通信情報保護學會論文誌
第 7 卷 第 1 號, 1997. 3

광 스레쉬홀드 발생기를 이용한 스트림 암호 시스템

한 종 욱*

Stream Cipher System using Opitical Threshold Generator

Jong-Wook Han

요 약

본 논문에서는 스트림 암호 시스템에서 사용이 되는 LFSR을 이용한 이진 수열 발생기중 하나인 Threshold 발생기에 대한 광학적 구현 방법을 새로이 제안하였다. 광학적 구현을 위하여 LCD를 이용하므로서 LFSR 및 Mod 2 덧셈 연산을 위한 각 비트 값을 표현, 2차원 처리가 가능하게 하였다. Threshold 발생기의 LFSR 기능은 Shadow Casting 기법을 이용하여, 또한 XOR 연산 및 내적 계산을 위한 Mod 2 덧셈 연산은 LCD가 갖고 있는 편광 특성을 이용하여 광학적으로 구현하였다. 특히 본 논문에서는 Mod 2 덧셈 연산을 위한 새로운 광학적 구현 방법인 RSPM을 제안하므로서 연산 결과 값 측정과 LCD상의 데이타 값 표현 과정을 제외한 전 부분을 완전한 광학적 방법으로 처리가 가능하게 하였다. 본 논문에서 제안한 광 Threshold 암호 시스템은 기존의 전자적인 H/W 구현 방법에서 문제가 되어오던 Tapping Point의 개수에 대한 한계성을 극복할 수 있는 장점을 지니고 있으며, 또한 2차원 데이타인 영상용 암호화 시스템의 광학적 구현에 그 응용이 가능하다.

Abstract

In this paper, a new optical threshold generator using LFSRs is suggested. To execute a LFSR operation and add operation in mod 2, we use conventional twisted nematic type SLMs for LCDs known as polarization control devices for representing 2D data. This proposed system is based on a shadow casting technique to represent a LFSR operation and a proposed RSPM method to realize add operation in mod 2 and XOR operation. The proposed optical RSPM method use the property of light's polarization on LCD and can be implemented optically to utilize optical computing system composed of LCDs and mirrors. In general, digital implementation of a LFSR needs much memory capacity for performing programmable tapping points. However such a difficult problem in digital H/W design is overcome easily by using the proposed optical system which has the property of 2D parallel processing. The proposed system also can be applied for 2D encryption system which requires processing of large amounts of data such as 2D image.

* 한국전자통신연구소

1. 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 선형성에 의해서 n단 LFSR에 의하여 생성된 이진 수열은 연속적인 2n개의 항을 가지고 전체 수열을 발생하게 되므로 암호 시스템용 이진 수열 발생기로서 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 발생기을 개선한 상호 대칭 시스템인 Threshold 발생기, MUX(Multiplication), BRM(Binary Rated Multiplexer) 등 여러가지가 있으나, 선형 복잡도 및 다른 여러 가지 특성에 의하여 MUX, BRM등[1]이 많이 사용되고 있다.

스트림 암호 시스템의 H/W 실현은 이제까지 전자적인 디지탈 회로에 의하여 구성이 되어 왔는데 기존의 전자적인 방법에서는 LFSR의 Feedback Constant를 구성하여 주는 Tapping Point가 많아지게 되면 H/W 게이트 수의 증가가 불가피하게 되고, 또한 안전한 스트림 암호 시스템의 실현을 위해서는 Tapping Point의 최소한의 개수가 보장되어야 하므로 H/W 실현시 어려움이 따르는 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 이러한 광 정보 처리 소자로서 각광을 받고 있는 LCD를 이용하여 기존의 디지탈적인 1차원 실현 방법이 아닌 새로운 광학을 이용한 2차원적인 실현 방법을 사용하여 스트림 암호 시스템에서 사용이 되는 이진 수열 발생기중에 하나인 Threshold 발생기를 실현하였다. 즉, m-LFSR을 LCD를 사용하여 표현을 하고, Shadow Casting 기법을 사용하여 벡터-벡터 곱을 계산하며, LCD의 편광 특성을 이용하여 XOR(Exclusive OR) 연산과 벡터간의 내적(Inner Product)계산을 위한 mod 2 덧셈 연산을 수행하게 하였다. LFSR을 구성하는 각 단의 값과 궤환 상수(Feedback Constant) 값을 두개의 LCD에 어레이 형태로 표현, Shadow Casting 기법으로 서로 곱셈을 수행하게 한다. 또한 본 논문에서 제안한 광 modular 연산은 각 비트 값을 광 소자만의 배열을 통해 차례로 거치면서 편광 성분이 변화하게 되며 마지막 검출기에 입력되는 상태의 광 세기를 검출하여 연산을 수행하게 된다.

따라서, 본 논문에서는 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.

먼저 2절에서는 간략하게 Threshold 발생기에 대하여 설명하였고, 3절에서는 m-LFSR의 광학적 구현 방법을 제시하였으며, 4절에서 광학적인 내적 값 계산을 위한 mod 2 덧셈 연산 방법을 제시하였다. 그리고 5절에서는 제안된 Threshold 발생기를 사용한 광 스트림 암호 시스템의 전체 구성도를 설명하였다.

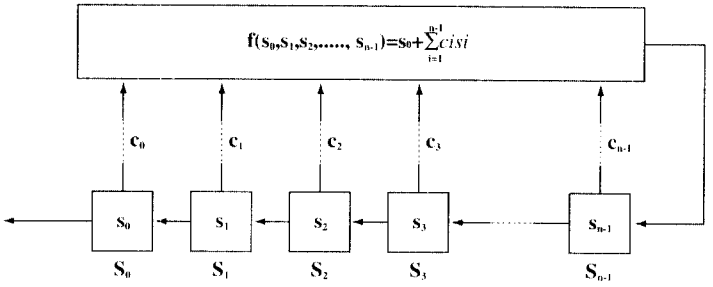


그림 1 n차 LFSR의 구조

2. Threshold 발생기[1, 6]

스트림 암호 시스템은 LFSR을 이용한 이진 수열 발생기를 사용하는 암호 시스템으로 주로 1970년대 초반부터 유럽에서 연구 발전되어 왔다. 스트림 암호 시스템은 최대 주기를 보장하는 LFSR을 비선형으로 결합한 비선형 이진 수열 발생기를 근간으로 하는 암호 시스템으로 평문을 이진 수열로 부호화하여 이진 수열 발생기에서 발생된 이진 수열과 비트별로 XOR하여 이진 수열로 된 암호문을 발생한다. 스트림 암호 시스템은 다른 암호 시스템과 달리 비교적 수학적인 분석이 가능하여 주기, 선형 복잡도 등 여러가지 중요한 수치에 대하여 이론적인 값을 정확하게 계산할 수 있는 장점이 있으며, 또한 데이타에 대한 에러 전파 현상이 발생하지 않고 알고리즘 실현이 용이하다.

그림 1은 n차 LFSR의 구조를 나타낸 것이다.

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 $s_0 s_1 s_2 \ldots s_{n-1}$로 나타낸다. 이때 선형 궤환 함수는 다음 식 (1)과 같이 표현이 된다.

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

식 (1)에서 $c_0, c_1, c_2, \ldots, c_{n-1}$은 모두 0 또는 1의 값을 취하며 c_i의 값은 S_i의 연결 상태를 나타내며 이를 궤환 상수라고 한다. $s_i(t)$를 시간 t에서의 S_i의 내용이라 할 때 i = 0, 1, 2, 3, ... , n-2인 경우에 $s_i(t+1) = s_{i+1}(t)$이고, $s_{n-1}(t+1) = s_0 + \sum_{i=1}^{n-1} c_i s_i(t)$로 나타낸다.

LFSR의 선형 이진 수열 s_i는 LFSR의 단 S_0의 내용이 출력됨으로써 얻어지게 되며 출력 수열 s_i는 다음 식 (2)와 같다.

$$s_0, s_1, s_2, \ldots, s_{n-1}, s_n = s_0+\sum_{i=1}^{n-1} c_i s_i,\ s_{n+1} = s_1+\sum_{i=1}^{n-1} c_{i-1}s_{i+1}, \ldots. \quad (2)$$

위의 식 (2)에서 s_0, s_1, s_2, ... , s_{n-1}을 제외한 각 항은 바로 이전의 n개의 항과 궤환 상수로 결정이 된다. 즉, 출력 수열 s_t는 궤환 상수 c_0 = 1, c_1, c_2, ... , c_{n-1}과 초기 상태 $s_0 s_1 s_2$.... s_{n-1}에 의하여 결정된다. 이때 출력 수열 s_t가 나타내는 상태의 총 경우의 수는 연속적인 n항이 모두 0인 경우는 존재 할 수 없으므로 최대 2^n-1이 된다. 그러므로 초기 상태 $s_0 s_1 s_2$.... 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 발생기로는 이러한 선형적인 특성을 배제할 수 있도록 비선형 알고리즘을 추가하여 몇 개의 m-LFSR을 비선형 논리를 사용하여 결합하는 비선형 시스템으로 구성한다. 일반적으로 스트림 암호 시스템에서 사용하는 비선형 알고리즘으로는 J-K 플립플롭 시스템, Geffe 시스템, Geffe 시스템을 개선한 상호 대칭 시스템인 Threshold 시스템, MUX, BRM등 여러가지가 있으나, 선형 복잡도 및 다른 여러가지 특성에 의하여 MUX, BRM등이 많이 사용되고 있다.

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

다음 그림 2는 Threshold 발생기를 나타낸 것이다.

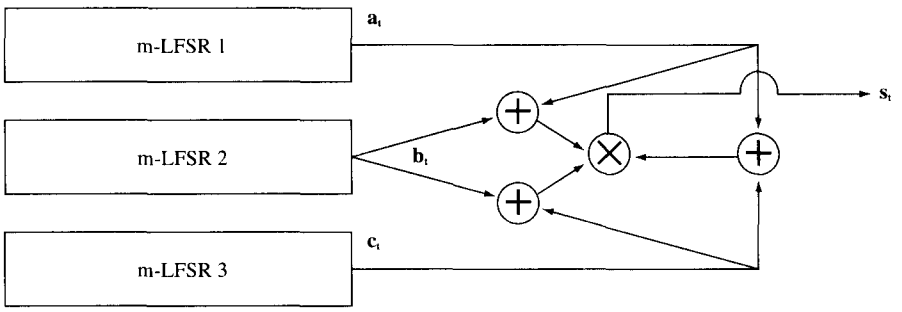


그림 2 Threshold 발생기

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

$$s_t = a_t b_t \otimes b_t c_t \otimes c_t a_t \qquad (3)$$

식 (3)에서 ⊗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 묶어서 AND 연산을 한 후 다시 그 결과를 XOR 연

산을 하여 최종 출력 수열을 얻는 것을 알 수가 있다. 그러므로 Threshold 발생기의 최종 출력 수열 s_t는 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.

3. LFSR 구현 방법

3.1. LCD 소자

본 논문에서 사용한 액정 소자인 LCD는 입사되는 광 신호의 편광 성분을 인가되는 전압의 크기에 따라 회전시키는 Twisted Nematic Cell 구조를 가지고 있다. 즉, 랜덤한 편광 성분을 갖고 있는 광 신호가 편광기에 의하여 수직 성분을 갖게 되어 LCD로 입력이 된다면 이 LCD에 전압을 인가하므로서 입사광의 수직 편광 성분을 0°에서 90°까지 회전을 시킬 수가 있다. 이때 LCD 뒤에 또하나의 편광기를 배치시키면 이 편광기에 의하여 LCD를 통과한 광 신호를 On/Off 제어할 수가 있는 것이다. 이러한 원리로 LCD, LCTV등의 액정 소자들이 동작을 하며 광정보처리 분야 등에서 액정 소자가 갖는 편광 성분을 이용하여 여러가지 응용에 많이 사용이 되고 있다.

그림 3은 Twisted Nematic Cell로 이루어진 LCD 구조를 나타내고 있다.

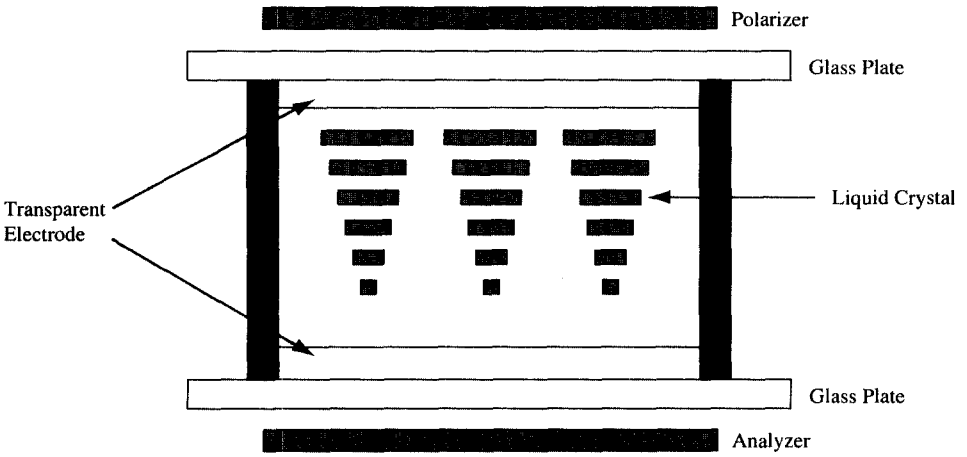


그림 3 LCD 내부 구조

위의 그림 3에서 두개의 편광기인 Polarizer와 Analyzer가 LCD 양쪽에 위치하여 인가 및 통과되는 광 신호를 제어하여 주게 되어 있으며, 이 두개의 편광기는 0°에서 360°까지 회전이 되어 수직 및 수평 성분의 투과량을 조절하여 주게 된다. 앞면의 편광기는 LCD에 입력되는 광 신호의 편광 성분을 제어하여 LCD로 입력되는 편광 성분을 결정하여 주게 되며, 뒷면의 편광기는 LCD를 통과한 편광 성분의 투과를 제어, 결정하여 준다.

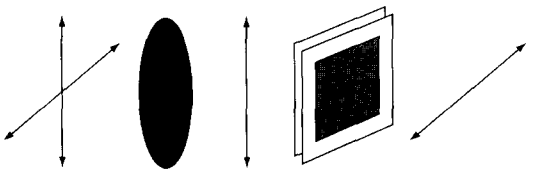
액정 분자들은 두 투명 전극층 사이에 위치하여 전계의 인가 정도로 입력 편광 성분의 회전 정도를 결정함으로써 입력 광의 수평, 수직 성분의 투과를 조절하여 준다. 양단의 전극에 전압이 인가되지 않으면 액정 분자들은 두 전극 사이에서 90°회전이 일어나게 되어 입력

편광 성분은 90°회전이 되며, 최대 전압 V가 인가되면 전극에 수직하게 배열이 되어 입력 편광 성분이 그대로 통과하게 된다.

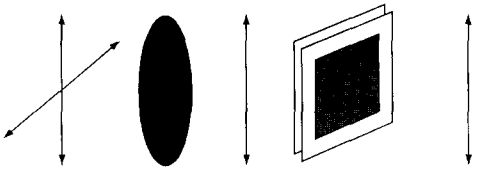
그림 4는 LCD의 편광 성분을 이용하여 논리 상태를 정의한 것이다.[7]

논리 0 상태는 입력 편광 성분을 회전없이 그대로 통과시키고, 논리 1 상태는 입력 편광 성분을 90°회전시키게 하여 수직 성분은 수평 성분으로 수평 성분은 수직 성분으로 되게 한다. 입력 편광 성분의 회전 여부를 결정하여 주는 두 전극간 전압은 LCD에 표현하여 주는 Gray 레벨 값으로 조절하여 주며 이 Gray 레벨 값은 시험에 의하여 0부터 255까지 차례로 LCD상에 표현하여 주면서 측정하여 구할 수 있다. 실제로 Gray 레벨과 입력 편광 성분간의 회전 정도를 특정하여 보면 선형적인 관계가 아니고 일정 값이 되면 포화 상태에 이르므로 이진수 표현이외의 여러 단계를 표현하고자 할 때는 반드시 Gray 레벨과 편광 성분의 회전 정도를 측정해 보아야 한다. 이후로 본 논문에서는 입력 편광 성분을 90°회전시키는 LCD상의 Gray 레벨을 논리 1 상태로, 입력 편광 성분을 회전 없이 통과시키는 경우를 논리 0 상태로 정의하여 사용한다.

전압에 따른 입력 편광 성분의 회전이 위에서 설명하였던 경우와 반대인 경우의 LCD 소자들도 사용이 되고 있다. 즉, 전압이 인가가 되지 않은 경우에는 회전이 되지 않고, 전압이 최대로 인가가 된 경우에는 90°회전되는 경우로서 두가지 경우가 다 사용이 되나 본 논문에서는 앞에서 설명한 경우의 소자를 사용하여 시스템을 구성하였다. 반대 경우의 소자를 사용하는 경우 편광기 배열 등에만 차이가 발생할 뿐 시스템 구성은 똑같게 된다.



(a) 논리 "1" 상태(V>0)



(b) 논리 "0" 상태(V=0)

그림 4 LCD 편광 특성을 이용한 논리 상태 정의

이상과 같이 본 논문에서는 이러한 특성을 갖는 LCD 소자를 이용하여 광 Threshold 발생기를 구성하였다. LCD를 이용하여 전기적인 신호를 광 신호로 바꾸어 변조시킴으로써 Shadow Casting에 의한 벡터-벡터 곱을 수행하였으며, 본 절에서 설명한 편광 특성을 이용하여 벡터간의 내적 값의 mod 2연산을 수행하게 하였다.

3.2. Shadow Casting에 의한 LFSR 구현 방법

앞의 2절에서 설명하였던 그림 1의 n차 LFSR에서 n번째 단 S_{n-1}의 상태 값인 s_{n-1}을 식 (2)에서 살펴보면 n개 단의 상태를 나타내는 벡터와 궤환 상수를 나타내는 벡터간 내적 계산을 위한 mod 2 덧셈 연산을 수행한 결과가 된다. 즉 LFSR에서 새로이 선형 궤환 함수 $f(s_0, s_1, s_2, \cdots, s_{n-1})$에 의하여 계산되어 n번째 단 S_{n-1}으로 입력되는 값은 $s_0, s_1, s_2, \cdots, s_{n-1}$등 모든 n개 단의 상태를 나타내는 상태 값 벡터와 각 단에 연결되어 있는 궤환 상수 값인 $c_1, c_1, c_2, \cdots, c_{n-1}$등 궤환 상수 벡터간 내적 계산을 위한 mod 2 덧셈 연산결과가 되며 이 값이 n번째 단 S_{n-1}으로 입력이 되는 것이다. 그러므로 이를 식으로 다시 표현하여 보면 다음 식 (4)와 같다.

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

여기서 벡터 $\mathbf{S}^T = [s_0, s_1, s_2, \cdots, s_{n-1}]$, 벡터 $\mathbf{C} = [c_0, c_1, c_2, \cdots, c_{n-1}]$를 나타내며 단, c_0는 항상 1이다.

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

그림 5는 2절의 그림 1에서 설명하였던 m-LFSR의 동작을 블럭도로 간략하게 설명하여 놓은 것이다.

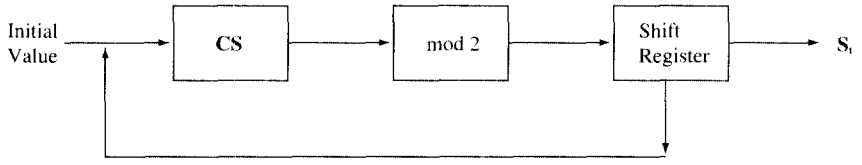


그림 5 m-LFSR의 동작 블럭도

위의 그림 5에서 보면 m-LFSR의 초기 상태가 설정이 되면 위의 식 (4)에서와 같이 두 벡터간 내적 계산을 위한 mod 2 덧셈 연산을 통하여 s_{n-1}단에 입력되는 비트 값으로 변환한 후 n단으로 연결된 플립 플롭을 한 단씩 shift 시키는 것이다. 그 결과로 2절의 그림 1에서 보았듯이 LFSR의 선형 이진 수열 s_i가 출력되게 된다. 또한 Shift되어 변화된 n개 단의 상태는 최초 설정되었던 초기 상태 값 대신에 두 벡터간의 내적 값 계산에 사용이 되어 S_{n-1} 단에 입력되는 비트 값을 생성하게 된다. 이와 같은 동작을 반복하게 되어 계속하여 선형 이진 수열 s_i가 출력되게 된다.

m-LFSR의 동작을 광학적으로 구현하기 위해서는 그림 5의 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 금 더하여 내적 값을 구하는 것이다. 그런데 내적 값 계산을 위한 mod 2 덧셈 연산을 수행하는 것이 실제로는 각 벡터 원소간에 XOR 연산을 수행하는 것과 같으므로 실제로는 벡

터-벡터 곱 과정과 그 결과 벡터의 합을 구하기 위한 mod 2 덧셈 연산 과정으로 구성된다고 할 수 있다.

그림 6은 그림 5의 동작 단계를 광학적으로 구현하기 위하여 본 논문에서 제안한 단계별 블럭도를 나타낸 것이다.

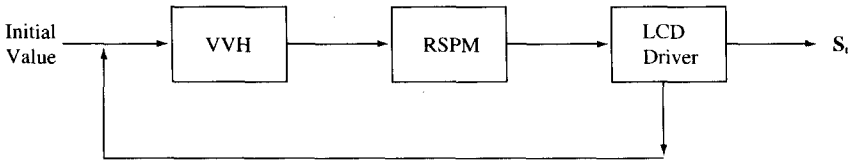


그림 6 광학적 구현을 위한 m-LFSR의 동작 블럭도

위의 그림 6에서 VVM(Vector-Vector Multiplication)은 벡터-벡터 곱, RSPM(Reflection and Shift Polarization Multiplication)은 본 논문에서 새로이 제안한 mod 2 연산 방법을, LCD Driver는 LCD 구동을 위하여 사용되는 구동용 H/W 및 S/W를 의미한다. 본 절에서는 순수한 벡터-벡터 곱 과정인 VVM만을 설명하고 다음 4절에서 벡터-벡터 곱 과정과 연계하여 완전한 내적 계산 기능을 겸하는 modular 연산을 수행하는 RSPM에 대하여 설명할 것이다.

그림 6은 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.[8] 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 못하도록 Gray 레벨의 패턴을 할당한다. 우선 각 벡터를 표현하기 위한 광 소자로는 LCD 2개를 사용하며 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 7은 Shadow Casting 기법에 의한 광 벡터-벡터 곱을 위한 간략화된 구성도이다.

그림 7에서 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. 이 경우 n=5이므로 각 벡터는 5×1 어레이가 되며 벡터의 원소 값이 0인 경우는 빛이 통과하지 못하게 1인 경우는 빛이 통과할 수 있도록 Gray 레벨로 표현하여 준다. 즉, LCD에 표현된 어레이에서 회색 부분은 빛이 통과하지 못하는 논리 0 상태이고 흰 부분은 논리 1 상태를 의미한다. 그림 7에서는 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.

그 LCD 1에 표현된 5×1 벡터를 평면파로 만들어진 빛이 통과하게 되면 [1, 0, 1, 0, 1]의 값을 가진 광 정보로 변하게 되며 이 값이 다시 LCD 2에 표현된 벡터 [1, 0, 1, 1, 0]에 곱해지게 되므로 LCD 2 나타나는 벡터는 [1, 0, 1, 0, 0]이 된다. 점선으로 나타낸 벡터는 실제로 LCD 2 뒤에서 볼 수 있는 벡터-벡터 곱의 결과로 나타난 벡터이며 이 벡터 값은 뒷단에 있는 5×1 어레이로 구성된 Photo-Detector에 의하여 검출되게 된다. 그러

므로 빛이 검출된 부분은 논리 1 상태가 되고 빛이 검출되지 않는 부분은 논리 0 상태가 되는 것이다. 따라서 위의 그림 6에서 벡터-벡터 곱인 VVM 단계는 그림 7로 구현이 가능함을 알 수가 있으며, 완전한 내적 계산을 위해서 mod 2 덧셈 연산인 XOR 연산은 뒤의 4절에서 설명할 RSPM으로 수행할 것이다.

그림 7에서 사용되는 LCD는 논리 0과 논리 1 상태만을 표현하므로 On/Off 두상태를 나타내기 위한 Gray 레벨이 2개만 사용이 되며 LCD 앞뒤에 부착된 Polarizer와 Analyzer는 그대로 사용을 하여야만 한다.

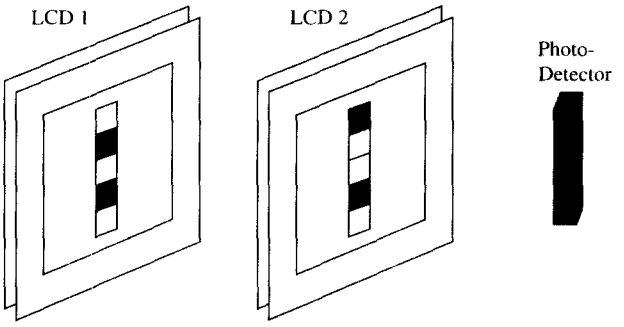


그림 7 벡터-벡터 곱을 위한 간략화된 구성도

4. Mod 2 덧셈 연산

그림 7에서 사용된 벡터-벡터 곱의 결과로 출력 벡터는 [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 값들 간의 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 SLM으로서 가장 많이 사용 되고 있다. 이러한 LCD를 이용하여 광 컴퓨터 구조의 실현을 위한 부울 대수의 광학적 구현 예들이 그 동안 많이 연구, 발표되었으나 LCD를 사용하여 mod 2 덧셈 연산을 광학적으로 구현한 예는 아직 없다.[9, 10] 따라서 본 논문에서는 LCD 자체가 갖고 있는 입사광을 편광 변조 신호로 변환시키는 기능을 사용한 RSPM 방법으로 내적 계산을 위한 mod 2 덧셈 연산을 수행하는 새로운 광 시스템을 제안하였다.

LCD의 액정 셀에 전압이 인가되면 입사되는 편광 성분이 그대로 통과되고, 전압이 인가되지 않으면 입사되는 광의 편광 성분을 90°회전시키는 특성을 갖고 있다. 또한 반대의 경우가 성립되는 LCD 소자도 있고 이를 이용하여 마찬가지로 시스템 제안이 가능하나 본 논문에서는 전자의 경우를 특성으로 갖는 LCD를 사용하여 구현 시스템을 제안하였다. 일반적으로 LCD 소자의 앞뒤에는 2개의 편광기가 부착되

어 있으므로 LCD를 편광 변조기로서 사용하기 위해서는 2개의 편광기인 Polarizer와 Analyzer를 제거하여 별도로 사용하여야만 한다.

그림 8은 LCD와 편광기 배열에 따른 기본 정의를 한 것이다.[10]

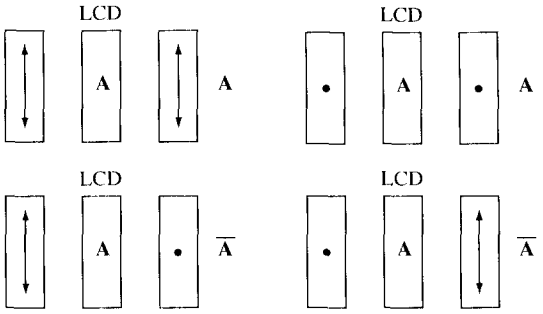


그림 8 LCD와 편광기 배열에 따른 기본 정의

그림 8에서는 LCD와 편광기 2개를 적절하게 조합하여 기본 논리 상태를 정의하였으며, LCD에 표현된 A는 논리 1 상태 또는 논리 0 상태를 의미한다. 모든 LCD에 부착된 2개의 편광기 Polarizer와 Analyzer는 분리하여 LCD 좌우에 배열하여 사용하였고, 입사되는 편광 성분은 왼쪽 그림의 경우 수직 성분만을 갖는 편광기에 의해서 또한 왼쪽 그림의 경우는 수평 성분만을 갖는 편광기에 의해 먼저 편광된 것이다. 그림 8에서 아래 그림 2개는 NOT 연산으로 위의 그림 2개는 Buffer 소자로서 동작함을 알 수가 있다. LCD에 표현된 Gray 레벨이 최대 전압이 가해진 경우이면 입사 편광 성분이 그대로 통과가 되고, LCD에 표현된 Gray 레벨이 전압이 가해지지 않은 상태이면 90°회전하여 통과가 된다.

그림 8에서 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 8에서 정의한 기본 논리를 사용하여 mod 2 덧셈 연산 과정을 수행할 수 있는 XOR 연산을 구성하여 보면 다음 그림 9와 같이 구성할 수 있다.

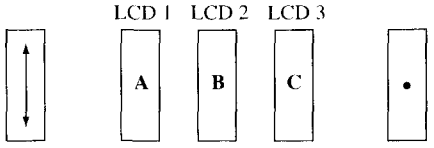


그림 9 A⊗B⊗C 연산을 위한 구성 배열

그림 9에서 보면 그림 8에서 사용하였던 기본 논리 정의를 사용하여 XOR 연산이 가능함을 알 수가 있다. 즉, 만약에 A = 0, B = 1, C = 0이고 논리 1 상태가 LCD에 전압이 인가

되지 않으므로 90°회전이 되는 상태이고 논리 0 상태가 회전이 되지 않도록 최대 전압이 인가된 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 수평성분이 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.

그러므로 그림 8에 정의하였던 기본 논리를 위한 배열을 직렬로 연결하여 적절하게 LCD들과 편광기들을 배열하면 좀 더 복잡한 논리 회로 구성이 가능함을 알 수가 있으며, 또한 XOR 연산의 경우 편광기들 사이에 LCD들을 배열하므로써 XOR 연산을 수행할 수가 있겠다.

앞에서 설명하였듯이 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 아래와 같이 제안하였다.

그림 10은 본 논문에서 mod 2 덧셈 연산을 위한 제안한 Mirror 어레이를 사용한 RSPM 방법이다.

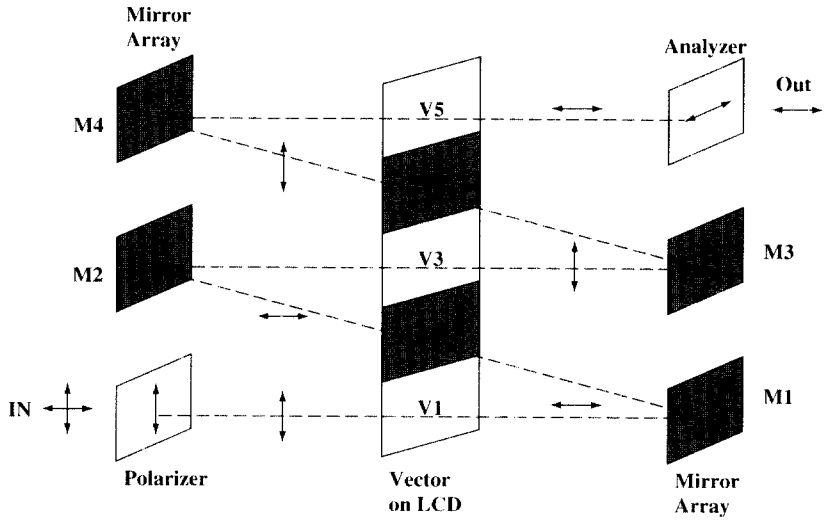


그림 10 광 RSPM 방법

그림 10에서 보면 LCD상에 5×1벡터가 구성이 되어 있고, 좌우에 M1, M2, M3, M4등 4개의 Mirror가 있으며 Polarizer와 Analyzer등 2개의 편광기가 있다. 단 LCD는 Polarizer와 Analyzer가 제거되어 그림 10과 같이 별도로 한 개씩만 사용이 된다. LCD상에 표현이 된 벡터는 원소로 V1, V2, V3, V4, V5를 갖고 있으며 이중 색칠된 부분은 논리 0 상태로서 입사 편광 성분이 회전 없이 통과되도록 최대 전압이 인가된 상태가 되는 Gray 레벨 값으로 표현이 된다. 색칠되지 않은 부분은 논리 1 상태로서 입사광의 편광 성분은 90°회전이 되어서 출력이 된다. 그림 10의 경우 벡터 값은 [1, 0, 1, 0, 1]이 되며 각 벡터 원소간의 XOR 연산 결과는 논리 1이고, mod 2 덧셈 연산 결과도 논리 1이 나오게 되므로 앞에서 설명하였듯이 mod 2 덧셈 연산을 XOR 연산으로 대신 사용하여도 가능함이 증명된다.

그림 9에서 사용된 LCD는 하나의 논리 상태만을 표현하는데 이 LCD들이 나타내는 논리 상태를 한개의 LCD상에 벡터 어레이 형태로 표현하여 Mirror 어레이를 사용하여 반사 및 벡터 원소간 Shift 기능을 부여하여 원소간 XOR 연산을 가능하게 한 것이 그림 10에 나타난 구성도이다.

그림 10을 설명하면 우선 입사되는 광은 Polarizer에 의하여 수직 성분으로 편광이 되어 LCD상에 표현된 벡터의 원소 **V1**을 통과하게 된다. **V1**은 논리 1 상태이므로 90°회전이 되어서 Mirror **M1**에 도착할 때는 수평성분의 편광만이 존재하게 된다. 그런 후 약간 기울어져 구성된 Mirror **M2**에 의하여 반사가 되어 벡터 원소 **V2**에 곱해지며 논리 상태가 0이므로 통과한 성분은 그대로 수평 성분을 유지하고 있게 된다. 다시 이 수평 성분은 Mirror **M3**에 의하여 벡터 원소 **V3**에 곱하여 지며 수직 성분으로 90°회전하게 된다. 이러한 방법으로 계속하여 각 벡터 원소 값에 곱하여져 편광 성분간의 곱셈 과정이 수행이 된 후 마지막에 출력되는 부분에 설치된 Analyzer에 의하여 On/Off 제어를 하게 된다. 그림 10의 경우 마지막 벡터 원소 **V3**를 통과하게 되면 수평 성분으로 되고 다시 수평 성분의 편광기를 통하여 출력 수평 성분이 나오게 된다. 그러므로 최종 출력단에 Photo-Detector를 설치하여 빛을 검출함으로서 논리 1 상태가 결정되는 것이다.

Mirror **M1**, **M3**는 약간 기울어져 반사 뿐만 아니라 Shift 기능을 함께 하도록 하여 벡터 원소간의 편광 성분에 의한 곱셈이 가능하도록 하였으며 반면에 Mirror **M2**, **M4**는 단지 입사되는 편광 성분을 유지하며 반사시키는 역할만을 수행하게 된다.

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. 본 절에서는 mod 2 덧셈 연산을 수행하는 과정을 RSPM 방법이라는 본 논문에서 제안한 방법을 통하여 가능하므로 LFSR의 궤환 함수에 의한 새로운 비트 값 생성이 이루어지게 되는 것이다.

5. 제안된 광학적 시스템

본 논문에서는 스트림 암호 시스템에서 사용하는 이진 수열 발생기중에 하나인 Threshold 암호 시스템의 광학적 구현 모델을 제안하였다. 제안된 모델은 액정 셀로 구성이 되는 LCD를 사용하였으며 Shadow Casting 방법을 이용하여 벡터-벡터 곱을 수행하였고, 또 RSPM이라는 연속적인 편광 곱셈 방법을 제안하여 mod 2 덧셈 연산을 광학적으로 수행하였다.

그림 11은 본 논문에서 제안한 광 Threshold 발생기에서 사용하는 LCD 1과 LCD 2에 표현된 백터를 나타낸 것이다.

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×1 벡터로 나타내었으며 궤환 상수도 마찬가지로 3개의 n×1 벡터로 표현이 된다.

본 논문에서 제안한 시스템에서 LCD 1과 LCD 2는 Threshold 암호 시스템을 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 LFSR이 발생하는 선형 이진 출력 수열을 각각 a_t, b_t, c_t라고 하면 각 단의 상태를 나타내는 벡터와

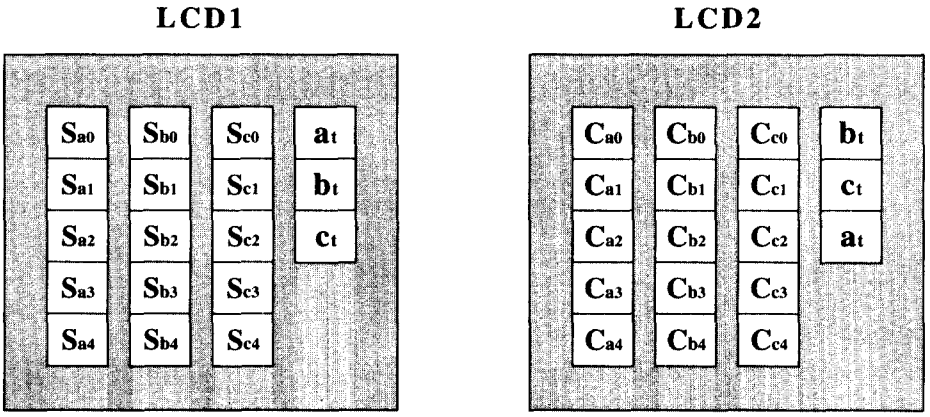


그림 11 벡터-벡터 곱을 위한 LCD 1과 LCD 2상의 벡터 표현

궤환 상수를 나타내는 벡터는 다음 식 (5)와 같이 각각 3개씩이 된다.

$$\begin{aligned} S^T_a &= [s_{a0}, s_{a1}, s_{a2}, s_{a3}, s_{a4}] \\ C_a &= [c_{a0}, c_{a1}, c_{a2}, c_{a3}, c_{a4}] \\ S^T_b &= [s_{b0}, s_{b1}, s_{b2}, s_{b3}, s_{b4}] \\ C_b &= [c_{b0}, c_{b1}, c_{b2}, c_{b3}, c_{b4}] \\ S^T_c &= [s_{c0}, s_{c1}, s_{c2}, s_{c3}, s_{c4}] \\ C_c &= [c_{c0}, c_{c1}, c_{c2}, c_{c3}, c_{c4}] \end{aligned} \quad (5)$$

식 (5)에 나타난 벡터중 3개의 벡터 S^T_a, S^T_b, S^T_c가 LCD 1상에 그림 11과 같이 표현이 되며 나머지 벡터 C_a, C_b, C_c가 LCD 2상에 표현이 된다. 또한 식 (3)에서 $s_t = a_t b_t \otimes b_t c_t \otimes c_t a_t$이므로 LCD 1상에는 그림 9와 같이 맨 오른쪽 벡터에 a_t, b_t, c_t차례로 배열이 되고 LCD 2상에는 b_t, c_t, a_t차례로 배열된다.

앞에서 설명하였듯이 벡터-벡터 곱에 의하여 LCD 1과 LCD 2상에 표현된 벡터가 서로 곱해지므로 LCD 1과 LCD 2간에 벡터-벡터 곱으로 나오는 것은 $C_a S^T_a$, $C_b S^T_b$, $C_c S^T_c$, $a_t b_t$, $b_t c_t$, $c_t a_t$ 등이며, 그 결과들은 Photo-Detector에 의하여 검출되어 계산된다.

그림 12는 본 논문에서 제안하는 Threshold 발생기를 위한 광학적 구현 시스템이다.

그림 12에서 S는 광원으로 레이저를 의미하고, CL은 Collimating Lens로 평행광을 만들며, BS 1과 BS 2는 빔 분할기, 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, LCD 3는 LCD 1과 LCD 2의 벡터-벡터 곱의 결과를 다시 표현하고, PDA 1은 LCD 1과 LCD 2의 벡터-벡터 곱의 결과를 검출하며, PDA 2는 RSPM의 결과를 검출하며, MA 1과 MA 2는 Mirror 어레이로 RSPM을 이용한 mod 2 덧셈 연산 계산을 위하여 반사 및 벡터 원소간 Shift에 이용되고, P1은 Polarizer로 수직 성분만을 통과 시키고, P2은 Analyzer로 수평 성분만을 통과시킨다.

그림 12는 앞절들에서 설명하였듯이 두개의 경로로 구성이 된다. 위쪽 부분은 벡터-벡터 곱에 사용이 되며 이 경로에서 검출된 값이 아래 경로의 입력 데이타로 사용이 되어 RSPM 방법에 의하여 내적 값의 mod 2연산을 수행하므로서 최종 이진 출력 수열이 생성되게 된다.

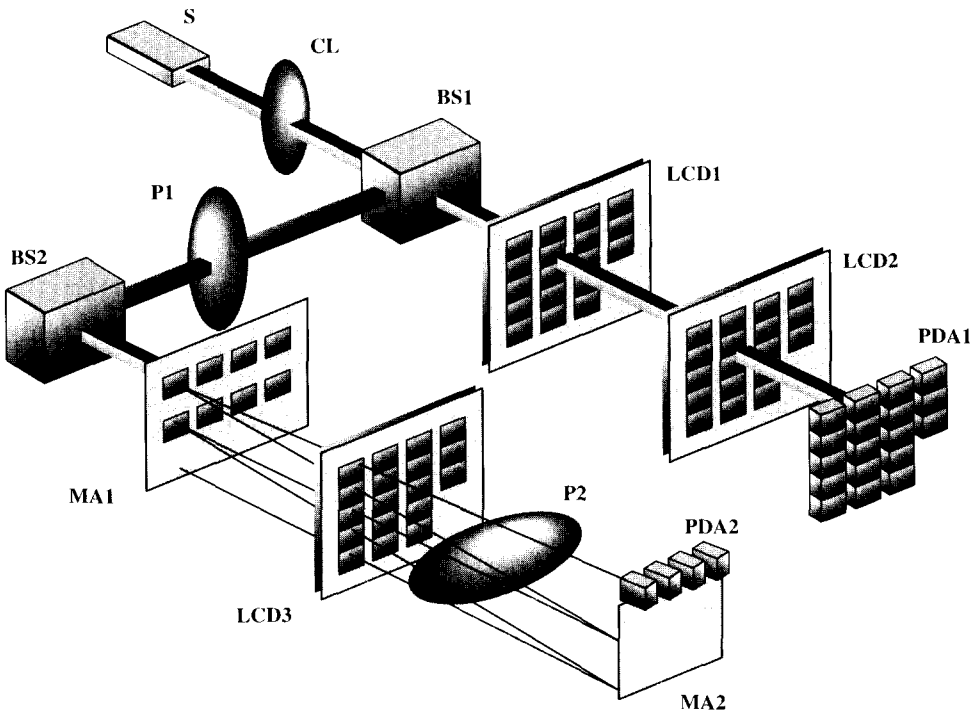


그림 12 Threshold 발생기를 위한 제안된 광학적 구현 시스템

LCD 1과 LCD 2에 표현된 벡터는 벡터-벡터 곱에 의하여 PDA 1에 의하여 검출되어 그 결과 값이 다시 LCD 3에 표현되며, 단 LCD 3에 벡터 어레이를 표현하는 경우 입사되는 광의 편광 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 $\mathbf{a}_t\mathbf{b}_t$, $\mathbf{b}_t\mathbf{c}_t$, $\mathbf{c}_t\mathbf{a}_t$으로서 XOR 연산에 사용이 된다. mod 2 덧셈 연산은 XOR 연산과 같으므로 LCD 3를 사용하여 구성한 RSPM 시스템은 앞 절의 설명과 같이 mod 2 덧셈 연산을 수행하여 식 (3)과 같은 최종 이진 수열을 생성하게 된다. 또한 벡터-벡터 곱의 결과로 발생된 새로운 벡터의 mod 2 덧셈 연산을 수행하여 Shift에 필요한 새로운 비트 값도 생성하게 된다.

BS 1과 BS 2를 통하여 아래 경로인 RSPM 시스템으로 입력되는 광은 MA 1인 Mirror 어레이 평면에 의하여 필터링되어 LCD 3상의 벡터 원소중 처음 원소로 가는 광만이 통과가 된다. 즉, 평면파 전체가 통과되는 것이 아니고 LCD 3상에 벡터 어레이중 각 벡터의 첫 원소 값으로 가는 광만을 통과시켜 이 광이 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 첨가하여 주어 실제로는 5×1 벡터가 되는 것이다.

편광기인 P1과 P2는 LCD 3를 사용한 RSPM 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 12는 광학 시스템만이 보여주었을 뿐 실제로는 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 값으로 암호화를 필요로 하는 장치로 최종 이진 출력 수열을 디지탈화하여 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 줄때는 한 비트씩 Shift하여야 한다.

본 논문에서 제안한 Threshold 발생기의 광학적 구현 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 Threshold 발생기뿐 아니라 스트림 암호 시스템에서 사용 가능한 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 고해상도의 소자들이 사용이 되고 계속 연구, 개발되고 있으므로 실제 높은 비도를 만족하기 위한 수백차 이상의 LFSR이 현재 개발된 소자로도 가능하며, 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.

6. 결 론

본 논문에서는 광 정보 처리 소자로서 각광을 받고 있는 LCD를 이용하여 기존의 디지탈적인 1차원 실현 방법이 아닌 새로운 광학을 이용한 2차원적인 실현 방법을 사용하여 스트림 암호 시스템에 사용하는 이진 수열 발생기 중에 하나인 Threshold 발생기를 실현하였다. 즉, m-LFSR을 LCD를 사용하여 표현을 하여 주고, Shadow Casting 기법을 사용하여 벡터

간 곱을 계산하며 LCD의 편광 특성을 이용하여 XOR 연산과 내적 값의 mod 2연산을 수행하게 하였다. LFSR을 구성하는 각 단의 값과 궤환 상수 값을 두개에 LCD에 어레이 형태로 표현, Shadow Casting 기법으로 서로 곱셈을 수행하게 한다. 또한 본 논문에서 제안한 내적 값 계산을 위한 mod 2 덧셈 연산인 광학적 RSPM은 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.

따라서, 본 논문에서는 제안한 광 Threshold 발생기는 기존의 디지탈 실현 방법에서 문제가 되는 Tapping Point의 개수에 대한 한계성을 극복할 수 있고, 1차원적인 실현 방법이 아닌 광학을 이용한 2차원적으로 시스템을 구성하는 새로운 방법을 제안하므로서 2차원 영상 암호 시스템으로의 확장 가능성을 보여 주었다.

본 논문에서 사용한 LCD의 경우 고 해상도 소자들에 대한 연구및 개발이 계속되고 있으므로 실제 높은 안전성을 만족하기 위한 수백차 이상의 LFSR이 현재 개발된 소자로도 가능하며, 또한 본 논문에서 의존한 검출 회로나 LCD Driver와 같은 전자적인 도움없이 완전한 광학만으로 시스템을 구성할 경우 광학의 고속성 및 병렬성의 특성으로 인하여 기존의 방법에서 문제가 되는 속도의 한계성 면을 해결할 수가 있겠다.

본 논문에서 제안한 광 Threshold 발생기는 가변이 가능한 LCD를 사용함으로 해서 언제든지 LFSR의 변화가 가능하고 Threshold 발생기뿐 아니라 다른 이진 수열 발생기로의 변형 등이 손쉽게 이루어 질 수가 있다.

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," Optical Engineering, Vol.28, No.8, pp.844-848, 1989.

[3] Mohammad A. Karim and Abdul S. Award, "Polarization-encoded optical shadow-casting logic units : design", Applied Optics, 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", Applied Optics, 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 optical shadow-casting scheme", Applied Optics, Vol.30, No.8, pp.936-942, 1991.

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

[7] 한종욱, "편광 인코딩을 이용한 암호화 방법", '95 한국통신정보보호학회 종합학술대회, Vol.5, No.1, pp.254 - 261, 1995.

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

[9] Altaf H. Khan and Umid R. Nejib, "Optical logic gates employing liquid crystal optical switches", Applied Optics, Vol.26, No.2, pp.270-273, 1987.

[10] 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", Optics Communication, Vol.115, pp.585-596, 1995.

□ 著者紹介

한 종 욱

1989년 광운대학교 전자공학과 졸업 (공학사)
1991년 광운대학교 전자공학과 졸업 (공학석사)
1991년 ~ 현재 한국전자통신연구원 선임연구원

※ 관심분야 : Optical Security, Quantum Cryptography, Optical Computing