계층 구조의 비선형 피드포워드 수열 발생기

정회원 은 유 창*, 준회원 홍 윤 표*, 진 석 용*, 종신회원 송 홍 엽*

Layered Nonlinear Feed-Forward Sequence Generator

Yu-Chang Eun* *Regular Member*, Yun-Pyo Hong*, Seok-Yong Jin* *Associate Members*,
Hong-Yeop Song* *A Life Member*

요 약

선형복잡도(linear complexity)가 크고 균형(balance) 특성이 좋은 수열은 스트림 암호(stream cipher) 또는 보안성이 요구되는 대역 확산 통신(spread spectrum communication) 등에 이용될 수 있다. 이러한 수열을 발생하기 위하여, 최대길이 수열(*m*-sequence)을 계층 구조의 비선형 피드포워드 로직(NLFFL: Non-Linear Feed-Forward Logic) 필터 함수에 통과 시켜 랜덤 수열을 얻는 방법이 Groth에 의해 제안되었다. 본 논문에서는 Groth의 계층 구조를 변형하여 Langford 연결법과 같은 특별한 비선형 연결 방법 없이도 잡음 특성이 좋은 수열을 발생 시킬 수 있는 방법을 제시한다.

Key Words : pseudonoise sequences, shift register sequences, nonlinear feedforward logic, linear complexity

ABSTRACT

In this paper, we propose a new simple scheme of layered nonlinear feedforward logic (NLFFL) overlaid on a linear feedback shift register (LFSR) to generate pseudonoise sequences, which have good balance property and large linear complexity. This method guarantee noiselike statistics without any designed connection scheme e.g. Langford arrangement.

Ⅰ. 서 론

쉬프트 레지스터(shift register)를 이용한 의사잡음(pseudo-noise) 수열들은 일반적으로 대역 확산 통신(spread spectrum communication)과 스트림 암호(stream cipher)에 사용될 수 있다. 높은 보안성이 요구되는 시스템에서 좋은 균형(balance) 특성과 큰 선형 복잡도(linear complexity)는 이러한 수열들에게 요구되는 기본적인 조건들이다.

의사 잡음 수열의 선형복잡도를 크게 하기 위한 한가지 방법으로 그림 1과 같이 피드백 함수 F가 비선형인 피드백 쉬프트 레지스터(FSR: Feedback Shift Register) 수열 발생기를 고려할 수 있다. 그러나 이러한 수열 발생기는 피드백 함수 F를 키(key)로서 변화시켜 순회적으로(cyclically) 다른 수열을 얻고자 할 때, 균형성 특성이 좋고 선형복잡도가 큰 완전 순환(full cycle) 또는 이에 가까운 주기의 수열을 발생 시키는 함수 F를 찾기가 용이하지 않다. 또한, 수열 발생기의 초기값에 따라 그 주기가 달라질 수 있는 문제점도 안고 있다.

반면, 최대길이 수열(*m*-sequence) 발생기는 0이 아닌 모든 초기값에 상관없이 최대길이 수열을 발생시키므로 초기값 문제가 발생하지 않는다. 그러나 이러한 최대길이 수열의 선형복잡도는 최소이므로

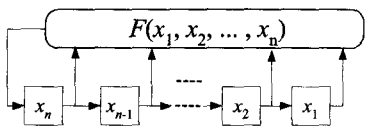


그림 1. 일반적인 feedback shift register 수열 발생기.

* 연세대학교 전기·전자공학과 부호 및 정보이론 연구실({yc.eun, yp.hong, sy.jin, hy.song}@coding.yonsei.ac.kr)
논문번호 : 040031-0119, 접수일자 : 2004년 1월 19일
※본 연구는 대학 IT연구센터 (인하 UWB-ITRC) 육성.지원사업의 연구결과로 수행되었음.

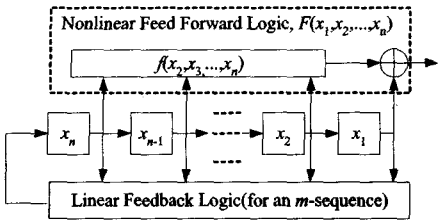


그림 2. 최대길이 수열 발생기와 결합된 비선형 feed forward logic 수열 발생기.

선형복잡도가 큰 수열로 변환시키기 위하여 이 수열을 비선형 피드포워드 로직(NLFFL: Non-Linear Feed-Forward Logic)에 통과시킨다. 이렇게 함으로써 초기값 문제가 없는 m-수열 발생기를 이용하여 선형복잡도가 큰 수열을 발생시킬 수 있다. 이때 비선형 피드포워드 필터 함수를 이진 변수 $x_1, x_2, \cdots, x_n$에 관한 대수적 정규형(ANF: Algebraic Normal Form)으로 표현하면 이 함수의 차수(order)로부터 선형복잡도의 상한 또는 하한을 결정할 수 있다[1][2].

위와 같은 비선형 필터함수를 사용할 경우, 이진 수열의 이상적인 균형성을 위하여 그림 2와 같은 NLFFL 함수

$$F(x_1, x_2, \cdots, x_n) = x_1 + f(x_2, x_3, \cdots, x_n) \quad (1)$$

가 사용될 수 있는데, 선형복잡도를 늘리기 위하여 함수 f의 차수를 키우면 키울수록, 출력 수열은 기초를 이루는 최대길이 수열과 상관성이 커지게 된다[3]. 따라서 이러한 구조는 상관공격에 약하다. 그러나 [4]에서 제안된 그림 3과 같은 구조를 사용하면 이런 상황을 피하면서 선형복잡도를 최대까지 단계적으로 빠르게 증가 시킬 수 있다. 즉, 그림3과 같은 구조의 각 층에서는 선형복잡도의 빠른 증가와 균형성 향상을 목적으로 Langford[5] 해를 이용하여 2-input AND 게이트만으로 비선형 함수를 구성하였다[4].

본 논문에서는 [4]에서와 같이 2-input AND 게이트만으로 NLFFL을 구성하지만 Langford 연결 같이 특별히 고안된 연결 방법을 사용하지 않아도 선형 복잡도 증가율은 기존 방법과 같이 최적이고 균형성은 향상되는 새로운 방법을 소개한다.

Ⅱ. 계층 구조의 NLFFL 발생기

기존에 제안된 그림 3과 같은 계층 구조의 NLFFL 수열 발생기를 Type I이라고 하자. 0번째 층의 출력은 최대길이 수열이므로 각 층의 출력 수

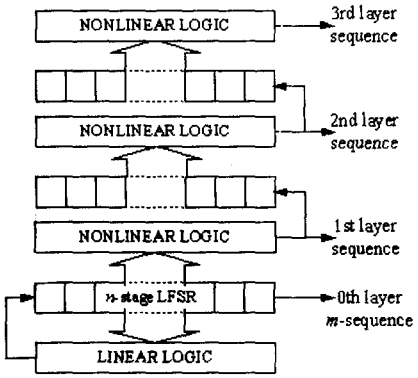


그림 3. Groth의 계층구조 NLFFL generator (Type I).

열은 주기가 2^n-1의 약수이다. 만약 2^n-1이 Mersenne 소수이면 0번째 출력 수열이 all-zero 수열이 아닌 이상 각층 출력 수열의 주기는 2^n-1임이 보장된다.

그림 3에서 각 층의 비선형 함수의 차수는 2이므로 NLFFL은 2-input AND 게이트들만으로 구성할 수 있으며 이것들의 연결은 Langford 해를 이용한다[5]. Langford 해는 다음과 같은 쌍(pair) 수열 $1,1,2,2,\cdots,h,h,\cdots,g,g$가 주어져 있을 때, 이 수열을 재배열하여 어떤 수의 쌍 h,h사이에 h개의 원소가 존재하도록 배열하는 방법을 말한다. 예를 들면 길이 8인 쌍 수열의 Langford 해는 4,1,3,1,2,4,3,2이고 길이 16인 것의 해는 6,7,5,1,8,1,4,6,5,7,3,4,2,8,3,2가 될 수 있다. 즉, 그림 3에서 0번째 층의 최대길이 수열 발생기의 단수 n이 짝수라고 가정하면, $1,1,2,2,\cdots,n/2,n/2$ 수열을 Langford 해로 배열한 다음, 같은 숫자를 갖는 위치의 시프트 레지스터 출력들을 같은 AND 게이트에 입력 시키면 된다. 결과적으로 1부터 $n/2$까지의 간격을 가지는 $n/2$개의 곱항들의 합(exclusive-OR)으로써 NLFFL 함수를 구성할 수 있다. 위와 같은 해의 개수는 n이 증가하면서 기하급수로 증가하지만 수열의 주기에 비하면 해의 개수가 매우 작은 편이다.

이러한 Langford 해들이 각층의 NLFFL 함수로 사용될 때 각층에는 서로 다른 간격의 곱들이 이 함수를 구성하므로 $\lfloor \log_2 n \rfloor$보다 작은 k번째 층에서 선형복잡도의 상한 L_k는 아래 식 (2)와 같다[4].

$$L_k = \sum_{i=1}^{2^k} \binom{n}{i} \quad (2)$$

따라서 $k \geq \lceil \log_2 n \rceil$인 층에서 출력 수열의 선형복잡도 상한은 2^n-1임을 알 수 있다.

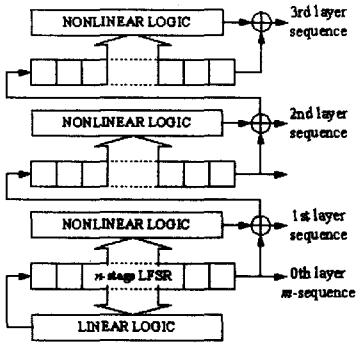


그림 4. 제안된 계층구조 NLFFL 수열 발생기 (Type II).

Ⅲ. 개선된 계층 구조의 NLFFL 발생기

그림 3에서 첫 번째 층(1st layer)의 NLFFL 함수는 그림 2 또는 식 (1)과 같은 형태를 이용하여 이진 수열의 0과 1에 대한 균형성을 최적으로 만들 수 있다. 위와 같은 구조를 확장하여 그림 4에서와 같이 모든 층의 NLFFL에 (1)과 같은 형태의 함수를 사용한 구조를 Type II라 정의한다. 여기서 n은 홀수, (1)에서 비선형 함수 f의 차수는 2이며, x_1을 제외한 모든 변수 $x_2, x_3, \cdots, x_n$는 Langford 연결처럼 이차 비선형 항에 한번씩만 사용된다고 가정한다. 그러나 각 비선형 항의 연결 간격은 Langford 연결과 달리 임의적이다. 그림 4에서 0번째 층의 최대길이 수열과 첫 번째 층의 수열은 이상적인 이진 균형 특성을 보이지만, 두 번째 이상의 층에서 발생되는 수열들은 Type I과 마찬가지로 이상적인 균형 특성을 보장할 수 없다. 이것은 첫 번째 층 이상에서 발생되는 수열들이 0번째 층의 최대길이 수열과 달리 span-n 성질을 가지고 있지 않기 때문이다. 그러나 이진 또는 r-tuple ($r \le n$) 균형 특성에 있어서는 제안된 Type II가 기존의 Type I보다 우수한 경향을 보인다. 또한, Type II는 비선형 함수 f가 Langford 연결이 아닐 때에도 균형성이 좋으며, Type I처럼 층이 증가함에 따라 선형복잡를 최대로 증가 시킬 수 있다.

그림 5는 $n = 17$이고 주기가 Mersenne 소수인 $2^{17}-1$일 때, 다음의 Langford 연결을 사용하는 수

lst lyr.	2	6	3	2	7	8	3	5	6	1	4	1	7	5	8	4
2nd lyr.	2	4	6	2	7	8	4	5	1	6	1	3	7	5	8	3
3rd lyr.	3	1	8	1	3	7	5	2	6	4	2	8	5	7	4	6
4th lyr.	1	6	1	7	2	8	5	2	6	3	4	7	5	3	8	4
5th lyr.	8	4	5	6	2	7	4	2	5	8	6	3	1	7	1	3

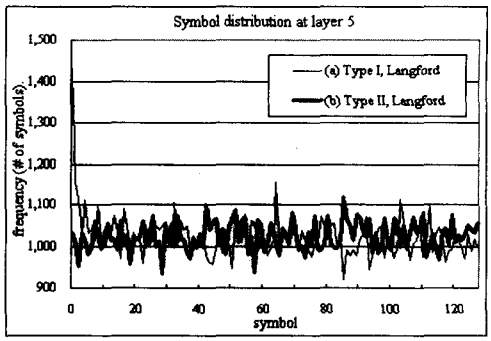


그림 5. Langford 연결을 사용한 (a) Type I 과 (b) Type II 에서 5번째 층 출력의 7-tuple 128 심볼의 발생 분포.

열에 대한 7-tuple 128심볼의 발생빈도를 측정한 Type I 또는 Type II 수열 발생기의 5번째 층 출력 것이다. 0번째부터 5번째 층까지 출력 수열의 선형 복잡도는 Type I의 경우 각각 17, 153, 3213, 65535, 131070, 131070으로 5번째 층이 상한과 1 차이가 나는 것 외에는 모두 (2)의 상한값을 만족하고 Type II는 모두 만족한다. 그림 5에서 Type I의 심볼 분포는 비록 Langford 연결을 사용하지 않은 (예를 들면 그림 6와 같은) Type I 방법에 비하여 우수하지만, 0 심볼의 발생 빈도가 Type II 경우에 비하여 월등히 큰 것을 관찰할 수 있다. 따라서 이진 심볼의 균형성도 Type I보다 Type II가 좋음을 확인할 수 있다.

그림 6은 그림 5의 Langford 연결 대신 첫 번째 층에서 5번째 층까지 각 층의 AND 게이트의 입력 간격이 다음과 같이 각각 0, 1, 2, 3, 4, 0으로 같은 층에서 모두 동일한 경우이다.

lst lyr.	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8
2nd lyr.	1	2	1	2	3	4	3	4	5	6	5	6	7	8	7	8
3rd lyr.	1	2	3	4	1	2	3	4	5	6	7	8	5	6	7	8
4th lyr.	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
5th lyr.	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8

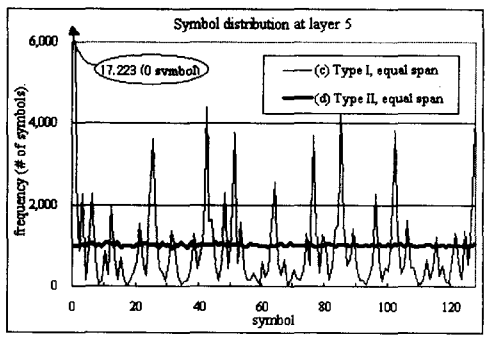


그림 6. 동일 간격 연결을 사용한 (a) Type I 과 (b) Type

이 경우 0번째부터 5번째 층까지 출력 수열의 선형복잡도는 Type I, II 모두 각각 17, 153, 3213, 65535, 131070, 131070으로 5번째 층이 상한과 1 차이가 나는 것 외에는 모두 (2)의 상한값을 만족한다. 그러나 Type I은 균형성이 상당히 악화되었고 Type II는 여전히 좋음을 볼 수 있다. 이러한 연결 방법은 Type I에서 균형성의 개선을 위하여 가장 피해야할 경험적인 조건[4]이지만 Type II의 경우는 이러한 비선형 NLFFL에 대해서도 상당히 좋은 균형 특성을 나타냄을 관찰할 수 있다.

Type II에서 최대 선형복잡도 증가를 보장하기 위해 각층마다 2-input AND 게이트 입력 한 쌍씩을 입력 간격이 서로 다르도록 고정하고 나머지는 임으로 선택한다고 가정한다면, 하나의 층에서 가능한 연결 방법의 수는

$$\prod_{i=1}^{(n-3)/2}\binom{n-1-2i}{2} \tag{3}$$

임을 쉽게 알 수 있다. 표 1은 LFSR의 단수 n에 따른 Langford 해의 개수와 (3)을 비교한 것으로 후자의 경우가 전자에 비해서 훨씬 큰 것을 관찰할 수 있다. Type II에서는 n이 홀수이므로 Langford 해의 수는 짝수 $n-1$에 대하여 구한 것이다.

표 1. Langford 연결과 임의 연결의 비교

n	Langford연결의 수	임의 연결의 수 (3)
7	1	6
9	1	90
15	26	7.5×10^6
17	150	6.8×10^8
23	17792	2.4×10^{15}
25	108144	5.5×10^{17}

Ⅳ. 특성 분석

표 2는 $n=17$인 그림 6의 Type II 실험에서 각 층의 1번 쌍만을 고정하고 나머지 쌍은 임의로 2-input AND gate에 연결 하였을 때, 3번째 층 수열의 선형복잡도와 1~3 tuple 심볼들의 발생빈도를 기록한 것이다. 즉, 아래와 같이 ①번은 고정하고 x 표시된 나머지는 임으로 연결하여 3600번 실험하였다.

1st lyr. ① ① x x x x x x x x x x x x x x x
2nd lyr. ① x ① x x x x x x x x x x x x x
3rd lyr. ① x x x ① x x x x x x x x x x x

표 2. Type II의 임의 연결에 대한 특성 비교
II 에서 5번째 층 출력의 7-tuple 128 심볼의 발생 분포.

비교항목		평균값	표준편차	불균형성
1-tuple 심볼빈도	최대	65680.5	108.4	±0.22%
	최소	65390.5	108.4	
2-tuple 심볼빈도	최대	32943.0	112.9	±0.53%
	최소	32593.2	111.7	
3-tuple 심볼빈도	최대	16560.6	89.1	±1.07%
	최소	16208.6	87.9	
선형복잡도		65534.4	3.2	65501(4회) 65518(120회) 65535(3476회)

이 실험에서는 각 수열의 한 주기에 대한 최대 출현 심볼과 최소 출현 심볼의 발생 회수를 구하여 평균을 구하였다. 이 수열의 주기는 $2^{17}-1$이므로 어떤 m-tuple 심볼의 이상적인 한 주기 발생 회수는 약 2^{17-m}이다. 이 값을 기준으로 할 때 최대 또는 최소 발생빈도의 평균값들은 이상적인 값으로부터 약 100심볼의 편차를 가짐을 관찰할 수 있으며, (최대값평균 또는 최소값평균 -2^{17-m})/2^{17-m}으로 계산된 불균형성이 1% 내외인 사실로부터 이러한 수열이 이상적인 분포에 근접함을 관찰할 수 있다.

선형복잡도의 경우는 3600회중 3476회 (96.6%)가 (2)에 의한 상한 L_3를 만족하고 나머지 120회 (3.33%), 4회 (0.11%) 역시 상한에 근접한다. 특히 n이 예제와 같이 소수인 경우, 비교적 정확하게 선형복잡도의 확률적인 예측이 가능하다. 즉 k번째 층에서 출력되는 이진 수열 $\{s(i)\}$를 GF(2)상에서 미지수 D에 관한 다항식

$$S(D)=\sum_{i=0}^{\infty}s(i)D^i \tag{4}$$

로 표현하면, 최대 선형복잡도는 L_k이므로 이 층의 출력 가능한 어떤 수열도 다음과 같은 멱급수 (power series) 형태로 표현할 수 있다.

$$S(D)=\frac{B(D)}{C(D)} \tag{5}$$

여기서 $\deg[B(D)]\le L_k-1$이고 $\deg[C(D)]=L_k$이며, $C(D)$의 기약 인수들(irreducible factors)의 차수는 n이 소수이므로 1이거나 n이다. 이때 최소 다항식 $C(D)$가 단순근(simple root)들을 가지므로 차수가

1인 $1+D$인수를 무시해도 선형복잡도가 1밖에 차이가 나지 않는다. 따라서 (5)를 부분 분수(partial fractions)로 전개하면

$$S(D)=\frac{B_1(D)}{C_1(D)}+\frac{B_2(D)}{C_2(D)}+\cdots+\frac{B_r(D)}{C_r(D)} \qquad (6)$$

으로 표현할 수 있고 $1+D$인수를 무시할 경우 $C_i(D)$는 차수 n인 기약 인수들이고 $\deg[B_i(D)]<n$이며 $r=L_k/n$이다. 이때 비선형 피드포워드 함수에 의한 선형복잡도가 축소(degenerate)없이 L_k일 확률 P_0는 (6)에서 모든 $B_i(D)$가 0이 아닐 확률을 구하는 것과 같다. 즉 $B_i(D)$가 0이 아닌 경우의 수는 $n-1$차 다항식의 모든 계수가 0 인 아닌 경우의 수인 2^n-1과 같으므로

$$P_0=\left(\frac{2^n-1}{2^n}\right)^r\approx e^{-r/2^n} \qquad (7)$$

이다[2]. 여기서 $\lim_{x\to\infty}(1-1/x)^x=e^{-1}$임을 이용하였다. 비슷한 방법으로 선형복잡도가 $L_k-t\cdot n$일 확률 P_t는 다음과 같이 구할 수 있다.

$$P_t=\binom{r}{t}\left(\frac{1}{2^n}\right)^t\left(1-\frac{1}{2^n}\right)^{r-t}\approx\binom{r}{t}\left(\frac{1}{2^n}\right)^t e^{-(r-t)/2^n} \qquad (8)$$

표 2에서 3번째 층의 출력 수열은 $P_0=0.971$이고 $P_1=0.029$이므로 실험치인 0.966, 0.033과 비교할 만하다. t가 증가할수록 (8)의 값은 지수적으로 감소함으로 임의 연결의 대부분이 선형복잡도의 상한값 또는 그것의 근사값에 접근함을 확인할 수 있다. 또한 n이 비록 소수가 아니더라도 비슷한 방법으로 선형복잡도를 축소시키는 비선형 함수의 비율이 매우 작음을 유추해볼 수 있다.

n이 소수가 아닌 경우나 n이 소수이지만 주기 2^n-1이 소수가 아닌 경우는 임의의 비선형 피드포워드 함수에 의하여 주기가 축소될 수 있다. L_k가 주기에 가까울 경우, 이러한 확률 P_p는 (6)에서 $C_i(D)$가 원시 다항식(primitive polynomial)인 모든 항의 $B_i(D)$가 0이 되는 다음과 같은 확률에 근접한다.

$$P_p\approx\left(\frac{1}{2^n}\right)^{\phi(2^n-1)/n} \qquad (9)$$

여기서 ϕ는 Euler 함수로 $\phi(2^n-1)/n$는 가능한 n차 원시 다항식의 개수이다. (9)의 확률은 매우 작지만 Type II에서는 이러한 확률조차 0이 된다. 이것은 각 층에서 비선형 출력과 시간 지연된 이전 출력이 선형적으로 더해지기 때문이며 결과적으로 (6)에서 기저의 LFSR 수열에 해당하는 항이 항상 포함기 때문이다..

V. 결 론

본 논문에서는 선형복잡도가 크고 균형성이 좋은 수열을 발생시키기 위하여 기존의 Type I 계층 구조를 변형하여 Langford 연결 같은 특별한 비선형 연결 방법 없이도 잡음 특성이 좋은 수열을 발생시킬 수 있음을 알아보았다. 이것은 Type II에서 NLFFL함수를 수열 발생기의 키(key)로 사용할 때 균형성을 나쁘게 하거나 선형복잡도 감소 없이 사용할 수 있는 비선형 함수의 개수를 늘임으로써 키의 크기를 크게 할 수 있음을 의미한다. 또한 LFSR의 단수 n이 소수일 때 실험적 또는 통계적 분석을 통하여 제안된 구조에서 발생된 수열의 선형복잡도가 최대값에서 많이 벗어나지 않음을 확인하였고 n이 소수가 아닐 때에도 비슷한 결과를 얻을 수 있음을 논의하였다. 마지막으로 기저 수열의 주기 2^n-1이 소수가 아닐 때 Langford 연결을 사용하는 Type I 수열의 주기는 (그 확률이 비록 작을지라도) 축소될 수 있지만 Type II에서는 이러한 경우가 발생하지 않음을 설명하였다.

참 고 문 헌

[1] E. L. Key, "An analysis of the structure and complexity of nonlinear binary sequence generators," IEEE Trans. Inform. Theory, vol. IT-22, pp. 732-736, Nov. 1976.

[2] R. A. Rueppel, Analysis and Design of Stream Ciphers, Springer-verlag, New York, 1986

[3] M. K. Simon, J. K. Omura, R. A. Scholtz, and B.K. Levitt, Spread Spectrum Communications Handbook, McGraw-Hill, New York, 1994.

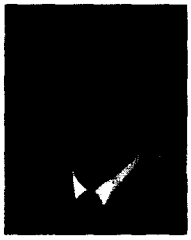
[4] E. J. Groth, "Generation of binary sequences with controllable complexity," IEEE Trans. Inform. Theory, vol. IT-17, No. 3, pp.

288-296, May 1971.

[5] C. Langford, "problem," Math. Gaz., vol. 42, p.228, Oct. 1958.

[6] S. W. Golomb, Shift Register Sequences, Aegean Park Press, Laguna Hills, CA, 1982

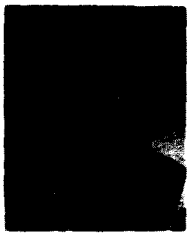
은 유 창 (Yu-Chang Eun) 정회원



1998년 2월 : 연세대학교 전자공학과 졸업 (공학사)
2000년 2월 : 연세대학교 대학원 전기전자공학과 졸업 (공학석사)
2000년 3월~현재 : 연세대학교 대학원 전기전자공학과 박사과정

<주관심분야> Application of PN Sequences to Spread Spectrum and Crypto Systems, Block Codes and Convolutional codes

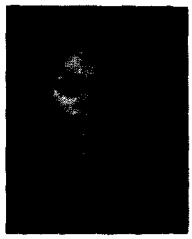
진 석 용(Seok-Yong Jin) 준회원



2001년 8월 : 연세대학교 전기전자공학과 졸업 (공학사)
2003년 8월 : 연세대학교 대학원 전기전자공학과 졸업 (공학석사)
2003년 9월~현재 : 연세대학교 대학원 전기전자공학과 박사과정

<주관심분야> Error Correcting Codes, PN Sequences, CDMA, Spread Spectrum Communication, Stream Cipher

홍 윤 표 (Yun-Pyo Hong) 준회원



2000년 2월 : 연세대학교 전자공학과 졸업 (공학사)
2002년 2월 : 연세대학교 대학원 전기전자공학과 졸업 (공학석사)
2002년 3월~현재 : 연세대학교 대학원 전기전자공학과 박사과정

<주관심분야> Application of PN Sequences to Spread Spectrum and Crypto Systems, Block Codes and Convolutional codes

송 홍 엽 (Hong-Yeop Song) 종신회원

1984년 2월 : 연세대학교 전자공학과 졸업 (공학사)
1986년 5월 : USC 대학원 전자공학과 졸업 (공학석사)
1991년 12월 : USC 대학원 전자공학과 졸업 (공학박사)
1992년 ~ 1993년 : Post Doc., USC 전자공학과
1994년~1995년 : Qualcomm Inc., 선임연구원
1995년 9월~현재 : 연세대학교 전기전자공학과 교수

<주관심분야> PN Sequences, Error Correcting Codes, Spread Spectrum Communication Systems, Steam Cipher Systems