Kasami 수열들과 No 수열들의 상호상관관계

김진경* · 조성진** · 최언숙*** · 황윤희****

Crosscorrelation of Kasami sequences and No sequences

Jin-gyoung Kim* · Sung-jin Cho** · Un-soon Choi*** · Yoon-hee Hwang****

요 약

Games는 같은 원시다항식을 갖는 m-수열과 GMW 수열의 상호상관관계 함수를 계산하는 방법을 제안하였다. 본 논문에서는 같은 원시다항식에 의해서 생성된 Kasami 수열과 No 수열들의 상호상관관계 함수를 두 개의 기준수열들의 주기적 상호상관관계함수를 이용하여 계산한다. 이 방법은 Games에 의해서 제안된 방법과는 다르다.

ABSTRACT

Games gave the calculation method for the crosscorrelation function of a Kasami sequence and a No sequence that have been generated by the same primitive polynomial. In this paper, we calculate the crosscorrelation function of a Kasami sequence and a No sequence that have been generated by the same primitive polynomial with the periodic crosscorrelation function of two base sequences. Our method is different from the Games's method.

키워드

m-수열, Kasami 수열, No 수열, 삽입수열, 트레이스

Ⅰ. 서 론

매우 긴 주기의 난수열을 발생시켜서 평문과 더함으로써 암호문을 생성하는 비밀키 암호인 스트림 암호는 많은 양의 데이터를 빠르게 암호화 할 수 있는 장점이 있다. 생성된 수열이 난수와 구별이 불가능 하여야 안전하므로 대부분은 LFSR을 결합하거나 여러 종류의 수열들을 다양하게 결합하여 생성시킨다.

이렇게 생성시킨 의사난수열들은 통신시스템과 스트림 암호에 아주 중요하게 사용되어지고 있다.

1962년에 Gordon, Mills와 Welch [1]는 Singer 차분 집합과 같은 매개변수들을 갖는 순환 차분 집합을 소개하였다. 이진 수열들은 이러한 차분 집합들에 의해서 정의할 수 있다. 1985년에 Games [2]는 트레이스를 이용하고 내적을 이용하여 1의 개수로 같은 원시다항식을 갖는 m-수열과 GMW 수열 [3]의 상호상관관계 함숫값을 계산하는 방법을 제안하였다. Kasami 수열 [4]은 m-수열의 낮은 자기상관관계를 개선한 수열이다. 1962년에 Gordon, Mills와 Welch는 m-수열과 자기상관관계 함숫값은 같으면서 높은 선형 스팬을 갖는 수열인 GMW 수열을 소개하였다. Kasami 수열은 자기상관관계 함숫값이 GMW 수열의 자기상관관계 함숫값의 2배가 된다. 1989년에 No 등 [5]은 GMW 수열들의 집합과 Kasami 수열들의 집합

* 부경대학교 응용수학과(5892587@hanmial.net)
** 교신저자 : 부경대학교 응용수학과(sjcho@pknu.ac.kr)
*** 동명대학교 멀티미어학과(choies@tu.ac.kr)
**** 부경대학교 응용수학과(pretty9723@hanmail.net)
접수일자 : 2010. 12. 02 심사(수정)일자 : 2011. 01. 06 게재확정일자 : 2011. 02. 09

을 함께 품는 새로운 수열인 No 수열들의 집합을 소개하였다. 그런데 No 수열들의 집합은 자기상관관계 함숫값이 Kasami의 것과 같으나 선형 스팬은 GMW 수열들의 집합보다 더 크다는 장점이 있다. 이러한 이유 때문에 본 논문에서는 Games가 제안한 방법과 다른 방법을 이용하여 Kasami 수열과 No 수열의 상호상관관계 함숫값을 계산하기로 한다.

II. 배경지식

임의의 두 정수 $k,l\ (>0)$, $k|l$에 대하여 $k|l$이므로 $GF(2^k)$은 $GF(2^l)$의 부분체(subfield)[6]이다. 따라서 $GF(2^l)$을 정의역으로 하고 $GF(2^k)$을 공역으로 하는 트레이스(trace) Tr_k^l를 다음과 같이 정의한다.

$$Tr_k^l(x)=\sum_{j=0}^{\frac{l}{k}-1}x^{2^{k\cdot j}} \tag{1}$$

그러면 Tr_k^l은 다음 성질들을 갖는다.

① 모든 $x\in GF(2^l)$와 모든 i에 대하여 $Tr_k^l(x^{2^{k\cdot i}})=Tr_k^l(x)$이다.

② Tr_k^l은 선형적이다. 즉, 모든 $a,b\in GF(2^k)$, $x,y\in GF(2^l)$에 대하여 $Tr_k^l(ax+by)=aTr_l^k(x)+bTr_k^l(y)$이다.

③ 하나의 $b\in GF(2^k)$에 대하여 방정식 $Tr_k^l(x)=b$는 $GF(2^l)$에서 2^{l-k}개의 해를 갖는다.

④ 모든 $x\in GF(2^l)$에 대하여 $Tr_1^k(Tr_k^l(x))=Tr_1^l(x)$이다.

선형 스팬이 n인 m-수열을 트레이스를 이용하여 나타낼 수 있다. 즉, $\boldsymbol{s}=(s_0,s_1,\cdots,s_{2^n-2})$를 주기가 2^n-1인 m-수열이라 하면 $\eta\in GF(2^n)$가 존재하여 s_i는 다음 식에 의해서 정의할 수 있다.

$$s_i=Tr_1^n(\eta\alpha^i)\ \ (0\le i\le 2^n-2) \tag{2}$$

그러면 $\boldsymbol{s}$는 α의 최소다항식 $f(x)$에 의해서 생성된 m-수열이다. $m|n$이라면 선형 스팬이 m인 m-수열은 $\boldsymbol{s}$와 관련지을 수 있다. 즉, $\boldsymbol{u}=(u_0,u_1,\cdots,u_{2^m-2})$를 주기가 2^m-1인 m-수열이라 하면 u_i는 다음 식에 의해서 정의할 수 있다.

$$u_i=Tr_1^m(\beta^i)\ \ (0\le i\le 2^m-2) \tag{3}$$

$N=2^n-1$이라 하고 $Q=\dfrac{2^n-1}{2^m-1}=2^m+1$이라 하자. $\boldsymbol{s}$를 $(2^m-1)\times Q$ 배열 $A(\boldsymbol{s})$로 간주했을 때, $A(\boldsymbol{s})$를 기준수열(base sequence) $\boldsymbol{u}$에 관한 $(2^m-1,Q)$ 삽입수열(interleaved sequence)이라 한다. $A(\boldsymbol{s}):=<A_j>$라 하자. 여기서 $0\le j\le Q-1$이다. A_j는 0-수열이거나 기준수열 $\boldsymbol{u}$와 위상이동차가 같거나 위상이동차가 다른 주기가 2^m-1인 m-수열들이다.

[예제 2.1] 수열 $\boldsymbol{s}=(1,1,0,0,1,0,0,0,0,0,1,1,0,0,1)$의 주기는 15이다. 따라서 $n=4$, $m=2$이다. 그러므로 다음 배열은 기준수열 $\boldsymbol{u}=(0,1,1)$에 관한 (3,5) 삽입수열이다.

$$A(\boldsymbol{s})=\begin{bmatrix}1&1&0&0&1\\0&0&0&0&0\\1&1&0&0&1\end{bmatrix} \tag{4}$$

임의의 $i\in\{0,1,\cdots,2^m-2\}$와 $j\in\{0,1,\cdots,Q-1\}$에 대하여

$$A(\boldsymbol{s})(i,j)=s_{iQ+j} \tag{5}$$

이다.

III. Kasami 수열과 No 수열

이 절에서는 Kasami 수열과 No 수열을 소개하고 합한 두 수열의 상호상관관계 함숫값에 대하여 살펴본다.

두 정수 n, m에 대하여 $N:=2^n-1$, $n=2m\ (m>0)$, $Q=\dfrac{2^n-1}{2^m-1}=2^m+1$라 하자. 또한 $\gcd(r,2^m-1)=1$이라 하자. $s_K(t)$와 $s_{N,r}(t)$을 각각 같은 원시다항식 $f(x)$에 의해서 생성된 Kasami 수열과 No 수열이라 하자. 여기서 α를 $f(x)$의 원시근이라 하고 $\beta=\alpha^Q$라 하자. 그러면 $s_{K,\eta}(t)$와 $s_{N,\gamma,r}(t)$는 다음과 같이 정의된다.

$$s_{K,\eta}(t)=Tr_1^m\left[Tr_m^n(\alpha^{2t})+\eta\beta^t\right]$$
$$s_{N,\gamma,r}(t)=Tr_1^m\left\{\left[Tr_m^n(\alpha^{2t})+\gamma\beta^t\right]^r\right\},\ \eta,\gamma\in GF(2^m) \tag{6}$$

(6)에서 $r=1$이면 No 수열은 바로 Kasami 수열이 된다. 따라서 No 수열에서 $r>1$인 경우만 생각하기로 한다.

$0\le t\le N-1$에 대하여

$$t=t_1Q+t_2\quad(0\le t_1\le 2^m-2, 0\le t_2\le Q-1)$$

라 하자. 그러면

$$\left(\beta^{2t_1}\right)^{2^m-1}=\left(\alpha^{2t_1}\right)^{2^{2m}-1}=\left(\alpha^{2t_1}\right)^{2^n-1}=1$$

이므로 $\beta^{2t_1}\in GF(2^m)$이다. 따라서

$$Tr_m^n\left(\alpha^{2(t_1Q+t_2)}\right)=\beta^{2t_1}Tr_m^n(\alpha^{2t_2})$$

이다. 또한

$$Q^2t_1-2Qt_1=(2^m+1)(2^m-1)t_1$$
$$\alpha^{2^{2m}-1}=\alpha^{2^n-1}=1$$

이므로

$$\alpha^{t_1Q^2-2t_1Q}=\left(\alpha^{2^n-1}\right)^{t_1}=1$$

이다. 따라서

$$\beta^{t_1Q}=\beta^{2t_1} \tag{7}$$

이다. 그러므로 $A(\boldsymbol{s}_{K,\eta})$와 $A(\boldsymbol{s}_{N,\gamma,r})$은 각각 다음과 같다.

$$A(\boldsymbol{s}_{K,\eta})=Tr_1^m\left\{\beta^{2t_1}\left[Tr_m^n\left(\alpha^{2t_2}\right)+\eta\cdot\beta^{t_2}\right]\right\} \tag{8}$$
$$A(\boldsymbol{s}_{N,\gamma,r})=Tr_1^m\left\{\beta^{2rt_1}\left[Tr_m^n\left(\alpha^{2t_2}\right)+\gamma\cdot\beta^{t_2}\right]^r\right\} \tag{9}$$

[예제 3.1] $f(x)=x^4+x+1$이라 하고 α를 $f(x)$의 원시근이라 하자. 또한 $\beta=\alpha^5$이라 하자. 즉, $n=4$이므로 $m=2$, $Q=5$이다. $r=2$, $\eta=\beta\,\gamma=\beta^2$이라 하자. 그러면

$$s_{K,\beta}(t)=Tr_1^2\left[Tr_2^4(\alpha^{2t})+\beta\cdot\beta^t\right]$$
$$s_{N,\beta^2,2}(t)=Tr_1^2\left\{\left[Tr_2^4(\alpha^{2t})+\beta^2\cdot\beta^t\right]^2\right\} \tag{10}$$

이다. 그러면 식 (8)과 (9)에 의하여 $A(\boldsymbol{s}_{K,\beta})$와 $A(\boldsymbol{s}_{N,\beta^2,2})$은 각각 다음과 같다.

$$A(\boldsymbol{s}_{K,\beta})=\begin{bmatrix}1&1&0&0&1\\0&0&0&0&0\\1&1&0&0&1\end{bmatrix}$$
$$A(\boldsymbol{s}_{N,\beta^2,2})=\begin{bmatrix}1&0&1&0&0\\1&0&1&1&0\\0&0&0&1&0\end{bmatrix} \tag{11}$$

식 (11)에서 보듯이 $A(\boldsymbol{s}_{K,\beta})$와 $A(\boldsymbol{s}_{N,\beta^2,2})$의 각 열은 0-수열이거나 기준 수열 $\boldsymbol{u}=(0,1,1)$와 위상동차가 같거나 위상이동차가 다른 주기가 3인 m-수열들이다.

예제 3.1에서 두 수열의 합 수열 $A(\boldsymbol{s}_{K,\beta})+A(\boldsymbol{s}_{N,\beta^2,2})$을 구해보면

$$A(\boldsymbol{s}_{K,\beta})+A(\boldsymbol{s}_{N,\beta^2,2})=\begin{bmatrix}0&1&1&0&1\\1&0&1&1&0\\1&1&0&1&1\end{bmatrix} \tag{12}$$

임을 알 수 있다. 이 합 수열 역시 각 열은 0-수

열이거나 기준 수열 $\boldsymbol{u}=(0,1,1)$와 위상이동차가 같거나 위상이동차가 다른 주기가 3인 m-수열들이다.

[정리 3.2] α를 원시근으로 갖는 차수가 $n(=2m)$인 원시다항식에 의해서 생성된 No 수열 $\boldsymbol{s}_{N,\gamma,r}$을 삽입수열로 간주했을 때 각 열은 0-수열이거나 β^{2r}에 의해서 생성된 주기가 2^m-1인 m-수열이다.

증명> 식 (10)에 의하여

$$A(\boldsymbol{s}_{N,\gamma,r}) = Tr_1^m\left\{\beta^{2rt_1}\left[Tr_m^n\left(\alpha^{2t_2}\right)+\gamma\cdot\beta^{t_2}\right]^r\right\} \tag{13}$$

이다. 여기서 $0\le t_1<2^m-1$이고 $0\le t_2<Q$이다. 식 (13)에서

$$f(t_2) := \left[Tr_m^n\left(\alpha^{2t_2}\right)+\gamma\cdot\beta^{t_2}\right]^r \tag{14}$$

라 두면 식 (13)은

$$A(\boldsymbol{s}_{N,\gamma,r}) = Tr_1^m\left\{\beta^{2rt_1}f(t_2)\right\} \tag{15}$$

이 된다. 따라서 $f(t_2)=0$이면 $A(\boldsymbol{s}_{N,\gamma,r})$의 t_2열은 0-수열이 되고 $f(t_2)\neq 0$이면 $A(\boldsymbol{s}_{N,\gamma,r})$의 t_2열은 β^{2r}에 의해서 생성된 주기가 2^m-1인 m-수열들이다.

[따름정리 3.3] α를 원시근으로 갖는 차수가 $n(=2m)$인 원시다항식에 의해서 생성된 Kasami 수열 $\boldsymbol{s}_{K,\eta}$을 삽입수열로 간주했을 때 각 열은 0-수열이거나 β^2에 의해서 생성된 주기가 2^m-1인 m-수열이다.

증명> 정리 3.2의 증명에서 $r=1$인 경우이므로 분명하다.

지금부터 같은 원시다항식 $f(x)$에 의해서 생성된 Kasami 수열과 No 수열의 상호상관관계 함숫값을 구하는 방법을 소개하기로 한다. $N:=2^n-1$, $m:=\frac{n}{k}(\gcd(k,N)=1)$, $Q=\frac{2^n-1}{2^m-1}$라 하자. α를 $f(x)$의 원시원소라 하고 $\beta=\alpha^Q$라 하자. 배열 $A(\boldsymbol{s}_{K,\eta})$과 배열 $A(\boldsymbol{s}_{N,\gamma,r})$를 각각 Kasami 수열과 No 수열을 배열로 간주한 것이라 하자. 또한 $\boldsymbol{u}$와 $\boldsymbol{v}=\boldsymbol{u}[r]$를 각각 $A(\boldsymbol{s}_{K,\eta})$와 $A(\boldsymbol{s}_{N,\gamma,r})$의 기준수열이라 하자.

$\boldsymbol{a}_0,\boldsymbol{a}_1,\cdots,\boldsymbol{a}_{Q-1}$와 $\boldsymbol{b}_0,\boldsymbol{b}_1,\cdots,\boldsymbol{b}_{Q-1}$을 각각 $A(\boldsymbol{s}_{K,\eta})$와 $A(\boldsymbol{s}_{N,\gamma,r})$의 첫 열부터 시작하여 Q개의 열들이라 하자. 또한 $\boldsymbol{a}_l$, $\boldsymbol{b}_l(0\le l\le Q-1)$를 각각 $Tr_1^m(\beta^{2i})$과 $Tr_1^m(\beta^{2ri})$ $(0\le i\le 2^m-2)$에 의해서 생성된 m-수열을 위상이동차를 가지고 배열된 수열들이라 하자. 즉,

$$\boldsymbol{a}_l=\left\{Tr_1^m(v_{l_j}\beta^{2i})\right\},\ \boldsymbol{b}_l=\left\{Tr_1^m(w_{l_j}\beta^{2ri})\right\}$$

라 하자. $t:=t_1Q+t_2$ $(0\le t_1\le 2^m-2,\ 0\le t_2\le Q-1)$일 때,

$$e_{t_2}:=\begin{cases}\infty, & v_{l_j}=0\\ e, & v_{l_j}\neq 0,\ v_{l_j}=\beta^e,\ e\in\{0,1,\cdots,2^m-1\}\end{cases} \tag{16}$$

$$f_{t_2}:=\begin{cases}\infty, & w_{l_j}=0\\ f, & w_{l_j}\neq 0,\ w_{l_j}=\beta^f,\ f\in\{0,1,\cdots,2^m-1\}\end{cases} \tag{17}$$

라 하자.

$A(\boldsymbol{s}_{K,\eta})$와 $A(\boldsymbol{s}_{N,\gamma,r})$의 위상이동수열인 $\boldsymbol{e}=(e_0,e_1,\cdots,e_{2Q-2})$와 $\boldsymbol{f}=(f_0,f_1,\cdots,f_{Q-1})$를 구한다. 여기서 각 i $(0\le i\le Q-1)$에 대하여

$$e_{Q+i}=\begin{cases}e_i+1, & e_i<\infty\\ \infty, & e_i=\infty\end{cases} \tag{18}$$

$e_{Q+i}=e_i+1(0\le i\le Q-1)$이라 하고 다음과 같은 $Q\times Q$ 배열을 만든다.

$$\begin{matrix} e_0-f_0 & e_1-f_1 & e_2-f_2 & \cdots & e_{Q-1}-f_{Q-1} \\ e_1-f_0 & e_2-f_1 & e_3-f_2 & \cdots & e_Q-f_{Q-1} \\ e_2-f_0 & e_3-f_1 & e_4-f_2 & \cdots & e_{Q+1}-f_{Q-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ e_{Q-1}-f_0 & e_Q-f_1 & e_{Q+1}-f_2 & \cdots & e_{2Q-2}-f_{Q-1} \end{matrix} \quad (19)$$

단, $e_{j+t_2}=f_j=\infty$인 경우는 $e_{j+t_2}-f_j:=\infty-\infty$라 둔다. $\infty-c$ 혹은 $c-\infty$는 x라 둔다.

Kasami 수열과 No 수열의 기준수열들 $\boldsymbol{u}$와 $\boldsymbol{v}$의 상호상관관계 함숫값을 구한다. 즉, $v\ (0\le v<2^m-1)$에 대하여 $E^v\boldsymbol{u}$와 $\boldsymbol{v}$의 상호상관관계 함숫값을 $a_0,a_1,\cdots,a_{2^m-2}$라 하자.

이 때, $\infty-\infty$는 2^m-1로 바꾸고 x는 -1로 둔다. $\tau=k\ (0\le k\le Q-1)$일 때 식 (19)의 k번째 행의 원소에 대하여 i를 a_i로 바꾼다. 이렇게 바꾸어진 값들을 더한 값이 바로 $\tau=k\ (0\le k\le Q-1)$에서의 Kasami 수열 $\boldsymbol{s}_{K,\eta}$와 No 수열 $\boldsymbol{s}_{N,\gamma,r}$의 상호상관관계 함숫값이다.

$1\le l<2^m-1$이고 $\tau=k\ \ (lQ\le k\le(l+1)Q-1)$일 때 l 번째 $Q\times Q$ 배열의 각 원소의 값들에 l씩 더한다. 이 때 배열의 원소가 $\infty-\infty$이면 그대로 $\infty-\infty$로 하고 마찬가지로 x도 그대로 x라 둔다. 이렇게 얻어진 l 번째 $Q\times Q$ 배열의 각 원소에 대하여 i를 a_i로 바꾼다. 이렇게 바꾸어진 값들을 더한 값이 바로 $\tau=k(lQ\le k\le(l+1)Q-1)$에서의 Kasami 수열 $\boldsymbol{s}_{K,\eta}$와 No 수열 $\boldsymbol{s}_{N,\gamma,r}$의 상호상관관계 함숫값이다.

[예제 3.4] $n=6,\ m=3,\ p=x^6+x^5+x^2+x+1$이라 하면 $Q=9$이다. $\eta=\beta^2,\ \gamma=\beta$이고, $r=3$이라 하자. 그러면 생성되는 Kasami 수열과 No 수열은 다음과 같다.

$$\boldsymbol{s}_{K,\beta}=(001000100\cdots110100101)$$
$$\boldsymbol{s}_{N,\beta^2,2}=(100011100\cdots010101101)$$

$\boldsymbol{s}_{K,\beta}$와 $\boldsymbol{s}_{N,\beta^2,2}$의 7×9 배열이 다음과 같다고 하자.

$$A(\boldsymbol{s}_{K,\beta})=\begin{bmatrix}0\,0\,1\,0\,0\,0\,1\,0\,0\\0\,0\,0\,0\,0\,0\,1\,1\,0\\1\,1\,1\,1\,0\,0\,0\,0\,1\\0\,0\,1\,0\,0\,0\,0\,1\,0\\1\,1\,1\,1\,0\,0\,1\,1\,1\\1\,1\,0\,1\,0\,0\,0\,1\,1\\1\,1\,0\,1\,0\,0\,1\,0\,1\end{bmatrix}$$

$$A(\boldsymbol{s}_{N,\beta^2,2})=\begin{bmatrix}1\,0\,0\,0\,1\,1\,1\,0\,0\\0\,0\,0\,1\,0\,1\,1\,0\,0\\0\,1\,0\,0\,0\,0\,0\,0\,1\\1\,1\,0\,0\,1\,1\,1\,0\,1\\1\,1\,0\,1\,1\,0\,0\,0\,1\\1\,0\,0\,1\,1\,0\,0\,0\,0\\0\,1\,0\,1\,0\,1\,1\,0\,1\end{bmatrix}$$

$\boldsymbol{u}:=(1001011)$, $\boldsymbol{v}:=(1110100)$가 각각 $\boldsymbol{s}_{K,\beta}$와 $\boldsymbol{s}_{N,\beta^2,2}$의 기준수열이다. Kasami 수열과 No 수열의 기준수열들 $\boldsymbol{u}$와 $\boldsymbol{v}$의 상호상관관계 함숫값은 -5, -1, -1, 3, -1, 3, 3이다. 그러면

$$\boldsymbol{e}=(1,1,3,1,\infty,\infty,6,2,1,2,2,4,2,\infty,\infty,0,3,2)$$
$$\boldsymbol{f}=(4,5,\infty,3,4,1,1,\infty,5)$$

이다. 이것을 이용하여 다음과 같은 $Q\times Q$ 배열을 만든다.

표 1. $Q\times Q$ 배열
Table 1. A $Q\times Q$ matrix

4	3	x	5	x	x	5	x	3
4	5	x	x	x	5	1	x	4
6	3	$\infty-\infty$	x	2	1	0	x	4
4	x	$\infty-\infty$	3	5	0	1	x	6
x	x	x	6	4	1	1	x	4
x	1	x	5	5	1	3	x	x
2	4	x	6	5	3	1	$\infty-\infty$	x
5	3	x	6	0	1	x	$\infty-\infty$	2
4	4	x	1	5	x	x	x	5

표 1의 각 행의 값들은 다음 표 2의 값들로 바꾼다.

표 2. $\boldsymbol{u}$와 $\boldsymbol{v}$의 상호상관관계 함숫값
Table 2. A crosscorrelation function of $\boldsymbol{u}$ and $\boldsymbol{v}$

0	-5
1	-1
2	-1
3	3
4	-1
5	3
6	3
$\infty - \infty$	7
x	-1

예를 들어 표 1의 첫 행은

4	3	x	5	x	x	5	x	3
-1	3	-1	3	-1	-1	3	-1	3

이 되고 모든 값들을 바꾸면 아래의 표 3과 같다.

표 3. $Q\times Q$ 행렬의 상호상관관계 함숫값
$\tau = k(0 \le k \le 8)$
Table 3. A crosscorrelation function of $Q\times Q$ matrix
$\tau = k(0 \le k \le 8)$

-1	3	-1	3	-1	-1	3	-1	3
-1	3	-1	-1	-1	3	-1	-1	-1
3	3	7	-1	-1	-1	-5	-1	-1
-1	-1	7	3	3	-5	-1	-1	3
-1	-1	-1	3	-1	-1	-1	-1	-1
-1	-1	-1	3	3	-1	3	-1	-1
-1	-1	-1	3	3	3	-1	7	-1
3	3	-1	3	-5	-1	-1	7	-1
-1	-1	-1	-1	3	-1	-1	-1	3

이때 표 3의 첫 행을 모두 더하면 7이 된다. 이 값이 $\tau = 0$일 때의 상호상관관계 함숫값이다. 이와 같은 방법으로 $\tau = 0$부터 $\tau = 8$까지의 $\tau = k$ $(0 \le k \le 8)$에서의 Kasami 수열 $\boldsymbol{s_{K,\eta}}$와 No 수열 $\boldsymbol{s_{N,\gamma,r}}$의 상호상관관계 함숫값 7, -1, 3, 7, -5, 3, 11, 7, -1을 구하고 $\tau = 9$부터 $\tau = 17$까지 $\tau = k$ $(9 \le k \le 17)$에 대하여 $l = 1$이므로 첫 번째 $Q\times Q$ 배열의 각 원소의 값들에 1씩 더한다. 이 때 배열의 원소가 $\infty - \infty$이면 그대로 $\infty - \infty$로 하고 마찬가지로 x도 그대로 x라 둔다. 이렇게 얻어진 첫 번째 $Q\times Q$ 배열은 다음 표 4와 같다.

표 4. $Q\times Q$ 배열 $l = 1$
Table 4. A $Q\times Q$ matrix $l = 1$

5	4	x	6	x	x	6	x	4
5	6	x	x	x	6	2	x	5
0	4	$\infty - \infty$	x	3	2	1	x	5
5	x	$\infty - \infty$	4	6	1	2	x	0
x	x	x	0	5	2	2	x	5
x	2	x	6	6	2	4	x	x
3	5	x	0	6	4	2	$\infty - \infty$	x
6	4	x	0	1	2	x	$\infty - \infty$	3
5	5	x	2	6	x	x	x	6

이 표 4의 각 원소에 대하여 i를 a_i로 바꾸면 아래의 표 5와 같다.

표 5. $Q\times Q$ 행렬의 상호상관관계 함숫값
$\tau = k$ $(9 \le k \le 17)$
Table 5. A crosscorrelation function of $Q\times Q$ matrix
$\tau = k$ $(9 \le k \le 17)$

3	-1	-1	3	-1	-1	3	-1	-1
3	3	-1	-1	-1	3	-1	-1	3
-5	-1	7	-1	3	-1	-1	-1	3
3	-1	7	-1	3	-1	-1	-1	-5
-1	-1	-1	-5	3	-1	-1	-1	3
-1	-1	-1	3	3	-1	-1	-1	-1
3	3	-1	-5	3	-1	-1	7	-1
3	-1	-1	-5	-1	-1	-1	7	3
3	3	-1	-1	3	-1	-1	-1	3

이렇게 바꾸어진 값들을 각 행으로 더한 값이 바로 $\tau = k$ $(9 \le k \le 17)$에서의 Kasami 수열 $\boldsymbol{s_{K,\eta}}$와 No 수열 $\boldsymbol{s_{N,\gamma,r}}$의 상호상관관계 함숫값 3, 7, 3, 3, -5, -1, 7, 3, 7이다. 이와 같은 방법으로 $\tau = 0$부터 $\tau = 62$까지의 Kasami 수열과 No 수열의 상호상관관계 함숫값을 구하면 다음과 같다.

7, -1, 3, 7, -5, 3, 11, 7, -1, 3, 7, 3, 3, -5, -1, 7, 3, 7, -5, -5, 11, 7, 7, -5, 7, 3, -5, -5, -17, 7, 3, -17, -5, 3, 11, -17, -17, -5, 7, 3, 3, -5, 7, 7, -5, -1, 3, 3,

11, -1, 7, 3, 7, 3, -5, -5, 7, 7, -5, -17, 3, 3, -5

따라서, 두 수열의 상호상관관계 함숫값은 [-17, -5, -1, 3, 7, 11]이다.

Ⅳ. 결 론

GMW 수열들의 집합과 Kasami 수열들의 집합을 포함하고, 자기상관관계 함숫값이 Kasami 수열의 것과 같으나 선형 스팬은 GMW 수열들의 집합보다 더 큰 새로운 수열들의 집합인 No 수열들과 Kasami 수열들의 상호상관관계 함숫값을 Games와 다른 방법으로 계산하였다.

감사의 글

이 논문은 2010년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2010-371-B00008)

참고 문헌

[1] B. Gordon, W.H. Mills and L.R. Welch, Some new difference sets, Canad. J. Math. 14, pp. 614-625, 1962.

[2] R.A. Games, Crosscorrelation of m-sequences and GMW-sequences with the same primitive polynomial, Discrete Appl. Math. Vol. 12, pp. 139-146, 1985.

[3] R.A. Scholtz and L. Welch, GMW sequences, IEEE Trans. Inform. Theory, Vol. IT-30, No. 3, pp. 548-553, 1984.

[4] T. Kasami, Weight distribution formula for some class of cyclic codes, Coordinated Science Laboratory, University of Illinois, Urbana, Tech. Rep. R-285 (AD632574), 1966.

[5] J.S. No and P.V. Kumar, A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span, IEEE Trans. Inform. Theory, Vol. 35, No. 2, pp. 37-379, 1989.

[6] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.

저자 소개

김진경(Jin-gyoung Kim)

2006년 부경대학교 대학원 응용수학과 졸업(이학석사)
2008년~현재 부경대학교 대학원 응용수학과(박사과정)
※ 관심분야 : 셀룰라 오토마타론, 유한체

조성진(Sung-jin Cho)

1981년 고려대학교 대학원 수학과 졸업(이학석사)
1988년 고려대학교 대학원 수학과 졸업(이학박사)
1988년~현재 부경대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론

최언숙(Un-sook Choi)

2000년 부경대학교 대학원 응용수학과 졸업(이학석사)
2004년 부경대학교 대학원 응용수학과 졸업(이학박사)
2009년 부경대학교 대학원 정보 보호학과 졸업(공학박사)
현재 동명대학교 미디어공학과 전임강사
※ 관심분야 : 셀룰라 오토마타론, 정보보호

황윤희(Yoon-hee Hwang)

2004년 부경대학교 대학원 응용수학과 졸업(이학석사)
2008년 부경대학교 대학원 정보보호학과 졸업(공학박사)
※ 관심분야 : 셀룰라 오토마타론, 정보보호