論文94-31B-3-7

CCD에 의한 GF(p^m)상의 다치 승산기 구성에 관한 연구

(A Study on Construction of Multiple-Valued Multiplier over GF(p^m) using CCD)

黃 鍾 學*, 成 賢 慶**, 金 興 壽***

(Jong Hak Hwang, Hyeon Kyeong Seong and Heung Soo Kim)

要 約

본 논문에서는 유한체 GF(p^m)상에서 두 다항식의 승산 알고리즘을 제시하고, 이 제시된 승산 알고리즘을 이용하여 CCD에 의한 직렬 입-출력 모듈 구조의 다치 승산기를 구성하였다. 제시된 CCD 다치 승산기는 승산 연산부, MOD 연산부, 원시 기약 다항식 연산부로 구성하였다. 승산 연산부와 원시 기약 다항식 연산부는 CCD의 오버플로워 게이트, 금지 게이트와 mod(p) 가산기로 구성하였으며, MOD 연산부는 CCD의 가산 게이트, 오버플로워 게이트, 금지 게이트로 이루워진 2개의 mod(p) 가산기로 구성하였다. 본 논문에서 제시한 CCD 다치 승산기는 회선 경로 선택의 규칙성, 간단성, 셀배열에 의한 모듈성의 특징을 가지며, 차수 m이 증가하는 유한체상의 두 원소들의 승산에서 확장성을 가지므로 VLSI화 실현에 적합할 것이다.

Abstract

In this paper, the multiplicative algorithm of two polynomials over finite field GF(p^m) is presented. Using the presented algorithm, the multiple-valued multiplier of the serial input-output modular structure by CCD is constructed. This multiple-valued multiplier on CCD is consisted of three operation units: the multiplicative operation unit, the modular operation unit, and the primitive irreducible polynomial operation unit. The multiplicative operation unit and the primitive irreducible operation unit are composed of the overflow gate, the inhibit gate and mod(p) adder on CCD. The modular operation unit is constructed by two mod(p) adders which are composed of the addition gate, the overflow gate and the inhibit gate on CCD. The multiple-valued multiplier on CCD presented here, is simple and regular for wire routing and possesses the property of modularity. Also, it is expansible for the multiplication of two elements on finite field increasing the degree m and suitable for VLSI implementation.

* 正會員, 那宇精密 中央研究所
(Central Research Institue of Now Precision)
** 正會員, 尙志大學校 電子計算學科
(Dept. of Computer Science Sangji Univ.)
*** 正會員, 仁荷大學校 電子工學科
(Dept. of Elec. Eng., Inha Univ.)
接受日字 : 1993年 4月 1日

Ⅰ. 서 론

유한체(Galois field)는 스위칭 이론, 오진 정정 부호, 디지탈 신호 처리 및 화상 처리, 디지탈 통신의 암호화 및 해독화를 요하는 보안 통신등에 많이 응용되고 있다. 특히, GF(2^m)은 신호 처리와 화상 처리 분야에서 특별한 계산을 요하거나 범용 컴퓨터 계산의 고속화를 보조하는 고성능 전용 컴퓨터의 설계에 효과적이며, VLSI 설계에 응용되고 있다. [1-3]

유한체 GF(p^m)(단 p≥3)상의 승산 알고리즘은 GF(2^m)상의 승산 알고리즘에 비하여 단자당 높은 함수 기능 및 고밀도 실현의 장점을 가지고 있다. 현재의 2진 논리를 수행하는 집적회로는 그동안 많은 발전을 이루어 왔지만 아직도 단자수 제한문제, 단자간 상호 연결문제, 보다 많은 정보처리 문제등의 해결방안이 필요한 실정이다. 이러한 면에서 다치 논리 이론의 연구가 대두되었고, 지난 수 년간의 연구에 의해서 이 방면에 많은 발전을 이루어 왔다. 그 중에서도 유한체는 2진 논리를 수행하는 부울체의 확장이라는 점에서 다치 논리 이론의 주관심 분야가 되었다. [4-6]

유한체상에서 가산과 승산은 관용 2진 산술 연산과는 현저하게 다르므로 실제적으로 유용성과 단순성에 기인하여 유한체에 관한 연구가 활발히 진행되고 있다. 유한체상의 가산은 직접적이고 비트 독립적인 mod(p) 연산으로 관용 2진 가산보다 쉬운 반면 승산은 관용 2진 승산 보다 어렵고 복잡한 계산을 요한다. [7,8]

VLSI 설계에서 모듈 구조와 규칙적 상호연결이 중요한 설계 객체이다. 유한체상의 승산을 위한 알고리즘이 지난 십 수년간 제안되어 왔으나 불행하게도 이들 알고리즘은 불규칙한 회선 경로 선택, 복잡한 제어 문제, 비모듈화 구조 및 병발성의 부족 때문에 VSLI 구조의 설계에 부적합하였다. [9,10]

최근 Yeh 등[2]은 표준 기저 표현식을 사용하여 유한체상의 승산을 실현하는 직렬입력/직렬 출력 시스토릭 배열 구조와 병렬 입력/병렬 출력 시스토릭 배열 구조의 승산기를 개발하였다. Scott 등[5]은 표준 기저로 표현된 각 원소들의 유한체 승산을 실행하는 고속 승산기를 제시하였고, Wang 등[10]은 Scott 등이 제안한 유한체상의 승산 알고리즘을 이용하여 시스토릭 배열의 승산기를 제시하였다. 그러나 이들이 제시한 승산기는 GF(2^m)인 2진 회로의 승산으로 제한되어 설계되었다.

본 논문에서는 Scott 등이 제시한 GF(2^m)상의 승산 알고리즘을 유한체 GF(p^m)(단 p≥3)상의 승산 알고리즘으로 확장하여 CCD에 의한 두 원소들의 승산을 실현하는 직렬 입-출력 모듈 구조의 다치 승산기를 제시하였다. 이 다치 승산기의 기본셀은 승산 연산부, MOD 연산부, 원시 기약 다항식 연산부로 구성된다. MOD 연산부는 CCD의 기본 게이트인 오버플로워 게이트, 금지 게이트, 가산 게이트로 구성하며, 승산 연산부는 오버플로워 게이트, 금지 게이트, mod(p) 가산기로 구성한다. 원시 기약 다항식 연산부는 오버플로워 게이트, 금지 게이트와 mod(p) 가산기로 이루어져 있다. 그리고 승산 계수를 입력하기 위하여 플립-플롭 회로를 사용하였고, 피승산 계수와 원시 기약 다항식 계수를 입력하기 위하여 레지스터를, 최종 승산 결과를 얻기 위하여 출력 천이 레지스터(OSR; output shift register)를 사용하였다.

Ⅱ. 유한체의 승산 알고리즘과 CCD 기본 게이트

1. 유한체의 승산 알고리즘 [5,10,11]

유한체 GF(p^m)은 p가 素數이고 m이 양의 정수인 p^m개의 원소들을 가지며 p개의 원소들을 갖는 기초체 GF(p)의 확대체이다. 유한체 GF(p^m)는 {0, 1, 2, …., p-1}의 원소들로 구성된다. GF(p^m)에서 모든 산술 연산은 mod(p) 연산으로 이루지며, GF(p^m)의 0이 아닌 모든 원소들은 원시 원소 α 에 의해 생성된다.

유한체 GF(p^m)상에서 피승산 다항식을 A(x), 승산 다항식을 B(x), 원시 기약 다항식을 F(x)라 하고, 다음과 같이 전개하여 표현할 수 있다.

$$A(x) = a_{m-1} \cdot x^{m-1} + \cdots\cdots + a_1 \cdot x + a_0 \quad (1)$$

$$B(x) = b_{m-1} \cdot x^{m-1} + \cdots\cdots + b_1 \cdot x + b_0 \quad (2)$$

$$F(x) = x^m + f_{m-1} \cdot x^{m-1} + \cdots\cdots + f_1 \cdot x + f_0 \quad (3)$$

여기서 F(x)는 최고 차수가 m이고 계수 f_m = 1인 모닉 다항식이고, 계수 a_i, b_i, f_i는 {0, 1, 2, …., p-1}의 값을 갖는다.

두 다항식 A(x)와 B(x)의 승산 알고리즘은 이들 다항식의 계수들을 곱하여 mod F(x) 연산을 수행하므로 구할 수 있으며 다음과 같다.

$$\begin{aligned} C(x) &= \{A(x) \cdot B(x)\} \bmod F(x) \\ &= A(x) \cdot \{b_{m-1} \cdot x^{m-1} + \cdots + b_1 \cdot x + b_0\} \bmod F(x) \\ &= \{A(x)b_{m-1} \cdot x^{m-1} + \cdots + A(x)b_1 \cdot x + A(x)b_0\} \bmod F(x) \\ &= c_{m-1} \cdot x_{m-1} + \cdots\cdots + c_1 \cdot x + c_0 \end{aligned} \quad (4)$$

여기서 C(x)는 승산 결과 다항식이다.

식 (4)에서 첫번째 항 $A(x)b_{m-1}\cdot x^{m-1}$를 $K_1(x)$로 놓으면 다음과 같다.

$$\begin{aligned} K_1(x) &= \left[A(x)b_{m-1}\cdot x^{m-1}\right] \bmod F(x) \\ &= \left[\{A(x)b_{m-1}\cdot x\}x^{m-2}\right] \bmod F(x) \\ &= \left[C_1(x)\cdot x^{m-2}\right] \bmod F(x) \end{aligned} \quad (5)$$

여기서 $C_1(x) = \{A(x)b_{m-1}\cdot x\} \bmod F(x)$ 이다.

식 (4)에서 첫번째 항과 두번째 항을 더하여 $K_2(x)$로 놓으면 다음과 같다.

$$\begin{aligned} K_2(x) &= \left[K_1(x) + A(x)b_{m-2}\cdot x^{m-2}\right] \bmod F(x) \\ &= \left[\{C_1(x) + A(x)b_{m-2}\}x^{m-2}\right] \bmod F(x) \\ &= \left[\{(C_1(x) + A(x)b_{m-2})\cdot x\}x^{m-3}\right] \bmod F(x) \end{aligned} \quad (6)$$

여기서 $C_2(x) = \left[\{(C_1(x) + A(x)b_{m-2})\cdot x\}\right] \bmod F(x)$ 이다.

이와 같은 방법으로 $K_{m-1}(x)$을 구하면 다음과 같다.

$$\begin{aligned} K_{m-1}(x) &= \left[K_{m-2}(x) + A(x)b_1\cdot x\right] \bmod F(x) \\ &= \left[\{C_{m-2}(x) + A(x)b_1\}x\right] \bmod F(x) \\ &= C_{m-1}(x) \end{aligned} \quad (7)$$

여기서 $C_{m-1}(x) = \left[\{C_{m-2}(x) + A(x)b_1\}\cdot x\right] \bmod F(x)$ 이다.

마지막으로 $K_m(x)$을 구하면 다음과 같다.

$$\begin{aligned} K_m(x) &= \left[K_{m-1}(x) + A(x)b_0\right] \bmod F(x) \\ &= \left[C_{m-1}(x) + A(x)b_0\right] \bmod F(x) \\ &= C_m(x) \\ &= c_{m-1}\cdot x^{m-1} + \cdots\cdots + c_1\cdot x + c_0 \end{aligned} \quad (8)$$

식 (8)이 $\{A(x)\cdot B(x)\} \bmod F(x)$ 연산 후의 승산 결과 다항식이다.

앞에서 논한 $GF(p^m)$상의 피승산 다항식 A(x)와 승산 다항식 B(x)의 승산 알고리즘을 단계별로 설명하면 다음과 같다. 여기서 식 (4)의 x^{m-1}항의 계수를 최상위 비트인 MSB(C)로 나타낸다.

[단계 1] 원시 기약 다항식 F(x), 피승산 다항식 A(x), 승산 다항식 B(x)의 계수들을 선택한다.

[단계 2] 승산 결과 다항식 C(x)의 LSB(c_0)를 0으로 초기화 한다.

[단계 3] 승산 다항식 B(x)의 최고 차수 계수인 b_{m-1}부터 b_0까지 한 비트씩 차례로 입력한다.

[단계 4] 피승산 다항식 A(x)의 계수들은 [단계 3] 에서 입력된 승산 다항식 B(x)의 계수에 의하여 $\{A(x) * b_i\}$와 같이 승산되고 이 승산 결과를 mod(p) 연산한다. 여기서 i는 B(x)의 i번째 계수이며, $i \in \{m-1, m-2, \cdots, 1, 0\}$이다.

[단계 5] 원시 기약 다항식 F(x)는 승산 결과 다항식의 최고 차수 계수인 MSB(C)의 값에 의하여 $F(x) * \{p-MSB(C)\}$와 같이 되고 이 승산 결과를 mod(p) 연산한다. $\{p-MSB(C)\}$를 하는 이유는 [단계 6] 에서 $C_{i+1}(x)$를 한 차수 높일 경우 차수를 높인 만큼 원시 기약 다항식 처리를 하여야 하기 때문이다.

[단계 6] [단계 4] 와 [단계 5] 에서 연산한 결과와 승산 결과 다항식 C(x)를 가산한다. 이결과는 승산 결과 다항식 $C_{i+1}(x)$가 되며 $C_{i+1}(x)$를 한 차수 높인 다음에 [단계 3] 을 반복 실행한다. 여기서 $C_{i+1}(x)$를 한 차수 높이는 이유는 [단계 3] 에서 입력되는 B(x)의 계수인 b_{i-1}과 차수를 동일한 형태로 만들기 위한 것이다. [단계 3] 에서 B(x)의 계수가 b_0일 때는 연산이 끝나므로 $C_{i+1}(x)$의 차수를 높이지 않고 승산 결과 다항식인 $C_{i+1}(x)$를 출력한다.

Scott 등이 제시한 알고리즘은 $GF(2^m)$으로 제한성을 가지며, 다항식의 계수가 0과 1만으로 처리된다. 그러나 본 논문에서 제시된 알고리즘은 유한체 GF(pm)상으로 확장하여 처리하며 다항식의 계수가 {0, 1, 2, ···, p-1}의 값을 갖는다. 본 논문에서 제시한 $GF(p^m)$의 승산 알고리즘을 C 언어로 표현하면 다음과 같다.

```
FiniteProduct (int A, int B, int F, int m, int p)
{
   extern i, C, MSB;
   C = 0;
   i = m - 1;

   while ( i >= 0 )
   {
      MSB = C;
      if (B == 0)
         MultiplierZero (MSB);
      else
         MultiplierNonzero ( MSB );
   }
   i = i - 1;
}
```

```
/* 승산 계수가 0이면 계산하는 함수 */
MultiplierZero (int MSB)
{
   if ( MSB == 0 )
      C = C % p;
   else {
      F = F * (p - MSB);
      C = (C + F) % p;
      }
}
/* 승산 계수가 0이 아니면 계산하는 함수 */
MulitplierNonzero ( int MSB)
{
   A = A * B;
   if ( MSB == 0 )
      C = (C + A) % p;
   else {
      F = F * (p - MSB);
      C = (C + F + A) % p;
}
```

2. CCD 기본 게이트[8,12,13]

논리값으로 표현되는 축적된 전하를 전달하는 CCD(charge coupled device)는 저전력 소비, 높은 집적 밀도와 VLSI 실현에 적합한 MOS와 호환성을 갖는 이점을 가지고 있다. CCD는 전하를 전압 또는 전류 변환하기가 용이하고 전압이나 전류를 전하로 변환하기가 쉽다. 그러므로 CCD가 여러 분야에서 다양하게 응용되고 있다.[8,12,13]

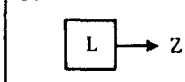
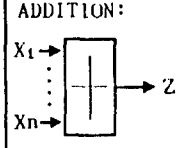
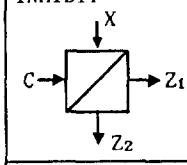
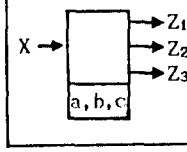
기 호	논 리 함 수	비용인수
CONSTANT: 	Z = L L = 1,2,...,p-1	1
ADDITION: 	$Z = \sum_{i=1}^{n} X_i$	2n-2
INHIBIT: 	Z1 = X if C>0 = 0 otherwise Z2 = X if C=0 = 0 otherwise	6 if X≤2 18 if X>2
OVERFLOW: 	Z1 = min(X,a) Z2 = min(X-a,b) Z3 = min(X-a-b,c)	4

그림 1. CCD의 기본 게이트
Fig. 1. The basic gates on CCD.

Butler와 Kerkhoff[12]는 이중 폴리실리콘 10μm nMOS 기술을 이용하여 P형 실리콘의 IC 기판위에 불순물을 첨가한 산화 실리콘층을 확장 영역으로 하고, 불순물이 첨가되지 않은 산화 실리콘층을 절연체로 한 다치 논리 (multi-valued logic:MVL) CCD의 기본 게이트들을 실현하였다. 이들은 상수 게이트가 칩상에서 가장 적은 면적으로 구성됨을 발견하였으며, 소비되는 칩면적을 기초로하여 게이트의 활성 영역, 제조 공정 파라메타의 내구성, 필요한 공급 라인수를 고려하여 각 게이트에 대한 비용인수를 할당하였다.

그림 1은 상수, 오버플로워, 금지, 가산의 4가지 CCD 기본 게이트들을 나타낸다. 그림 1의 각 열은 각 게이트에 대한 기호, 실현하는 논리 함수식, 게이트의 상대 비용인수를 나타낸다.

Ⅲ. CCD에 의한 다치 승산기 구성

이 장에서는 앞장에서 논한 유한체 GF(p^m)상에서 두 다항식간의 승산 알고리즘을 고속으로 실행하는 CCD에 의한 직렬 입-출력 모듈 구조의 다치 승산기를 그림 2와 같이 구성하였다. 이 다치 승산기는 GF(p^m)상의 두 다항식의 승산을 실행하는 승산 연산부, 임의의 주어진 원시 기약 다항식에 의해 연산을 실행하는 원시 기약 다항식 연산부, 승산 연산부의 출력과 원시 기약 다항식 연산부의 출력에 대하여 mod (p) 연산을 수행하는 MOD 연산부로 구성하였다. 그림 2에서 피승산 다항식 A(x)와 원시 기약 다항식 F(x)의 계수들 a_i와 f_i가 직렬로 각각의 레지스터들로 이동하며 입력된다. 여기서 원시 기약 다항식 F(x)의 차수가 승산 결과 다항식 C(x)의 차수보다 한 차수 높기 때문에 C(x)와 F(x)의 차수를 동일한 형태로 만들기 위해서 F(x)의 최상위 비트는 계산에 사용하지 않는다.

그림 2의 셀 L_i의 내부 구조는 그림 3과 같다. 이 셀 L_i는 두 다항식 A(x)와 B(x)의 계수들을 승산하는 승산 연산부, MSB(C)와 원시 기약 다항식 F(x)의 계수를 연산하는 원시 기약 다항식 연산부, 이들 각각의 출력과 전단에서 입력된 승산 결과 다항식의 계수 c_i를 mod(p) 연산하는 MOD 연산부로 구성한

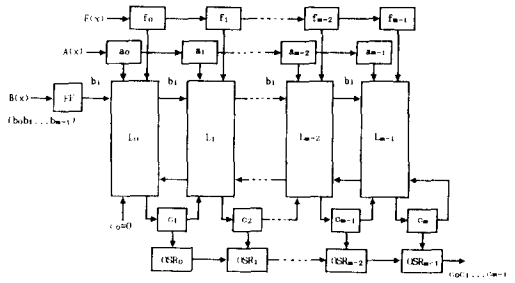


그림 2. GF(p^m)상의 CCD 다치 승산기
Fig. 2. The CCD multiple-valued multiplier on GF(p^m).

다. 셀 L_i의 내부 구조(그림 3)에서 승산 연산부는 플립-플롭 회로에 입력된 승산 다항식 B(x)의 계수 b_i와 피승산 다항식 A(x)의 계수 ai를 {$a_i * b_i$}한 후 MOD 연산부에 가해진다. 원시 기약 다항식 연산부는 승산 결과 다항식 C(x)의 최상위 비트 MSB(C)의 값과 원시 기약 다항식 F(x)의 계수 f_i를 {p-MSB(C)} * f_i 하여 MOD 연산부의 입력으로 가해진다. MOD 연산부는 전단의 승산 결과 다항식 C(x)의 계수 c_i와 승산 연산부 출력과 원시 기약 다항식 연산부 출력을 mod(p) 연산하며, MOD 연산부의 출력 c_{i+1}은 c_i+($a_i * b_i$)+ [{p-MSB(C)} * f_i] 가 된다. 그림 2에서 셀 L_i의 출력은 승산 결과 레지스터 c_{i+1}로 이동하고 셀 L_{i+1}의 입력으로 사용된다. 승산이 완전히 이루어졌을 때 최종 승산결과는 출력 천이 레지스터(OSR)에 전달되고 직렬로 연속 출력된다.

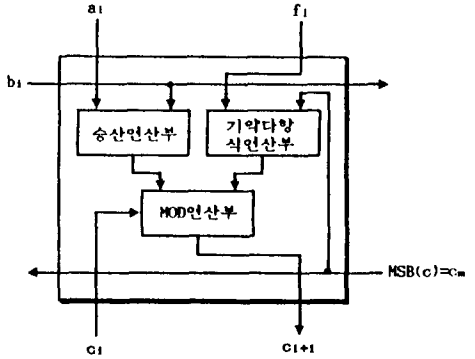


그림 3. 셀 L_i의 구조
Fig. 3. The structure of cell L_i.

그림 4는 CCD에 의한 mod(p) 가산기의 회로도 및 기호이다. 그림 4의 mod(p) 가산기에서 X 입력 {0,1,2,…,p-1}의 한 값과 Y 입력 {0,1,2,…,p-1}의 한 값이 가산 게이트에 의해 합해지며, 가산 게이트 출력은 {0,1,2,…,2p-2}의 한 값이 된다. 이 값은

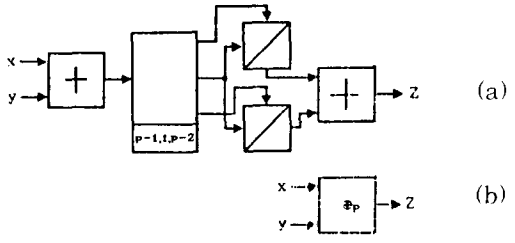


그림 4. mod(p) 가산기: (a) 회로, (b) 기호
Fig. 4. The mod(p) adder: (a) circuit, (b) symbol.

오버플로워 게이트의 입력으로 오버플로워 게이트의 첫번째 출력은 {0,1,2,…,p-1}의 한 값이고, 두번째 출력은 {0,1}중 한 값이고 세번째 출력은 {0,1,2,…,p-2}의 한 값이 된다. 오버플로워 게이트의 두번째 출력은 금지 게이트를 동작시킨다. 오버플로워 게이트 두번째 출력이 0일 경우 그림 4의 상단 금지 게이트는 {0,1,2,…,p-1}의 한 값이고, 하단 금지 게이트는 {0,0,…,0}의 한 값이 출력되어 이들 값이 다음 단의 가산 게이트 입력으로 되고 출력은 {0,1,2,…,p-1}의 한 값이 된다. 또한 오버플로워 게이트의 출력이 1일 경우 상단 금지 게이트는 {0,0,0,…,0}의 한 값이고 하단 금지 게이트는 {0,1,2,…,p-2}의 한 값이 출력된다. 이들 값이 다음 단의 가산 게이트 입력으로 되고 {0,1,2,…,p-2}의 한 값을 갖는다. 그러므로 출력 Z은 X와 Y의 합을 mod(p)한 Z=(X+Y) mod(p)를 수행한다.

1. 원시 기약 다항식 연산부

그림 5는 원시 기약 다항식 연산부의 회로이며 CCD의 오버플로워 게이트, 금지 게이트와 mod(p) 가산기로 구성하였다. 그림 5에서 승산결과의 최상위 비트 MSB(C)가 0인 경우 가장 아래에 있는 금지 게이트에 의하여 출력이 0이 되며, 그 외의 경우는 {p-MSB(C)}가 된다. {p-MSB(C)}한 값을 원시 기약 다항식 F(x)의 계수에 의하여 {f_i * [p-MSB(C)] } 된 후 mod(p) 연산되어 출력된다. MSB(C)가 1인 경우 가장 위에 있는 금지 게이트는 원시 기약 다항식 F(x)의 계수 fi가 출력되고 위에서 두번째 금지 게이트는 앞단의 오버플로워 게이트에 의하여 0이 출력되므로 fi가 출력된다. 세번째 금지 게이트도 두번째 금지 게이트와 동일한 수행을 하며 그 이하의 모든 금지 게이트도 두번째 금지 게이트와 동일한 수행을 한다. 따라서 MSB(C)가 1일 때는 {f_i * (p-1)} mod(p) 연산을 행하며, MSB(C)가 2일 때는 {f_i * (p-2)}mod(p) 연산을 행한다. 이와 같은 방법으로

MSB(C)가 p-1일 때는 {f * (2p-1)}mod(p) 연산을 행한다.

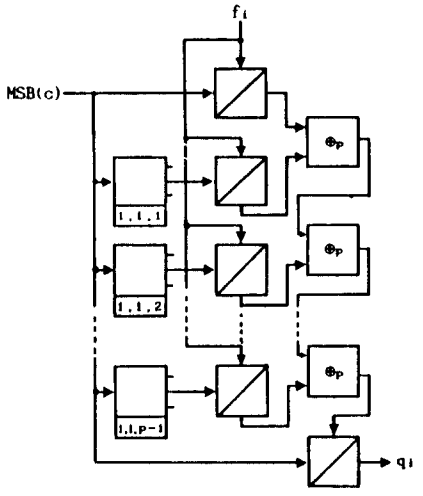


그림 5. 원시 기약 다항식 연산부
Fig. 5. The primitive irreducible operation unit.

2. 승산 연산부

GF(p^m)상에서 두 다항식 계수들의 승산을 실행하는 승산 연산부는 CCD의 오버플로워 게이트, 금지 게이트 및 mod(p) 가산기로 구성된다. 그림 6은 승산 연산부의 회로이다. 그림 6의 승산 연산부는 피승산 다항식 A(x)의 계수 a_i와 승산 다항식 B(x)의 계수 bi를 $\{a_i * b_i\}$mod(p) 연산하여 출력한다. 승산 다항식의 계수가 0인 경우는 가장 아래에 있는 금지 게이트에 의하여 0을 출력한다. 승산 다항식의 계수가 1인 경우 가장 위에 있는 금지 게이트는 피승산 다항식의 계수 a_i를 출력하고 위에서 두번째의 금지 게이트는 앞단의 오버플로워 게이트에 의하여 0을 출력한다. 세번째 금지 게이트도 두번째 금지 게이트와 동일한 연산을 수행하여 0을 출력한다. 그 이하의 모든 금지 게이트들은 두번째 금지 게이트와 동일한 연산을 수행한다.

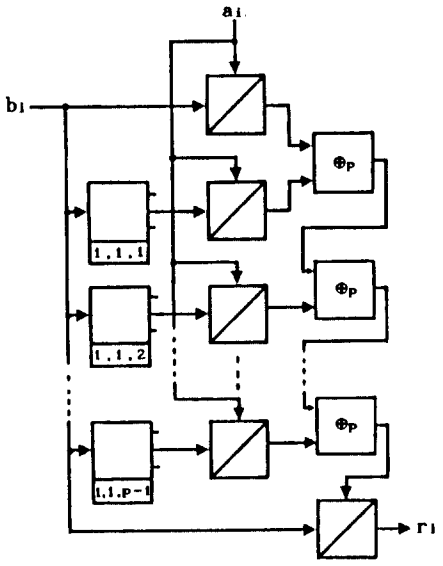


그림 6. 승산 연산부
Fig. 6. The multiplicative operation unit.

따라서 승산 다항식의 계수가 1인 경우 $\{a_i * 1\}$ mod(p) 연산을 행하고, 승산 다항식의 계수가 2인 경우 $\{a_i * 2\}$mod(p) 연산을 행한다. 이와 같은 방법으로 승산 다항식의 계수가 p-1인 경우 $\{a_i * (p-1)\}$ mod(p) 연산을 행한다.

3. MOD 연산부

원시 기약 다항식 연산부의 출력(Qi), 승산 연산부의 출력(Ri)과 승산 결과(Ci)를 입력으로 하는 MOD 연산부는 2개의 mod(p) 가산기를 사용하여 그림 7과 같이 구성하였다. MOD 연산부는 원시 기약 다항식 연산부의 출력과 승산 결과를 mod(p) 연산한 결과와 승산 연산부의 출력과 mod(p) 연산을 행한다.

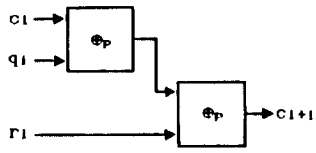


그림 7. MOD 연산부
Fig. 7. The modularity operation unit.

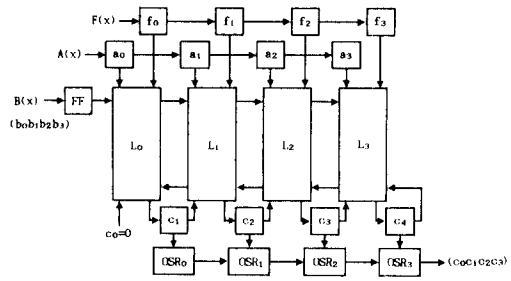


그림 8. GF(P^l)상의 CCD 다치 승산기
Fig. 8. The CCD multiple-valued multiplier on GF(P^l).

앞에서 논한 승산 알고리즘을 이용하여 CCD에 의한 GF(p^1)상의 다치 승산기를 구성하면 그림 8과 같다. GF(P^1)상의 승산기는 m=4이므로 셀 L_i와 피승산 다항식 레지스터, 원시 기약 다항식 레지스터, 승산결과 레지스터, 출력 천이 레지스터가 각각 4개씩 사용된다.

Ⅳ. 비교 및 검토

이 장에서는 CCD에 의한 GF(p^m)상의 다치 승산기를 타 연구의 승산기들과 비교하였으며, 비교표가 표 1과 같다. 비교된 승산기들은 주로 CMOS에 의해 설계되었고 GF(2^m)으로 제한성을 가지며, 다항식의 계수가 0과 1만을 처리한다. 그러나 본 연구에서 제시한 GF(p^m)상의 다치 승산기는 일반성을 가지며, 다항식의 계수가 {0, 1, …, p-1}의 논리값을 갖는다. 타 연구의 승산기들과 본 논문에서 제시한 CCD에 의한 다치 승산기를 각 게이트별로 비교하면 다음과 같다. 여기서 비교된 게이트들은 CMOS에 의한 게이트의 구조와 CCD에 의한 게이트의 구조가 차이가 있으므로 기본 게이트가 같다고 가정하였으며, 클럭 시간과 전달 지연 시간도 단일 게이트에 전달되는 시간이 같다 가정하여 단위 시간으로 계산하였다.

1) 금지 게이트(AND 게이트): Yeh[2]의 연구는 $2m^2$의 소자수가 필요하고 Wang[10]의 연구도 $2m^2$의 소자수를 요한다. 본 논문에서는 GF(p^m)에서 p=2인 경우 CCD의 금지 게이트가 AND 게이트로 동작하므로 2m개의 소자수가 필요하다. p≥3인 경우 2mp의 소자수가 요구되며 타 연구에 비하여 금지 게이트가 줄어드는 장점이 있다.

2) mod(p) 가산기(XOR 게이트): Yeh의 연구는 1-D 시스토릭 구조인 경우 2m의 소자수를 요구하며, Wang의 연구는 2m의 소자수를 요구한다. 반면 본 논문의 다치 승산기는 p=2인 경우 mod(p) 가산기가 XOR 게이트로 동작하므로 2m의 소자수가 필요하다. p 3인 경우 2m(p-1)의 소자수를 요구한다.

3) 오버플로워 게이트: 타 연구에서는 필요하지 않다. 본 논문에서는 p=2인 경우 오버플로워 게이트를 요구하지 않으며 p≥3인 경우만 2m(p-2)의 소자수를 요구한다.

4) 레지스터: Yeh의 연구는 2-D 시스토릭 구조인 경우 $7m^2+16$의 소자수가 필요하며, Wang의 연구는 $7m^2$의 소자수가 필요하다. 본 논문에서는 2치 논리와 3치 논리 이상인 경우에 관계없이 레지스터를 4m+1개 요구하는 장점이 있다.

5) 클럭시간: Yeh와 Wang의 연구는 3m의 단위 시간이 필요하다. 본 논문에서는 p=2, p≥3인 경우 피승산 다항식의 계수 a_i와 원시 기약 다항식의 계수 f_i가 이미 레지스터에 입력되었다고 가정하면 m 단위시간이 요구되므로 연산 시간이 줄어드는 장점이 있다.

또한, 제안된 GF(P^m)상의 CCD 다치 승산기는 회로 설계시 차수 m이 증가함에 따라 기본셀을 부가하므로 설계가 용이한 모듈성과 회로 소자수가 m에 비례하여 증가하는 규칙성을 가지므로 VLSI 실현에 적합할 것으로 사료된다.

표 1. CCD 다치 승산기의 성질

Table 1. Some properties of the CCD multiple-valued multiplier.

비교 항목	Yeh[2]		Wang[10]		Scott[5]	본 논 문	
	1-D	2-D	1-D	2-D		p≥3	p=2
금지회로 (AND)	3m	$2m^2$	3m	$2m^2$	-	2mp	2m
mod(p)가산기 (XOR)	2m	$2m^2$	2m	$2m^2$	2m	2m(p-1)	2m
오버플로워	-	-	-	-	-	2m(p-2)	-
레지스터	10m+2	$7m^2+16$	9m	$7m^2$	4m+1	4m+1	4m+1
인버터	-	-	-	-	2	-	-
스위치	m	-	-	-	8m	-	-
클럭시간	3m	3m	3m	3m	m	m	m

Ⅴ. 결 론

본 논문에서는 GF(p^m)상에서 두 다항식의 승산 알고리즘을 제시하였고, CCD에 의한 GF(p^m)상의 두 다항식의 승산을 실현하는 직렬 입-출력 모듈 구조의 다치 승산기를 제시하였다. 제시된 CCD 다치 승산기는 승산 연산부, MOD 연산부, 원시 기약 다항식 연산부로 구성하였다. 승산 연산부는 CCD에 의한 오버플로워 게이트, 금지 게이트와 mod(p) 가산기로 구성하였다. MOD 연산부는 2개의 mod(p) 가산기로 구성하였으며, mod(p) 가산기는 CCD의 금지 게이트, 가산 게이트, 오버플로워 게이트로 구성하였다. 원시 기약 다항식 연산부는 금지 게이트, 오버플로워 게이트와 mod(p) 가산기를 사용하여 구성하였다.

본 논문에서 제시한 CCD에 의한 GF(p^m)상의 다치 승산기에서 CCD의 금지 게이트는 GF(2^m)상에서는 AND 게이트로 동작하고, mod(p) 가산기는 XOR 게이트로 동작하므로 2치 논리 회로 및 다치 논리 회로에서 호환성을 갖는 장점이 있다. 또한 제시된 CCD의 다치 승산기의 동작 시간은 피승산 다항식의 계수들과 원시 기약 다항식의 계수들이 각 레지스터들에 이미 입력되었다고 가정하면 m 단위시간이 소요되므로 고속의 승산을 행하는 장점이 있다.

본 논문에서 제시한 CCD의 다치 승산기는 회선 경로 선택의 규칙성, 간단성, 셀배열에 의한 모듈성의 이점을 가지며 특히 차수 m이 증가하는 유한체의 두 다항식의 승산에서 확장성을 가지므로 VLSI화 실현에 적합할 것으로 사료된다.

參 考 文 獻

[1] H.M.Shao, T.K.Truong, L.J.Deutsch, J.H.Yaeh and I.S.Reed, "A VLSI design of a pipeling Reed-Solomon decoder," *IEEE Trans.* Comput., vol.C-34, pp.393-403, May 1985.

[2] C.S. Yeh, I.S. Reed and T.K. Truong, "Systolic multipliers for finite field GF (2m)," *IEEE Trans.* Comput., vol.C-33, pp.357-360, Apr. 1984.

[3] C.C. Wang, T.K. Truong, H.M. Shao, L.J. Deutsch, J.K. Omura and I.S. Reed, "VLSI architecture for computing multiplications and inverses in GF (2m)," *IEEE Trans.* Comput., vol.C-34, pp.709-717, Aug. 1985.

[4] K.C.Smith, "The prospect for multivalued logic:A technology and applications view," IEEE Trans. Comput.,vol.C-30, pp.619-634, Sept. 1981.

[5] S.L. Hurst, "Multiple-valued logic-its future," *IEEE Trans.* Comput., vol. C-33, pp.1161-1179, Dec. 1984.

[6] J.T. Butler, "Multiple-valued logic in VLSI", *IEEE Computer Soc.* Press, 1991.

[7] H.K.Seong and H.S.KIM, "A construction of celluar array multiplier over GF (2m)," KITE, vol.26, no.4, pp.81-87, April 1989.

[8] P.A. Scott, S.E. Tarvares and L.E. Peppard, "A fast VLSI multiplier for GF (2^m)," *IEEE J. Select.* Areas Common., vol. SAC-4, Jan. 1986.

[9] S. Bandyopadhyay and A. Sengupta, "Algorithms for multiplication in Galois field for implementation using systolic arrays", *IEE Proc.*, vol.135, Pt.E, no. 6, pp.336-339, Nov. 1988.

[10] C.L. Wang and J.L. Lin, "Systolic array implementation of multipliers for finite fields GF(2^m)", *IEEE Trans.* Circuits and Systems, vol.38, no.7, July 1991.

[11] R.Lidl, H.Niederreiter and P.M. Cohn, "Finite fields," Reading, MA, Addison-Wesley, 1983.

[12] J.T.Butler and H.G.Kerkhoff, "Multiple-valued CCD circuits," *IEEE. Comput.*, pp.58-67, Apr.1988.

[13] M.H. Abd-El-Barr and Z.G. Vranesic, "Cost reduction in the CCD Realization of MVMT functions", *IEEE Trans.* Comput., vol.C-39, no.5, May 1990.

著 者 紹 介

黃 鍾 學(正會員)

1964年 6月 12日生. 1988年 2月 인하대학교 전자공학과 졸업(공학사). 1990年 2月 인하대학교 대학원 전자공학과 졸업(공학석사). 1990年 2月 ~ 1991年 2月 필코주식회사 연구소 연구원. 1992年 3月 ~ 현재 나우정밀주식회사 중앙연구소 전임 연구원. 주관심 분야는 다치논리 회로설계, ASIC, ISDN 등임.

金 興 壽(正會員) 第 31卷 B編 第 1號 參照
현재 인하대학교 전자공학과 교수

成 賢 慶(正會員)

1955年 12月 21日生. 1982年 2月 인하대학교 전자공학과 졸업(공학사). 1984年 2월 인하대학교 대학원 전자공학과 졸업(공학석사). 1991年 2月 인하대학교 대학원 전자공학과 졸업(공학박사). 1989年 3月 ~ 1991年 11月 부천전문대학 전자계산과 조교수. 1991年 12月 ~ 현재 상지대학교 전자계산학과 전임강사. 주관심 분야는 다치논리 회로설계, 컴퓨터 구조설계 및 VLSI 설계, 퍼지논리 회로설계, 디지탈 신호처리 등임.