(n-1)/2}+p^{n-1}\end{cases} \quad (16b)$$

그림 7은 부호계열 $s_{5,n}^{(1)}$의 자기상관함수 $R_{5,1,1}(\tau)$의 특성을 보인다. 그림 8은 부호계열 $s_{5,n}^{(1)}$와 $s_{5n}^{(6)}$의 상호상관함수 $R_{5,1,6}(\tau)$의 특성을 보여준다. 이 결과로부터 $\tau \neq 0$에서 3종류의 상관함수 값을 가짐을 확인할 수 있다.

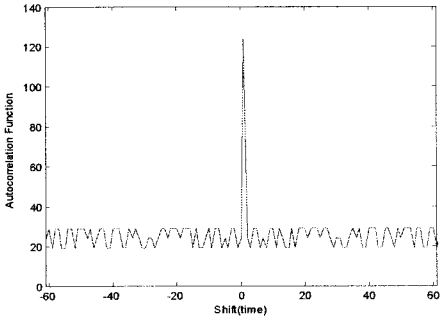

그림 7. 부호계열 $s_{5,n}^{(1)}$의 자기상관함수.
Fig.7. Autocorrelation function of the code sequence $s_{5,n}^{(1)}$.

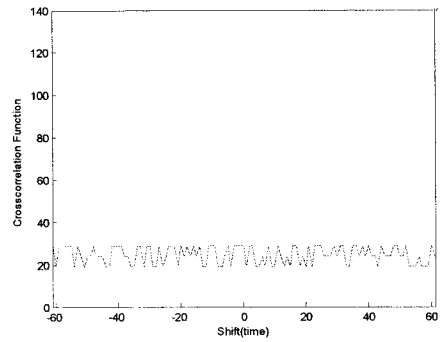

그림 8. 부호계열 $s_{5,n}^{(1)}$와 $s_{5,n}^{(6)}$의 상호상관함수
Fig.8. Crosscorrelation function between code sequence $s_{5,n}^{(1)}$ and $s_{5,n}^{(6)}$.

VI. 결 론

C.Bracken 등에 의하여 제안된 두 종류의 APN 함수를 이용하여 새로운 부호계열 발생알고리즘을 제안하고 GF(2) 상과 GF(p), $p \geq 3$ 상에서 각각 이원부호계열과 비이원부호계열을 발생하였다. $GF(2^6)$에서 발생된 이원부호계열에서 $\tau \neq 0$일 때의 상관함수 값이 Gold 부호계열과 유사함을 확인하였다. 또한 $GF(5^3)$에서 비이원부호계열을 발생시키고 $\tau \neq 0$일 때 3종류의 부호계열간의 상관함수 값을 도출하였다. 이러한 모든 결과는 Matlab을 이용하여 제한된 조건에서 시뮬레이션을 통하여 이루어 졌으며 향후 일반화를 위한 심층 분석이 더욱 진행될 것이다.

참고문헌

[1] O.S. Rothaus, "On Bent Functions," J. Comb. Theory, series A20, pp.300-305, 1976.

[2] F.J.MacWilliams, N.J.A.Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, Amsterdam, pp.426 -430, 1977.

[3] K.Khoo, G.Gong, and D.R.Stinson, "A new characterization of semi-bent and bent function on finite field," Designs, Codes, and Cryptography, Vol.38-2, pp.279-295, Feb.2006.

[4] C.Bracken, Z.Zha, "On the Fourier Spectra of the Infinite Families of Quadratic APN Functions," Advances in Mathematics of Communications, Vol. 3, No. 3, pp.219-226, 2009.

[5] J.Olsen, R.A.Scholtz, and L.R.Welch, "Bent-Function Sequences,"IEEE Trans. Inform. Theory, Vol. IT-28, No.6, pp.858-864, Nov. 1982.

[6] R.Gold, "Optimal binary sequences for spread spectrum multiplexing," IEEE Trans. Inform. Theory, Vol. IT-13, No.4, pp.619-621, Oct. 1976.

이 정재(Jeong-Jae Lee)

1969.3-1973.2 서강대학교 전자공학과(공학사)

1981.3-1990.8 한양대학교 전자통신공학과 (학,석사, 공학박사)

1987.3-현재: 동의대학교 정보통신공학과 교수

관심분야: 디지털통신시스템, 이동통신, 부호이론