論文97-34D-11-13

스트림 암호 시스템을 위한 광 Threshold 발생기

(An Optical Threshold Generator for the Stream Cipher Systems)

韓 鍾 旭 *, 姜 昌 求 *, 金 大 豪 *, 金 恩 洙 **

(Jong-Wook Han, Chang-Goo Kang, Dae-Ho Kim, and Eun-Soo Kim)

요 약

본 논문에서는 스트림 암호 시스템에서 랜덤 이진 수열 발생을 위하여 사용되는 비선형 이진 수열 발생기 중 하나인 threshold 발생기의 광학적 구현 모델을 제안하였다. Threshold 발생기를 구성하는 LFSR 기능은 shadow casting 기법을 이용하여, 또한 XOR 연산과 벡터간 내적 계산을 위한 mod 2 덧셈 연산은 편광 특성을 이용하여 광학적으로 구현하였다. 특히 본 논문에서는 mod 2 덧셈 연산을 위한 새로운 광학적 구현 방법인 PMRS를 제안하므로서 연산 결과 값 측정과 LCD상의 데이타 값 표현 과정을 제외한 전 부분을 완전한 광학적 방법으로 처리가 가능하게 하였다. 본 논문에서 제안한 광 스트림 암호 시스템은 기존의 전자적인 H/W 구현시 문제인 tapping point의 개수에 대한 한계성을 극복할 수 있는 장점 있고, 또한 2차원 데이타인 영상 암호화 시스템의 광학적 구현에 그 응용이 가능하다. 제안된 광 스트림 암호화 시스템을 컴퓨터 시뮬레이션 결과를 통하여 실제로 광학적 구현이 가능함을 보였다.

Abstract

In this paper, we propose a new optical threshold generator as a key-stream generator for stream cipher systems. The random key-bit stream is generated by a digital generator that is composed of LFSRs and nonlinear logics. Digital implementation of a key-stream generator requires large memory to implement programmable tapping points. This memory problem may be overcome easily by using the proposed optical system which has the property of 2D parallel processing. To implement the threshold generator optically, we use conventional twisted nematic type SLMs (LCDs). This proposed system is based on the shadow casting technique for the AND operation between taps and register stages. It is also based on the proposed PMRS method for modulo 2 addition. The proposed PMRS method uses the property of light's polarization on LCD and can be implemented optically using one LCD and some mirrors. One of the major advantages of the proposed system is that there is no limitation of the number of the programmable tapping points. Therefore, the proposed system can be applied for the 2D encryption system which processes large amounts of data such as 2D images. We verify the proposed system with some simulation.

* 正會員, 韓國電子通信研究院

(Electronics and Telecommunications Research Institute)

** 正會員, 光云大學校 電子工學科

(Dept. of Electronic Eng., Kwangwoon Univ.)

接受日字:1997年7月19日, 수정완료일:1997年10月15日

Ⅰ. 서 론

스트림 암호 시스템은 주로 최대 주기를 보장하는 m-LFSR(maximum length linear feedback shift register)을 비선형적으로 결합한 비선형 이진 수열 발생기를 기본으로 하여 구성이 되며, 다른 암호 시스템과 달리 비교적 수학적 분석이 가능하여 여러 중요

수치에 대한 이론적인 값을 정확하게 계산할 수 있는 장점이 있다. 또한 데이타에 대한 에러 전파 현상이 발생하지 않고 H/W 실현이 용이하다는 점에서도 장점을 가지고 있다. 하지만 m-LFSR은 특성 다항식이 갖는 선형성 때문에 연속적인 2n개의 항을 가지고 전체 수열을 발생하게 되므로 암호 시스템용으로서 사용하기에는 적합하지 못하다. 그러므로 이러한 선형 특성을 배제할 수 있도록 비선형 논리를 사용하여 몇 개의 m-LFSR을 결합하는 비선형 시스템으로 구성한다. 일반적으로 스트림 암호 시스템에서 사용하는 비선형 알고리즘을 이용한 이진 수열 발생기로는 Geffe 발생기, Geffe 발생기를 개선한 상호 대칭 시스템인 threshold 발생기, MUX(multiplication), BRM(binary rated multiplexer)[1]등 여러가지가 있으나, 선형 복잡도 및 다른 여러 가지 특성에 의하여 MUX, BRM등이 많이 사용되고 있다.

스트림 암호 시스템의 H/W 실현은 이제까지 전자적인 디지탈 회로에 의하여 구성되어 왔으나 기존의 전자적인 방법에서는 LFSR의 궤환상수(feedback constant)를 구성하여 주는 tapping point가 많아지게 되면 H/W 게이트 수의 증가가 불가피하게 되고, 또한 안전한 스트림 암호 시스템의 실현을 위해서는 최소한의 tapping point가 보장되어야 하므로 H/W 실현상 어려운 단점을 지니고 있다. 그러므로 기존의 전자적인 방법이 가지고 있는 이러한 tapping point 개수의 한계성을 극복할 수 있는 새로운 실현 방법에 대한 필요성이 요구되고 있다.

최근 광정보처리 분야에서 급속하게 발전되고 있는 실시간 공간 광 변조기(SLM: spatial light modulator)중의 하나인 LCD(liquid crystal device)는 액정 셀의 특성에 의하여 입사되는 광의 편광(polarization) 성분을 에너지의 변화 없이 인가 전압에 따라 회전을 시키는 특징을 지니고 있으므로[2], 이러한 편광 현상을 이용하여 광 정보 처리 분야에서 SLM으로서 많이 사용이 되어 오고 있다.[3 - 5] 본 논문에서는 LCD를 이용하여 기존의 디지탈적인 1차원적 방법이 아닌 새로운 광학을 이용한 2차원적인 실현 방법을 사용하여 스트림 암호 시스템에서 사용이 되는 이진 수열 발생기중에 하나인 threshold 발생기의 광학적 구현 모델을 제안하였다. 즉, m-LFSR을 LCD를 사용하여 표현을 하고, shadow 기법을 사용하여 벡터-벡터 곱을 계산하며, LCD의 편광 특성을 이용하여 XOR(exclusive OR) 연산과 벡터간의 내적(inner product)계산을 위한 mod 2 덧셈 연산을 수행하였다.

따라서, 본 논문에서 제안한 광 threshold 발생기는 기존의 디지탈 실현 방법에서 문제가 되는 tapping point의 개수에 대한 한계성을 극복할 수 있고, 1차원적인 실현 방법이 아닌 광학을 이용한 2차원적 시스템을 구성하는 새로운 방법을 제안하므로서 2차원 영상 암호 시스템으로의 응용 가능성을 보여 주었다.

Ⅱ. Threshold 발생기

스트림 암호 시스템은 LFSR을 이용한 이진 수열 발생기를 사용하는 암호 시스템이다. 이 스트림 암호 시스템은 최대 주기를 보장하는 LFSR을 비선형으로 결합한 비선형 이진 수열 발생기를 근간으로 하는 암호 시스템으로 평문을 이진 수열로 부호화한 후 이진 수열 발생기에서 발생된 이진 수열과 비트별로 XOR하므로서 암호문을 발생한다. 스트림 암호 시스템은 다른 암호 시스템과 달리 비교적 수학적인 분석이 가능하여 주기, 선형 복잡도 등 여러가지 중요 수치에 대한 이론적인 값을 정확하게 계산할 수 있으며, 또한 에러 전파 현상이 발생하지 않고 알고리즘 실현이 용이한 장점이 있다.

그림 1은 n차 LFSR의 구조를 나타낸 것이다[1, 6].

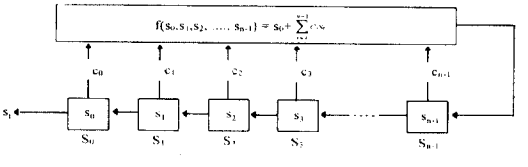


그림 1. n차 LFSR
Fig. 1. n-stage LFSR.

그림 1의 n차 LFSR은 n개의 단(stage)와 선형 궤환 함수(feedback function) $f(s_0, s_1, s_2, \ldots, s_{n-1})$로 구성이 된다. n개의 단을 각각 $S_0, S_1, S_2, \ldots, S_{n-1}$로 나타내고, n개의 단의 내용 $s_0, s_1, s_2, \ldots, s_{n-1}$을 하나의 상태로 정의하고 $s_0s_1s_2\ldots s_{n-1}$로 나타낸다. 이때 선형 궤환 함수는 식 (1)과 같이 표현이 된다.

$$f(s_0, s_1, s_2, \ldots, s_{n-1}) = s_0 + c_1s_1 + c_2s_2 + \ldots\ldots + c_{n-1}s_{n-1} \quad (1)$$

식 (1)에서 $c_0, c_1, c_2, \ldots, c_{n-1}$은 모두 0또는 1이고

c_i의 값은 S_i의 연결 상태를 나타내며 궤환 상수라고 한다. LFSR의 선형 이진 수열 s_t는 LFSR의 단 S_0의 내용이 출력됨으로써 발생이 되며 출력 수열 s_t는 식 (2)와 같다.

$$S_0,S_1,S_2,\ldots,S_{n-1},S_n=S_0+\sum_{i=1}^{n-1}c_iS_i,\ S_{n+1}=S_1+\sum_{i=1}^{n-1}c_{i+1}S_{i+1},\ldots. \quad (2)$$

식 (2)에서 S_0, S_1, S_2,...., S_{n-1}을 제외한 각 항은 바로 이전의 n개의 항과 궤환 상수로 결정이 된다. 출력 수열 s_t는 궤환 상수 $c_0 = 1$, c_1, c_2,...., c_{n-1}과 초기 상태 $S_0S_1S_2....S_{n-1}$에 의하여 결정된다. 이때 출력 수열 s_t의 총 경우의 수는 연속적인 n항이 모두 0인 경우는 존재 할 수 없으므로 최대 2^n-1이 된다. 그러므로 초기 상태 $S_0S_1S_2....S_{n-1}$은 처음 2^n-1개 상태 내에서 적어도 한번은 되풀이 되며, 그 과정을 반복함으로서 주기를 갖게 된다. 그러나 m-LFSR은 특성 다항식이 갖는 선형성에 의해서 n단 LFSR에 의하여 생성된 이진 수열 s_t는 연속적인 2n개의 항을 가지고 전체 수열을 발생하게 되므로 암호 시스템용 이진 수열 발생기로서 사용하기에는 적합하지 못하다. 그러므로 스트림 암호 시스템에서 사용하는 이진 수열 발생기는 이러한 선형적인 특성을 배제할 수 있도록 비선형 알고리즘을 추가하여 몇 개의 m-LFSR을 비선형 논리를 사용하여 결합하는 비선형 시스템으로 구성한다.

상호 대칭인 threshold 발생기는 1973년 Geffe가 제시한 비선형 시스템인 Geffe 시스템을 개선한 것으로 3개의 m-LFSR로 구성이 되며, 3개의 m-LFSR에서 출력되는 이진 출력중 majority 비트를 출력 수열로 사용하도록 비선형 알고리즘이 구성되어 있다.

그림 2는 threshold 발생기를 나타낸 것이다.

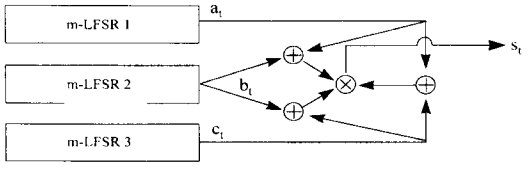


그림 2. Threshold 발생기
Fig. 2. Threshold generator.

m-LFSR 의 이진 출력 수열을 각각 a_t, b_t, c_t이라고 하면, threshold 발생기의 출력 수열 st은 식 (3)과 같다.

$$s_t = a_t \oplus b_t b_t \oplus c_t c_t a_t \quad (3)$$

식 (3)에서 $\oplus$는 XOR 연산을 의미한다.

이때, m-LFSR 1 - m-LFSR 3의 차수를 각각 다른 값 m, n, k라고 할 때, threshold 발생기에서 발생이 되는 최종 출력 수열 s_n의 주기와 선형 복잡도는 각각 $(2^m-1)(2^n-1)(2^k-1)$과 mn+nk+km이 된다.

위의 식 (3)을 분석하여 보면 m-LFSR 1, m-LFSR 2, m-LFSR 3에서 각각 출력 되는 3개의 이진 출력 수열중 각각 2개씩을 AND 연산을 한 후 다시 그 결과들을 XOR 연산을 하여 최종 비선형 이진 수열을 얻는 것을 알 수가 있다. 그러므로 threshold 발생기의 최종 출력 수열 s_n는 m-LFSR 1, m-LFSR 2, m-LFSR 3에서 각각 나온 이진 출력 수열 비트 값 3비트중 majority 비트 값이 최종 출력 수열 값이 되는 것이다.

Ⅲ. LFSR 구현 방법

앞의 2절에서 설명하였던 그림 1의 n차 LFSR에서 n번째 단 S_{n-1}의 상태 값인 s_{n-1}은 식 (2)로 부터 n개 단의 상태를 나타내는 벡터와 궤환 상수를 나타내는 벡터간 내적 값의 mod 2 덧셈 연산을 수행한 결과가 된다. 그러므로 이를 식으로 다시 표현하여 보면 다음 식 (4)와 같다.

$$s_{n-1} = \sum_{i=0}^{n-1} = c_i s_i CS \quad (\text{mod } 2) \quad (4)$$

여기서 벡터 $S^T = [\,S_0, S_1, S_2,\ldots, S_{n-1}\,]$, 벡터 $C = [\,c_0, c_1, c_2,\ldots, c_{n-1}\,]$를 나타내며 단, c_0는 항상 1이다.

그러므로 위의 식 (4)는 $1 \times n$의 벡터 S^T와 $1 \times n$ 벡터 C 간의 벡터-벡터 곱을 수행하여 계산된 벡터의 각 원소 값을 모두 더하는 mod 2 덧셈 연산을 수행한 결과가 된다.

그림 3은 2절의 그림 1에서 설명하였던 m-LFSR의 동작을 블럭도로 간략하게 설명하여 놓은 것이다.

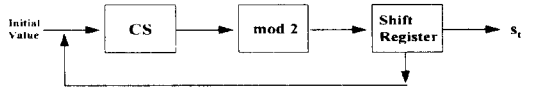


그림 3. m-LFSR의 동작 블럭도
Fig. 3. Block diagram of m-LFSR.

그림 3에서 보면 m-LFSR의 초기 상태가 설정이 되면 식 (4)에서와 같이 두 벡터간 내적 계산을 위한 mod 2 덧셈 연산을 통하여 S_{n-1}단에 입력되는 비트 값을 결정한 후 n단으로 연결된 플립 플롭을 한 단씩 shift시키는 것이다. 그 결과로 그림 1에서 보았듯이 LFSR의 선형 이진 수열 S_t가 출력이 된다. 또한 shift되어 변화된 n개 단의 상태는 초기 상태 값 대신에 두 벡터간의 내적 값 계산에 사용되어 S_{n-1}단에 입력되는 새로운 비트 값을 생성하게 된다. 이와 같은 동작을 반복하게 되어 계속하여 선형 이진 수열 S_t가 출력되게 된다.

m-LFSR의 동작을 광학적으로 구현하기 위해서는 그림 3의 두 벡터간 내적 계산을 위한 mod 2 덧셈 연산을 하여야만 한다. 그러므로 본 논문에서는 우선 두 벡터간의 내적 값 계산을 광학적으로 구현하기 위하여 내적 계산을 벡터-벡터 곱 과정과 벡터 원소들의 합산 과정으로 나누어서 구성하였다. 즉 벡터-벡터 곱을 수행하여 그 결과로 또 다른 한개의 벡터를 만든 후에 그 결과 벡터의 원소를 다시 더하여 내적 값을 구하는 것이다. 그런데 내적 값 계산을 위한 mod 2 덧셈 연산은 실제로는 각 벡터 원소간에 XOR 연산을 수행하는 것과 같으므로 실제로는 벡터-벡터 곱 과정과 그 결과 벡터의 합을 구하기 위한 XOR 연산 과정으로 구성이 된다.

그림 4는 그림 3의 단계를 광학적으로 구현하기 위한 단계별 블럭도를 나타낸 것이다.

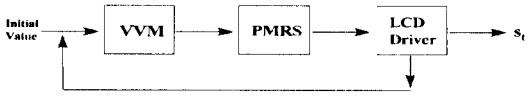


그림 4. 광학적 구현을 위한 m-LFSR의 동작 블럭도

Fig. 4. Block diagram of m-LFSR for optical implementation.

위의 그림 4에서 VVM(vector-vector multiplication)은 벡터-벡터 곱, PMRS(polarization multiplication by reflection and shift)는 본 논문에서 새로이 제안한 광학적 mod 2연산 방법을, LCD driver는 LCD 구동을 위하여 사용되는 구동용 H/W 및 S/W를 의미한다.

그림 4는 우선 벡터-벡터 곱을 계산한 후 결과 벡터를 가지고 mod 2 덧셈 연산을 수행하여 내적 값 및 새로운 연산 결과 비트를 생성하며, LCD driver를 이용하여 처음의 레지스터 상태를 한 비트씩 shift시키는 것이다.

본 논문에서 광학적인 벡터-벡터 곱은 shadow casting 기법을 사용하여 구현하였다.[7] shadow-casting 기법에서는 LCD상에 벡터 원소의 논리 상태를 빛의 투과 여부로 결정될 수 있도록 gray 레벨을 부여하는데 논리 1 상태는 빛이 통과되도록 투명한 패턴의 gray 레벨을 부여하고 논리 0 상태는 빛이 투과되지 못하는 gray 레벨의 패턴을 할당한다. 우선 각 벡터를 표현하기 위한 광 소자로는 polarizer와 analyzer가 부착된 LCD를 사용, 2개의 LCD를 직렬로 배열하여 벡터-벡터 곱을 수행하는 것이다. 각 벡터는 LCD 상에 n × 1의 어레이 형태로 표현이 되며 벡터의 각 원소는 동일한 개수의 LCD pixel로 구성이 된다.

그림 5는 shadow casting 기법에 의한 광 벡터-벡터 곱을 위한 간략화된 구성도이다.

그림 5에서 LCD 1과 2에는 각각 LFSR의 n개의 단 상태를 나타내는 벡터 $S^T = [\, s_0, s_1, s_2, \ldots, s_{n-1} \,]$와 궤환 상수를 나타내는 벡터 $C = [\, c_0, c_1, c_2, \ldots, c_{n-1} \,]$가 표현이 된다. LCD에 표현된 어레이에서 회색 부분은 빛이 통과하지 못하는 논리 0 상태이고 흰색 부분은 논리 1 상태를 의미한다. 그림 5에서는 n = 5인 경우이고 벡터 어레이의 아래 부분이 최하위 비트이므로 벡터 $S^T = [\, 1, 0, 1, 0, 1 \,]$, 벡터 $C = [\, 1, 0, 1, 1, 0 \,]$이 된다. 벡터-벡터 곱 결과는 LCD 2뒤에 점선으로 표현된 벡터 [1, 0, 1, 0, 0]이 되며, 이 벡터 값은 뒷단에 있는 5 × 1 어레이로 구성된 photo-detector에 의하여 검출되게 된다.

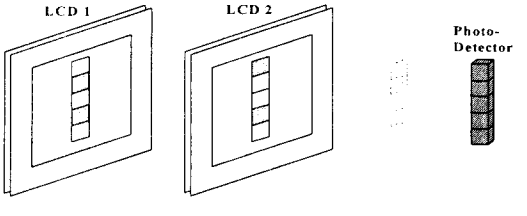


그림 5. 광 벡터-벡터 곱

Fig. 5. Optical vector-vector multiplication.

Ⅳ. Mod 2 덧셈 연산

그림 5에서 사용된 벡터-벡터 곱의 결과로 출력 벡

터는 [1, 0, 1, 0, 0]이 되며 다시 이 원소 값의 합인 내적 계산을 위한 mod 2 덧셈 연산을 수행하면 최종 결과는 논리 0 상태가 된다. 그러므로 내적 값 계산을 위한 mod 2 덧셈 연산은 벡터 원소를 구성하는 비트 값들간의 XOR와 같음을 알 수가 있다. 따라서 본 논문에서는 mod 2 덧셈 연산 기능을 XOR 기능으로 대치 사용하여 구현할 수 있는 광학적 시스템을 제안하였다.

최근 광정보처리 분야에서 급속하게 발전되고 사용이 되고 있는 실시간 공간 광 변조기인 SLM중 하나인 LCD는 액정 셀의 특성에 의하여 입사되는 광의 편광 성분을 에너지의 변화없이 인가 전압에 따라 회전을 시키는 특징을 지니고 있으므로, 이러한 편광 현상을 이용하여 광 정보 처리 분야에서 많이 사용 되고 있다. 이러한 LCD를 이용하여 광 컴퓨터 구조의 실현을 위한 부울 대수의 광학적 구현 예[8, 9]들이 그 동안 많이 연구, 발표되었으나 LCD를 사용하여 mod 2 덧셈 연산을 광학적으로 구현한 예는 아직 없다. 따라서 본 논문에서는 LCD 자체가 갖고 있는 입사광을 편광 변조 신호로 변환시키는 기능을 사용한 PMRS 방법으로 내적 계산을 위한 mod 2 덧셈 연산을 수행하는 새로운 광 시스템을 제안하였다.

LCD의 액정 셀에 전압이 인가되지 않으면 입사되는 광의 편광 성분을 90° 회전시키고 최대 전압이 인가되면 입사되는 편광 성분이 그대로 통과되는 특성을 갖고 있다. 일반적으로 LCD 소자의 앞뒤에는 2개의 편광기가 부착되어 있으므로 LCD를 편광 변조기로서 사용하기 위해서는 2개의 편광기인 polarizer와 analyzer를 제거하여 별도로 사용하여야만 한다.

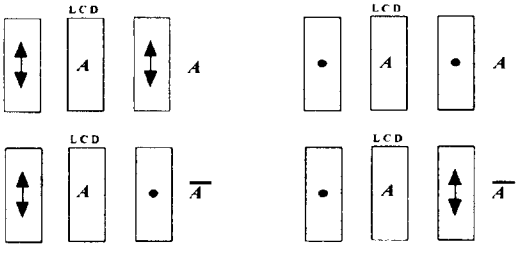


그림 6. 논리 정의
Fig. 6. Logic definition.

그림 6은 LCD와 편광기 배열에 따른 기본 정의를 한 것이다.[9, 10] 그림 6에서는 LCD와 편광기 2개를 적절하게 조합하여 기본 논리 상태를 정의하였으며, LCD에 표현된 A는 논리 1 상태 또는 논리 0 상태를 의미한다. 입사되는 편광 성분은 왼쪽 그림의 경우 수직 성분만을 갖는 편광기에 의해서 또한 오른쪽 그림의 경우는 수평 성분만을 갖는 편광기에 의해 먼저 편광된 것이다. 그림 6에서 아래 그림 2개는 NOT 연산으로 위의 그림 2개는 buffer 소자로서 동작함을 알 수가 있다.

그림 6에서 보면 입사 광의 편광 성분에 관계 없이 인가 전압에 의해서만 회전 정도가 정해지는 것을 볼 수 있으므로 LCD를 직렬로 연결하여 새로운 논리 회로 설계가 가능하겠다. 즉 NOT 연산을 하는 LCD 상태를 연속으로 2개 연결하면 최종 결과가 buffer와 같은 기능이 수행되는 것이다.

그림 6에서 정의한 기본 논리를 사용하여 mod 2 덧셈 연산 과정을 수행할 수 있는 XOR 연산을 구성하여 보면 그림 7과 같이 구성할 수 있다.

그림 7에서 보면 그림 6의 기본 논리 정의를 사용하여 XOR 연산이 가능함을 알 수가 있다. 즉, 만약에 A=0, B=1, C=0이고 논리 1 상태가 LCD에 전압이 가해지지 않아 90° 회전이 되는 상태이고 논리 0 상태가 회전이 되지 않도록 최대 전압이 가해진 상태라고 정의한다면 LCD 1과 2 사이에서의 편광 상태는 수직 성분 상태이고 LCD 2와 3 사이에서는 수평성분 상태가 된다. 그리고 LCD 3와 뒤의 수평 편광기 사이에선 수평 성분이 되므로 최종 출력은 수평 편광기를 통하여 수평 성분이 나오게 되는 것이다. 따라서 최종 출력 단에 검출기인 photo-detector를 배치하면 빛의 세기를 검출할 수 있으므로 논리 1 상태가 결정되게 되는 것이다.

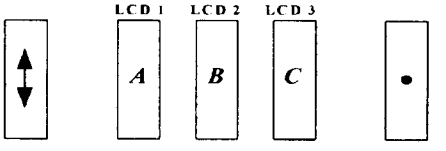


그림 7. A ⊕ B ⊕ C 연산
Fig. 7. A ⊕ B ⊕ C operation.

본 논문에서는 mod 2 덧셈 연산이 XOR 연산으로 대치 수행할 수 있으므로 LCD의 편광 변조 기능을 사용하여 내적 값 계산을 위한 mod 2 덧셈 연산을 광 XOR 기능으로 수행하는 새로운 광 시스템을 제안하였다.

그림 8은 본 논문에서 mod 2 덧셈 연산을 위한 제안한 mirror 어레이를 사용한 PMRS 방법[10, 11]이다.

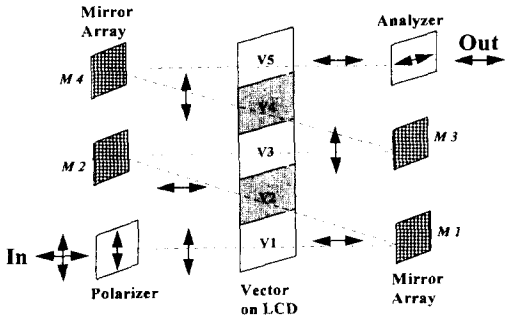


그림 8. 광 PMRS 방법
Fig. 8. Optical PMRS method.

그림 7에서 사용된 LCD는 하나의 논리 상태만을 표현하는데 이 LCD들이 나타내는 논리 상태를 한개의 LCD상에 벡터 어레이 형태로 표현하고 mirror 어레이를 사용하여 반사 및 벡터 원소간 shift 기능을 부여하여 원소간 XOR 연산을 가능하게 한 것이 그림 8에 나타낸 PMRS 방법이다.

그림 8에서 보면 LCD상에 5 × 1벡터가 구성이 되어 있고, 좌우에 M1, M2, M3, M4등 4개의 mirror가 있으며 polarizer와 analyzer등 2개의 편광기가 있다. LCD상에 표현되는 벡터는 원소로 V1, V2, V3, V4, V5를 갖고 있으며 색칠된 부분은 논리 0 상태로서 입사 편광 성분이 회전없이 통과되도록 일정한 전압이 가해진 상태가 되는 gray 레벨 값으로 표현된다. 색칠되지 않은 부분은 논리 1 상태로 입사광의 편광 성분은 90° 회전되어 출력이 된다. 이 경우 벡터 값은 [1, 0, 1, 0, 1] 이므로 각 벡터 원소간의 XOR 연산 결과는 논리 1이고, mod 2 덧셈 연산 결과도 논리 1이므로 앞에서 설명하였듯이 mod 2 연산 대신 XOR 연산을 사용하여도 가능함을 알 수 있다.

그림 8은 우선 입사되는 광은 polarizer에 의하여 수직 성분으로 편광이 되어 LCD상에 표현된 벡터의 원소 V1을 통과하게 된다. V1은 논리 1 상태이므로 90° 회전이 되어서 mirror M1에 도착할 때는 수평성분의 편광만이 존재하게 된다. 그런 후 약간 기울어져 구성된 mirror M2에 의하여 반사가 되어 논리 0 상태인 벡터 원소 V2에 곱해지며 통과한 성분은 수평성분을 유지하고 있게 된다. 다시 이 수평 성분은 mirror M3에 의하여 벡터 원소 V3에 곱해지며 90° 회전하게 된다. 이러한 방법으로 계속하여 각 벡터 원소 값간의 편광 성분의 곱셈이 수행되어 마지막에 출력단에 설치된 analyzer에 의하여 on/off 결과로 출력되게 된다. 마지막 벡터 원소 V5를 통과하게 되면 수평 성분으로 되고 다시 수평 성분의 편광기를 통하여 출력 수평 성분이 나오게 된다. 그러므로 최종 출력단에 photo-detector를 설치하여 검출함으로서 논리 1 상태가 되는 것이다.

앞절에서 설명하였던 벡터-벡터 곱은 본 절에서 제안한 mod 2 덧셈 연산과 함께 LFSR의 새로운 비트 생성에 사용이 된다. 즉 내적 값은 벡터-벡터 곱을 수행한 후 나온 결과 벡터의 모든 원소를 mod 2 덧셈 연산하여 얻게 되며 이 값을 최종 출력으로 하는 것이다.

V. 제안된 광학적 시스템

1. 광 스트림 암호 시스템

본 논문에서는 스트림 암호 시스템에서 사용하는 이진 수열 발생기중에 하나인 threshold 암호 시스템의 광학적 구현 모델을 제안하였다.

본 논문에서 구현하고자 하는 threshold 발생기는 3개의 m-LFSR로 구성이 되며 비선형 알고리즘은 식 (3)과 같이 주어지게 된다. 그러므로 광 시스템 구현시 레지스터의 표현은 하나의 LCD 상에 3개의 n × 1벡터로 나타내었으며 궤환 상수도 마찬가지로 3개의 n × 1 벡터로 표현이 된다. LCD 1과 LCD 2는 threshold 발생기를 구성하는 3개의 LFSR에서 각 단의 상태를 나타내는 벡터와 궤환 상수를 의미하는 벡터 간의 벡터-벡터 곱 계산을 위한 벡터 어레이와 최종적으로 출력되는 3개의 선형 이진 출력 수열 간의 곱 등을 표현하여 준다. 즉, 3개의 LFRS가 발생하는 선형 이진 출력 수열을 각각 a_t, b_t, c_t라고 하면 각 단의 상태를 나타내는 벡터와 궤환 상수를 나타내는 벡터는 $S^T_a = [\, S_{a0}, S_{a1}, S_{a2}, S_{a3}, S_{a4} \,]$, $C_a = [\, C_{a0}, C_{a1}, C_{a2}, C_{a3}, C_{a4} \,]$, $S^T_b = [\, S_{b0}, S_{b1}, S_{b2}, S_{b3}, S_{b4} \,]$, $C_b = [\, C_{b0}, C_{b1}, C_{b2}, C_{b3}, C_{b4} \,]$, $S^T_c = [\, S_{c0}, S_{c1}, S_{c2}, S_{c3}, S_{c4} \,]$, $C_c = [\, C_{c0}, C_{c1}, C_{c2}, C_{c3}, C_{c4} \,]$ 등이 된다.

그림 9는 제안된 광 threshold 발생기에서 사용하는 LCD 1과 LCD 2에 표현된 벡터를 나타낸 것이다.

3개의 벡터 S^T_a, S^T_b, S^T_c가 LCD 1상에 그림 9와

같이 표현이 되며 나머지 벡터 C_a, C_b, C_c가 LCD 2상에 표현이 된다. 또한 LCD 1상에는 그림 7과 같이 맨 오른쪽 벡터에 a_t, b_t, c_t 차례로 배열이 되고 LCD 2상에는 b_t, c_t, a_t 차례로 배열된다.

벡터-벡터 곱에 의하여출력되는 결과는 $C_aS^T{}_a$, $C_bS^T{}_b$, $C_cS^T{}_c$, a_tb_t, b_tc_t, c_ta_t 등이 되며, 이 결과 값들은 photo-detector에 의하여 검출되어 진다.

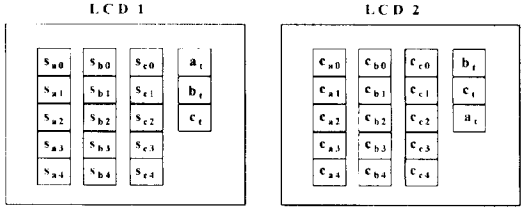


그림 9. 벡터-벡터 곱을 위한 LCD 1과 LCD 2상의 벡터 표현

Fig. 9. Vector represented on LCD 1 and LCD 2 for vector-vector multiplication.

그림 10은 본 논문에서 제안하는 threshold 발생기의 광학적 구현 시스템이다.

그림 10은 두개의 경로로 구성되어 위쪽 부분은 벡터-벡터 곱에 사용되며 이 경로에서 검출된 값이 아래 경로의 LCD 3의 입력 데이타로 사용되어 PMRS 방법에 의하여 최종 이진 출력 수열이 생성되게 된다.

그림 10에서 S는 광원으로 레이저를 의미하고, CL은 collimating lens로 평행광을 만들며, BS는 빔 분할기이다. LCD 1은 식 (4)에서 LFSR의 n단 상태 값을 나타내는 벡터 S^T와 3개 LFSR의 선형 이진 출력 수열을, LCD 2는 궤환 상수 값을 나타내는 벡터 C와 3개 LFSR의 선형 이진 출력 수열을 나타내며, LCD 3는 LCD 1과 LCD 2의 벡터-벡터 곱 결과를 다시 표시한다. PDA 1은 LCD 1과 LCD 2의 벡터-벡터 곱의 결과를, PDA 2는 PMRS의 결과를 검출한다. MA 1과 MA 2는 mirror 어레이로 PMRS를 이용한 mod 2 덧셈 연산 계산을 위하여 반사 및 벡터 원소간 shift에 이용되고, M은mirror, P 1과 P 2는 편광기를 의미한다. 여기서 LCD 1과 2는 세기 변조(amplitude modulation), LCD 3는 위상변조(phase modulation) 방식으로 사용이 된다

LCD 3에 표현되는 벡터-벡터 곱 결과는 입력 편광 성분의 변조가 가능하도록 2개의 gray 레벨을 적절하게 선택하여야만 한다. LCD 3에는 LFSR의 5단 상태와 궤환 상수 간의 곱 결과가 3개의 벡터 형태로 표현이 되어 mod 2 덧셈 연산에 이용이 되고, 맨 오른쪽의 3 × 1 벡터는 3개의 LFSR이 생성하는 선형 이진 출력 수열을 LCD 1과 LCD 2를 통하여 각각 곱하여 생성된 값인 a_tb_t, b_tc_t, c_ta_t으로서 XOR 연산에 사용이 된다. LCD 3를 사용하여 구성한 PMRS 시스템은 mod 2 덧셈 연산을 수행하여 식 (3)과 같은 최종 이진 수열을 생성하게 되며, 벡터-벡터 곱의 결과로 발생된 새로운 벡터의 mod 2 덧셈 연산을 수행하여 shift에 필요한 새로운 비트 값도 생성하게 된다.

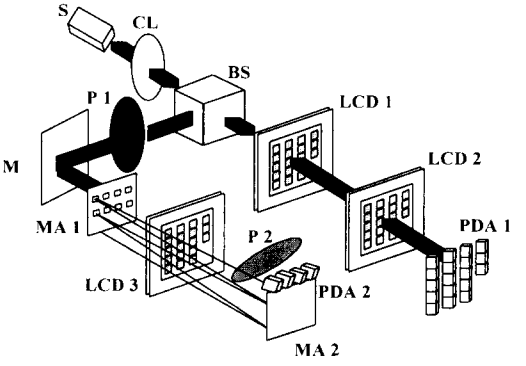


그림 10. 제안된 광학 시스템

Fig. 10. The proposed optical system.

BS와 M을 통하여 아래 경로인 PMRS 시스템으로 입력되는 광은 MA 1인 mirror 어레이 평면에 의하여 필터링되어 LCD 3상에 표현된 4개의 벡터에서 처음 원소로 가는 광만이 통과된다. 그런 후 MA 2에서 반사되고 이동이 되어 그 다음 벡터 원소로 경로가 바뀌어 진행하게 되는 것이다. LCD 3의 맨 오른쪽에 위치하는 3 × 1 벡터를 위한 입력 광을 다른 벡터들과 마찬가지로 사용하기 위해서 편광 성분이 바뀌지 않는 gray 레벨로 두 원소 값을 더 표현하여 3 × 1 벡터에 첨가하므로서 실제로는 5 × 1 벡터로 구성이 된다.

편광기인 P 1과 P 2는 LCD 3를 사용한 PMRS 방법의 구현을 위하여 사용이 되며, LCD 3에 부착되어 있던 양쪽의 편광기는 제거되어야만 한다. PDA 2는 P 1을 통해 나오는 최종 출력 값의 세기 성분을 검출하여 LFSR의 shift 기능과 최종 이진 출력 수열 생성에 관여하게 된다.

그림 10은 광학 시스템만이 보여주었을 뿐 실제로

는 여기에 LCD driver 및 디지탈 시스템 등이 추가가 되어야 한다. LCD driver/디지탈 시스템은 LCD 1과 LCD 2에 필요로 하는 벡터 어레이를 gray 레벨로 표현하여 주며, 또한 PDA 1에서 벡터-벡터 곱의 결과 값을 검출하여 LCD 3에 해당 벡터를 편광 변조를 가능하게끔 gray 레벨로 표현하여 준다. PDA 2에서 검출된 결과 값인 최종 이진 출력 수열은 암호화를 필요로 하는 장치로 전달하게 된다. 또한 LCD 1에서 필요로 하는 데이타인 새로운 LFSR의 처음 단 입력 값을 표현하게끔 하여준다. 이때 새로운 비트 값이 입력되므로 LCD 1에 LFSR의 단 상태를 표현하여 줄 때는 한 비트씩 shift하여야 한다.

2. 시뮬레이션

본 논문에서는 제안된 광 암호화 시스템이 실제로 광학적 구현이 가능함을 보이기 위하여 제안된 모델로 컴퓨터 시뮬레이션을 수행하였다. 즉, 그림 10과 같이 LCD 1과 LCD 2에 표현이 되는 3개의 LFSR의 각 단 상태를 나타내는 벡터와 궤환 상수를 의미하는 벡터에 초기값을 부여한 후 벡터-벡터 곱을 실현하고, 다시 LCD 3에 표현되는 그 결과를 mod 2 덧셈 연산하여 새로이 삽입될 비트 값을 생성하는 것이다. 또한 동시에 3개의 LFSR 출력 값들을 식 (3)과 같이 AND 및 XOR 연산을 수행하여 최종 비선형 이진 수열을 생성하게 하는 것이다.

그림 11은 제안된 시스템의 시뮬레이션을 위한 threshold 발생기의 초기값을 나타낸 것이다.

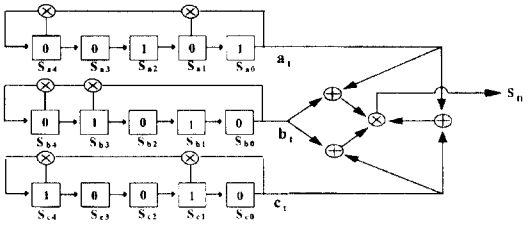
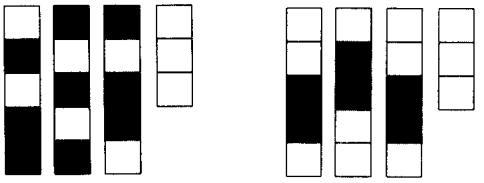


그림 11. 시뮬레이션을 위한 threshold 발생기의 초기 상태

Fig. 11. Initial value of the threshold generator for computer simulation.

그림 11과 같이 3개 LFSR의 초기 상태는 각각 $S^T_a = [1, 0, 1, 0, 0]$, $C_a = [1, 1, 0, 0, 1]$, $S^T_b = [0, 1, 0, 1, 0]$, $C_b = [1, 0, 0, 1, 1]$, $S^T_c = [0, 1, 0, 0, 1]$, $C_c = [1, 1, 0, 0, 1]$가 되며 이 값들은 5차 LFSR이 최대 주기인 31을 갖는 tapping point를 시뮬레이션을 통하여 구한 후 임의로 초기의 상태 값을 부여한 것이다. 시뮬레이션 결과 5차에서 2개의 경우만이 최대 주기를 갖게되어 편의상 LFSR 1에서 사용하였던 tapping point를 의미하는 C_a를 LFSR 3에서 C_c로동일하게 사용하였고 초기값만을 달리하였다. 또한 초기의 3개의 LFSR 출력 값은 모두 논리 0 상태로 가정하였고 최종 threshold 발생기의 출력 또한 논리 0 상태로 초기값을 설정하였다.

그림 11에서 나타낸 초기의 threshold 발생기의 상태를 제안된 방식으로 그림 12와 같이 배열하여 시뮬레이션을 하였다.

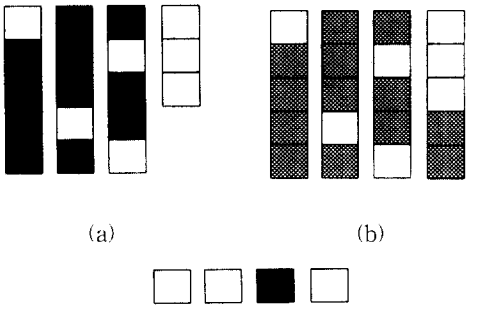


(a) (b)

그림 12. 제안된 방법에 의한 시뮬레이션용 초기값
(a) LCD1 (b) LCD 2

Fig. 12. Initial value for computer simulation using
(a) LCD1 (b) LCD 2

그림 12는 그림 10에서 나타낸 제안된 광학 시스템의 검증을 위하여 제안된 모델로 그림 9에서 나타내었던 LCD 1과 LCD 2에 초기값을 배열한 것이다. 그림 12에서 검게 색칠이 된 부분은 논리 0 상태, 흰색으로 색칠이 된 부분은 논리 1 상태를 의미한다.



(a) (b)

(c)

그림 13. 한 Clock Cycle 후의 벡터-벡터 곱 결과와 내적 및 XOR 연산 결과
(a) PDA 1 (b) LCD 3 (c) PDA 2

Fig. 13. The results of vector-vector multiplication and XOR operation after one clock cycle.
(a) PDA 1 (b) LCD 3 (c) PDA 2

그림 13은 그림 12의 초기값에서 한 clock cycle 후의 상태를 시뮬레이션 한 결과 값으로 그림 10의 광학 시스템을 고려한 배열로 결과를 출력하였다.

그림 13의 (a)는 그림 12의 (a)와 (b)의 벡터 값들을 사용하여 벡터-벡터 곱을 수행한 결과로 그림 10의 검출기인 photo-detector에서 출력되는 값을 나타낸 것이다. PDA 1상의 패턴도 그림 12의 LCD상의 표현 방식과 같이 논리 1 상태는 흰색으로 논리 0 상태는 검은 색으로 표현하였다. 그림 13의(b)는 (a)의 값이 LCD 3에 재 표현되는 상태를 나타낸 것으로 무늬가 있는 것은 논리 0 상태로 편광 성분이 회전이 되지 않는 상태를 표현하는 gray 레벨 값이며, 흰색은 논리 1 상태로 편광 성분이 90° 회전이 되는 상태의 gray 레벨을 의미한다. 그림 12의 입력 벡터 값을 벡터-벡터 곱을 한 경우 동일한 결과가 그림 13의 (a)에 나타남을 알 수가 있다. 그림 13의 (b)에 표현이 된 배열로 PMRS 및 XOR를 시뮬레이션을 한 결과 최종 출력 값을 그림 13의 (c)에 나타내었으며 이것은 그림 10의 최종 출력인 PDA 2에서 출력되는 값이다. 그림 13의 (c)와 같이 PMRS 및 XOR 연산 결과가 1101로 나타나며 여기서 threshold 발생기의 3개 LFSR로 입력 되는 새로운 비트는 각각 1, 1, 0이 되고 최종 비선형 이진 수열 출력 값은 1이 된다. Threshold 발생기의 3개 LFSR로 입력되는 비트 값 110은 그림 12의 (a) 상태 값에 각각 입력이 되어 각 LFSR은 한 비트씩 shift하게 된다.

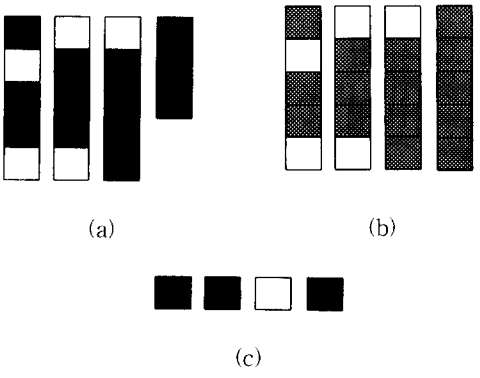


그림 14. 10 Clock Cycle 후의 벡터-벡터 곱 결과와 내적 및 XOR 연산 결과
(a) PDA 1 (b) LCD 3 (c) PDA 2

Fig. 14. The results of vector-vector multiplication and XOR operation after ten clock cycles.
(a) PDA 1 (b) LCD 3 (c) PDA 2

그림 14는 10 clock cycle 후의 벡터-벡터 곱 결과, 내적 값의 mod 2 덧셈 연산과 XOR 연산의 PMRS 실현을 위한 배열, 그리고 최종 결과 등을 나타내고 있다. (c)의 결과를 보면 3개의 LFSR로 새로이 입력되는 비트가 각각 0, 0, 1이므로 그림 15의 (a)에 나타낸것과 같이 새로이 입력이 되어 한 비트씩 shift되게 된다. 10 clock cycle 후 출력되는 비선형 이진 수열은 (c)에서와 같이 논리 0 상태가 된다.

그림 15는 그림 14의 결과로 만들어진 3개의 LFSR로 입력이 되는 새로운 비트 값에 의하여 shift 되므로서 갱신된 각 LFSR의 상태를 나타낸 것이다.

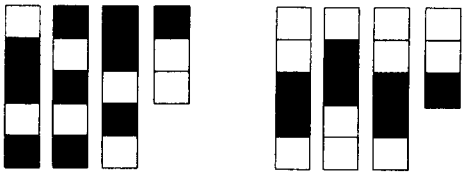


그림 15. 10 Clock Cycle 후의 threshold 발생기의 각 단의 상태 및 궤환 상수 값
(a) LCD 1 (b) LCD 2

Fig. 15. The values of stages and feedback constants in the threshold generator after ten clock cycles.
(a) LCD 1(b) LCD 2

그림 15에서 궤환 상수를 나타낸는 (b)는 고정된 값이므로 초기 상태와 동일함을 알 수가 있다.

이상과 같이 제안된 모델로 시뮬레이션을 한 결과가 원래의 threshold 발생기를 시뮬레이션한 결과와 마찬가지로 나타났다. 그러므로 본 논문에서 제안한 광 스트림 암호 시스템이 실제로 구현 가능함을 컴퓨터 시뮬레이션을 통하여 알 수가 있다.

VI. 결 론

본 논문에서는 새로이 광학을 이용한 2차원적 실현 방법을 사용하여 스트림 암호 시스템에 사용하는 이진 수열 발생기중에 하나인 threshold 발생기의 광학적 구현 시스템 모델을 제안하였다. 즉, m-LFSR을 LCD를 사용하여 표현을 하여 주고, shadow casting 기법을 사용하여 벡터-벡터간 곱을 계산하며 LCD의 편광 특성을 이용하여 XOR 연산과 내적 값의 mod 2

덧셈 연산을 수행하게 하였다. LFSR을 구성하는 각 단의 값과 궤환 상수 값을 두개의 LCD에 벡터 어레이 형태로 표현, shadow casting 기법으로 곱셈을 수행하게 하며, 또한 본 논문에서 제안한 내적 값 계산을 위한 mod 2 덧셈 연산인 광학적 PMRS는 각 비트 값을 mirror 배열을 통해 차례로 반사, 벡터 원소를 이동하면서 편광 성분이 변화하게 되며 마지막 검출기에 입력되는 상태의 광 세기를 검출하여 연산을 수행하게 된다.

본 논문에서 제안한 시스템은 LCD상에 벡터 표현과 출력 값 검출 과정만이 전자회로의 도움을 받을 뿐 다른 과정은 순수한 광학으로만 병렬 처리가 되기 때문에 2차원 영상 암호화 장치와 연계하여 사용할 경우 그 응용성이 매우 클 것이라고 생각되며, 또한 가변이 가능한 LCD를 사용함으로 해서 언제든지 LFSR의 변화가 가능하고 다른 이진 수열 발생기로의 변형 등이 손쉽게 이루어 질 수가 있겠다.

안전한 스트림 암호 시스템의 실현을 위해서는 tapping point의 최소한의 개수가 보장이 되어야 하나 디지탈적인 방법으로 프로그래머블한 논리 회로로 실현하는 경우 궤환 상수인 tapping point 개수로 인한 메모리 용량의 증가가 발생되어 tapping point의 개수를 제한할 수 밖에 없는 문제가 발생이 된다. 그러나 본 논문에서 제안한 광학 시스템을 사용는 경우에는 메모리 용량의 한계로 인한 tapping point 개수 제한과 같은 문제점이 발생되지 않으므로 실제 응용에 큰 장점이라고 볼 수 있겠다.

본 논문에서 사용한 LCD 소자의 경우 고 해상도의 소자들이 사용되고 계속 연구, 개발되고 있으므로 실제 제안된 시스템의 응용이 가능하리라 사료가 되며, 또한 완전한 광학만으로 시스템을 구성할 경우 광학의 특징인 고속 처리 및 병렬성의 특성으로 인하여 기존의 방법에서 문제가 되는 속도의 한계성 면에서 해결 방안이 될 수가 있을 것이다.

참 고 문 헌

[1] D. Gollmann and W. G. Chambers, "Clock-controlled shift register: a review," IEEE Journal on Selected Areas in Communications, vol. 7, no. 4, pp. 525-533, 1989.

[2] M.Kranzdorf, "Optical connectionist machine with polarization-based bipolar weight values," Opt. Eng., vol. 28, no. 8, pp. 844-848, 1989.

[3] Mohammad A. Karim and Abdul S. Award, "Polarization-encoded optical shadow-casting logic units : design," Appl. Opt., vol. 26, no. 14, pp. 2720-2725, 1987.

[4] Francis T. S. Yu, Suganda Jutamulia, and Don A. Gregory, "Real-time liquid crystal TV XOR- and XNOR- gate trinary image substraction," App. Opt., vol. 26, no. 14, pp. 2738-2742, 1987.

[5] Rizwan A. Rizi, K. Zaheer ,and M. Suhail Zubairy, "Implementation of trinary logic in a polarization encoded opticalshadow-casting scheme," Appl. Opt., vol. 30, no. 8, pp. 936-942, 1991.

[6] Gustavus J. Simmons, Contemporary Cryptography, IEEE Press, pp. 106-115, 1992.

[7] Alastair D. Mcaulay, Optical Computer Architectures, John Wiley & Sons, pp. 203-207, 1991.

[8] Altaf H. Khan and Umid R. Nejib, "Optical logic gates employing liquid crystal optical switches," Appl. Opt., vol. 26, no. 2, pp. 270-273, 1987.

[9] Feihong Yu and Guowu Zheng, "An improved polarization-encoded logic algebra (PLA) used for the design of an optical gate for a 2D data array : theory," Opt. Comm., vol. 115, pp. 585-596, 1995.

[10] Jong-Wook Han and Eun-Soo Kim, "RSPM을 이용한 광 스레쉬홀드 발생기," 대한전자공학회 추계종합학술대회 논문집, vol. 19, no. 2, pp. 832-836, 1996

[11] Jong-Wook Han and Eun-Soo Kim, "Optical threshold generator for stream cipher systems," SPIE Proc., vol. 3159, 1997. (to be published).

저 자 소 개

韓 鍾 旭(正會員)

1989년 광운대학교 전자공학과 졸업(공학사). 1991년 광운대학교 대학원 전자공학과 졸업(공학석사). 1996년 ~ 현재 광운대학교 대학원 전자공학과 박사과정 재학중. 1991년 ~ 현재 한국전자통신연구원 선임연구원. 주관심분야는 Optical Security, Optical Image Encryption, Quantum Cryptography, Optical Computing

金 大 豪(正會員)

1977년 한양대학교 전자공학과 졸업(공학사). 1984년 한양대학교 산업대학원 전자공학과 졸업(공학석사). 1993년 Univ. of Maryland at College Park, Dept. of Computer Science Visiting Scholar. 1977년 ~ 현재 한국전자통신연구원 책임연구원 부호기술연구부장. 주관심분야는 전송분야, 통신 및 컴퓨터 보안

姜 昌 求(正會員)

1979년 한국항공대학교 항공전자공학과 졸업(공학사). 1986년 충남대학교 대학원 전자공학과 졸업(공학석사). 1993년 충남대학교 대학원 전자공학과 졸업(공학박사). 1979년 ~ 1982년 한국공군 기술장교. 1987년 ~ 현재 한국전자통신연구원 책임연구원 부호5실장. 주관심분야는 부호이론, 통신프로토콜, 통신 및 컴퓨터 보안, 정보보호 서비스 및 메카니즘

金 恩 洙(정회원) 第 34卷 D編 第 7號 參照
광운대학교 전자공학과 교수