通信情報保護學會誌
第3卷 第4號, 1993. 12

PN 시퀀스의 암호학적인 비도 특성

노 종 선*

1. 서 론

지난 수십년 동안 PN(pseudonoise) 시퀀스는 확산스펙트럼 통신방식을 비롯한 여러 분야에서 핵심적인 요소기술로서 사용되며 발전되어 왔는데 그 응용분야가 점점 넓어지면서 그 중요성이 증대되고 있다. 즉 PN시퀀스는 확산스펙트럼 통신방식의 직접시퀀스(direct sequence) CDMA(code division multiple access) 통신방식 및 주파수도약(frequency hopping) CDMA 통신방식에 사용될 뿐 아니라 거리를 측정하는 시스템 그리고 컴퓨터에서 랜덤데이타를 발생시키는데 사용되며, 또한 global positioning system(GPS) 및 영상신호를 스크램블링하는 시스템에서 사용되고 있다. 그리고 최근들어 이동무선통신시스템에서의 암호화 문제가 널리 대두되고 있는데 이러한 이동무선통신시스템은 bandlimited 시스템이며 powerlimited 시스템이므로 이동무선통신시스템에 사용될 수 있는 암호화시스템은 다음과 같은 조건을 갖추어야 한다.

- 비트오류가 증가하는 것을 방지하기 위하여 암호화 및 복호화에 의한 비트오류 확산(bit error propagation)을 최소화할 수 있는 방식이어야 한다.
- 채널의 대역폭이 증가하지 않도록 암호화를 위해 첨가되는 redundant비트가 최소화되는 암호화 방식이어야 한다.
- 높은 비도(cryptographic security)를 갖는 방식이어야 한다.
- 암호화 및 복호화알고리즘이 간단히 구현될 수 있어야 한다.

따라서 위와 같은 조건을 갖추고 있는 암호화방식으로 스트림암호화(stream cipher) 시스템이 있다. 그런데 PN시퀀스는 또 하나의 응용분야로서 이러한 스트림암호화시스템의 핵심기술인 키스트림(key stream)으로 사용될 수 있어 이에 대한 많은 연구가 되고 있다.

본 논문에서는 현재까지 발견되어 사용되고 있는 여러가지 특성이 우수한 PN시퀀스에 대한 정의 및 성질들에 대해서 기술하였고 또한 PN시퀀스들이 스트림암호화시스템의 키스트림으로 사용될때 이러한 여러가지 성질들이 어떻게 암호화시스템에 적합하고 또한 이러한 성질들이 암호학적인 비도와 어떠한 연관을 가질 수 있는가를 논하였다.

2. 여러가지 PN시퀀스의 정의

지금까지 PN시퀀스는 우선 다음과 같은 경우에 촛점을 맞추어 연구되어 왔고 또한 그러한 경우의 PN시퀀스가 대부분의 경우에 활용되어 왔다.

* 건국대학교 전자공학과

- Binary PN시퀀스들, 즉
$$s(t) \in \{0,1\}$$
- PN시퀀스의 주기는 $N=2^n-1$, 여기서 n은 정수, 즉
$$N=7,15,31,63,127,255,511,1023,$$
$$2047,4095,\ldots$$
- PN시퀀스는 주기를 갖는다. 즉,
$$s(t)=s(t+N),\ 0 \le t \le N-1$$

위와 같은 경우의 PN시퀀스에 대해 지난 수십년 동안 발견되어 연구되고 있는 좋은 특성을 갖는 PN시퀀스는 다음과 같은 것을 들 수 있다.

- M-시퀀스
- GMW시퀀스
- Kasami시퀀스
- Gold시퀀스
- Bent시퀀스
- 노(No)시퀀스

이러한 PN시퀀스를 정의하기 위하여는 trace 함수에 대한 정의를 먼저 논하여야 한다. Trace 함수는 finite field로부터 subfield로의 선형매핑인데 이 함수는 PN시퀀스의 디자인과 분석을 위한 중요한 수학적 도구로써 널리 사용된다. 즉, 대부분의 binary PN시퀀스들은 trace 함수의 형태로 표현될 수 있다. 임의의 두 정수 $n,m>0$, $m|n$에 대해, trace 함수, $tr_m^n(\cdot)$은 다음과 같은 관계식에 의해 정의된다.

$$tr_m^n(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{i\cdot m}} \qquad (1)$$

여기서 x는 $GF(2^n)$의 한 원소이다.

위에서 정의된 trace 함수를 이용하여 주기가 $N=2^n-1$인 여러가지 PN시퀀스를 다음과 같이 정의할 수 있다. 양의 정수 n에 대하여 m-시퀀스, $m(t)$는

$$m(t) = tr_1^n(\alpha^t), \qquad (2)$$

여기서 α는 finite field, $GF(2^n)$의 primitive 원소이고 m-시퀀스의 주기는 $N=2^n-1$이므로 t는 0과 2^n-2 사이의 값을 갖는다. GMW시퀀스, $g(t)$의 정의는 다음과 같다.

$$g(t)=tr_1^m\{[tr_m^n(\alpha^t)]^r\}, \qquad (3)$$

여기서 α는 $GF(2^n)$의 한 primitive 원소이고, $m|n$, $1 \le r < 2^m-1$, $gcd(2^m-1, r)=1$이다. 위에서 정의된 m-시퀀스와 GMW시퀀스는 하나의 시퀀스에 대해서 autocorrelation 성질을 고려하는 경우이고 다음에 정의되는 시퀀스들은 시퀀스의 군(family)에서 군내에 있는 시퀀스들사이의 crosscorrelation 및 각 시퀀스들의 autocorrelation을 고려하는 경우이다.

먼저 Gold시퀀스군은 다음과 같이 정의될 수 있다.

$$S_{Gold} = \{s_i(t) \mid 0 \le t \le N-1,\ 0 \le i \le 2^n\} \qquad (4)$$
$$s_i(t) = tr_1^n(\alpha^t) + tr_1^n(\alpha^{q\cdot(t+i)}) \qquad (5)$$

여기서 α는 finite field, $GF(2^n)$의 한 primitive 원소이며 q는 다음을 만족시키도록 선택되어야 한다.

- $n \neq 0 \ mod\ 4$, 즉, n은 홀수 또는 $n=2 \ mod\ 4$
- q는 홀수이면서, $q=2^k+1$ 또는 $q=2^{2k}-2^k+1$
- n이 홀수이면 $gcd(n,k)=1$, $n=2 \ mod\ 4$이면 $gcd(n,k)=2$

그리고 $s_{2^n-1}(t)$는 $tr_1^n(\alpha^t)$이고, $s_{2^n}(t)$는 $tr_1^n(\alpha^{q\cdot t})$라 하면 이 두시퀀스는 q가 위의 조건을 만족시킬때 prefered pair 시퀀스라 한다. 위에서 정의된 Gold시퀀스군의 경우에 각 시퀀스의 주기는 $N=2^n-1$이며, 시퀀스군내의 시퀀스의 수(family size)는 $N+2=2^n+1$이다.

Kasami시퀀스군의 정의는 Gold시퀀스의 경우와 비슷하게 아래와 같이 정의될 수 있다.

$$S_{Kasami} = \{s_i(t) \mid 0 \le t \le N-1,\ 0 \le i \le 2^m-1\} \qquad (6)$$
$$s_i(t) = tr_1^n(\alpha^t) + tr_1^m(\gamma_i \cdot \alpha^{T\cdot t}) \qquad (7)$$

여기서

- $\gamma_i \in GF(2^m)$
- 주기 : $N=2^n-1$
- $n = 2m$
- $T = \dfrac{2^n-1}{2^m-1} = 2^m+1$
- 군의 크기 : 2^m
- α : $GF(2^n)$의 primitive 원소

마지막으로 노시퀀스군은 다음과 같이 정의된다.

$$S_{No} = \{s_i(t) | 0 \le t \le N-1,\ 0 \le i \le 2^m-1\} \quad (8)$$

$$s_i(t) = tr_1^m\{[tr_m^n(\alpha^{2t}) + \gamma_i \cdot \alpha^{T \cdot t}]^r\} \quad (9)$$

여기서

- $\gamma_i \in GF(2^m)$
- 주기 : $N=2^n-1,\ n=2m$
- $T = \dfrac{2^n-1}{2^m-1} = 2^m+1$
- 군의 크기 : 2^m
- α : $GF(2^n)$의 primitive 원소
- $1 \le r < 2^m-1,\ gcd(r, 2^m-1)=1$

3. PN시퀀스의 성질과 비도의 관계

이러한 시퀀스에 있어서 고려되고 있는 일반적인 성질들을 보면 다음과 같은 것들이 있다.

- Out-of-phase 자기상관값(autocorrelation values)
- 상호상관값(crosscorrelation values)
- Nontrivial partial-period 상관값
- Linear span
- Balance properties
- Cyclically different시퀀스의 갯수
- 구현의 용이성

우선 여러가지 상관값에 대한 정의를 보면 다음과 같다. 주기가 N인 PN시퀀스, $s(t)$의 자기상관함수, $R_a(\tau)$는

$$R_a(\tau) = \sum_{t=0}^{N-1} (-1)^{s(t)+s(t+\tau)} \quad (10)$$

로 정의되는데 낮은 nontrivial 또는 out-of-phase 자기상관값은 통신에서는 동기화(synchronization), ranging, 다중경로파에 대한 diversity를 위해서 중요한 특성이다. 그리고 이러한 PN시퀀스가 암호화에 사용될 경우에는 correlation 공격에 대해서 높은 안전성을 갖기 위해 out-of-phase 자기상관값이 작아야 한다. 주기가 N인 binary PN시퀀스에 대한 이상적인 자기상관함수는 nontrivial인 경우에 -1, trivial인 경우에 N값을 취하는 등 단지 두개의 값만을 갖는 함수이다. 즉,

$$R_a(\tau) = \begin{cases} N, & \text{if } \tau = 0 \ mod\ N \\ -1, & \text{otherwise} \end{cases} \quad (11)$$

여러개의 시퀀스가 존재하는 PN시퀀스군의 경우에는 시퀀스군내의 여러 시퀀스들 사이의 correlation 특성인 crosscorrelation 함수를 고려해야하는데 이 경우도 PN시퀀스가 암호화시의 correlation 공격에 대해서 높은 안전성을 유지하기 위해 작은 값을 갖는 것이 바람직한데 두개의 시퀀스 $s_i(t)$, $s_j(t)$의 crosscorrelation에 대한 정의는 다음과 같이 주어진다.

$$R_{i,j}(\tau) = \sum_{t=0}^{N-1} (-1)^{s_i(t)+s_j(t+\tau)} \quad (12)$$

Welch에 의해서 유도된 최대상관값에 대한 lower bound는 PN시퀀스군의 상관관계 성질을 평가하는데 자주 이용된다. 우선 주기가 N인 A개의 PN시퀀스군에 대해서 최대 out-of-phase autocorrelation값, P_a와 최대 crosscorrelation값, P_c는 각각 다음과 같이 정의된다.

$$P_a = \underset{i}{MAX}\ \underset{1 \le \tau \le N-1}{MAX} |R_i(\tau)| \quad (13)$$

$$P_c = \underset{i \ne j}{MAX}\ \underset{0 \le \tau \le N-1}{MAX} |R_{i,j}(\tau)| \quad (14)$$

위의 두식으로부터 PN시퀀스군에서의 최대 nontrivial correlation 값, P_{max}는 다음과 같이 정의된다.

$$P_{max} = MAX(P_a, P_c) \quad (15)$$

P_{max}값은 Welch bound에 의해서 다음과 같이 lower bound된다.

$$P_{max} \ge N \cdot \sqrt{\frac{A-1}{A \cdot N-1}} \quad (16)$$

주기가 $N=2^n-1$이고 PN시퀀스군에서 PN시퀀스의 갯수가 $A \pm 1$이고 $n = 2m$인 경우, Welch bound는 다음과 같이 표현될 수 있다.

$$P_{max} \ge 2^m + 1 \quad (17)$$

따라서 어떤 PN시퀀스군에서 P_{max}가 2^m+1의 값을 갖는다고 하면 그 PN시퀀스군은 correlation 성질에 관한한 최적인 시퀀스군이다. 그런데 사실상 PN시퀀스는 주기가 매우 긴 시퀀스가 사용되는 경우가 대부분으로서 그러한 경우에는 전주기(full-period)에 대한 correlation을 구하는 것보다는 partial-period에 대한 correlation을 구하는 것이 실용적인 면에서 유용한 것으로 최근들어서 많은 연구가 되고 있는데, PN시퀀스의 partial-period correlation 성질들은 분석하기가 어렵고 심지어는 경계의 결정조차 어려운 경우가 대부분이다. 이 경우 정의를 보면 다음과 같다. Partial-period, M에 대한 partial-period autocorrelation 함수는

$$C_a(\delta,\tau)=\sum_{t=0}^{M-1}(-1)^{s(t+\delta)+s(t+\tau)} \tag{18}$$

로 정의되고 partial-period crosscorrelation 함수는

$$C_c(\delta,\tau)=\sum_{t=0}^{M-1}(-1)^{s_i(t+\delta)+s_j(t+\tau)} \tag{19}$$

로 정의된다.

PN시퀀스의 복잡성을 나타내주는 척도로 시퀀스의 linear span은 최근에 많은 관심의 대상이 되고 있으며, 그것의 중요성은 큰 linear span을 갖고 있는 시퀀스들을 사용함에 의해서 얻게되는 intelligent jamming에 대한 증대되는 protection에 의해 기인된다. 그리고 암호화에 사용되는 경우에는 linear span이 클수록 비도가 높아지는 것이므로 암호에의 응용에서는 매우 중요한 성질로 볼 수 있다. Linear span, L은 현재의 비트를 생성하기 위해서 미리 알아야할 과거의 비트수로 정의되는데 다음과 같은 수식으로 표현될 수 있다.

$$s(t)=\sum_{i=1}^{L}a_i\cdot s(t-i) \tag{20}$$

여기서 a_i는 0 또는 1의 값을 취하는 계수이다.

전송된 신호의 스펙트럼분석은 개략적으로 같은 수의 심볼을 갖는 PN시퀀스를 채택하는 것이 바람직하다는 것을 나타낸다. 이것을 balance property라 하는데 이는 PN시퀀스의 한 주기내에서 1의 갯수와 0의 갯수의 차로서 정의된다. 이러한 차가 1보다 작을때 즉,

$$\left|\sum_{t=0}^{N-1}(-1)^{s(t)}\right|\le 1 \tag{21}$$

이러한 시퀀스는 balance property를 갖는다고 한다.

사용가능한 시퀀스군의 갯수는 사용된 시퀀스군과 관련하여 도청자에 대한 불확실성의 척도로서 간주될 수 있으므로 서로 다른 시퀀스군의 갯수가 많다는 것은 바람직한 것이다. 그리고 한 시퀀스군내에서의 서로 다른 시퀀스의 갯수는 클수록 바람직스러운 것으로 간주되고 있다.

그리고 span property라는 것이 있는데 이는 다음과 같은 예를 통하여 설명할 수 있다. 주기가 15인 PN시퀀스가 다음과 같이 반복적으로 주어져 있을때

0111101011001000**1**11···

아래와 같이 각 비트에서 시작하는 15개의 4-tuple 벡터를 생각할때 15개의 벡터가 (0,0,0,0)를 제외한 모든 4-tuple 벡터를 나타내는 경우 이러한 PN시퀀스는 span property가 있다고 한다.

(0111) (1111) (1110) (1101) (1010)
(0101) (1011) (0110) (1100) (1001)
(0010) (0100) (1000) (0001) (0011)

주기가 2^n-1인 PN시퀀스가 다음과 같은 성질을 만족시키는 경우 run property가 있다고 한다.

No. of Run Length i of 1's or 0's for $1\le i\le n-2$: 2^{n-i-2}
No. of Run Length $n-1$ of 0's : 1
No. of Run Length n of 1's : 1

아래에 run property를 갖는 주기가 15인 PN시퀀스의 예를 들었다.

Example : **0**111101011001000**1**11···

No. of Run Length 1 of 1's or 0's : 2
No. of Run Length 2 of 1's or 0's : 1
No. of Run Length 3 of 0's : 1
No. of Run Length 4 of 1's : 1

4. 여러가지 PN시퀀스의 비도특성

앞절에서 언급한 바와 같이 PN시퀀스의 성질들 중에서 비도와 관련하여 고려될 수 있는 것들은 다음과 같다.

- Period
- Full-period autocorrelation
- Full-period crosscorrelation
- Partial-period autocorrelation
- Partial-period crosscorrelation
- Linear span
- Cyclically different한 PN시퀀스군의 갯수
- 한 시퀀스군내에서의 시퀀스의 갯수
- Balance property
- Existence

이러한 PN시퀀스군들의 비도와 관련된 성질 즉 주기, 시퀀스의 갯수, linear span, balance property들이 실제의 여러가지 PN시퀀스에 적용될 때 대부분의 경우에 정확한 수식으로 표현될 수 있으므로 기존의 알려진 PN시퀀스가 스트림 암호화시스템의 키스트림으로 사용되는 경우 PN시퀀스의 비도를 계량적으로 수치화할 수 있다는 장점을 갖고 있다. 앞에서 언급된 이미 알려진 여러가지의 PN시퀀스의 경우에 위의 성질들이 어떻게 적용될 수 있는지를 보면 다음과 같다. 우선 full-period autocorrelation 성질을 보면 m-시퀀스, GMW시퀀스는 하나의 시퀀스로서 앞서 정의된 ideal autocorrelation 성질을 갖는다. 그리고 시퀀스군을 고려하는 경우는 autocorrelation과 crosscorrelation 성질을 함께 고려해야 하는데, Gold시퀀스, Kasami시퀀스, 노시퀀스의 correlation 성질은 Welch bound의 견지에서 최적인 성질을 갖는다. 앞서 정의된 주기가 $2^{2m}-1$인 Kasami 시퀀스, bent시퀀스, 그리고 노시퀀스의 correlation 값은 다음과 같이 주어지게 된다.

$$\{-2^m-1,\ -1,\ 2^m-1\} \tag{22}$$

따라서 위의 시퀀스들은 최적인 correlation 특성을 갖고 있으므로 암호시스템에 사용되는 경우 correlation 공격에 강한 특성을 갖는다고 볼 수 있다.

앞서 언급한 시퀀스들을 partial-period correlation의 견지에서 보면 m-시퀀스가 가장 최적인 경우라고 알려져 있으나 그 이외의 내용은 거의 알려져 있는 것이 없다. 왜냐하면 원래 partial-period correlation이 매우 분석하기 어려운 성질이기 때문이다.

시퀀스의 linear span은 비교적 잘 알려진 시퀀스의 성질 중의 하나로서 주기가 2^n-1인 m-시퀀스의 linear span은 n이고, 같은 주기를 갖는 Gold 시퀀스군 내의 각 시퀀스의 linear span은 n 또는 $2n$이며, 주기가 $2^{2n}-1$인 Kasami 시퀀스군 내의 각 시퀀스 경우에는 최대 linear span이 $n+m$으로서, 주기에 비해 linear span이 매우 짧은 시퀀스로 높은 비도를 요하는 스트림암호화시스템의 키스트림으로 사용되기 어려운 시퀀스들이다. 이러한 linear span이 짧은 단점을 보완하여 발견된 linear span이 매우 긴 시퀀스들을 보면 아래와 같다. 우선 주기가 $2^n-1=2^{e\cdot m}-1$ 인 GMW시퀀스의 linear span은 다음과 같다.

$$L_{GMW}=n\cdot\left(\frac{n}{m}\right)^{wt(r)-1} \tag{23}$$

여기서 $wt(t)$는 r을 binary로 표현하였을 경우의 Hamming weight에 해당된다. 그리고 앞절에서 정의된 주기가 $2^{2m}-1$인 노시퀀스군내의 i-번째 시퀀스의 linear span은 다음과 같이 주어진다.

$$L_{No}(i)=m\cdot\prod_{j=1}^{R}\left\{2^{L_j+1}-1-2\ \lfloor\ \frac{2^{L_j}-1}{(2^m+\varepsilon_i)/g_i}\ \rfloor\right\} \tag{24}$$

각 시퀀스군내의 시퀀스들은 서로 다른 linear span 값을 갖고 있으나 GMW시퀀스나 bent시퀀스의 경우와 마찬가지로 노시퀀스의 모든 경우에도 대단히 큰 linear span을 갖고 있다. 따라서 이러한 GMW시퀀스, bent시퀀스, 그리고 노시퀀스의 경우는 linear span의 견지에서 볼때 암호화시스템에 적합한 키스트림이 될 수 있다.

주어진 주기에 대하여 cyclically different한 PN시퀀스군 또는 PN시퀀스의 갯수는 크면 클수록 암호해독자에게 현재 사용되고 있는 시퀀스의 불확실성을 증대시켜주는 것이 되므로 비도를 증대시켜주는

바람직스러운 성질인데 다음과 같이 주어진다. 먼저 주기 2^n-1인 cyclically different한 m-시퀀스의 갯수는

$$\frac{\phi(2^n-1)}{n} \tag{25}$$

여기서 $\phi(A)$는 A와 서로소의 관계에 있으면서 A보다 작은 양의 정수의 갯수로 정의되는 함수이다. 그리고 주기가 2^n-1인 Kasami시퀀스군의 갯수는 위의 경우와 같은 수식으로 표현될 수 있다.

$$\frac{\phi(2^n-1)}{n} \tag{26}$$

주기가 $2^n-1=2^{e\cdot m}-1$인 GMW시퀀스의 경우에 cylically different한 시퀀스의 갯수는

$$\frac{\phi(2^m-1)}{m}\cdot\frac{\phi(2^n-1)}{n} \tag{27}$$

로 표현될 수 있고 같은 주기를 갖는 노시퀀스군의 갯수는 같은 수식으로 표현된다.

$$\frac{\phi(2^m-1)}{m}\cdot\frac{\phi(2^n-1)}{n} \tag{28}$$

여러가지 n값에 대해서 Kasami시퀀스군과 노시퀀스군에 대해서 cyclically different한 시퀀스군의 갯수가 표1에 주어져 있다.

M-시퀀스와 GMW시퀀스 그리고 bent시퀀스군의 경우는 balance property를 갖고 있으나 다른 시퀀스들은 balance property를 갖고 있지 않다. 그러나 주기가 $2^n-1=2^{2m}-1$인 Kasami시퀀스군이나 노시퀀스군의 경우 각 시퀀스군내의 시퀀스들은 0와 1의 imbalance의 정도가 1에서 2^m+1으로서 주기에 비해 비교적 작은 값을 갖고 있다.

마지막으로 PN시퀀스가 존재하는 주기를 보면 다음과 같다. M-시퀀스의 경우에는 모든 정수 n에 대하여 시퀀스가 존재하고 Gold시퀀스의 경우에는 $n=2m+1$ 또는 $n=4m+2$일때 시퀀스가 존재하고

표1. Cyclically Different한 PN 시퀀스의 갯수

n	Period	N_{Kasami}	N_{No}
4	15	2	2
6	63	6	12
8	255	16	32
10	1,023	60	360
12	4,095	144	864
14	16,383	756	13,608
16	65,535	2,048	32,768
18	262,143	7,776	373,248
20	1,048,575	24,000	1,440,00
22	4,194,303	120,032	21,125,632
24	16,777,215	276,480	39,813,120
26	67,108,863	1,719,900	1,083,537,000
28	268,435,455	4,741,632	3,584,673,792
30	1,073,741,823	17,820,000	32,076,000,000
32	4,294,967,295	67,108,864	137,438,953,472
34	17,179,869,183	336,849,900	2,597,112,790,000

표2. 여러가지 PN 시퀀스군의 특성

Family	Period	n	Size of Family	Maximum Correlation Value	Maximum Linear Span	Range of Sequence Imbalance
Gold	2^n-1	$2m+1$	2^n+1	$2^{(n+1)/2}+1$	$2n$	$2^{(n+1)/2}+1$
Gold	2^n-1	$4m+2$	2^n+1	$2^{(n+1)/2}+1$	$2n$	$2^{(n+1)/2}+1$
Kasami (Small)	2^n-1	$2m$	$2^{n/2}$	$2^{n/2}+1$	$3n/2$	$2^{n/2}$
Kasami (Large)	2^n-1	$2m$	$2^{n/2}(2^n+1)$	$2^{(n+1)/2}+1$	$5n/2$	$2^{(n+1)/2}+1$
Bent	2^n-1	$4m$	$2^{n/2}$	$2^{n/2}+1$	*	1
노	2^n-1	$2m$	$2^{n/2}$	$2^{n/2}+1$	*	$2^{n/2}+1$

* 시퀀스군내의 각 시퀀스의 linear span은 대단히 크다.

Kasami시퀀스와 노시퀀스는 n이 짝수일때만 시퀀스가 존재한다. 그러나 bent시퀀스는 n이 4의 배수일때만 존재하는 단점이 있다. 지금까지 설명한 여러가지 시퀀스들의 성질들이 다음의 표2에 요약되어 있다.

위에서 언급된 여러가지 PN시퀀스들의 암호학적 성질을 고려해 볼 때, 스트림암호화방식에서 사용되는 키스트림이 높은 비도특성을 요구하는 경우에 사용될 수 있는 PN시퀀스로는 GMW시퀀스, 노시퀀스, 그리고 bent시퀀스 등을 들 수 있다.

참 고 문 헌

[1] S.W. Golomb, *Shift Register Sequences*. San Francisco, CA : Holden-Day, 1967 ; revised edition, Laguna Hills, CA : Aegeam Park Press, 1982.

[2] J.S. No., *A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span*. University of Southern California, Dept. of Electrical Engineering, PhD Thesis, 1988.

[3] J.S. No, P.V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span,"*IEEE Trans. Inform. Theory*, vol.IT-35, no.2, pp.371-379, March 1989.

[4] J.S. No, P.V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Int. Conf. Communications* (Philadelphia, PA), Conference Record, pp.25.4.1-25.4.5., June 12-15, 1988.

[5] J.S. No, P.V. Kumar, "On the partial-period correlation moments of GMW sequences," in *IEEE MILCOM '87 Conference Record* (Washington D.C.), pp.33.6.1-33.6.4, Oct. 1987.

[6] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, the Netherlands : North-Holland, 1977.

[7] E.R. Berlekamp, *Algebraic Coding Theory*, New York, McGraw-Hill, 1968.

[8] D.V. Sarwarte, M.B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol.68, pp. 593-620, May 1980.

[9] R.A. Scholtz, "The origins of spread-spectrum communications," *IEEE Trans. Commun.*, vol. COM-30, pp. 822-854, May 1982.

[10] R.A. Scholtz, "The spread-spectrum concept," *IEEE Trans. Commun.*, vol.COM-25, pp.748-755, Aug. 1977.

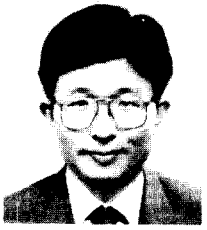
[11] R.A. Scholtz, L.R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol.IT-30, pp.548-553, May 1984.

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

[13] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol.IT-13, pp.619-621, Oct. 1967.

[14] L.R. Welch, "Lower bounds on the maximum crosscorrelation of signals," *IEEE Trans. Inform. Theory*, vol.IT-20, pp.397-399, May 1974.

□ 著者紹介



盧 宗 善(終身會員)

서울대학교 공과대학 전자공학과 (학사)
서울대학교 대학원 전자공학과 (석사)
University of Southern California Dept. of Electrical Eng. (공학박사)
1988.2 ~ 1990.7 미국 Hughes Network Systems 연구원
1990.9 ~ 현재 건국대학교 공과대학 전자공학과 조교수
관심분야 : 위성통신, 이동통신, 암호학, Error Correcting Codes