최대주기 수열의 1-심볼 추가 선형복잡도

준회원 정 진 호*, 종신회원 양 경 철*

Linear Complexity of 1-Symbol Insertion Sequences from m-Sequences

Jin-Ho Chung* *Associate Member*, Kyeongcheol Yang* *Lifelong Member*

요 약

주기 수열에서 각 주기의 임의의 위치에 r개의 심볼을 추가하는 경우, 더 긴 주기를 가지는 수열을 얻을 수 있다. 본 논문에서는 주기 수열에 r개의 심볼을 추가한 수열의 선형복잡도에 대한 기존 결과들을 정리하고 $GF(p)$ 상에서 정의된 최대주기 수열에 1개의 심볼을 추가함으로써 얻어지는 수열들의 선형복잡도의 분포를 분석한다. 그리고 이진 최대주기 수열들의 1-심볼 추가 k-오류 선형복잡도에 대한 새로운 사실들을 유도함으로써 수열의 안정성을 평가한다.

Key Words : Linear complexity, p-ary sequences, m-sequences, 1-symbol insertion.

ABSTRACT

From a periodic sequence, we can obtain new sequences with a longer period by r-symbol insertion to each period. In this paper we review previous results on the linear complexity of periodic sequences obtained by r-symbol insertion. We derive the distribution of the linear complexity of 1-symbol insertion sequences obtained from m-sequences over $GF(p)$, and prove some relationship between their linear complexity and the insertion position. Then, we analyze the k-error linear complexity of the 1-symbol insertion sequences from binary m-sequences.

Ⅰ. 서 론

선형복잡도와 k-오류 선형복잡도는 의사불규칙 수열(pseudorandom sequence)의 암호학적 특성을 나타내는 중요한 척도이다. 주기(period)가 N인 수열 S의 선형복잡도 $L(S)$는 S에 의해 만족되는 선형 점화식(linear recursion)들의 차수(order) 중에서 최소값으로 정의된다. 또한 S의 k-오류(k-error) 선형복잡도 $L_k(S)$는 다음과 같이 정의된다[8]:

$$L_k(S) = \min\{L(S+E) \mid 0 \le w_H(E) \le k\},$$

여기서 E는 주기가 N인 오류수열이고 $w_H(E)$는 E의 해밍 무게(Hamming weight)이다. 암호학적인 관점에서 수열은 주기에 대해 너무 작지 않은 선형복잡도를 가져야 할 뿐만 아니라 적은 비트 변화에 선형복잡도가 크게 감소하지 않아야 한다.

어떤 소수 p에 대해 p^n-1의 주기를 가지는 유한체(finite field) $GF(p)$ 상의 수열을 S라 하자. 이때 S의 한 주기의 임의의 위치에 $GF(p)$에 속하는 한 심볼(symbol)을 넣음으로써 주기가 p^n인 수열을 생성할 수 있다. Imamura 등[4]과 Uehara, Imamura

※ 본 연구는 정보통신연구진흥원 및 정보통신부의 대학 IT연구센터 육성·지원사업의 지원을 받고 있는 포항공과대학교의 OFDM 기반 광대역 이동 인터넷 연구센터 (BrOMA) (IITA-2007-C1090-0701-0037)와 2008년도 두뇌한국21사업에 의해 공동지원되었음.

* 포항공과대학교 전자전기공학과 통신 및 신호설계 연구실(kcyang@postech.ac.kr)

논문번호 : KICS2007-06-250, 접수일자 : 2007년 6월 9일, 최종논문접수일자 : 2007년 12월 21일

[9]는 $GF(p)$ 상의 p^n-1 주기 수열에 1개의 심볼을 추가한 수열의 선형복잡도에 대한 경계(bound)들을 유도하였다[4], [9]. 특히, 제로섬(zero-sum) 성질을 가지는 최대주기 수열(m-sequences), GMW 수열, 벤트(bent) 수열 등의 1-심볼 추가 선형복잡도에 대한 상계(upper bound)와 하계(lower bound)를 유도하였다[9]. 또한, Jiang 등은 임의의 주기를 가지는 $GF(p)$ 상에서의 수열에 r개의 심볼을 추가, 삭제, 또는 교체하였을 경우의 선형복잡도에 대한 경계들을 유도하였다[5].

본 논문에서는 최대주기 수열에 대해서 [9]의 결과를 보강하여 1-심볼 추가 선형복잡도의 분포(distribution)와 심볼이 들어간 위치에 따른 선형복잡도를 분석한다. 또한, Stamp-Martin 알고리즘[8]을 적용하여 이진(binary) 최대주기 수열들의 k-오류 선형복잡도를 분석한다.

본 논문의 구성은 다음과 같다. II절에서는 임의의 주기 수열에 대해서 r개의 심볼을 추가한 수열들의 선형복잡도에 대한 기존의 결과들을 살펴본다. III절에서는 최대주기 수열에 1개의 0을 추가한 수열의 선형복잡도의 분포를 분석하고 최대주기 수열의 선형복잡도와 비교한다. 또한 0을 추가한 위치에 따른 선형복잡도의 분포를 분석한다. IV절에서는 Stamp-Martin 알고리즘[8]을 적용하여 최대주기 수열에 1개의 심볼을 추가한 수열의 k-오류 선형복잡도에 대해 분석함으로써 암호학적 안정성을 평가한다. V절에서는 결론을 맺는다.

II. 주기 수열의 r-심볼 추가 선형복잡도

주기가 N인 $GF(p)$ 상의 수열 $S=(s_0, s_1, \cdots, s_{N-1})^\infty$에 대해서 $S(x)=s_0+s_1x+\cdots+s_{N-1}x^{N-1}$라 두자. 또한,

$$f(x)=\frac{x^N-1}{\gcd(x^N-1, S(x))} \tag{1}$$

라 두면

$$L(S)=\deg(f(x)) \tag{2}$$

라는 것이 잘 알려져 있다. 이 때 $f(x)$를 S의 극소 다항식(minimal polynomial)이라 부른다[2].

어떤 정수 τ, $0\le\tau\le N-1$에 대해서 $S_\tau=(s_\tau, s_{\tau+1}, \cdots, s_{\tau+N-1})^\infty$이라 하자. 이 때, S_τ를 S의 순환 이동(cyclic shift)이라 부른다. 임의의 주기 수열의 선형복잡도는 자기 자신의 순환 이동에 대해 변하지 않는다. 따라서 S의 원소 s_i와 s_{i+1} 사이에 한 심볼을 추가한 수열 S^+의 선형복잡도는 S_i의 각 주기의 마지막에 같은 심볼을 추가한 수열의 선형복잡도 S^*와 같다.

$N=p^n-1$일 때, S^+의 선형복잡도에 대해서 다음과 같은 정리가 성립한다:

정리 1 [9]. 주기가 p^n-1인 수열 S의 각 주기의 끝에 $GF(p)$의 원소 b를 추가한 수열을 S^*이라 하자. $b_0=\sum_{i=0}^{p^n-2}s_i$라 두면 S^*의 선형복잡도 $L(S^*)$는 다음을 만족한다:

$$L(S^*)=p^n \quad \text{if } b\neq -b_0,$$
$$L(S^*)\le p^n-1 \quad \text{if } b=-b_0.$$

특히, $b_0=0$인 경우에는 다음과 정리가 성립한다:

정리 2 [9]. S에 대해 $\sum_{i=0}^{p^n-2}s_i=0$가 성립하면 $L(S^*)$는 다음을 만족한다:

$$L(S^*)=p^n \quad \text{if } b\neq 0,$$
$$p^n-L(S)\le L(S^*)\le p^n-1 \quad \text{if } b=0.$$

Jiang 등은 주기가 N인 $GF(p)$ 상의 수열 S의 각 주기의 임의의 위치에 r개의 심볼을 추가한 수열 S^{+r}의 선형복잡도에 대해서 다음 정리를 유도하였다:

정리 3 [5]. 제로수열이 아닌 S^{+r}의 선형복잡도 $L(S^{+r})$는 다음을 만족한다:

$$\frac{N}{r}-L(S)<L(S^{+r})\le N+r.$$

III. 최대주기 수열의 1-심볼 추가 선형복잡도

길이가 $N=p^n-1$인 최대주기 수열 S는 차수가 n인 $GF(p)$ 상의 어떤 원시다항식(primitive polynomial) $m(x)$를 극소다항식으로 가진다. 따라서 $\gcd(x^N-1, S(x))=g(x)$이라 두면 차수가 $n-1$ 이하이고 0이 아닌 다항식 $a(x)$에 대해

$$S(x)=a(x)\cdot g(x),\ x^N-1=m(x)\cdot g(x) \tag{3}$$

이 성립한다. 여기서 $\deg(g(x))=p^n-1-n$이다.

S의 각 주기의 임의의 위치에 1개의 심볼을 추가한 수열을 S^+라 하자. 추가한 심볼이 0일 때, S^+의 선형복잡도에 대해 다음과 같은 결과를 유도할 수 있다:

정리 4. 주기가 $N=p^n-1$인 최대주기 수열 $S=(s_0, s_1, \ldots, s_{N-1})^\infty$의 각 주기의 임의의 위치에 0을 추가한 수열을 S^+이라 하자. $1\le k\le n$에 대해서

$$L(S^+)=p^n-k$$

가 성립하는 S^+의 경우의 수는 $(p-1)p^{n-k}$이다.

증명) (3)에서 서로 다른 $a(x)$에 해당하는 수열들은 서로의 순환 이동(cyclic shift)임을 쉽게 알 수 있다. 따라서 임의의 서로 다른 위치에 0을 넣는 것은 서로 다른 $a(x)$에 해당하는 수열들의 주기의 끝에 0을 넣는 것과 같다. 어떤 $a(x)$에 해당하는 수열 S의 각 주기의 끝에 0을 넣은 수열 S^*에 대해

$$S^*(x)=S(x)=a(x)\cdot g(x)$$

이 성립한다. 또한,

$$\gcd(x^{p^n-1}-1, x^{p^n}-1)=\gcd(g(x),(x-1)^{p^n})=x-1$$

이므로

$$\gcd(x^{p^n-1}-1, a(x)\cdot g(x))=(x-1)\cdot\gcd((x-1)^{p^n-1}, a(x))$$

이다. $0\le k\le n-1$에 대해 $\deg(\gcd(a(x),(x-1)^{p^n}))=l$를 만족하는 $a(x)$의 개수는 $(p-1)p^{n-l}$이므로 주어진 정리가 성립한다. □

정리 2와 4로부터 최대주기 수열의 선형복잡도는 주기에 대해 최소의 값을 가지지만, 각 주기에 1 심볼을 넣은 후에는 선형복잡도가 주기에 매우 가까워진다는 사실을 알 수 있다.

길이가 p^n-1인 최대주기 수열의 한 주기에는 $(0,0,\ldots,0)$을 제외한 길이가 n인 임의의 벡터(vector)들이 한번씩 나타난다. 최대주기 수열 S에 0을 넣은 위치에 따라 다음과 같은 경우들로 나눌 수 있다:

(a) $(n-1)$-벡터 $(0,0,\ldots,0)$에 0을 추가: (3)에서 $a(x)=1, x, \ldots, x^{n-1}$인 경우로서 항상

$$L(S^+)=p^n-1$$

을 만족한다.

(b) $(n-1)$-벡터 $(0,0,\ldots,0)$에 0을 추가$(2\le l\le n-1)$: (3)에서 $a(x)=a^*(x), a^*(x)x, \ldots, a^*(x)x^{n-l}$, $\gcd(x, a^*(x))=1$, $\deg(a(x))\le l-1$인 경우로서

$$L(S^+)\ge p^n-l$$

이 성립한다.

(c) 두 개의 1 사이에 0을 추가: (a), (b)의 결과에 의해

$$L(S^+)\ge p^n-n$$

이 성립하므로 $L(S^+)$가 최소값을 가지는 경우를 포함한다.

그림 1은 (a), (b), (c)의 경우를 설명한다. (1)과 (2)를 통해서 위의 결과를 유도할 수 있다.

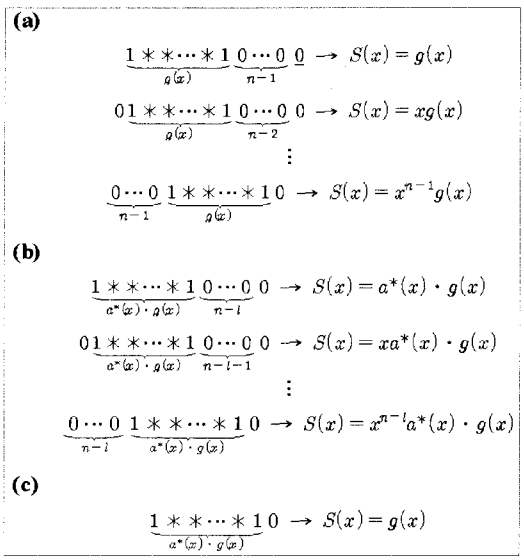


그림 1. 0의 추가 위치에 따른 선형복잡도

예제 1. $p=2$이고 주기가 $7=2^3-1$인 최대주기 수열 $S=(0010111)$에 하나의 0을 추가한 수열 S^+의 선형복잡도는 다음과 같이 주어진다:

$L(S^+)=7$: 00101110, 01011100, 10111000, 11001010,
$L(S^+)=6$: 01110010, 11100100,
$L(S^+)=5$: 10010110.

예제 2. $p=5$이고 주기가 $24=5^2-1$인 최대주기 수열의 각 주기의 임의의 위치에 $c\in GF(5)$를 추가했을 때의 선형복잡도 $L(S^+)$의 분포는 그림 2와 같이 주어진다. $c=0$일 때, $6=(5^2-1)/(5-1)$의 간격으로의 값이 반복된다. 이것은 최대주기 수열의 원소들이 $(p^n-1)/(p-1)$길이의 부분수열 단위로 0이 아닌 상수배가 되어서 나타나기 때문이다 [3]. $c\neq0$인 경우에는 항상 주기와 $L(S^+)$의 값이 같다는 것을 알

수 있다. 그림 3은 $p=5$이고 주기가 $124=5^3-1$인 경우를 나타낸다. 이러한 예를 통해 정리 4의 결과를 확인할 수 있다.

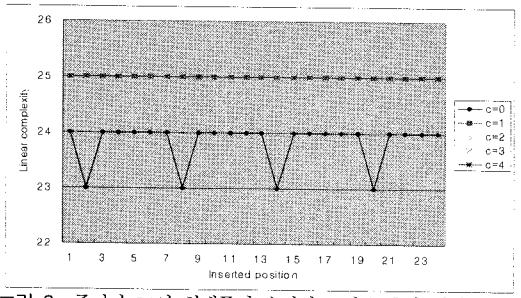


그림 2. 주기가 24인 최대주기 수열의 1-심볼 추가 선형복잡도

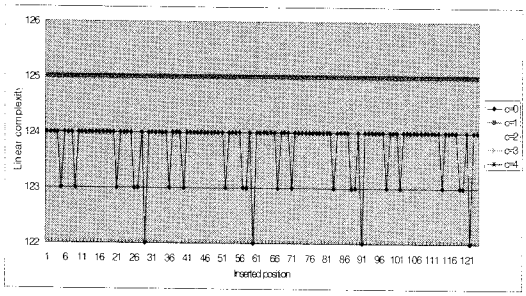


그림 3. 주기가 124인 최대주기 수열의 1-심볼 추가 선형복잡도

Ⅳ. 1-심볼 추가 이진 최대주기 수열의 k-오류 선형복잡도

주기가 N인 이진 수열의 S의 자기상관(autocorrelation) $\theta_s(\tau)$는 다음과 같이 정의된다:

$$\theta_s(\tau)=\sum_{t=0}^{N-1}(-1)^{s_t+s_{t+\tau}},$$

여기서 $0\le\tau\le N-1$이다. $N=2^n-1$일 때, $\theta_s(\tau)$가 다음을 만족하면 S는 최적의 자기상관 특성을 가진다고 부른다:

$$\theta_s(\tau)=\begin{cases}2^n-1, & \tau=0,\\ -1, & \tau\neq 0.\end{cases}$$

최적의 자기 상관 특성을 가지는 2^n-1 주기 이진 수열은 균형성(balancedness)을 만족하며, 임의의 에 대해 다음 성질을 만족한다는 것이 알려져 있다 [2], [3]:

$$|\{t\,|\,(a_t,a_{t+\tau})=(a,b)\neq(0,0)\}|=2^{n-2},$$
$$|\{t\,|\,(a_t,a_{t+\tau})=(0,0)\}|=2^{n-2}-1.$$

이러한 성질을 2쌍 균형성(2-tuple balancedness)이라 부른다. 최대주기 수열 S는 이러한 성질을 모두 만족하며 임의의 $0\le t\le N-1$에 대해서 다음 식을 만족하는 τ, $0\le\tau\le N-1$이 존재한다:

$$s_i+s_{i+t}=s_{i+\tau},$$

여기서 이다. 이러한 성질을 shift-and-add 성질이라 부른다. 최대주기 수열의 2쌍 균형성과 shift-and-add 성질을 Stamp-Martin 알고리즘 [8]에 적용하여 다음 정리를 유도할 수 있다.

정리 5. $n\ge 2$에 대해 주기가 $N=2^n-1$인 최대주기 수열 S에 1 심볼을 추가한 2^n 주기 수열을 S^+라 두자. S^+의 k-오류 선형복잡도 $L(S^+)$가 2^{n-1}보다 작아지는 최소의 k를 $k_{\min}$이라 두면 $k_{\min}$은 다음을 만족한다:

$$k_{\min}\ge 2^{n-3}-1.$$

증명) $S_1=(s_0,s_1,\ldots,s_{N/2-2})$, $S_2=(s_0,s_1,\ldots,s_{N/2-2})$라 두면 S의 각 주기의 끝에 한 심볼 $c\in GF(2)$를 추가한 수열 S^+은 $(S_1:s_{N/2-1}:S_2:c)$의 형태로 나타낼 수 있다. 최대주기 수열의 shift-and-add 성질을 가지므로 어떤 위상이동 δ, $0\le\delta\le N-1$에 대해서 $S_1\oplus S_2=(s_\delta,s_{\delta+1},\ldots,s_{\delta+N/2-2})$이 성립한다. $s_{N/2-1}=0$이라 가정하고 $a,b\in GF(2)$에 대해서

$$N_1(a)=|\{t\,|\,s_t=a,\delta\le t\le\delta+N/2-2\}|,$$
$$N_2(a)=|\{t\,|\,s_t=a,N/2\le t\le N-2\}|,$$
$$N_{1,2}(a,b)=|\{t\,|\,s_{\delta+t}=a,s_{t+N/2}=b,0\le t\le N/2-2\}|$$

을 정의하자. $N_1(1)=x$이라 두면 $N_1(0)=2^{n-1}-x-1$, $N_2(0)=x-1$, $N_2(1)=2^{n-1}-x$임을 알 수 있다. S의 2쌍 균형성에 의해

$$N_1(0)-N_2(0)\le N_{1,2}(0,1)\le 2^{n-2}$$

이 성립하므로

$$x=N_1(1)=w_H(S_1\oplus S_2)\ge 2^{n-3}$$

이다. Stamp-Martin 알고리즘 [8]에 의해 $L_k(S^+)\le 2^{n-1}$인 최소의 k는 $w_H(S_1\oplus S_2)+(s_{N/2-1}\oplus c)$이므로 주어진 정리가 성립함을 알 수 있다. $s_{N/2-1}=1$인 경우도 같은 방법으로 증명할 수 있다. □

정리 5의 증명과정에서 $k_{\min}$은 길이가 $2^{n-1}-1$인 부분 수열의 해밍 무게에 의해 결정된다는 것을 알 수 있다. Kumar와 Wei는 최대주기 수열의 부분 수열의 해밍 무게에 대해서 다음과 같은 정리를 유도하였다:

정리 6 [6]. S를 주기가 $N=2^n-1$인 최대주기 수열이라 하자. 임의의 실수 μ, $0<\mu\le 1$와 $\epsilon>0$을 정하면 모든 $n>n_{\epsilon,\mu}$에 대해서 다음을 만족하는 자연

수 $n_{\epsilon,\mu}$이 존재한다.

$$\left|\frac{\lambda(\lfloor \mu N \rfloor)}{\lfloor \mu N \rfloor} - \frac{1}{2}\right| < \epsilon,$$

여기서 $\lambda(\lfloor \mu N \rfloor)$는 길이가 $\lfloor \mu N \rfloor$인 S의 어떤 부분 수열의 해밍 무게이다.

정리 6을 통해 n이 커질 때, 최대주기 수열의 길이가 $2^{n-1}-1$인 부분 수열의 해밍 무게는 근사적으로 2^{n-2}에 가까운 값을 가진다는 것을 알 수 있다. 따라서 정리 5에서 정의된 $k_{\min}$은 주기가 길어질수록 2^{n-2}에 가까워진다. 이것은 최대주기 수열에 1-심볼을 추가한 수열의 선형복잡도를 주기의 절반 이하로 낮추기 위해서는 주기의 1/4 정도의 비트를 바꾸어야 한다는 것을 의미한다.

표 1은 정리 6에서 정의된 $\lambda(2^{n-1}-1)$의 n에 따른 최소값들을 나타낸다.

표 1. 최대주기 수열의 길이가 $2^{n-1}-1$인 부분수열의 해밍 무게의 최소값

n	주기	$\min\{\lambda(2^{n-1}-1)\}$
2	3	0
3	7	1
4	15	2
5	31	5
6	63	12
7	127	27

Kurosawa 등은 임의의 2^n주기 수열 S에 대해서 $L_k(S) < L(S)$를 만족하는 최소의 k가 $2^{w_H(2^n - L(S))}$와 같다는 것을 유도하였다 [7]. 따라서 정리 2와 4의 결과와 결합하면 2^n-1 주기의 최대주기 수열로부터 얻어진 수열 S^+에 대해 $L_k(S) < L(S)$가 성립하는 최소의 k는 n보다 작거나 같다는 것을 알 수 있다.

V. 결 론

최대주기 수열의 각 주기마다 하나의 심볼을 추가한 수열에 대한 선형복잡도의 분포를 분석하였다. 최대주기 수열은 주기에 비해 최소의 선형복잡도를 가지지만 한 심볼을 추가하였을 때는 거의 주기에 가까운 선형복잡도를 가진다는 것을 알 수 있었다. 또한 이진 최대주기 수열에 한 심볼을 추가한 수열의 k-오류 선형복잡도를 부분 수열의 해밍 무게를 통해 분석하였다. 이러한 수열의 선형복잡도를 주기의 절반 이하로 감소시키기 위해서는 최소한 주기의 1/8 정도가 되는 비트를 바꾸어야 한다는 것을 유도하였다. 최대주기 수열의 선형복잡도는 매우 작지만 1 심볼을 추가함으로써 선형복잡도와 k-오류 선형복잡도가 더 커진다는 것을 확인하였다. 하지만 이러한 수열은 1 심볼을 삭제하였을 경우에 선형복잡도와 k-오류 선형복잡도가 크게 감소하는 약점을 가지고 있다. 최대주기 수열뿐만 아니라 최적 자기상관 특성을 가지는 수열들에 한 심볼을 추가한 수열의 선형복잡도와 k-오류 선형복잡도의 분석은 앞으로 연구해 볼만한 주제라고 할 수 있다.

참 고 문 헌

[1] R. A. Games and A. H. Chan, "A fast algorithm for determining the complexity of a binary sequence with period 2^n," *IEEE Trans. Inform. Theory*, vol. 29, no. 1, pp. 144-146, Jan 1983.

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

[3] S. W. Golomb and G. Gong, *Signal Design for Good Correlation: for wireless communications, cryptography and radar applications*. Cambridge University Press, 2005.

[4] K. Imamura, T. Moriuchi, and S. Uehara, "Periodic sequences of the maximum linear complexity simply obtained from an *m*-sequence," in *Proc. IEEE 1991 Inter. Symp. Inform. Theory*, June 1991, pp. 175.

[5] S. Jiang, Z. Dai, and K. Imamura, "Linear complexity of a sequence obtained from a periodic sequence by either substituting, inserting, or deleting *k* symbols within one period," *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 1174-1177, May 2000.

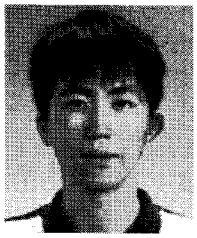
[6] P. V. Kumar and V. K. Wei, "Minimum distance of logarithmic and fractional partial *m*-sequences," *IEEE Trans. Inform. Theory*, vol. 38, no. 5, pp. 1474-1482, Sep. 1992.

[7] K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, "Relationship between linear complexity and k-error linear complexity," *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 694-698, Mar. 2000.

[8] M. Stamp and C. Martin, "An algorithm for the k-error linear complexity of binary sequences with period 2^n," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1398-1401, July 1993.

[9] S. Uehara and K. Imamura, "Linear complexity of periodic sequences obtained from $GF(p)$ sequences with period q^n-1 by one-symbol insertion," *IEICE Trans. Fund.*, vol. E79-A, no. 10, pp. 1739-1740, Oct. 1996.

정 진 호 (Jin-Ho Chung) 준회원



2005년 2월 포항공과대학교 전자전기공학과 졸업

2007년 2월 포항공과대학교 정보통신대학원 석사

2007년 2월~현재 포항공과대학교 전자전기공학과 박사과정

<관심분야> 신호설계, 정보보호, 부호이론, 디지털 통신

양 경 철 (Kyeongcheol Yang) 종신회원

1986년 2월 서울대학교 전자공학과 졸업

1988년 2월 서울대학교 전자공학과 석사

1992년 12월 University of Southern California 전기공학과 박사

1993년 3월~1999년 2월 한양대학교 전자통신공학과 조교수

1999년 2월~현재 포항공과대학교 전자전기공학과 교수

<관심분야> 디지털 통신, 부호이론, 다중 안테나 시스템, 신호설계, 정보보호