p^m-주기 이진 수열의 k-오류 선형복잡도와 이진 순환 부호에의 응용

정회원 한 윤 경*, 종신회원 양 경 철*

On the k-Error Linear Complexity of p^m-Periodic Binary Sequences and Its Applications to Binary Cyclic Codes

Yun Kyoung Han* ***Regular Member***, Kyeongcheol Yang* ***Lifelong Member***

요 약

k-오류 선형복잡도는 통신 시스템 및 스트림 암호 시스템 등에 사용되는 수열의 안정성 여부를 판단하는 중요한 척도이다. 본 논문은 p가 소수이고 2가 모듈로 p^2의 원시근일 때 p^m-주기 이진 수열의 k-오류 선형복잡도와 해당 오류벡터를 효과적으로 구할 수 있는 알고리듬을 소개한다. 또한 암호학적인 관점에서 정의된 k-오류 선형복잡도의 의미를 부호 이론의 관점에서 살펴봄으로써 부호어의 길이가 p^m인 이진 순환 부호를 효과적으로 복호할 수 있는 알고리듬을 소개하며 이러한 부호의 최소 거리에 관한 중요한 성질들을 유도한다.

Key Words : Linear complexity, Stream ciphers, Cyclic codes, Minimum distance, Periodic sequences

ABSTRACT

The k-error linear complexity is a key measure of the stability of the sequences used in the areas of communication systems, stream ciphers in cryptology and so on. This paper introduces an efficient algorithm to determine the k-error linear complexity and the corresponding error vectors of p^m-periodic binary sequences, where p is a prime and 2 is a primitive root modulo p^2. We also give a new sense about the k-error linear complexity in viewpoint of coding theory instead of cryptographic results. We present an efficient algorithm for decoding binary cyclic codes of length p^m and derive key properties of the minimum distance of these codes.

Ⅰ. 서 론

의사불규칙 수열(pseudorandom sequences)의 응용 범위는 스트림 암호 시스템(stream ciphers)을 비롯하여 대역확산 통신 시스템 그리고 몬테 카를로 방법(Monte Carlo methods)을 이용한 전산실험에 이르기까지 매우 다양하다. 암호학적으로 선형복잡도(linear complexity)는 이러한 의사불규칙 수열의 성능을 평가하는 중요한 척도로서 사용된다. 선형복잡도의 두 배에 해당하는 연속된 길이의 수열만 알고 있다면 Berlekamp-Massey(BM) 알고리듬을 통해 LFSR(linear feedback shift register)을 이용하여 전체 수열을 합성해낼 수 있기 때문이다[5]. 이러한 BM 알고리듬에 기반한 공격에 취약하지 않으려면 수열은 큰 선형복잡도를 가져야 함은 물론 약간의 비트 변화에도 선형복잡도의 크기가 크게 감소하지 않아야 한다. Ding 등은 이러한 개념을 선형복잡도의 안정성(stability)이라 부르고 구형복잡도(sphere

※ 본 연구는 한국과학재단 특정기초 연구지원(R01-2003-000-10330-0)으로 수행되었습니다.
* 포항공과대학교 전자전기공학과 통신 및 신호설계 연구실 ({gldsndz, kcyang}@postech.ac.kr)
논문번호 : KICS2006-05-235, 접수일자 : 2006년 5월 26일, 최종논문접수일자 : 2006년 9월 14일

complexity)를 하나의 척도로 정의하였다[2]. 뒤이어 Stamp 등은 구형복잡도와 거의 동일한 개념인 k-오류 선형복잡도(k-error linear complexity)를 새로 정의하고 Games-Chan 알고리듬[1]에 비용(cost)의 개념을 도입하여 2^n-주기 이진 수열의 k-오류 선형복잡도를 간단한 방법으로 계산하였다[9].

F_q는 q개의 원소로 이루어진 유한체라 하자. F_q상의 수열 $S=s_0,s_1,s_2,...$는 c_i, $1 \leq i \leq d$가 F_q상의 계수라 할 때 다음의 선형재귀식(linear recursion)을 만족한다고 하자.

$$s_t + \sum_{i=1}^{d} c_i s_{t-i} = 0, \ \forall t \geq d.$$

이 재귀식에 해당하는 S의 *소멸다항식(annihilator polynomial)*은 다음과 같이 정의된다.

$$g_S(x) = x^d + c_1 x^{d-1} + \cdots + c_{d-1}x + c_d.$$

또한 이 중에서 최소의 차수를 가지는 다항식을 S의 *특성다항식(characteristic polynomial)* $f_S(x)$라 하며 $f_S(x)$의 차수는 S의 *선형복잡도* $L(S)$라 한다. 모든 정수 $i \geq 0$에 대해 $s_i = s_{i+N}$인 경우 S는 N-*주기 수열*이라 하며 $S=(s_0,s_1,\cdots,s_{N-1})^\infty$로 표기한다. 이때 N-주기 수열 S의 k-*오류 선형복잡도*[9]를 $L_k(S)$라 하고 다음과 같이 정의한다.

$$L_k(S) = \min\{L(S+E) \mid w_H(e^N) \leq k\}.$$

여기에서 k는 $0 \leq k \leq N$인 정수이고 E는 주기가 N인 수열로서 e^N은 수열 E의 한 주기에 해당하는 벡터이며 w_H는 해밍무게를 나타낸다.

BM 알고리듬은 $O(N^2)$의 복잡도를 가지므로 BM 알고리듬으로 k-오류 선형복잡도를 계산하는 것은 매우 비효율적이다[9]. 따라서 k-오류 선형복잡도를 효과적으로 구하는 알고리듬을 개발하는 것은 매우 가치있는 연구 주제이다. Kaida 등은 Stamp-Martin (SM) 알고리듬의 일반화된 형태로서 F_{p^m}상의 p^n-주기 수열의 k-오류 선형복잡도를 구하는 알고리듬을 소개하였다[3]. Lauder와 Paterson은 SM 알고리듬을 기반으로 주기가 2^n인 이진 수열의 오류 선형복잡도 프로파일을 구할 수 있는 알고리듬을 소개하였으며 Reed-Muller 부호의 부분부호의 일종인 repeated-root 이진 부호의 복호 알고리듬으로 응용할 수 있음을 보였다[8].

앞에 언급한 오류 선형복잡도에 관한 연구들은 모두 수열의 주기가 수열을 이루는 심볼의 유한체 특성(field characteristic)의 거듭제곱 형태로 나타나는 경우에만 적용할 수 있다. 위의 결과들과는 별개로 p가 소수이고 q가 모듈로 p^2에 대한 원시근이라는 조건하에 F_q상의 p^m-주기 수열에 대하여 선형복잡도와 k-오류 선형복잡도를 효과적으로 구할 수 있는 알고리듬이 연구되었다[10, 11].

최근 Salagean은 2^n-주기 이진 수열이 가지는 암호학적 취약점을 지적하는 대신 SM 알고리듬을 이용하여 repeated-root 이진 부호를 복호할 수 있음을 보였다[8]. 본 논문은 [8], [11], [12]의 연구 결과에 대한 연장선 상에 있다. 2가 모듈로 p^2에 대한 원시근일 때 p^m-주기 이진 수열의 k-오류 선형복잡도를 구하는 알고리듬을 변형하여 길이가 p^m인 이진 순환 부호를 부호 및 복호할 수 있는 알고리듬을 제안하고 이러한 부호의 최소 거리 특성을 유도한다.

본 논문의 구조는 다음과 같다. 우선 II장에서는 p^m-주기 이진 수열의 특수한 성질을 이용하여 k-오류 선형복잡도와 오류 벡터를 구하는 알고리듬을 소개한다. III장에서는 길이가 p^m인 이진 순환 부호의 특성을 살펴보고 이러한 부호의 복호 알고리듬을 제안한다. 끝으로 IV장에서 결론을 맺는다.

II. p^m-주기 이진 수열의 k-오류 선형복잡도를 구하는 알고리듬

p는 소수이고 n은 p와 서로소인 양의 정수라 하자. α는 F_q의 어떤 확장 유한체에 속하는 n차 원시원(primitive n-th root of unity)이라 할 때 F_q상의 n번째 원분다항식(cyclotomic polynomial) $\Phi_n(x)$는 다음과 같이 정의된다.

$$\Phi_n(x) = \prod_{\substack{i=1 \\ \gcd(n,i)=1}}^{n} (x-\alpha^i).$$

ϕ를 오일러 함수라 할 때 $\Phi_n(x)$의 차수는 $\phi(n)$이며 q가 모듈로 n에 대한 원시근일 조건과 $\Phi_n(x)$가 F_q상에서 기약다항식(irreducible polynomial)일 조건은 필요충분 관계이다.

보조정리 1.[7] p는 홀수인 소수라 하자. 만약 q가 모듈로 p^2에 대한 원시근이라면 q는 모든 정수

$m \geq 1$에 대하여 모듈로 p^m의 원시근이다. 따라서 $\Phi_{p^m}(x)$는 F_q상에서 기약다항식이다.

앞으로 P_q는 q가 모듈로 p^2의 원시근이며 2가 아닌 소수 p들의 집합으로 표기한다. 예를 들어 $P_2 = 3,5,11,13,19,29,\cdots$이다. $N=p^m$일 때 N-주기 수열 $S=(s_0,s_1,\cdots,s_{N-1})^\infty$의 한 주기에 해당하는 $s^N=(s_0,s_1,\cdots,s_{N-1})$을 p등분한 수열들을 $i=0,\ldots,p-1$일 때 $s_i=(s_{ip^{m-1}},\cdots,s_{(i+1)p^{m-1}-1})$라 하자. 마찬가지로 S_i는 $(s_i)^\infty$를 의미한다고 하자. 다음의 유명한 보조정리는 p^m-주기 수열의 선형복잡도에 관한 매우 흥미로운 특성을 보여준다.

보조정리 2.[10] (XWLI 알고리듬) $p \in P_q$이고 S는 F_q상의 p^m-주기 수열이라 하자.

1) $s_0=s_1=\cdots=s_{p-1}$이라면 $f_S(x)=f_{S_1}(x)$이고 $L(S)=L(S_1)$이다.
2) $s_0=s_1=\cdots=s_{p-1}$이 성립하지 않는다면, $f_S(x)=f_B(x)\Phi_{p^m}(x)$, $L(S)=L(B)+(p-1)p^{m-1}$이다. 여기에서 $B=(s_0+s_1+\cdots+s_{p-1})^\infty$이다.

XWLI 알고리듬을 m번 재귀 적용하고 마지막으로 남은 항이 0인지 아닌지 여부에 따라 0과 1을 더하면 최종적으로 S의 선형복잡도 $L(S)$를 구할 수 있다. 이때 각 단계 마다 한 주기를 p등분한 수열들이 $s_0=s_1=\cdots=s_{p-1}$을 만족하는 경우에만 $L(S)$가 증가하지 않는다는 사실에 주목하자. 따라서 주어진 k값 이내에서 최대한 인위적으로 적당한 오류를 넣어 $s_0=s_1=\cdots=s_{p-1}$인 상태를 만들어 줌으로써 오류가 포함된 수열의 최소 선형복잡도를 구할 수 있다. 여기서 주의할 점은 재귀 입력 수열에서 바꿔 준 비트수는 원래의 수열에서 바꿔 준 비트수와 다를 수 있다는 것이다. 따라서 재귀적인 방법으로 $L_k(S)$를 계산하는 알고리듬을 진행하려면 SM 알고리듬처럼 비용의 개념을 도입해야 한다.

보조정리 3.[11, 12] $p \in P_2$일 때 아래의 알고리듬은 주어진 k에 대해 p^m-주기 이진 수열S의 k-오류 선형복잡도를 계산한다.

INPUT: $s=s^N$, $l=p^m$, $K=k$, $c=0$
$cost[i]=1$ for $i=0,1,\ldots,l-1$
OUTPUT: $c \rightarrow L_k(S)$

if $l \neq 1$ then $l=l/p$;
for $0 \leq j \leq l-1$,
$T_{1j}=\sum_{i=0}^{p-1} s_{il+j}\,cost[il+j]$;
$T_{0j}=\sum_{i=0}^{p-1} cost[il+j]-T_{1j}$;
$T_j=\min\{T_{0j},T_{1j}\}$;
end_for
$T=\sum_{i=0}^{l-1} T_i$;

if $T \leq K$ then \\Update Rule A
$K=K-T$;
for $0 \leq j \leq l-1$,
if $T_j=T_{1j}$, then $A(s)[j]=0$;
else $A(s)[j]=1$;
$A(cost)[j]=\max\{T_{0j},T_{1j}\}-T_j$;
end_for
$s=A(s)$; $cost=A(cost)$;

else \\$T>K$ Update Rule B
$c=c+(p-1)l$;
for $0 \leq j \leq l-1$,
$B(s)[j]=\bigoplus_{i=0}^{p-1} s_{il+j}$; \\$\bigoplus$: modulo 2 sum
$B(cost)[j]=\min\{cost[il+j] \mid 0 \leq i \leq p-1\}$;
end_for
$s=B(s)$; $cost=B(cost)$;

else \\ $l=1$
if $s=1$ and $cost[0]>K$ then $c=c+1$;

위에서 $cost[j]$는 비용 벡터 $cost$의 j번째 원소를 나타내며 새롭게 갱신된 비트 s_j의 값을 뒤집기 위해 이전 단계에서의 결과를 방해하지 않고 원래의 수열s^N에서 바꾸어줘야 하는 비트수를 말한다. T_{1j}는 $s_j=s_{l+j}=\cdots=s_{(p-1)l+j}=0$으로 강제적으로 만들기 위해 드는 비용이며 T_{0j}는 1로 동일하게 만들어 주기 위한 비용을 의미한다. 그 둘 중 낮은 비용을 T_j라 하면 $0 \leq j \leq l-1$에 대해 모든 T_j의 합이 $s_0=s_1=\cdots=s_{p-1}$를 만족하기 위해 소비해야 하는 총 비용 T가 된다. $\tilde{s}$는 원래의 수열 s에 강제적으로 오류가 포함되어 있음을 나타내는 것이라 할 때 $T(s)$는 다음을 의미한다.

$$T(s)=\min cost(s \rightarrow \tilde{s}_0=\tilde{s}_1=\cdots=\tilde{s}_{p-1}).$$

$T>K$라면$\tilde{s}_0=\tilde{s}_1=\cdots=\tilde{s}_{p-1}$로 강제적으로 만들어 줄 수 없으므로 $T \leq K$인지 여부에 따라 갱신규칙 A, B에 의해 $A(s)$, $B(s)$가 각각 다음 단계를 위한 재귀 입력 수열 s가 되며 재귀 입력 비용 수열 $cost$는 $A(cost)$, $B(cost)$로 각각 갱신된다[12].

보조정리 4.[12] $A(s)\in F_2^{p^r}$, $0\le r\le m-1$에 대하여 $h\in F_2^{p^r}$의 A-pull up은 다음을 만족하는 $e\in F_2^{p^{r+1}}$라고 정의하자:

$$A(s+e)=A(s)+h,\quad T(s+e)=0.$$

이때 h의 A-pull up e는 다음과 같이 구한다:

```
for 0 ≤ j ≤ p^r − 1,
  if T_j = T_uj  then  \\u = 0 or 1
    for 0 ≤ i ≤ p−1
      if s_{ip^r+j} = u  then e_{ip^r+j} = h_j ⊕ 1;
      else e_{ip^r+j} = h_j;
    end_for
end_for
```

보조정리 5.[12] $B(s)\in F_2^{p^r}$, $0\le r\le m-1$에 대하여 $h\in F_2^{p^r}$의 B-pull up은 $cost(s\to s+e)$값이 최소이고 다음을 만족하는 $e\in F_2^{p^{r+1}}$라고 정의하자:

$$B(s+e)=B(s)+h.$$

이때 h의 B-pull up e는 다음과 같이 구한다:

```
for 0 ≤ j ≤ p^r − 1
  if h_j = 1  then
    d = arg min_{0 ≤ i ≤ p−1} { cost[ip^r + j] };
    for 0 ≤ i ≤ p−1
      if i = d then e_{ip^r+j} = 1; else e_{ip^r+j} = 0;
    end_for
  else e_{ip^r+j} = 0 for 0 ≤ i ≤ p−1;
end_for
```

Ⅲ. 길이가 p^m인 이진 순환 부호

이 장에서는 암호학적인 관점에서 정의된 k-오류 선형복잡도의 의미를 부호 이론의 관점에서 살펴봄으로써 길이가 p^m인 이진 순환 부호를 효과적으로 복호할 수 있는 알고리듬을 소개하며 이러한 부호의 중요한 성질들을 유도한다.

3.1 길이가 p^m인 이진 순환 부호의 특성

C는 $[N,K]$ 이진 순환 부호로서 길이가 N이고 차원(dimension) 즉 정보어의 길이가 K인 이진 순환 부호라 하자. 이진 순환 부호 C는 환(ring) $F_2[x]/(x^N-1)$의 아이디얼(ideal)이며 x^N-1을 나누는 생성다항식 $g(x)$에 의하여 생성된다.

$C=(g(x))$는 $p\in P_2$일 때 부호어의 길이가 p^m인 $[p^m,K]$ 이진 순환 부호라 하자. 이때 생성다항식 $g(x)$는 보조정리 1에 의해 다음과 같이 표현할 수 있다:

$$g(x)=(x+1)^{\epsilon}\prod_{i\in G}\Phi_{p^i}(x).$$

여기서 $\epsilon\in F_2$이고 $G\subseteq\{1,\ldots,m\}$이며 $g(x)$의 차수는 p^m-K이다. 이때 패리티 검사 다항식 $h(x)$는 $x^{p^m}-1/g(x)$이므로 다음과 같이 표현된다:

$$h(x)=(x+1)^{\bar{\epsilon}}\prod_{i\in H}\Phi_{p^i}(x).$$

여기서 $\bar{\epsilon}=\epsilon+1 \bmod 2$이고 $H=\{1,\ldots,m\}\setminus G$이다. $h(x)$의 차수는 K이며 다음과 같이 표현된다:

$$K=\bar{\epsilon}+\sum_{i\in H}(p-1)p^{i-1}. \tag{1}$$

이때 임의의 부호어 다항식 $c(x)\in C$는 다음을 만족한다:

$$c(x)h(x)\equiv 0 \bmod(x^{p^m}-1). \tag{2}$$

따라서 임의의 이진 벡터 $s\in F_2^{p^m}$가 C에 속할 조건은 패리티 검사 다항식 $h(x)$가 p^m-주기 이진 수열 $S=(s)^\infty$의 소멸 다항식일 조건과 동일하다. S의 소멸 다항식 차수는 K이므로 부호어 s와 일대일 대응되는 p^m-주기 이진 수열 S의 선형복잡도는 최대 K가 된다. $[p^m,K]$ 이진 순환 부호의 복호 알고리듬을 살펴보기 전에 먼저 부호의 성능을 결정하는 최소 거리에 관한 정리를 살펴보도록 하자.

정리 6. $p\in P_2$이고 C_1은 $[p^m,K]$ 이진 순환 부호라 하자. K가 정수 $1\le r\le m$에 대하여 $(p-1)p^{r-1}\le K\le p^r-1$를 만족한다면 C_1의 최소거리는 $2p^{m-r}$이다.

증명) $(p-1)p^{r-1}\le K\le p^r-1$인 경우 식 (1)에 의하여 패리티 검사 다항식 $h(x)$는 다음과 같다:

$$h(x)=\Phi_{p^r}(x)\prod_{i\in I}\Phi_{p^i}(x),\quad I\subset\{0,1,\ldots,r-1\}.$$

$h(x)$는 반드시 제일 큰 차수의 인수로서 기약다항식 $\Phi_{p^r}(x)$를 포함하며 I는 $\{0,1,\ldots,r-1\}$의 진부분집합으로 나타난다. 따라서 (2)에 의해 부호어 다항식

$s(x)$는 반드시 $\prod_{j=r+1}^{m}\Phi_{p^j}(x)$를 인수로 갖는다. 만약 $0\le l\le p^m-1$에 대하여

$$s(x)=x^l(x^{p^{r-1}}+1)\prod_{j=r+1}^{m}\Phi_{p^j}(x) \mod x^{p^m}-1$$

라고 결정한다면, 이 경우

$$\begin{aligned}&h(x)s(x)\\&=\Phi_{p^r}(x)\prod_{i\in I}\Phi_{p^i}(x)\cdot x^l(x^{p^{r-1}}+1)\prod_{j=r+1}^{m}\Phi_{p^j}(x)\\&=\left\{\Phi_{p^r}(x)(x^{p^{r-1}}+1)\prod_{j=r+1}^{m}\Phi_{p^j}(x)\right\}\cdot x^l\cdot\prod_{i\in I}\Phi_{p^i}(x)\\&=(x^{p^m}+1)\cdot x^l\cdot\prod_{i\in I}\Phi_{p^i}(x)\\&\equiv 0 \mod x^{p^m}-1\end{aligned}$$

이므로 $s(x)$는 부호어이다. 이때 계수가 0이 아닌 $s(x)$의 항의 개수를 다항식 무게 $W(s(x))$라고 하자. $W(\prod_{j=r+1}^{m}\Phi_{p^j}(x))=p^{m-r}$이고 $\prod_{j=r+1}^{m}\Phi_{p^j}(x)$의 각 항의 차수 차이는 p^r로 동일하므로 $x^{p^{r-1}}+1$이 곱해져도 각 항들은 서로 상쇄되지 않는다. 따라서 $W(s(x))=2p^{m-r}$을 만족한다.

이제 무게가 p^{m-r}인 다항식 $x^l\prod_{j=r+1}^{m}\Phi_{p^j}(x) \mod x^{p^m}-1$가 부호어라 가정하자. 그렇다면 $h(x)$는 식 (2)를 만족시키기 위해 반드시 다음 형태를 가진다.

$$h(x)=\prod_{i=0}^{r}\Phi_{p^i}(x)=x^{p^r}+1.$$

이것은 $(p-1)p^{r-1}\le K\le p^r-1$이라는 가정에 위배되므로 p^{m-r}의 무게를 가지는 부호어는 존재하지 않는다. 따라서 C_1의 최소거리는 $2p^{m-r}$이다. □

위의 증명에 의해 다음의 따름정리도 유도된다.

따름정리 7. $p\in P_2$이고 C_2는 $[p^m,K]$ 이진 순환 부호라 하자. K가 정수 $1\le r\le m$에 대하여 $K=p^r$을 만족한다면 C_2의 최소거리는 p^{m-r}이다.

3.2 부호 및 복호 알고리듬

대부분의 $[N,K]$ 순환 부호의 경우 생성다항식 $g(x)$를 이용하여 정보어를 부호화하는 과정은 일반적으로 $O(K(N-K))$의 복잡도를 가진다[8]. 그러나 앞에서 살펴본 p^m-주기 이진 수열의 선형복잡도에 관한 구조적인 성질을 이용하면 $[p^m,K]$ 이진 순환 부호 C는 $O(N)$의 알고리듬으로 부호 및 복호를 할 수 있다. 수신된 벡터 $r\in F_2^{p^m}$을 복호하는 것은 $r+e\in C$를 만족하는 $e\in F_2^{p^m}$중에서 최소 무게를 갖는 e를 찾는 문제와 같다. 이것을 p^m-주기 이진 수열의 문제로 대응시키면, 부호어 s를 한 주기로 갖는 p^m-주기 이진 수열 S의 선형복잡도는 최대 K를 만족하므로 p^m-주기 이진 수열 $R=(r)^\infty$의 k-오류 선형복잡도가 K보다 작거나 같게 되는 최소값 k 만큼의 해밍 무게를 갖는 p^m-주기 이진 수열 $E=(e)^\infty$를 찾는 문제와 같다.

$$L_k(R)=L(R+E)\le K.$$

정리 8. m, K는 양의 정수, $p\in P_2$이고 $S=(s)^\infty$와 $E=(e)^\infty$는 p^m-주기 이진 수열이라 하자. 다음의 알고리듬은 $L_k(S)=L(S+E)\le K$를 만족하는 최소값 k 만큼의 무게를 갖는 벡터 e를 계산한다.

INPUT: K, $s=(s_0,s_1,\ldots,s_{p^m-1})\in F_2^{p^m}$,
$\mathrm{cost}=(\mathrm{cost}[0],\mathrm{cost}[1],\ldots,\mathrm{cost}[p^m-1])\in R^{p^m}$
OUTPUT: $e=(e_0,e_1,\ldots,e_{p^m-1})\in F_2^{p^m}$

```
k=0, c=0;
for 0≤n≤m-1,
    l=p^{m-n-1};
    compute T;
    if K≤c+(p-1)l or T=0 then
        update[n]=1; k=k+T;
        for 0≤j≤l-1,
            if T_j=T_{uj} then \\u=0 or 1
                for 0≤i≤p-1,
                    if s_{il+j}=u then
                      pullup[n][il+j]=1;
                    else pullup[n][il+j]=0;
                end_for
                s_j=u⊕1; \\⊕: modulo 2 sum
            cost[j]=max{T_{0j}, T_{1j}}-T_j;
        end_for
    else
        update[n]=0;  c=c+(p-1)l;
        for 0≤j≤l-1,
            h=min[arg min_{0≤i≤p-1}{cost[il+j]}];
            for 0≤i≤p-1,
                if i=h then pullup[n][il+j]=1;
                else pullup[n][il+j]=0;
            end_for
            s_j=⊕_{i=0}^{p-1} s_{il+j} ;
            cost[j]=cost[hl+j];
        end_for
end_for
e=0;
if s_0=1 then
    if K<c+1 or cost[0]=0 then
        k=k+cost[0]; e=1;
    else c=c+1;
```

```
for 0 ≤ n ≤ m−1,
    e=repeatp-times(e)
    if update[m−n−1]=1 then
        e=e⊕pullup[n]; //⊕:pairwise bit XOR
    else
        e=e⊙pullup[n]; //⊙:pairwise bit AND
end_for
end
```

증명) k-오류 선형복잡도를 구하는 기존의 알고리듬은 수열 s에서 최대 k비트 만큼 교체하여 얻을 수 있는 최소의 선형복잡도를 계산하는 것이 목적이다. 그러나 본 알고리듬은 s에서 최소 k비트 만큼 교체하여 K보다 작거나 같은 선형복잡도를 얻는 것이 목적이다. 따라서 기존의 갱신 규칙 A와 B의 기본 개념은 그대로 가져가되 k-오류 선형복잡도가 K보다 작거나 같은 값을 가지도록 갱신 규칙 A를 최소로 거치도록 기존의 알고리듬을 조정한 것이 본 알고리듬이다. 알고리듬의 후반부는 보조정리 4, 5의 내용을 재귀적으로 이용한 것으로서 오류 벡터 e를 찾기 위해 n번째 과정에서 갱신규칙 A 혹은 B를 거쳤는지 알 필요가 있다. 따라서 각각 대응되는 update[n]값을 1 혹은 0으로 설정하여 구별한다. 이러한 방법으로 최종적으로 해밍 무게가 k인 p^m짝 오류 벡터 e를 얻을 수 있다. □

위의 알고리듬을 이용하여 실제로 정보 벡터 $m \in F_2^K$을 $[p^m, K]$ 이진 순환 부호로 구조적으로 부호화하는 방법을 살펴보자. 우선 입력 수열 $s \in F_2^{p^m}$의 첫 K개 비트는 m으로, 이에 대응되는 비용은 1로 설정한다. 그리고 s의 첫 K개 비트를 제외한 나머지 비트들은 임의의 비트로, 이에 대응되는 비용은 0으로 설정한다. 그 후 알고리듬을 적용하면 $L(S+E) \leq K$를 만족하며 최소의 무게를 갖는 벡터 e를 구할 수 있다. s의 첫 K개 비트만 대응 비용이 할당되어 있으므로 반드시 e의 처음 K개 비트는 0을 만족한다. 최종적으로 부호어 c는 $s+e$와 같으므로 구조적인 부호화가 가능하다.

수신된 벡터를 s로 놓고 알고리듬을 진행하면 마찬가지로 오류벡터 e를 구할 수 있으므로 $s+e$를 계산하여 복호화 할 수 있다. 우리는 s에 대응되는 비용벡터 $cost$를 정수가 아니라 실수 상에서 정의하였다. 만약 $cost=(1,1,\ldots,1)$로 설정하면 경판정 복호를 할 수 있음은 물론이고 $cost$를 LLR (log-likelihood ratio)을 비롯한 비트의 신뢰도 값으로 설정한다면 연판정 복호도 할 수 있다.

예제 1. $g(x)=\Phi_{27}(x)\Phi_1(x)$, $h(x)=\Phi_9(x)\Phi_3(x)$인 [27,8] 순환 부호로 m=10000000을 구조적으로 부호화하는 과정을 보인다. 입력 벡터 s에 대응되는 비용은 아래첨자로 표기하였다.

$n=0$: update[0]$=1$, $c=0$

$s=$ $1_1 0_1 0_1 0_1 0_1 0_1 0_1 0_1 0_0$ pullup$=$ 000000000

$0_0 0_0 0_0 0_0 0_0 0_0 0_0 0_0 0_0$ 100000000

$\underline{0_0 0_0 0_0 0_0 0_0 0_0 0_0 0_0 0_0}$ 100000000

$1_1 0_1 0_1 0_1 0_1 0_1 0_1 0_1 0_0$

$n=1$: update[1]$=0$, $c=6$

$s=$ $1_1 0_1 0_1$ pullup$=$ 110

$0_1 0_1 0_1$ 000

$\underline{0_1 0_1 0_0}$ 001

$1_1 0_1 0_0$

$n=2$: update[2]$=0$, $c=8$

$s=$ 1_1 pullup$=$ 0

0_1 0

$\underline{0_0}$ 1

1_0

$e=1 \rightarrow \underset{001}{\underset{\odot 001}{111}} \rightarrow \underset{000000001}{\underset{\odot 110000001}{001001001}}$

$\rightarrow \underset{000000001100000001100000001}{\underset{\oplus 000000000100000000100000000}{000000001000000001000000001}}$

$c=s+e=100000001100000001100000001$

예제 2. $r=000000001000000001100000001$을 수신한 경우 복호하는 과정은 다음과 같다.

$n=0$: update[0]$=1$, $c=0$

$s=0_1 0_1 0_1 0_1 0_1 0_1 0_1 0_1 1_1$ pullup$=$ 000000000

$0_1 0_1 0_1 0_1 0_1 0_1 0_1 0_1 1_1$ 000000000

$\underline{1_1 0_1 0_1 0_1 0_1 0_1 0_1 0_1 1_1}$ 100000000

$0_1 0_3 0_3 0_3 0_3 0_3 0_3 0_3 1_3$

$n=1$: update[1]$=0$, $c=6$

$s=0_1 0_3 0_3$ pullup$=$ 111

$0_3 0_3 0_3$ 000

$\underline{0_3 0_3 1_3}$ 000

$0_1 0_3 1_3$

$n=2$: update[2]$=0$, $c=8$

$s=0_1$ pullup$=$ 1

0_3 0

$\underline{1_3}$ 0

1_1

$e=1 \rightarrow \underset{100}{\underset{\odot 100}{111}} \rightarrow \underset{100000000}{\underset{\odot 111000000}{100100100}}$

$\rightarrow \underset{100000000100000000000000000}{\underset{\oplus 000000000000000000100000000}{100000000100000000100000000}}$, $k=2$

$c=s+e=100000001100000001100000001$

Ⅳ. 결 론

본 논문은 p가 소수이고 2가 모듈로 p^2에 대한 원시근일 때 p^m-주기 이진 수열의 k-오류 선형복잡

도를 구하는 알고리듬을 변형하여 $[p^m, K]$ 순환 부호를 부호 및 복호할 수 있는 알고리듬을 제안하였고 이러한 부호의 최소 거리 특성을 유도하였다. 일반적으로 $[N,K]$ 순환 부호의 부호 및 복호는 $O(K(N-K))$의 복잡도를 가진다. 보조정리 3의 알고리듬은 기본적으로 [11], [6]에 소개된 $O(N)$의 복잡도를 가지는 k-오류 선형복잡도를 구하는 알고리듬으로부터 유도되고 e를 계산하는 과정 역시 N에 대해 선형적이므로 경판정 복호를 사용하는 경우 $O(N)$의 복잡도를 가진다. 또한 비용의 개념을 사용하므로 연판정 복호 역시 가능한 장점이 있다. 그러나 무엇보다 본 결과가 의미있는 이유는 암호학적인 관점에서의 k-오류 선형복잡도가 갖는 의미가 부호 이론의 관점에서 새롭게 해석될 수 있다는데 있다.

참 고 문 헌

[1] A. H. Chan and R. A. Games, "A fast algorithm for determining the complexity of a binary sequence with period 2^n," *IEEE Trans. Inform. Theory*, vol. 29, pp. 144-146, Jan. 1983.

[2] C. Ding, G. Xiao and W. Shan, *The stability theory of stream ciphers*, LNCS, vol. 561, Springer-Verlag, 1991.

[3] T. Kaida, S. Uehara and K. Imamura, An algorithm for the k-error linear complexity of sequences over $GF(p^m)$ with period p^n, p a prime," *Inform. Comput.*, vol. 151, pp. 134-147, May, 1999.

[4] A. G. B. Lauder and K. G. Paterson, "Computing the error linear complexity spectrum of a binary sequence of period 2^n," *IEEE Trans. Inform. Theory*, vol. 49, pp. 273-280, Jan. 2003.

[5] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. IT-15, pp. 122-127, Jan. 1969.

[6] W. Meidl, "How many bits have to be changed to decrease the linear complexity?," *Des. Codes Cryptogr.*, vol. 33, pp. 109-122, Sept. 2004.

[7] K. H. Rosen, *Elementary number theory and its applications*, Addison-Wesley, 2000.

[8] A. Salagean, "On the computation of the linear complexity and the k-error linear complexity of binary sequences with period a power of two," *IEEE Trans. Inform. Theory*, vol. 51, pp. 1145-1150, Mar. 2005.

[9] 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, pp. 1398-1401, July. 1993.

[10] G. Xiao, S. Wei, K. Y. Lam, and K. Imamura, "A fast algorithms for determining the linear complexity of a sequence with period p^n over $GF(q)$," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2203-2206, Sept. 2000.

[11] G. Xiao and S. Wei, "Fast algorithms for determining the linear complexity of period sequences," *Proc. on Indocrypt. '02*, LNCS vol. 2551, Springer-Verlag, pp. 12-21, 2002.

[12] 한윤경, 양경철, "p^n의 주기를 갖는 이진 수열의 오류 선형복잡도 프로파일을 구하는 알고리듬," *제15회 통신정보합동학술대회 (JCCI '05)* 논문집, 제 15권, pp. FM13-6. 1~5, 대구, 2005년 4월.

한 윤 경 (Yun Kyoung Han) 정회원

2004년 2월 홍익대학교 전자전기공학부 졸업

2006년 2월 포항공과대학교 전자전기공학과 석사

2006년 3월~현재 포항공과대학교 전자전기공학과 박사과정

<관심분야> 부호이론, 신호설계, 정보보호, 다중 안테나 시스템

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