通信情報保護學會誌
第5卷 第1號, 1995. 3

시각제어 쉬프트 레지스터에 관하여

성 수 학*

요 약

이진수열 발생기인 시각제어 쉬프트 레지스터의 몇가지 예와 일반화된 상관 공격법을 살펴본다.

1. 서 론

LFSR(Linear Feedback Shift Register)은 간단한 대수적 구조, 좋은 통계적 특성과 구현의 용이함으로 스트림 암호를 설계할 때 많이 이용될 수 있다. 앞으로 언급하는 LFSR는 최대주기를 갖는 LFSR(보통 m-LFSR이라고 함)이라고 가정한다. LFSR은 대수적 성질(선형성)때문에 하나의 LFSR을 스트림 암호에 바로 사용할 수 없다. 여러개의 LFSR을 비선형 함수로 결합하면 주기와 선형복잡도를 크게 할 수 있으나, 비선형 함수의 입력과 출력 사이에 상관관계가 있으면 대응되는 LFSR의 초기 입력벡터를 구할 수 있어서 쉽게 암호 공격이 가능하다[13]. 여기서 암호공격을 한다는 것은 키로 사용되는 LFSR의 초기 입력벡터와 궤환함수(궤환함수를 사용자가 임의로 사용할 경우)를 찾는 것이다. 이와같은 약점을 피하고 LFSR의 좋은 통계적 성질을 유지하는 이진수열 발생기로는 시각제어 쉬프트 레지스트(CCSR, Clock Controlled Shift Register)가 있으며, 최근 10여년간 많이 연구되고 있다. CCSR은 다음 그림과 같이 LFSR에서 발생된 이진수열(x_n)이 decimation 수열(d_n)에 의해서 제어받아 출력수열 $y_n = x(\Sigma_{i=0}^{n} d_i)$을 발생한다. 달리 말하면, LFSR이 한 스텝씩 쉬프트 하지 않고 불규칙적으로 또는 여러 스텝씩 쉬프트 한다.

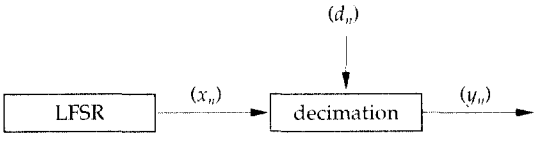

그림 1 CCSR의 구조

Decimation 수열이 취하는 값에 따라서 여러 형태의 CCSR을 생각할 수 있다. 이를 위해서 이 수열이 취하는 값의 집합을 D라고 두자. 즉 $D = \{d_n | n \geq 0\}$이다. 집합 D의 원소는 하나, 여러개 그리고 무한히 많을 수 있다. 종래의 CCSR은 D의 원소가 하나인 경우이다. $D = \{r\}$, 즉 $d_n = r(n \geq 0)$이면 LFSR를 r스텝씩 쉬프트하여 얻은 수열이 되며, 특히 $r = 1$일때 CCSR은 바로 LFSR이다. D가 하나의 원소를 가지면 CCSR은 LFSR의 선형구조를 그대로 지니므로 쉽게 암호공격이 가능하다. $D = \{0, 1\}$인 경우를 stop-and-go 발생기라고 하며, $d_n = 0$일때 출력비트

* 배재대학교 응용수학과

y_n은 전시각의 출력비트 y_{n-1}과 같은 값을 가지므로 출력비트 사이에 상관관계가 존재하여 쉽게 암호해독이 가능하다. CCSR 중에는 decimation 수열과 LFSR 출력 수열이 독립인 것과 종속인 것이 있다. 종속인 것으로는 Rueppel[12]이 제안한 [d, k]self-decimation 발생기와 최근에 Meier와 Staffelback[10]가 제안한 self-shrinking 발생기가 있다. 독립적인 것으로는 Coppersmith, Krawczyk와 Mansour[3]가 제안한 shrinking 발생기가 있다.

위의 것보다 구조가 복잡한(여러개의 LFSR로 구성된)대표적인 CCSR로는 cascade 발생기가 있다. 이 발생기는 여러개의 LFSR로 구성되며 첫째 LFSR를 제외한 나머지 LFSR은 다음 LFSR를 제어하며 인접하는 2개의 LFSR은 stop-and-go 구조를 가져 통계적 약점을 지니고 있다. Chambers와 Gollmann[2]은 lock-in-effect방법으로, Manicocci([8], [9])는 상관공격(correlation attack)방식과 유사한 방법을 사용하여 분석하였다. 특히 최근에 박상준, 이상진, 고승철 박사팀은 컴퓨터 시뮬레이션을 통하여 cascade를 쉽게 공격할 수 있음을 보였다[1]. 그러나 cascade와 다음장에서 소개할 [d, k]self-decimation 발생기를 제외한 제안된 대부분의 CCSR의 비도(복잡도)는 LFRS의 크기에 따라 지수값으로 증가하기 때문에 LFSR의 크기가 크면 안전한 것으로 알려져 있다.

본고에서는 CCSR의 몇가지 예와 일반화된 상관 공격법을 살펴 보고자 한다.

2. CCSR의 예

2.1 [d, k]self-decimation 발생기

LFSR의 출력값이 0일때 LFSR을 d 스텝 쉬프트, 1일때 k 스텝 쉬프트 하여 이진수열을 발생하는 CCSR를 [d, k]self-decimation 발생기라고 한다[12]. 따라서 이 발생기는 $D = \{0, d, k\}$이고,

$$d_n = \begin{cases} 0, & n = 0 \\ d, & x(\Sigma_{i=0}^{n-1} d_i) = 0 \ (n \geq 1) \\ k, & x(\Sigma_{i=0}^{n-1} d_i) = 1 \ (n \geq 1) \end{cases}$$

인 CCSR이다. 또 출력수열(y_n)으로부터 decimation 수열(d_n)을 다음과 같이 찾을 수 있다.

$$d_n = \begin{cases} 0, & n = 0 \\ d, & y_{n-1} = 0 \ (n \geq 1) \\ k, & y_{n-1} = 1 \ (n \geq 1) \end{cases}$$

즉 출력수열 y_n은 LFSR을 $\Sigma_{i=0}^{n} d_i$번 쉬프트하여 얻은 것이므로 LFSR에 대한 선형방정식을 이용하여 쉽게 LFSR의 초기 입력벡터(키)를 찾을 수 있다. [d, k] self-decimation 발생기를 쉽게 공격할 수 있는 것은 출력수열로 부터 LFSR을 얼마만큼 쉬프트 한 것인지 알 수 있기 때문이다.

예 LFSR의 출력수열이 11111001001100001...이면, [1, 2]self-decimation의 출력은 111010100001...이다. 따라서 $d_0 = 0$, $d_1 = 2$, $d_2 = 2$, $d_3 = 2$, $d_4 = 1$, $d_5 = 2$, $d_6 = 1$, $d_7 = 2$, $d_8 = 1$, $d_9 = 1$, $d_{10} = 1$, $d_{11} = 1$, ...이고, $y_0 = x_0$, $y_1 = x_2$, $y_2 = x_4$, $y_3 = x_6$, $y_4 = x_7$, $y_5 = x_9$, $y_6 = x_{10}$, $y_7 = x_{12}$, $y_8 = x_{13}$, $y_9 = x_{14}$, $y_{10} = x_{15}$, $y_{11} = x_{16}$ ...이다.

다음 절에서 소개할 shrinking 발생기는 [d, k] self-decimation과 같이 LFSR의 출력수열의 일부분으로 구성되나 LFSR을 얼마만큼 쉬프트 했는지 알 수 없어서 쉽게 키를 찾을 수 없다.

2.2 Shrinking 발생기

Shrinking 발생기는 2개의 LFSR로 구성되며 Coppersmith, Krawczyk와 Mansour[3]에 의해서 제안되었다. 좀 더 구체적으로 말하면, x_0, x_1, ...을 LFSR-1의 출력수열, s_0, s_1, ...를 LFSR-2의 출력수열이라고 하자. 그러면 shrinking 발생기의 출력수열 y_n은 다음과 같이 정의 된다.

$$y_n = x(t_n)$$

여기서

$$t_0 = \inf\{i | s_i = 1\}$$
$$t_n = \inf\{i | i > t_{n-1}, s_i = 1\} \ (n \geq 1)$$

이다. $d_0 = t_0$, $d_n = t_n - t_{n-1}$ $(n \geq 1)$로 두면 $y_n = x(\Sigma_{i=0}^{n} d_i)$가 된다. 따라서 shrinking 발생기는 $D = \{1, 2, \ldots\}$이고 (d_n)은 LFSR-2의 출력수열로부터 구성된 것이므로 LFSR-1의 출력수열과 독립이다(LFSR-1과 LFSR-2는 서로 다름). 그리고 $[d, k]$self-decimation 발생기와는 달리 출력수열 (y_n)으로부터 decimation 수열 (d_n)을 찾을 수 없다. LFST-1과 LFST-2가 최대주기를 갖고, 두 주기값이 서로 소이면 shrinking 발생기의 주기는 $(2^{N_1} - 1) \cdot (2^{N_2 - 1})$이다[3] ($N_1$ 과 N_2는 각각 LFST-1과 LFST-2의 크기이다). 또 선형 복잡도는 $N_1 2^{N_2 - 2}$와 $N_1 2^{N_2 - 1}$ 사이의 값이다[13]. Coppersmith, Krawczyk와 Mansour는 shrinking 발생기의 출력은 랜덤 이진수열과 거의 비슷하여 여러 암호 공격법으로부터 안전하다고 주장하였으나, 다음 장에서 언급할 일반화된 상관 공격법을 사용하면 LFSR-1의 크기가 작을 때 쉽게 공격 가능하다. Shrinking 발생기의 구체적인 예를 들어 보자.

예 LFSR-1의 특성함수(characteristic function) $f(x) = 1 + x + x^2 + x^3 + x^5$, 초기 입력벡터 $(x_0, x_1, x_2, x_3, x_4) = (1, 1, 1, 1, 1)$, LFSR-2의 특성함수 $g(x) = 1 + x + x^4$, 초기 입력벡터 $(s_0, s_1, s_2, s_3) = (1, 0, 0, 0)$이라고 가정하자. 그러면

LFSR-1의 출력은

111110010011000 ....

LFSR-2의 출력은

1000100110101111 ...., 그리고

shrinking 발생기의 출력은

11101000 ... 이다.

2.3 Self-shrinking 발생기

Self-shrinking 발생기는 Meier와 Staffelbach[10]가 제안한 것으로 하나의 LFSR로 구성되어 있다. LFSR의 출력수열을 $x_0, x_1, \ldots$이라고 할 때 각 쌍 (x_{2i}, x_{2i+1})이 (1, 0)일때는 0, (1, 1)일때는 1을 출력하고 (0, 0)이나 (0, 1)일때는 아무것도 출력하지 않는 이진수열 발생기이다.

예 LSFR의 출력이 11111001001100...이면, 연속적인 각 쌍에 대해서 (1, 1) → 1, (1, 1) → 1, (1, 0) → 0, (0, 1), (0, 0), (1, 1) → 1, (0, 0), ...이므로 self-shrinking 발생기의 출력은 1101 ... 이다.

Self-shrinking 발생기는 shrinking 발생기와 밀접한 관계가 있다. 즉 self-shrinking은 shrinking으로부터 만들 수 있고, 역으로 shrinking은 self-shrinking으로부터 만들 수 있다. 그러나 후자의 경우에는 최대 주기를 갖는 LFSR로는 만들 수 없다. Self-shrinking 발생기가 shrinking 발생기의 특수한 형태인 것을 보기 위하여 $a_0, a_1, \ldots$를 self-shrinking의 LFSR의 출력수열이라고 하자. 그러면 self-shrinking의 설계 원칙에 따라 $(a_0, a_2, \ldots)$는 출력을 제어한다. 즉 a_{2i}가 1일때 a_{2i+1}이 출력된다. $(a_0, a_2, \ldots)$는 초기 입력벡터가 $(a_0, a_2, \ldots, a_{2N-2})$인 LFSR로부터, $(a_1, a_3, \ldots)$는 초기 입력벡터가 $(a_1, a_3, \ldots, a_{2N-1})$인 LFSR로부터 생성된다($N$은 LFSR의 크기). 따라서 초기 입력벡터가 $(a_0, a_2, \ldots, a_{2N-2})$와 $(a_1, a_3, \ldots, a_{2N-1})$인 LFSR을 LFSR-1과 LFSR-2로 두면 shrinking 발생기의 출력수열이 바로 주어진 self-shrinking 발생기의 출력수열이 된다. 역으로 shrinking 발생기는 self-shrinking 발생기로부터 만들 수 있다[10].

3. 일반화된 상관 공격법

상관공격(correlation attack)의 핵심은 길이

가 같은 두 수열사이의 Hamming distance를 측정하는 것이나[13], 이 공격 방식은 CCSR에 직접 적용할 수 없다. 왜냐하면, LFSR의 출력수열의 일부분만이 CCSR의 출력수열이기 때문이다. 일반화된 상관 공격법(generalized correlation attack)은 길이가 다른 두 수열의 관계를 측정하여 보다 많은 관계가 있는 수열을 찾아내는 방법이다. 좀 더 구체적으로 말하면, LFSR의 초기 입력벡터(CCSR의 키)로부터 생성된 수열이 다른 입력벡터로 부터 생성된 수열보다 (y_n)과 보다 많은 상관관계를 가지고 있을 것이다. 이러한 상관관계를 측정하는 기준을 만들어 주어진 CCSR의 출력수열 (y_n)을 만들어낸 LFSR의 초기 입력벡터(CCSR의 키)를 찾는 방법이다.

3.1 거리측도 공격법

길이가 다른 두 수열의 거리를 측정하는 기준으로 Levenstein distance가 있다. Golic과 Mihaljevic[5]은 $D = \{1, 2, \ldots, d\}$일때 Levenstein distance 개념을 일반화하여 크기가 다른 두 수열을 측정하여 CCSR의 키를 찾는 알고리듬을 제안하였다. 같은 CCSR하에서, Levenstein distance를 조금 변경한 측도로 키를 찾는 알고리듬도 제안되었다[11]. 또 Levenstein distance에 decimation의 확률분포를 고려한 측도를 사용하여 키를 찾는 알고리듬도 제안되었다[6]. 두 수열사이의 거리측도(distance measure)는 한 수열이 다른 수열의 부분일 필요는 없다. 다음 절에서 소개할 embedding 공격법은 한 수열이 다른 수열의 부분일 때 가능하다.

3.2 Embedding 공격법

CCSR의 출력수열은 LFSR의 초기 입력벡터(키)로부터 출력된 수열의 일부분이므로, 주어진 CCSR의 출력수열 (y_n)은 다른 입력벡터로부터 발생한 출력수열의 일부분일 가능성은 작을 것이다. 이와 관련된 개념을 구체적으로 보기 위하여 다음 정의를 살펴 보자.

■ 정 의 길이 n인 이진수열 $(y_i)_{i=0}^{n}$ 와 길이 m인 이진수열 $(x_i)_{i=0}^{m}$ 가 다음 조건을 만족할 때 $(y_i)_{i=0}^{n}$는 $(x_i)_{i=0}^{m}$에 D-embedding 한다고 정의한다.

$$y_i = x(\sum_{j=1}^{i} d_j),\ 1 \le i \le n,\ \text{단 } d_i \in D$$

■ 정 의 길이 n인 이진수열 $Y = (y_i)_{i=1}^{n}$ 가 길이 m인 일양분포를 갖는 랜덤 이진수열 $(X_i)_{i=1}^{m}$에 D-embedding될 확률을 $P_{D,Y}(n, m)$이라고 표시한다.

$P_{D,Y}(n, m)$의 값은 CCSR를 공격할때 CCSR의 출력수열의 크기, LFSR의 출력수열의 크기, 그리고 다른 입력벡터로부터 발생된 LFSR의 출력수열을 초기 입력벡터로부터 발생된 LFSR의 출력수열로 받아들일 가능성(false alarm probability)을 결정해 준다. n이 클때 $P_{D,Y}(n, m)$이 0에 수렴하면 LFSR의 초기입력 벡터를 찾을 수 있다(물론 CCSR의 출력수열과 LFSR의 출력수열의 크기가 클때). 이와 같은 공격법을 D-embedding 공격법이라고 한다. $D = \{1, 2, \ldots\}$일때 unconstrained embedding 공격법이라고 하며, 그렇지 않을 때를 constrained D-embedding 공격법이라고 한다. $P_{D,Y}(n, m)$이 0에 수렴하지 않으면 D-embedding되는 수열이 너무 많아서 키를 찾을 수 없다. 즉 $(y_i)_{i=1}^{n}$는 많은 입력벡터로부터 생성된 LFSR의 출력수열과 embedding 가능하여 어느 입력벡터가 LFSR의 진짜 초기 입력벡터인지 알 수 없다. 또 decimation 수열 (d_n)은 embedding 공격과 많은 관련이 있다. 왜냐하면, CCSR의 출력수열이 LFSR의 출력수열의 아주 작은부분이면 두 수열 사이에 상관성이 줄어든다. 이를 측정할 수 있는 다음 정의를 생각해 보자.

■ 정 의 Decimation 수열의 확률분포 $\{p(d)|d$

$\in D$}에 대한 CCSR의 제거율(deletion rate)p_d를 다음과 같이 정의한다.

$$p_d = 1 - (1/\bar{d})$$

여기서 $\bar{d} = E(D_1)$이다. 즉 $\bar{d} = \Sigma_{d \in D} dP(d)$이다.

예 $D = \{1, 2\}$, decimation 수열의 확률분포가 $P(D_1 = 1) = P(D_1 = 2) = 1/2$ 일때 $E(D_1) = 3/2$이므로 제거율은 1/3이다.

제거율을 좀 더 구체적으로 살펴 보기 위하여, 제거 기호를 θ를 두고, 위의 예를 확률모델로 바꾸어 입력수열 X_n이 제거될 확률을 계산하여 보자.

$$\begin{aligned}
P(X_1 = \theta) &= P(D_1 = 2) = 1/2 \\
P(X_2 = \theta) &= P(X_2 = \theta | X_1 = \theta)P(X_1 = \theta) \\
&\quad + P(X_2 = \theta | X_1 \neq \theta)P(X_1 \neq \theta) \\
&= P(D_2 = 2)P(X_1 \neq \theta) \\
&= \frac{1}{2} - \frac{1}{2^2} \\
&\vdots \\
P(X_n = \theta) &= \frac{1}{2} - \frac{1}{2^2} + \frac{1}{2^3} + \\
&\quad \ldots + (-1)^{n+1} \frac{1}{2^n}
\end{aligned}$$

따라서 $\lim_{n \to \infty} P(X_n = \theta) = \Sigma_{n=1}^{\infty} (-1)^{n+1} 1/2^n = 1/3$이다. 즉 제거율은 n이 클 경우에 X_n이 제거될 확률과 거의 같음을 알 수 있다.

$D = \{1, 2, \ldots\}$일때 $P_{D,Y}(n, m)$의 정확한 값을 구할 수 있으며, 제거율이 1/2 보다 작을 때 공격 가능하다[4]. $D = \{1, 2\}$인 경우에는 $P_{D,Y}(n, m)$의 정확한 값을 계산하기 어렵지만, Zivkovic[14]은 $P_{\{1,2\}}, Y^{(n, 2n)}$의 좋은 상한값을 구하였고 이 값은 n에 대하여 지수승으로 감소함을 보였다. Golic과 O' Connor[4]는 $D = \{1, 2, \ldots, d\}$인 경우에 $P_{D,Y}(n, dn + d - 1)$의 값이 n에 대하여 지수승으로 감소함을 보였다. 그러나 이러한 공격법은 $2^N - 1$개의 (N은 LFSR의 크기) LFSR의 입력벡터에 대한 출력수열과 주어진 이진수열 $(y_i)_{i=1}^{n}$를 비교해야 하기 때문에 LFSR의 크기가 크면 사실상 공격은 불가능하다.

3.3 확률 공격법

Embedding 공격법은 embedding 확률을 계산할때 decimation 수열의 확률분포를 고려하지 않았다. Decimation 수열의 확률분포를 고려하여 D-embedding 확률을 계산하는 것이 바람직하다. 이 확률을 이용하여 CCSR의 키를 찾는 방법을 확률공격법(probabilistic attack)이라고 한다. $D = \{1, 2, \ldots\}$일때를 unconstrained 확률 공격법이라고 한다. 우선 CCSR의 확률 모델을 생각해 보자.

$X = \{X_n\}_{n=1}^{\infty}$는 독립이고 일양분포를 갖는 이진 확률변수열이라고 하고, $D = \{D_n\}_{n=1}^{\infty}$는 독립이고 음이 아닌 정수값을 갖는 확률변수열로 X와 독립이라고 가정하자. $p(d)$를 D_n의 확률분포라고 하자. 즉 $p(d) = P(D_n = d)$, $d \in D$. 그리고 $Y_n = X(\Sigma_{i=1}^{n} D_i)$라고 두자. 이때 $\{Y_i\}_{i=1}^{n}$가 $\{X_i\}_{i=1}^{m}$에 embedding될 확률을 CCSR의 제거율을 이용하여 구한다. LFSR의 초기 입력벡터가 아닌 다른 입력벡터로 부터 발생한 LFSR의 출력수열은 주어진 CCSR의 출력수열과 독립인 수열로 볼 수 있으므로 위의 확률모델에 적용가능하다. 물론 확률공격이 성공하기 위해서 embedding 확률은 n이 증가함에 따라 0에 수렴해야 한다. Golic과 O' Connor[4]는 $D = \{1, 2, \ldots\}$일때 embedding 확률을 구하는 알고리즘을 제안하였으며, 제거율이 1보다 작으면 이론적으로 공격이 가능함을 보였다. Embedding 공격법으로는 제거율이 1/2보다 작을때 공격이 가능하므로 확률 공격법이 보다 좋은 공격법이다. 앞장에서 언급한 shrinking 발생기의 제거율은 1/2이므로 확률공격법을 이용하면 shrinking 발생기의 키를 찾을 수 있다.

4. 결 론

CCSR는 간단한 구조와 좋은 통계적 특성으로 스트림 암호에 많이 이용될 수 있다. Casacde와 [d, k]self-shrinking 발생기를 제외한 제안된 대부분의 CCSR는 주기와 선형복잡도가 큰 좋은 이진수열 발생기이다. 그러나, $D = \{1, 2, \ldots, d\}$일때 embedding 공격법으로 공격가능하다. 또 $D = \{1, 2, \ldots\}$일때 제거율이 1/2보다 작으면 embedding 공격법으로, 제거율이 1보다 작으면 확률공격법으로 공격 가능하다. 즉 LFSR의 초기 입력벡터로 부터 발생된 수열과 다른 입력벡터로 부터 발생된 수열을 구별할 수 있다. 이러한 공격법들은 LFSR의 모든 입력벡터에 대해 이진수열을 출력하여 주어진 CCSR의 출력수열과 비교해야하므로 LFSR의 크기가 크면 사실상 공격은 불가능하다.

참 고 문 헌

[1] 박상준, 이상진, 고승철, Cascade 생성기 : 2단계 m-LFSR cascade 분석, 통신정보보호학회논문집 4(1), 51-58, 1994.

[2] W.G. Chambers and D. Gollmann, Lock in effect in cascades of clock controlled shift registers. Eurocrypt' 88, 1988.

[3] D. Coppersmith, H. Krawczyk, and Y. Mansour, The shrinking generator. Crypto' 93, 1993.

[4] J. Dj. Golic and L. O'Conor, Embedding and probabilistic correlation attacks on clock controlled shift registers. Eurocrypt' 94, 1994.

[5] J. Dj. Golic and S. V. Mihaljevic, A generalized correlation attack on a class of stream ciphers based on Levenstein distance. Journal of Cryptology, 3(3), 201-212, 1991.

[6] J. Dj. Golic and S. V. Petrovic, A generalized correlation attack with a probabilistic constrained edit distance. Eurocrypt' 92, 1992.

[7] D. Gollmann and W. G. Chambers, Clock controlled shift registers : a review. IEEE Journal on Selected Area in Communications, 7(4), 525-533, 1989.

[8] R. Manicocci, Short Gollmann cascade generators are insecure. Abstract of the Fourth IMA Conference on Coding and Cryptography, Cirencester, 1993.

[9] R. Manicocci, Cryptanalysis of a two stage Gollmann cascade generator. Proceedings of SPRC' 93, Rome, 62-69, 1993

[10] W. Meier and O. Staffelbach, The self-shrinking generator. Eurocrypt' 94.

[11] M. J. Mihaljevic, An approach to the initial state reconstruction for a clock controlled shift register based on a novel distance measure,. Auscrypt' 92, 1992.

[12] R. A. Reuppel, When shift registers clock themselves. Eurocrypt' 87, 1987.

[13] T. Siegenthaler, Decrypting a class of steam ciphers using ciphertext only. IEEE Transaction on Computers, 34(1), 81-85, 1985.

[14] M. V. Zivkovic, An algorithm for the initial state reconstruction of the clock controlled shift register. IEEE Transactions on Information Theory, 37, 1488-1490, 1991.

□ 著者紹介

성 수 학(成 洙 學) 정회원

1982년	경북대학교 수학과 학사
1985년	KAIST 응용수학과 석사
1988년	KAIST 응용수학과 박사
1988년 ~ 1991년	한국전자통신연구소 선임연구원
1991년 ~ 현재	배재대학교 응용수학과 조교수