1차원 CA 기반의 인증과 기밀성을 제공하는 보안 기술의 분석

One Dimensional Cellular Automata based security scheme providing both authentication and confidentiality

저자
(Authors)

황윤희, 조성진, 최언숙
Yoon-Hee Hwang, Sung-Jin Cho, Un-Sook Choi

출처
(Source)

한국정보통신학회논문지 14(7), 2010.7, 1597-1602 (6 pages)
Journal of the Korea Institute of Information and Communication Engineering 14(7), 2010.7, 1597-1602 (6 pages)

발행처
(Publisher)

한국정보통신학회
The Korea Institute of Information and Communication Engineering

URL

http://www.dbpia.co.kr/Article/NODE02254982

APA Style

황윤희, 조성진, 최언숙 (2010). 1차원 CA 기반의 인증과 기밀성을 제공하는 보안 기술의 분석. 한국정보통신학회논문지, 14(7), 1597-1602.

1차원 CA 기반의 인증과 기밀성을 제공하는 보안 기술의 분석

황윤희* · 조성진** · 최언숙***

One Dimensional Cellular Automata based security scheme providing both authentication and confidentiality

Yoon-Hee Hwang* · Sung-Jin Cho** · Un-Sook Choi***

요 약

Sarkar 등은 메시지의 기밀성과 메시지 인증을 보장하는 새로운 암호 시스템을 개발하였다. 이 암호시스템은 일차원 셀룰라 오토마타를 기반으로 하여 하드웨어 구현이 용이하고 고속계산이 가능하며 작은 단위로 확장 연결이 가능한 장점을 지녔다. 하지만 Sarkar 등이 제안한 방법은 보안상 취약점을 가지고 있다. 본 논문에서는 선형 셀룰라 오토마타의 특성을 분석하여 Sarkar 등이 제안한 방법에 대하여 비밀 키를 생성해 낼 수 있는 공격법을 제시한다.

ABSTRACT

Sarkar et al. proposed a new Cellular Automata(CA) based security scheme providing both authentication and confidentiality. The application of CA for designing the scheme makes it suitable for hardware implementation. But the proposed method by Sakar dt al. has some problems. In this paper, we analyze CA and give a method for detecting secret key.

키워드

인증, 기밀성, 셀룰라 오토마타, 전이행렬

Key word

Authentication, Confidentiality, Cellular Automata, transition matrix

* 부경대학교

** 부경대학교 (교신저자, sjcho@pknu.ac.kr)

*** 동명대학교

접수일자 : 2010. 02. 17

심사완료일자 : 2010. 03. 22

Ⅰ. 서 론

메시지의 기밀성과 더불어 메시지 인증은 중요한 네트워크 보안 기능 중 하나이다. 암호화(Encryption)는 수동적 공격(도청, 트래픽 분석 등)에 대하여 보호하지만 메시지 인증은 능동적 공격(변조 사입, 삭제, 재생 등)에 대하여 보호한다. 개략적으로 기본적인 보안 문제는 기밀성, 인증, 부인봉쇄, 무결성이 요구된다. 기밀성은 비밀 키 및 공개 키 암호 시스템에 의해서 보장될 수 있으며, 인증은 실제인증 또는 개인식별 등에 의해서 보장될 수 있다. 이에 셀룰라 오토마타(Cellular Automata, CA) 기반의 알고리즘이 응용되어 소개되어졌다[1-4]. 특히 [4]에서는 1차원 90/150 CA를 이용하여 메시지를 주고받기 전의 인증과 인증을 마친 후 보내고자 하는 메시지의 기밀성을 제공하는 보안 기술을 제안하였다. 본 논문에서는 [4]에서 제안한 방법이 인증과 기밀성을 제공하지 못함을 밝힌다.

Ⅱ. 기초 지식

2.1 셀룰라 오토마타와 규칙의 정의

CA는 von Neumann과 Wolfram에 의해서 스스로 조직화 하고 재생산할 수 있는 모델로 소개되었으며, 동역학계를 해석하는 하나의 방법으로 공간과 시간을 이산적으로 다루고 이산적인 공간을 셀룰라 공간의 기본단위인 각 셀이 취할 수 있는 상태를 유한하게 처리하며 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다[5-6].

가장 간단한 구조를 가지는 1차원 CA에서는 모든 셀들이 선형으로 배열되어 있으며 국소적 상호 작용이 세 개의 셀, 즉 자기 자신과 인접한 두 셀에 의해서 이루어지며, 이러한 CA를 3-이웃 CA라고 한다.

3-이웃 CA에 대한 상태전이함수는 다음과 같다.

$$q_i(t+1) = f[q_i(t), q_{i+1}(t), q_{i-1}(t)]$$

여기서 i는 일차원으로 배열되어 있는 각 셀들의 위치, t는 시간 단계, $q_i(t)$는 시간 t에서 i번째 셀의 상태, f는 결합 논리를 가지는 국소전이 함수를 나타낸다. f는 3개의 변수를 가지는 부울함수로 $f:\{000,001,010,\cdots,110,111\}\rightarrow\{0,1\}$이다.

$GF(2)$상에서 3-이웃 CA에는 서로 다른 2^3개의 이웃의 배열상태가 있으며 그러한 CA에는 2^{2^3}, 즉 256개의 상태전이함수가 있게 된다. 이것을 CA의 규칙이라고 한다. 규칙은 십진수 7에서 0까지 내림차순으로 3비트 이진수로 표시하고 결합논리에 의해서 구해진 이진수를 십진수로 다시 표시한 것이다. 예를 들어 아래와 같이 f가 정의된다고 가정하자.

표 1. 규칙 90과 150
Table 1. Rule 90 and 150

이웃상태	111	110	101	100	011	010	001	000	규칙
다음상태	0	1	0	1	1	0	1	0	90
다음상태	1	0	0	1	0	1	1	0	150

여기서 첫 행은 시간 t에서 인접한 세 개의 셀들의 8가지 총 상태의 배열이고 다음 행들은 시간 $t+1$에서 i번째 셀의 갱신된 다음상태이다.

두 번째 행의 다음상태 결과를 이진법의 수로 간주하면 8비트 이진수 $01011010_{(2)}$는 십진수로 변환하면 $1\times2^6+1\times2^4+1\times2^3+1\times2^1=90$이므로 이 함수를 규칙 90이라고 한다. 같은 방법으로 이진수 $10010110_{(2)}$는 십진수 150이며 규칙 150이라고 한다. 규칙에 대한 결합논리는 다음 식으로 표현될 수 있으며 $\oplus$는 XOR 논리를 나타낸다.

$$\text{규칙 } 90: q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$$
$$\text{규칙 } 150: q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$$

2.2 CA 분류

CA는 셀의 배열상태, 적용되는 규칙의 논리, 적용된 규칙의 개수, 상태전이 그래프의 모양 그리고 양끝 셀의 경계조건에 따라서 분류된다. 셀의 배열상태에 따라 셀이 선형으로 배열되어 있는 1차원 CA, 셀이 평면으로 배열되어 있는 2차원 CA, 셀이 공간으로 배열되어 있는 3차원 CA로 분류된다. 또한 적용되는 규칙에 따라 모든 셀의 규칙이 XOR 논리로만 이루어진 선형(Linear) CA와 모든 셀의 규칙이 XOR과 XNOR 논리의 조합으로 이

루어진 여원 CA로 분류된다. 선형 CA와 여원 CA를 가산(Additive) CA라 한다. 적용되는 규칙의 개수에 따라 모든 셀에 동일한 규칙만 적용한 유니폼 CA(Uniform CA)와 그렇지 않은 Hybrid CA로 분류되며, 또한, 상태전이 그래프의 형태에 따라 모든 셀의 상태가 몇 개의 사이클을 이루며 반복되는 그룹 CA와 그렇지 않은 비그룹 CA로 분류된다. 여기서 그룹 CA는 모든 셀의 상태가 몇 개의 사이클을 이루며 반복되는 CA이며 임의의 한 상태에 대한 이전상태가 유일한 특징을 갖는다. 반면에 비그룹 CA는 상태전이 그래프가 트리 구조를 이루고 있으며 상태전이 함수에 의해서 얻어질 수 있는 상태인 도달 가능한 상태와 상태전이 함수에 의해서 나타날 수 없는 도달 불가능한 상태로 나누어진다. 비그룹 CA는 임의의 한 상태에 대한 이전상태가 2개 이상 존재하거나 존재하지 않을 수 있다.

2.3 CA 전이 행렬

n개의 셀을 가지는 1차원 CA에서 현재 상태를 다음 상태로 전이시키는 작용소를 $n \times n$행렬로 나타낼 수 있으며 이것을 CA의 전이행렬(transition matrix) 또는 특성행렬(characteristic matrix)이라고 한다. 전이행렬 $T=[t_{ij}]$에서 i번째 행은 i번째 셀의 규칙을 나타낸다. CA가 다음 상태로 전이될 때 i번째 셀이 j번째 셀에 영향을 받으면 $t_{ij}=1$이고 그렇지 않으면 $t_{ij}=0$이다. 3-이웃 NBCA의 전이행렬은 정방행렬의 주대각선과 그 위대각선과 아래 대각선을 제외한 나머지가 0인 삼중대각행렬이다. 예를 들어 4-셀 NBCA의 규칙이 <90, 150, 150, 90>이면 전이행렬은 다음과 같다.

$$T=\begin{bmatrix}0&1&0&0\\1&1&1&0\\0&1&1&1\\0&0&1&0\end{bmatrix}$$

시간 t에서의 CA의 상태를 S_t라고 하면 시간 $t+1$에서 CA의 상태는 $S_{t+1}=TS_t$이다. 또한 시간 $t+2$에서의 CA의 상태는 $S_{t+2}=TS_{t+1}==T(TS_t)=T^2S_t$이다. 따라서 p단계 후의 CA의 상태는 $S_{t+p}=T^pS_t$이다.

Ⅲ. 1차원 CA기반의 인증과 기밀성을 제공하는 보안 기술의 분석

3.1 인증의 기술 방법 분석

우선 인증을 하기 위한 기술은 보내는 쪽에서 의미 없는 데이터($n \times n$ 행렬)를 생성하고 이를 공유된 키를 이용하여 태그(Tag)를 생성하게 된다. 그런 다음 이 의미 없는 데이터와 태그를 동시에 상대방에게 보내면 상대방이 공유된 키를 이용하여 태그를 생성하고 이를 받은 태그와 비교함으로써 인증이 완료된다. 이 과정은 그림 1과 같다.

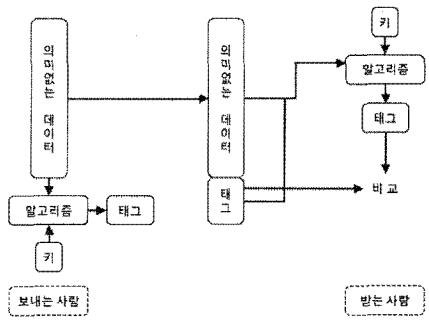

그림 1. 인증과정
Fig. 1 Authentication scheme

예제 1은 인증과정에서 태그를 생성하는 방법을 보여준다.

<예제 1> 보내는 사람과 받는 사람의 공유된 키 K와 인증을 위하여 보내는 사람은 의미 없는 데이터를 임의로 D와 같이 만든다고 하자.

$$K=\begin{pmatrix}0&1&0&0&0\\0&1&0&0&0\\1&1&1&0&0\\0&1&1&0&0\\0&0&1&1&1\end{pmatrix},\ D=\begin{pmatrix}1&1&0&1&0\\0&0&1&1&1\\1&0&1&0&1\\0&1&0&1&0\\0&0&1&1&1\end{pmatrix}$$

그러면 태그($n \times n$ 행렬)의 i번째 행은 데이터의 $(1,i)$ 성분이 0이면 키의 i번째 행을 전이규칙이 90인 유니폼 CA를 이용하여 상태전이 시킨 벡터로, 1이면 키의 i번째 행을 전이규칙이 150인 유니폼 CA를 이용하여 상태전이 시킨 벡터로 둔다. 이러한 방법으로 태그를 구성하면 다음과 같다. 태그의 1행은 데이터의 $(1,1)$ 성분이 1이므로

$$\begin{pmatrix}1&1&0&0&0\\1&1&1&0&0\\0&1&1&1&0\\0&0&1&1&1\\0&0&0&1&1\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}$$

이고, 태그의 4행은 데이터의 $(1,4)$ 성분이 0이므로

$$\begin{pmatrix}0&1&0&0&0\\1&0&1&0&0\\0&1&0&1&0\\0&0&1&0&1\\0&0&0&1&0\end{pmatrix}\begin{pmatrix}0\\1\\1\\0\\0\end{pmatrix}=\begin{pmatrix}1\\1\\1\\1\\0\end{pmatrix}$$

이다. 같은 방법으로 태그 T를 구성하면

$$T=\begin{pmatrix}1&1&1&0&0\\1&0&1&0&0\\0&1&0&1&0\\1&1&1&1&0\\0&1&1&0&1\end{pmatrix}$$

이다. 그러면 송신자는 수신자에게 $(T|D)$을 보내고, 이를 공유된 키를 이용하여 수신자가 확인함으로써 인증이 완료된다.

인증은 전이규칙이 90 또는 150을 갖는 유니폼 CA를 사용하고 있다. 이러한 90/150 유니폼 CA는 다음과 같은 성질을 가지고 있다.

<성질>

1. n -셀 90 유니폼 CA는 n 이 짝수이면 그룹 CA이다.
2. n -셀 150 유니폼 CA는 $n \neq 2 \pmod 3$ 이면 그룹 CA이다.

위 두 성질을 정리해 보면 n -셀 90/150 유니폼 CA는 $n=6m$ 이거나 $n=6m+4$ 이면 그룹 CA이다. 그룹 CA는 상태전이행렬의 역행렬이 존재하여 셀의 수가 $n=6m$ 이거나 $n=6m+4$ 이면 의미 없는 데이터와 태그를 전송과정에서 송수신자가 아닌 제삼자가 이를 도청하게 된다면 이를 이용하여 공유된 키의 복호가 간단하게 이뤄질 수 있다.

<예제 2> 제삼자가 전송과정에서 다음과 같은 6×6 행렬인 의미 없는 데이터와 태그를 도청했다면

$$D=\begin{pmatrix}1&0&1&1&0&0\\0&1&0&0&0&0\\0&0&0&1&1&1\\0&1&0&1&0&1\\0&0&1&1&0&0\\0&1&0&0&0&1\end{pmatrix},\quad T=\begin{pmatrix}1&1&0&0&0&0\\0&1&0&0&0&1\\0&0&0&0&0&1\\1&0&0&1&1&1\\0&0&1&0&1&0\end{pmatrix}$$

키의 첫 행은 데이터의 $(1,1)$성분이 1이므로

$$\begin{pmatrix}1&1&0&0&0&0\\1&1&1&0&0&0\\0&1&1&1&0&0\\0&0&1&1&1&0\\0&0&0&1&1&1\\0&0&0&0&1&1\end{pmatrix}\begin{pmatrix}1\\1\\0\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0&1&1&0&1&1\\1&1&1&0&1&1\\1&1&0&0&0&0\\0&0&0&0&1&1\\1&1&0&1&1&1\\1&1&0&1&1&0\end{pmatrix}\begin{pmatrix}1\\1\\0\\0\\0\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\\0\\0\end{pmatrix}$$

이고, 키의 두 번째 행은 데이터의 $(1,2)$성분이 0이므로

$$\begin{pmatrix}0&1&0&0&0&0\\1&0&1&0&0&0\\0&1&0&1&0&0\\0&0&1&0&1&0\\0&0&0&1&0&1\\0&0&0&0&1&0\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\\0\\0\end{pmatrix}=\begin{pmatrix}0&1&0&1&0&1\\1&0&0&0&0&0\\0&0&0&1&0&1\\1&0&1&0&0&0\\0&0&0&0&0&1\\1&0&1&0&1&0\end{pmatrix}\begin{pmatrix}0\\1\\0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\\1\\0\end{pmatrix}$$

이다. 같은 방법으로 키를 구성하면 다음과 같다.

$$K=\begin{pmatrix}1&0&0&0&0&0\\0&0&1&0&1&0\\1&0&1&0&1&0\\0&0&0&0&0&0\\0&1&0&1&1&0\\0&0&0&1&0&0\end{pmatrix}$$

예제 2에서와 같이 특정한 셀에 대하여 주어진 데이터와 태그에 의해여 송수신자만 공유해야 할 키가 인증과정에서 안전하지 못함을 알 수 있다.그러면 예제 1에서와 같이 특정한 셀이 아닐 때에도 일반적인 90/150 CA의 성질에 의하여 그 또한 안전하지 못하다. 일반적으로 90/150 CA는 그 이전의 상태의 개수가 0, 1 이거나 2이다. 따라서 특정한 셀이 아니다 하더라도 주어진 데이터와 태그에 의해여 송수신자만 공유해야 할 키가 인증과정에서 안전하지 못하다. 예를 들면 다음과 같다.

<예제 3> 예제 1에서 5셀 90/150 유니폼 CA는 그룹이 아니어서 주어진 데이터와 태그만으로는 바로 키를 알아내기 어렵다. 그러나 90/150 유니폼 CA만을 사용하고 있으며, 그 이전상태 또한 많아야 2개이므로 셀의 수가 늘어남에 따라 그 역을 알아내기 쉬워진다. 예제 1에서 데이터와 태그가 다음과 같다고 할 때

$$D=\begin{pmatrix}11010\\00111\\10101\\01010\\00111\end{pmatrix},\quad T=\begin{pmatrix}11100\\10100\\01010\\11110\\01101\end{pmatrix}$$

데이터의 첫 열에 의하여 태그의 각 행은 다음의 CA를 사용하였음을 알 수 있다.

행	1	2	3	4	5
전이규칙	150	90	150	90	90

그러면 태그의 각 행의 그 이전 상태는 각각에 적용된 전이규칙에 의하여 각각 2개의 이전상태를 가지게 된다. 예를 들어 태그의 첫 행은 150 유니폼 CA에 의하여 생성된 것이므로 키의 첫 행이 K_1이라 하면 다음이 성립한다.

$$\begin{pmatrix}11000\\11100\\01110\\00111\\00011\end{pmatrix}K_1=\begin{pmatrix}1\\1\\1\\0\\0\end{pmatrix}$$

이 때 150 유니폼 CA는 역행렬이 존재하지 않으므로 K_1이 유일하게 존재하지 않는다. 즉, $K_1=(0,1,0,0,0)^t$ 이거나 $K_1=(1,0,0,1,1)^t$이 된다.

같은 방법으로 K_i을 키의 i 번 째 행이라 두면 다음과 같다.

키행	규칙	가능한 이전 상태
K_1	150	$(0,1,0,0,0)^t$ 이거나 $(1,0,0,1,1)^t$
K_2	90	$(0,1,0,0,0)^t$ 이거나 $(1,1,1,0,1)^t$
K_3	150	$(1,1,1,0,0)^t$ 이거나 $(0,0,1,1,1)^t$
K_4	90	$(1,1,0,0,1)^t$ 이거나 $(0,1,1,0,0)^t$
K_5	90	$(0,0,1,1,1)^t$ 이거나 $(1,0,0,1,0)^t$

따라서 키를 알아내는데 주어진 n 셀에 대하여 가능한 키의 개수는 $(2^n)^n=2^{n^2}$개이지만 90/150 유니폼 CA의 성질에 의하여 가능한 키의 개수는 2^n 개로 줄어들게 된다. 이 또한 작은 수는 아니지만 인증한 후 기밀성을 보장하여 메시지를 보내는 과정에서 키를 알아 낼 수 있다는 문제점이 있다. 이는 다음에서 보인다.

3.2. 기밀성을 보장하기 위한 기술 방법 분석

[4]에서 위의 인증단계 후에 보내고자하는 메시지를 보내기 위하여 인증과정과 같은 방법으로 보내고자 하는 데이터를 이용하여 태그를 생성하게 된다. 이 때 인증에서는 의미 없는 데이터의 첫 열과 키를 이용하여 태그를 생성하고, 상대방에게 의미 없는 데이터와 태그를 전송하였으나 기밀성을 보장하며 데이터를 보내고자 할 때는 송신자가 보내고자 하는 데이터는 각 열(n 개)과 키를 이용하여 n 개의 태그를 생성하고, 상대방에게 이 n 개의 태그만을 전송하게 된다. 그러면 상대방이 공유된 키를 이용하여 데이터를 복호하게 된다. 다음은 [4]에서 제안한 기밀성을 보장하는 기술을 간단히 보이고 이를 분석한 것이다.

<예제 4> 예제 1에서와 같이 키 K가 다음과 같고, 이 때 송신자가 보내고자 하는 데이터 D가 다음과 같다고 하자.

$$K=\begin{pmatrix}01000\\01000\\11100\\01100\\00111\end{pmatrix},\quad D=\begin{pmatrix}10000\\11000\\01010\\10111\\00101\end{pmatrix}$$

데이터의 i 번째 열과 키를 이용하여 생성된 태그를 T_i $(i=1,\cdots,n)$라 하면 T_1 은 다음과 같다. 표기상의 편리함을 위하여 각 행의 십진표기로 나타내기로 한다.

$$T_1=\begin{pmatrix}11100\\11100\\10110\\10010\\01101\end{pmatrix}=\begin{pmatrix}28\\28\\22\\18\\13\end{pmatrix}$$

나머지 각각의 열들과 키를 이용하여 생성된 태그는 $T_2=(20,28,10,30,13)^t$, $T_3=(20,20,22,18,10)^t$ $T_4=(20,20,10,18,13)^t$, $T_5=T_3$이다. 여기서 A^t는 벡터 A의 전치이다. 이렇게 생성된 5개의 태그만 수신자에게 보내게 되므로 데이터의 기밀성을 보장하게 된다. 그러나 태그를 보내는 과정에서 태그만을 알게 되어도 키를 생성할 수 있다는 문제점이 있다. 우선 각 태그의 첫 행인 28과 20은 키의 첫 행에 90이나 150 유니폼 CA에 의해 생성된 것들이다. 그러면 다음 표를 이용하여 키의 첫 행이 8(0,1,0,0,0)임을 알 수 있다.

	이전상태	다음상태
90 유니폼 CA	13, 24	28
150 유니폼 CA	8, 19	

	이전상태	다음상태
90 유니폼 CA	8, 29	20
150 유니폼 CA	없음	

같은 방법으로 주어진 태그를 이용하여 키를 생성하면 $K=\begin{pmatrix}01000\\01000\\11100\\01100\\00111\end{pmatrix}$ 이다.

Ⅳ. 결 론

[4]에서는 1차원 90/150 CA를 이용하여 메시지를 주고 받기 전의 인증과 인증을 마친 후 보내고자 하는 메시지의 기밀성을 제공하는 보안 기술을 제안하였다. 본 논문에서는 [4]에서 제안한 방법이 인증과 기밀성을 제공하지 못함을 90/150 유니폼 CA의 성질을 분석함으로써 비밀 키를 알아 낼 수 있음을 보였다.

참고문헌

[1] D. de la Guia Martinez and A. Peinado Dominguez, "Pseudorandom Number Generation based on Nongroup Cellular Automata," Security Technology, 1999, Proceedings, IEEE 33rd Annual 1999 International Carnahan Conference, 45, pp. 370-376, 1999.

[2] P.D. Hortensius, R.D. McLeod and H.C. Card, "Parallel Random Number Generation for VLSI Systems using Cellular Automata." IEEE Trans. Computers, 38, pp. 1466-1473, 1989.

[3] A. Martin del Rey et al., "A Secret Sharing Scheme based on Cellular Automata," Applied Mathematics and Computaion, vol. 170, pp. 1356-1364, 2005.

[4] S.K. Sarkar, T. Karmakar, A .Kumar, K.Sharma, P.C. Pradhan and Puttamadappa, "A One Dimensional Cellular Automata based Security Scheme providing both Authentication and Confidentiality, IE(I) Journal-CP, Vol87, pp. 1-8, May 2006.

[5] P.P. Chaudhuri, D.R. Chowdhury, S. Nandi and C. Chattopadhyay, Additive cellular automata theory and applications, 1, IEEE Computer Society Press, California, 1997.

[6] S.J. Cho et al., New Synthesis of One-Dimensional 90/150 Linear Hybrid Group Cellular Automata, IEEE Transactions On COmputer-Aided Design of Integrated Circuits and Systems, Vol. 26, No. 9, pp. 1720-1724, 2007.

저자소개

황윤희(Yoon-Hee Hwang)

2002년 2월 : 부경대학교 통계학과 학사
2004년 2월 : 부경대학교 응용수학과 석사
2008년 8월 : 부경대학교 정보보호학과 박사
※관심분야 : 셀룰라 오토마타론, 정보보호, 유한체, 컴퓨터 구조론

조성진(Sung-Jin Cho)

1979년 2월: 강원대학교 수학교육과 학사
1981년 2월: 고려대학교 수학과 석사
1988년 2월: 고려대학교 수학과 박사
1988년 ~ 현재 : 부경대학교 수리과학부 정교수
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론

최언숙(Un-Sook Choi)

1992년 2월 : 성균관대학교 산업공학과 학사
2000년 2월 : 부경대학교 응용수학과 석사
2004년 2월 : 부경대학교 응용수학과 박사
2004년 3월~2006년 2월 : 영산대학교 자유전공학부 단임교수
2009년 8월 : 부경대학교 정보보호협동과정 박사
2006년 3월~현재 : 동명대학교 미디어공학과 전임강사
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론