論文 90-27-5-13

GF(3^m)上의 乘算器 및 逆元生成器 構成

(A Construction of the Multiplier and Inverse Element Generator over GF(3^m))

朴 春 明*, 金 泰 漢**, 金 興 壽*

(Choon Meung Park, Tae Han Kim, and Heung Soo Kim)

要 約

本 論文에서는 有限體 GF(3^m)상의 乘算器와 逆元生成器 構成의 한 가지 방법을 제시하였다. 乘算과 mod F(X) 演算을 동시에 수행시키기 위해 내림차순 mod F(X) 연산을 제안하였으며, 제안된 乘算器는 (1) 乘算部, (2) data 選別部, (3) Pj항 累算 및 順次選擇部, (4) 내림차순 mod F(X) 生成部 및 (5) 乘算處理部로 구성된다. 또한 逆元生成器는 (1) 乘算器, (2) 出力 레지스터군 Rs, (3) 乘算 및 세제곱 選擇 gata G1, (4) Ri항 順次選擇部, (5) 세제곱처리부 및 (6) 내림차순 mod F(X) 生成部로 이루어진다. 특히 본 論文에서 제안한 乘算器 및 逆元生成器는 回路設計의 單純性, 規則性, 擴張性 및 모듈화 가능성을 갖는다.

Abstract

In this paper, we presented a method of constructing a multiplier and an inverse element generator over finite field GF(3^m). We proposed the multiplication method using a descending order arithmetics of mod F(X) to perform the multiplication and mod F(X) arithmetics at the same time. The proposed multiplier is composed of following parts. 1) multiplication part, 2) data assortment part, 3) P_j term accumulation and sequential selection part, 4) descending order mod F(X) generation part and 5) multiplication processing part. Also the inverse element generator is constructed with following parts. 1) multiplier, 2) group of output registers R_s, 3) multiplication and cube selection gate G1, 4) Ri term sequential selection part. 5) cube processing part and 6) descending order mod F(X) generation part. Especially, the proposed multiplier and inverse element generator give regularity, expansibility and modularity of circuit design.

I. 序 論

現在 사용되고 있는 2進論理回路는 많은 발전을 이루어 왔으나 VLSI chip面積의 약 70%가 內部結線에 사용됨으로써 발생되는 chip面積의 效率性 低下 및 內部結線의 복잡성, chip들 사이의 結線의 복잡성, 端子數의 制限 問題, 入出力回路의 簡潔性 요구와 같은 문제들이 대두되었다.[1,2] 이러한 문제들을 해결하기 위하여 1970년대 초부터 2進論理回路에 비하여 단위 면적당 data 처리 능력이 크고, 높은 函數密度를 가지며, 하나의 回線에 더 많은 情報를 다룰 수 있어 단자수와 내부 결선의 복잡성을 감소시킬 수 있는 多値論理回路에 관한 연구가 활발하게 진행되어 왔다.[3,4]

*正會員, **準會員, 仁荷大學校 電子工學科
(Dept. of Elec. Eng., Inha Univ.)

接受日字 : 1989年 9月 30日

한편, 多値論理回路는 有限體인 Galois體를 이용하여 構成할 수 있다. Galois體 GF(p^m)上의 元素들 사이의 加算은 mod p 合으로 간단하게 해석되나, 乘算은 많은 계산과정이 요구되어 이에 대한 많은 연구가 진행되어 왔으며, 특히 GF(2^m)上에서는 2進論理를 수행하는 Boole體의 擴張이란 점과 2進論理素子로 實現할 수 있다는 점에서 많은 논문들이 발표되었다.[5,6] 또한 제산의 경우, 우선 젯수의 逆元을 구하여야 하며, 逆元을 구하는 데는 Euclid 알고리즘과 테이블 조사방법이 이용되어 왔으나 이 방법들은 VLSI 구조로의 실현이 적합치 못하다.

近來에 C. C. Wang등[7]은 GF(2^m)上의 乘算과 逆元回路를 Massay-Omura 乘算器를 이용하여 VLSI 화가 容易하도록 提案하였으나, 逆元回路에서 逆元 檢索에 많은 시간이 소요된다. 한편 Kim 등[8]은 GF(2^m)上에서 VLSI에 적합하며 函數獨立的인 動作速度를 제공하는 可變型乘算 및 乘算逆回路를 제안하여 逆元 檢索시간의 단축을 시도하였다.

일반적으로 多値論理回路는 I^2L, MOS, CCD 등의 素子를 사용하여 구성이 가능하며 이에 대한 많은 논문들이 발표되었다.[9-11]

本 論文에서는 CMOS소자를 사용하여 GF(3^m) 上의 乘算器와 逆元生成器를 設計하였다. 原始既約多項式 F(X)를 사용하여 LSD 치환다항식 T(α)를 구한 후 이를 이용하여 乘算과 mod F(X) 연산을 동시에 수행하는 내림차순 mod F(X) 연산을 乘算방법으로 제안하였으며, C. C. Wang[7] 등이 제안한 GF(2^m) 상의 역원생성방법을 GF(p^m) 상의 역원생성방법으로 확장하고 이를 GF(3^m) 상에 적용하였다. 제안된 乘算器는 (1) 乘算部, (2) data 選別部, (3) Pj항累算 및 順次選擇部, (4) 내림차순 mod F(X) 生成部 및 (5) 乘算處理部로 構成되며, 回路 構成의 規則性, 擴張性 및 모듈화 가능성 등을 갖고 있다. 또한 逆元生成器는 (1) 乘算器, (2) 出力 레지스터군 Rs, (3) 乘算 및 세제곱 선택 gata G1 및 (4) Ri항 順次選擇部, (5) 세제곱처리부 및 (6) 내림차순 mod F(X) 生成部로 구성된다.

本 論文의 構成은 다음과 같다. Ⅱ절에서 Galois體의 性質 및 이를 바탕으로 한 乘算및 제곱, 세제곱 방법을 제시하고, Ⅲ절에서 이 방법들을 토대로 逆元 生成 方法을 기술하였다. Ⅳ절과 Ⅴ절은 GF(3^m) 상의 乘算器 및 逆元生成器를 설계하고 이를 GF(3^4)의 경우에 적용하였다. Ⅵ절에서는 제안한 乘算器를 GF(2^m) 상의 乘算器로 전환시켜 타 논문과 비교한 결과를 제시하였다. 그리고 Ⅶ절에서는 본 論文에 대한 結論으로 提案한 GF(3^m)上의 乘算器 및 逆元生成器의 特徵을 要約하고 앞으로의 展望을 記述하였다.

Ⅱ. GF(3^m)上의 乘算 및 제곱, 세제곱 방법

1. GF(p^m) 上의 數學的 性質

GF(p^m)은 p^m개의 元素로 이루어지며, 本 論文에서 사용한 GF(p^m)의 性質은 다음과 같고 그외의 本論文 展開에 필요한 數學的 性質들은 參考文獻[12,13]에서 引用하였다.

1) $a \in GF(p^m)$에 대해서
$a^{p^m} = a$이고, $a^{p^m-1} = 1 (a \neq 0)$이다.

2) $a, b \in GF(p^m)$이고, 임의의 陽의 整數 k에 대하여
$(a \pm b)^{p^k} = a^{p^k} \pm b^{p^k}$

3) $a \in GF(p^m)$에 대하여
$a^i \cdot a^j = a^{i+j \pmod{p^m-1}}$

4) GF(p^m)의 元素들은 $A(\alpha) = \sum_{0}^{m-1} a_i \alpha^i$로 一意的으로 表示된다. 단 α는 p를 法으로 한 整數體 Z_P의 元素를 係數로 하는 m次 原始既約多項式

$$F(X) = X^m + f_{m-1}X^{m-1} + f_{m-2}X^{m-2} + \cdots + f_1 X_1 + f_0 \quad (1)$$

의 根이고, $a_i \in Z_P$ (i=0, 1, 2, ⋯, m−1)이며 $f_0 \neq 0$ 이다. 여기서 m次 原始既約多項式 F(X)는 Z_P의 元素를 係數로 한 多項式 $X^{p^m} - X$의 既約因子를 말한다.

2. GF(3^m)上의 승산 및 제곱 방법

GF(3^m)은 3^m個의 元素를 가지며 이를 集合으로 표현하면 식(2)와 같다.

$$\{0, \alpha, \alpha^2, \cdots, \alpha^{3^m-2} = \alpha^{-1}, \alpha^{3^m-1} = 1\} \quad (2)$$

한편, 原始既約多項式 F(X)를 사용하여 mod F(X) 演算을 하면 α의 m차 이상인 항은 최고 m−1차의 α의 다항식으로 표현할 수 있으므로 GF(3^m)의 임의의 원소 A는 식(3)과 같이 α의 慣用基底多項式으로 표현된다.

$$A = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + \cdots a_1\alpha^1 + a_0 = \sum_{i=0}^{m-1} a_i \alpha^i \quad (3)$$

여기서, $a_i \in GF(3)$, i=0, 1, 2, ⋯, m−1

GF(3^m)상의 任意의 한 元素 A에 대한 右側循還移動(right rotate)을 다음과 같이 表現한다.

$A \rightarrow^i$: A를 i回 右側循還移動(right rotate)시킴

예) 식(3)으로 표현된 한 원소 A에 대하여 i(i=0, 1, ⋯, m−1)回 右側循還移動시키면 다음과 같고 항상 A와 동일하다.

$$A=a_{m-1}\alpha^{m-1}+a_{m-2}\alpha^{m-2}+\cdots a_1\alpha^1+a_0$$
$$=e_{m-1}+e_{m-2}+\cdots+e_1+e_0$$
$$A\rightarrow^0=e_{m-1}+e_{m-2}+\cdots+e_1+e_0=A$$
$$A\rightarrow^1=e_0+e_{m-1}+\cdots+e_2+e_1=A$$
$$A\rightarrow^2=e_1+e_0+\cdots+e_3+e_2=A$$
$$\vdots \qquad \vdots$$
$$A\rightarrow^{m-2}=e_{m-3}+e_{m-4}+\cdots+e_{m-1}+e_{m-2}=A$$
$$A\rightarrow^{m-1}=e_{m-2}+e_{m-3}+\cdots+e_0+e_{m-1}=A$$

단, $ei=a_i\alpha^i$

$A\rightarrow^1$(여기서 $A\in GF(3^m)$)는 右側循環移動된 元素의 表現方法일 뿐 元素間의 乘算에는 아무런 영향을 주지 않는다. 따라서 $GF(3^m)$上의 두원소 A, B 사이의 승산은 식(4)와 같이 나타낼 수 있으며, 以下에서 使用된 元素들 사이의 乘算과 加算은 mod 3곱과 mod 3 합이다.

$$A=\sum_{i=0}^{m-1}a_i\alpha^i=A\rightarrow^1,\quad B=\sum_{i=0}^{m-1}b_j\alpha^j$$

$$A\cdot B=A\rightarrow^1\cdot(b_{m-1}\alpha^{m-1}+b_{m-2}\alpha^{m-2}+\cdots+b_1\alpha^1+b_0)$$
$$=A\rightarrow^0\cdot b_{m-1}\alpha^{m-1}+A\rightarrow^1\cdot b_{m-2}\alpha^{m-2}+\cdots+A\rightarrow^{m-2}\cdot b_1\alpha^1$$
$$+A\rightarrow^{m-1}\cdot b_0 \qquad (4)$$

식(4)의 각항들을 順次的으로 乘算하여 整理하면 식(5)와 같다.

$$A\cdot B=\sum_{i=0}^{m-1}P_i\alpha^i+\sum_{i=m}^{2m-2}P_i\alpha^i \qquad (5)$$

여기서 $P_{i+j}=\sum_{i=0}^{m-1}(\sum_{j=0}^{m-1}a_i\,b_j)$, $0\le i+j\le 2m-2$

식(4)를 順次的으로 乘算하면 최고차항(α^{2m-2})부터 생성되므로 식(5)의 두 번째 항인 α^{2m-2}항부터 α^m 항까지 내림차순으로 mod F(X) 演算을 하면 식 (6)과 같다.

$$A\cdot B=\sum_{i=0}^{m-1}R_i\alpha^i \qquad (6)$$

여기서, $P_i\alpha^i=P_i\alpha^i+(\sum_{j=m}^{2m-2}P_j\alpha^j)\bmod F(X)$

제곱의 경우는 두 입력 A, B가 A=B인 경우이므로 승산과 같은 방법으로 연산할 수 있으며, 그 결과는 식(7)과 같고 이는 식(6)과 同一하다.

$$A^2=A\cdot A=A\cdot B$$
$$=\sum_{i=0}^{m-1}R_i\alpha^i \qquad (7)$$

따라서 제곱생성기는 승산기로 構成할 수 있다.

3. $GF(3^m)$上의 세제곱 방법

$GF(3^m)$上의 한 元素 A를 식(3)과 같이 選擇하였을 때, A^3은 수학적 성질에 의해 식(8)과 같이 整理된다.

$$A^3=\sum_{i=0}^{m-1}a_i\alpha^{3i} \qquad (8)$$

한편, α의 m次 以上인 項에 대하여 내림차순 mod F(X) 演算을 하면 A^3은 식(9)와 같이 된다.

$$A^3=\sum_{i=0}^{m-1}D_i\alpha^i \qquad (9)$$

여기서, $D_i\alpha^i=a_i\alpha^i+(\sum_{k=[m/3+0.8]}^{m-1}a_k\alpha^{3k})\bmod F(X)$,

[ ]는 Gauss 記號

식(8), (9)에서 보는 바와 같이 $GF(3^m)$上의 한 元素에 대한 세제곱은 어떠한 乘算過程도 필요없으며, 내림차순 mod F(X) 演算으로 α의 m次 以上인 項을 α의 慣用基底多項式으로 置換하면 된다.

4. LSD 置換多項式 $T(\alpha)$ 生成 알고리듬

原始既約多項式 F(X)에서 X^{m-1}項의 係數와 常數項을 각각 MSD(most significant digit), LSD(least significant digit)로 표시할 때 $GF(3^m)$상에서 α^m의 慣用基底多項式은 식(10)과 같이 표현된다.

$$\alpha^m=\underset{\text{MSD}}{(3-f_{m-1})}\alpha^{m-1}+(3-f_{m-2})\alpha^{m-2}+\cdots+\underset{\text{LSD}}{(3-f_1)\alpha+(3-f_0)} \qquad (10)$$

내림차순 mod F(X) 연산에 필요한 LSD 置換多項式 $T(\alpha)$를 求하는 알고리듬은 다음과 같다.

〈LSD 置換多項式 $T(\alpha)$ 生成 알고리듬〉

[단계 1] α^m項을 慣用基底多項式으로 표현한다.

[단계 2] α^{m+1}項의 慣用基底多項式을 구한다.

[단계 3] LSD가 存在하는지 調査하여 LSD가 없으면 存在할 때까지 α의 次數들을 하나씩 높인다.

[단계 4] α^j項에서 LSD가 존재하면 LSD를 除外한 α^j項의 慣用基底多項式의 α의 次數를 하나씩 낮춘항을 α^j로 하고 이를 α^{j-1}項과 減算을 한다. ($m\le j\le 2m-2$)

[단계 5] LSD=1이면 減算한 결과를 $T(\alpha)$로 하고, LSD=2이면 減算한 결과를 2로 나누어 그 결과를 $T(\alpha)$로 한다. $T(\alpha)$의 一般形式은 식(11)과 같다.

$$T(\alpha)=T_{m-1}\alpha^{m-1}+T_{m-2}\alpha^{m-2}+\cdots+T_1\alpha+T_0$$
여기서, $Ti\in GF(3)$ (11)

예) $GF(3^4)$에서 原始既約多項式 $F(X)=X^4+X+2$

일 때 T(α)를 구하면

$\alpha^4=2\alpha+1$
$\alpha^5=2\alpha^2+\alpha$
$\alpha^6=2\alpha^3+\alpha^2$
$\alpha^7=2\alpha^4+\alpha^3$
$=\alpha^3+\alpha+2$(LSD)
$\alpha^6-\alpha^{7'}=(2\alpha^3+\alpha^2)-(\alpha^2+1)$
$=2\alpha^3+2$

LSD=2이므로 $T(\alpha)=\alpha^3+1$이 된다.

5. 내림차순 mod F(X) 演算 알고리듬

2-4절의 LSD 置換多項式 T(α) 生成 알고리듬으로 T(α)를 구한 후 다음의 알고리듬을 이용하면 내림차순 mod F(X) 연산을 遂行할 수 있다.

〈내림차순 mod F(X) 연산 알고리듬〉

[단계 1] T(α)를 입력한다.
[단계 2] α^k項을 慣用基底多項式으로 표현하고 LSD의 값을 조사한다.(k>m)
[단계 3] LSD와 T(α)의 곱을 LT라 한다.
[단계 4] $\alpha^{k'}$ 항을 구한다.
[단계 5] LT와 $\alpha^{k'}$의 합이 α^{k-1}항의 慣用基底多項式이 된다.
[단계 6] 위의 과정을 α^m항을 구할 때까지 계속한다.

예) GF(3⁴)상의 내림차순 mod F(X) 연산

原始旣約多項式 $F(X)=X^4+X+2$일때, $T(\alpha)=\alpha^3+1$이 된다. 따라서 k=9인 경우 내림차순 전개는 다음과 같다.

$\alpha^9=\alpha^3+\alpha^2+\alpha$
$\alpha^8=\alpha^2+\alpha+1$ (LSD)
$\alpha^7=\alpha+1+(\alpha^3+1)$
$=\alpha^3+\alpha+2$ (LSD)
$\alpha^6=\alpha^2+1+2(\alpha^3+1)$
$=2\alpha^3+\alpha^2$
$\alpha^5=2\alpha^2+\alpha$
$\alpha^4=2\alpha+1$

Ⅲ. GF(3^m)上의 逆元 生成 알고리듬

이 절에서는 C. C. Wang[7] 등이 제안한 GF(2^m) 上의 逆元生成方法을 일반적인 경우인 GF(p^m) 으로 확장하였으며, 이를 p=3인 경우에 적용하였다.

GF(p^m)상의 한 元素를 A라 할 때, A의 逆元 A^{-1}는 [定理 1]과 같이 전개된다.

[定理 1]

$A^{-1}=A^{P^m-2}$
$=A^{P-2}\cdot(A^{P-1})^{P^1}\cdot(A^{P-1})^{P^2}\cdot(A^{P-1})^{P^3}\cdots(A^{P-1})^{P^{m-1}}$
$=A^{P-2}\cdot(A^{P-1}\cdot(\cdots(A^{P-1}\cdot(A^{P-1})^P)^P\cdots)^P)^P$

[證 明]

$A^{-1}=A^{P-2}\cdot(A^{P-1}\cdot(\cdots(A^{P-1}\cdot(A^{P-1})^P)^P\cdots)^P)^P$
$=A^{P-2}\cdot(A^{P-1})^{P^1}\cdot(A^{P-1})^{P^2}\cdot(A^{P-1})^{P^3}\cdots(A^{P-1})^{P^{m-1}}$
$=A^{P-2}\cdot(A^{P-1})^{P^1+P^2+P^3+\cdots+P^{m-1}}$

여기서 等比數列의 合은 $\frac{P(P^{m-1}-1)}{P-1}=\frac{P^m-P}{P-1}$ 이므로

$A^{-1}=A^{P-2}\cdot(A^{P-1})^{\frac{P^m-P}{P-1}}$
$=A^{P-2}\cdot A^{P^m-P}$
$=A^{P^m-2}$

(證明 끝)

定理1에 의하면 GF(p^m)上의 한 元素 A의 逆元은 A의 (p-1)乘과 p乘을 m-1회의 반복하여 승산한 결과와 A의 (p-2)乘을 승산하면 구할 수 있다. 위의 내용을 p=3인 경우에 적용하면 GF(3^m)上의 한 元素 A의 逆元 A^{-1}를 구하는 알고리듬은 다음과 같다.

〈逆元 生成 알고리듬〉

[단계 1] GF(3^m)上의 元素 A를 받아들인다.
[단계 2] 元素A의 제곱을 구한다.
[단계 3] 단계2 또는 단계5의 결과를 세제곱한다.
[단계 4] (m-1)회의 세제곱을 하였으면 단계6으로 간다.
[단계 5] 단계3의 결과와 A^2을 승산한 후 단계3으로 간다.
[단계 6] 단계4의 결과와 A를 승산하면 A의 역원A^{-1}이 된다.

Ⅳ. GF(3^m)上의 乘算器 構成

Ⅱ절의 내용을 근거로 GF(3^m)상의 승산기를 블록도로 나타내면 그림 1과 같고 각 블록들의 내부구조는 그림2, 3, 4, 5 그리고 6과 같다.

1. 乘算部

그림 2는 레지스터를 통하여 입력되는 두 元素를

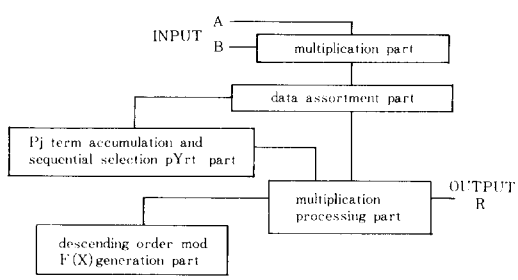


그림 1. GF(3^m)上의 乘算器의 블록도
Fig. 1. Block diagram of multiplier over GF(3^m).

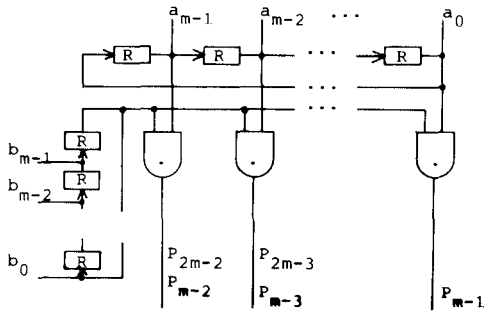


그림 2. 乘算部
Fig. 2. Multiplication part.

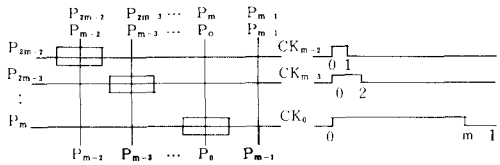


그림 3. Data 選別部
Fig. 3. Data assortment part.

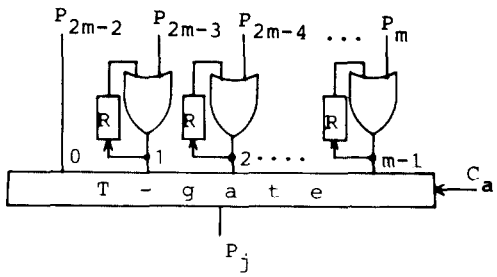
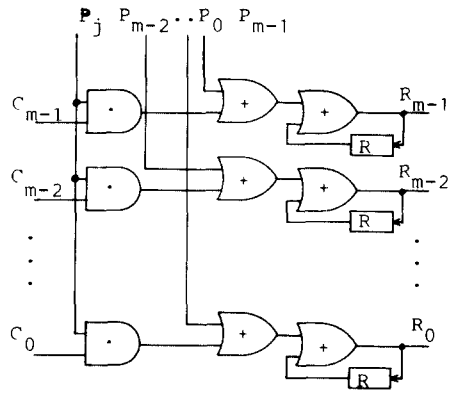


그림 4. p_j항 累算 및 順次選擇部
Fig. 4. p_j term accumulation and sequential selection part.

받아들여 mod 3곱을 하는 乘算部로 한 元素는 竝列로 다른 한 元素는 直列로 입력되어 直竝列混合形態의 乘算을 수행한다.

2. Data 選別部

分配gate들로 구성된 data 選別部는 그림3과 같고 각각의 분배 gate들은 制御信號 $CK_i(0\leq i\leq m-2)$ 에 의하여 乘算部의 出力중 p_m이상인 항은 p_j항 累算및



Pi(0≤i≤m−1):outouts of data assortment part
Pj:outout of Pj accumulation and sequential selection part
Ci:outouts Jof Descending order mod F(X) generation part

그림 5. 乘算處理部
Fig. 5. Multiplication processing part.

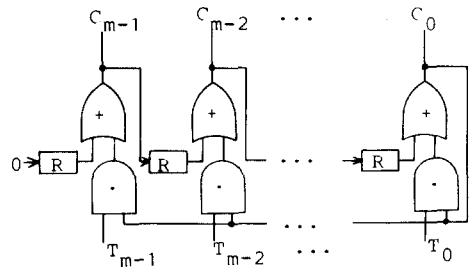


그림 6. 내림차순 mod F(X) 生成部
Fig. 6. Descending order mod F(X) generation part.

順次選擇部로, p_{m-1}이하인 항은 乘算處理部로 전송된다.

3. p_j항 累算 및 順次選擇部

그림4는 p_j항 累算 및 順次選擇部를 나타낸 것으로 data 選別部의 출력 $p_j(m\leq j\leq 2m-2)$항을 累算하고 累算된 결과를 제어신호 Ca에 따라 p_{2m-2}항부터 順次的으로 선택하여 乘算處理部로 전송한다.

4. 乘算處理部

그림 5는 乘算處理部로 p_j항 累算 및 順次選擇部의 出力 $p_j(m-1\leq j\leq 2m-2)$와 내림차순 mod F(X) 生成部의 出力 C_i가 mod 3 곱gata애 입력되고 그 出

力은 mod 3 합gate 입력된다. 한편, data 選別部의 出力중 p_k항($0 \le k \le m-1$)은 바로 mod 3 합 gate로 전송되며 mod 3 합gate에 입력되는 값들의 累算 결과는 레지스터에 貯藏된다.

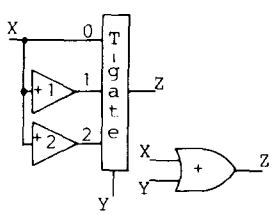
5. 내림차순 mod F(X) 生成部

그림 6은 내림차순 mod F(X) 生成部로, mod 3곱gate의 입력으로 LSD 置換多項式 $T(\alpha)$를 사용하여 $\alpha^j (m \le j \le 2m-2)$항을 최고 $m-1$차의 α의 慣用基底多項式으로 置換한다. 置換된 $\alpha^j (m \le j \le 2m-2)$항의 일반형태는 식(12)와 같다.

$$\alpha^j = C_{m-1}\alpha^{m-1} + C_{m-2}\alpha^{m-2} + \cdots C_1\alpha^1 + C_0 \qquad (12)$$

이 내림차순 mod F(X) 生成部는 α의 내림차순으로 동작하고 $T(\alpha)$의 계수 T_i는 慣用基底多項式 F(X)의 선택에 따라 바뀌며, 레지스터에는 α^{2m-2}항의 慣用基底多項式 $S_i (0 \le i \le m-1)$가 입력된다.

위의 그림2, 3, 4, 5 그리고 6에서 사용된 回路素子들은 참고문헌[14]에서 引用하여 사용하였고, 참고문헌에서 제시되지 않은 회로소자인 mod 3 합gate, mod 3 곱gate, 分配gate들을 참고문헌[14]를 근거로 구성하여 그림 7, 8및 9에 나타내었으며 레지스터는 참고문헌에서 제시된 3値 D형 F/F를 이용하였다.

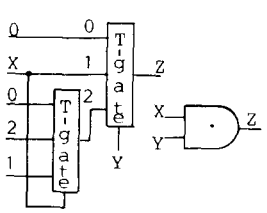


X, Y : input
Z : output

+	X=0	X=1	X=2	
0	0	1	2	X
Y1	1	2	0	X+1
2	2	1	0	X+2

(a) 회로도 (b) 기호 (c) 진리표

그림 7. Mod 3 합gate
Fig. 7. Mod 3 sum gate.

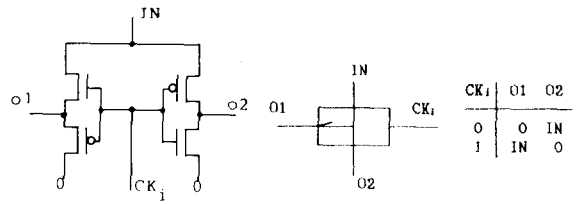


X, Y : input
Z : output

·	X=0	X=1	X=2	
0	0	0	0	0
Y1	0	1	2	X
2	0	2	1	T-입력

(a) 회로도 (b) 기호 (c) 진리표

그림 8. Mod 3 곱gate
Fig. 8. Mod 3 product gate.



(a) 회로도 (b) 기호 (c) 진리표

IN : input
CK_i : control signal
1, 2 : ouput directions

그림 9. 分配 gate
Fig. 9. Distribution gate.

[適用例]

4절에서 제안된 GF(3^m)상의 乘算器를 GF(3^4) 의 경우에 적용하여 구성하면 그림10과 같다. 여기서 $F(X) = X^4 + X + 2$이고 $T(\alpha) = \alpha^3 + 1$이며 S_i는 $\alpha^6 = 2\alpha^3 + \alpha^2$이다.

V. GF(3^m)상의 逆元生成器

본 절에서는 2, 3, 4절의 내용을 근거로 GF(3^m) 上의 逆元生成器를 구성하였다. 제안된 逆元生成器는

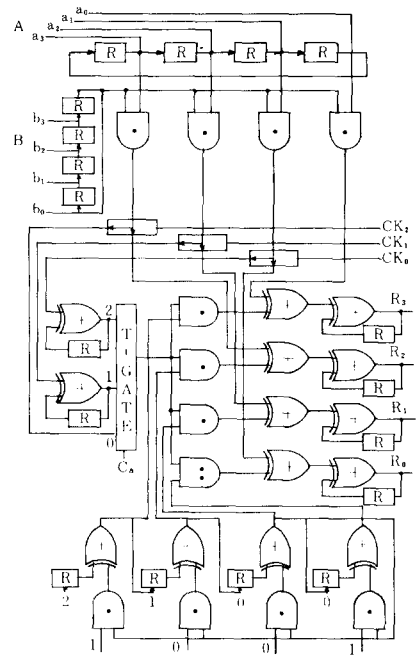


그림10. GF(3^4)上의 乘算器 適用例
Fig. 10. An example of multiplier in GF(3^4).

4절에서 제안한 乘算器를 근간으로 出力 레지스터群 R_s, 乘算 및 세제곱선택 gate G1, R_i항 順次選擇部, 세제곱처리부 및 내림차순 mod F(X) 生成部등을 추가하여 구성하였다.

그림11은 逆元生成器의 블록도로 입력된 元素 A에 대한 제곱연산을 하여 그 결과(A^2)를 出力 레지스터群 R_s에 저장한 후 세제곱된 결과와 乘算을 하게된다. m−1회의 세제곱을 하면 乘算部의 왼쪽 레지스터에 저장된 元素 A와 乘算을하여 出力 레지스터群 R_s를 통하여 出力된다.

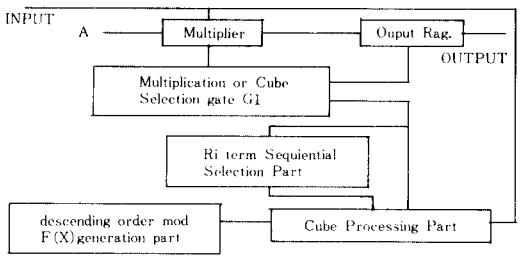


그림11. GF(3^m)상의 逆元生成器의 블록도
Fig. 11. Block diagram of inverse element generator over GF(3^m).

1. 出力 레지스터群 R_s

出力 레지스터群 R_s는 A^2을 저장한 후 세제곱된 결과와 A^2을 乘算하기 위해 乘算器로 A^2을 반복하여 전송하며 최종출력인 逆元도 이곳에서 出力된다.

2. 乘算 및 세제곱 선택gate G1

乘算 및 세제곱 선택gate G1은 제어신호 C1에 의해 입력된 값의 출력방향을 出力 레지스터群 R_s 또는 R_i항 順次選擇部와 세제곱처리부로 선택한다.

3. R_i항 順次選擇部

R_i항 順次選擇部는 乘算器에서 전송되는 값들 중에서 mod F(X)演算을 하여야 할 R_j항([m/3+0.8] ≤j≤m−1)들을 레지스터에 저장한 후 제어신호 C_b에 의하여 최고차항부터 선택하여 세제곱 처리부로 전송한다. 그림12는 R_i항 順次選擇部를 나타낸 것이다.

4. 세제곱처리부

그림13은 세제곱처리부로 乘算處理部와 乘算 및 세제곱 선택gate G1으로 구성되며, 乘算 및 세제곱 선택gate G1은 mod 3 합 gate의 出力을 C3=0이면

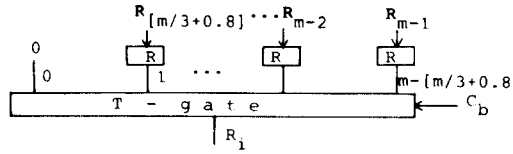


그림12. R_i항 順次選擇部
Fig. 12. R_i term sequential selection part.

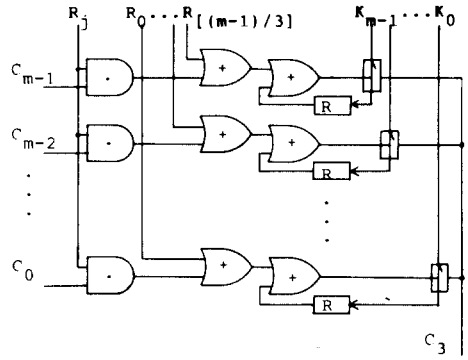


그림13. 세제곱처리부
Fig. 13. Cube processing part.

세제곱처리부의 레지스터로 전송하고, C3=1이면 乘算器 內의 레지스터로 전송한다.

5. 내림차순 mod F(X) 生成部

내림차순 mod F(X) 生成部는 乘算器의 경우와 동일하며 다만 레지스터에 α^{3m-3}항의 慣用基底多項式 I_i ($0 \le i \le m-1$)가 입력된다.

[適用例]

GF(3^4)上의 逆元生成器를 구성하면 그림14와 같고 F(X), T(α), S_i는 乘算器의 경우와 같고 I_i는 $\alpha^9 = \alpha^3 + \alpha^2 + \alpha$이다. 그림15는 逆元生成器의 제어신호를 나타낸 것이다.

Ⅵ. 比較 및 檢討

本 論文에서 제안한 乘算器는 GF(p^m) 上에서 p=3인 경우를 다루었으므로 타논문과 比較하기 위해 본 논문에서 제안한 乘算器 構成 方法을 GF(2^m) 상의 乘算器로 轉換시켜 그 結果를 표 1에 나타내었다.

먼저 本 論文에서 제안한 GF(3^m)上의 乘算器 構成時 사용한 mod 3 합gate, mod 3 곱gate, T-gate를 각각 XOR gate, AND gate, (m−1)入力MUX로 대치하여 GF(2^m)上의 乘算器를 구성하면 그 블록도는 그림 1과 동일하다. 또한, GF(2^4)上의 乘算器를 構成하면 그림16과 같다.

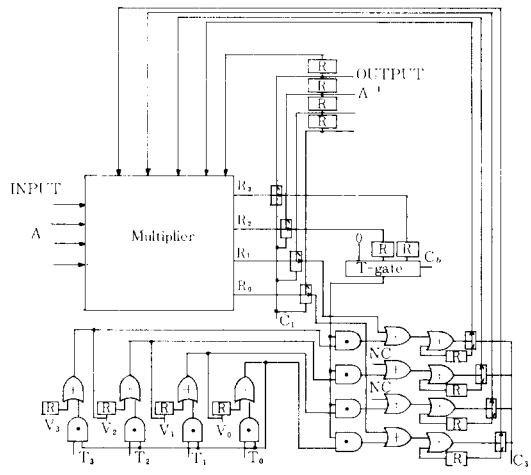


그림14. GF(3⁴)上의 逆元生成器의 適用例
Fig. 14. Example of inverse element generator over GF(3⁴).

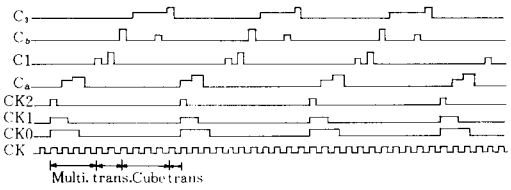


그림15. GF(3⁴)上의 逆元生成器의 제어신호
Fig. 15. Control signals of inverse element generator over GF(3⁴).

여기서 i는 XOR 레벨수이고, [X]는 X보다 더 큰 가장 작은 정수

위 표 1에서 본바와같이 이들 여러 素子들 중에서

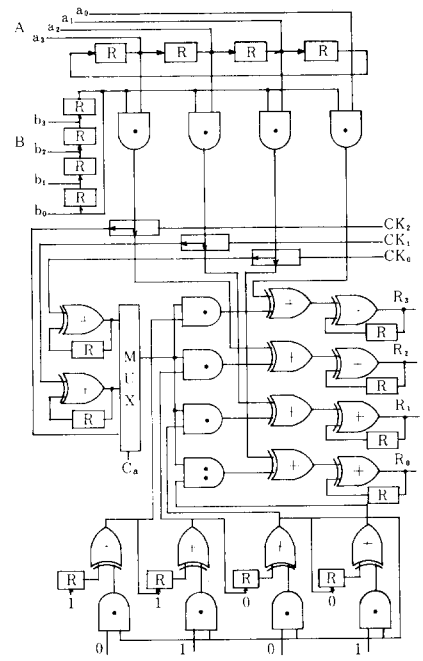


그림16. GF(2⁴)上의 乘算器
Fig. 16. A multiplier over GF(2⁴)

레지스터의 수를 줄이는 것이 回路面積을 감소시킬 수 있는 重要한 요소이다. Yeh등이 제안한 Systolic 형태의 乘算器는 많은 레지스터가 필요하지만 本 論文에서 제안한 乘算器는 이 보다는 적은 수의 레지스터가 필요하며 C. C. Wang 등이 제안한 Massey-Omura 乘算器는 原始旣約多項式이 변하면 PLA 부분을 변경해야 하는 불편이 있으나 本 論文에서는 T(α)의 계수값만 바꾸어 주면 간단하게 구성할 수 있다. 그러나 原始旣約多項式 F(X)를 사용하여 LSD 치환다항식 T(α)를 먼저 生成시켜야 하는 단점이있다.

표 1. 比較表
Table 1. Comparison table.

	Yeh[5]		Wang[7]	Kim[10] GF(3^m)	This paper
	1-D Systolic	2-D Systolic			
AND	2m	$2m^2$	2m+1	m^2	3m
XOR	3m	$2m^2$	$\sum[m/2i]$	$(3m^2-5m)/2+1$	4m-2
REGISTER	10m+2	$7m^2+5m-4$	4m-2	-	4m-2
INVERTOR	-	-	2	-	-
SWITCH	m	-	-	-	-
Pass-Tr	-	-	6m-2	-	m-1
T-gate	-	-	-	$(m^2-m)/2$	(m-1)input MUX
CK TIME	2m	2m	2m-1	-	m

단, 本 論文에서 제안된 乘算器의 동작시간은 素子지연 시간을 고려하지 않은 結果이다.

Ⅶ. 結 論

本 論文에서는 有限體 $GF(3^m)$上의 乘算器 및 逆元生成器 構成의 한 가지 方法을 제시하였다. 제안한 내림차순 mod F(X) 연산을 이용한 乘算器는 直並列 混合 형태의 乘算器로 回路 設計時 次數 m에 따라 構成 素子들을 규칙적으로 배열하면 되므로 확장이 용이하며, 乘算器의 각 부분들의 모듈화가 용이하며 回路設計가 단순한 편이다. 또한 並列처리 형태의 乘算器에 比하여 次數 m이 증가할 경우 算術的으로 回路素子가 증가하여 回路素子 면에서도 다소 우수하며 mod F(X) 演算과 乘算을 동시에 수행함으로써 동작 시간을 감소 시킬 수 있다.

한편, 逆元生成器는 乘算器 세제곱처리를 위한 회로부분만을 추가하여 구성하였으며, 입력부분을 수정하면 乘算과 除算을 逆元生成器上에서 실현 할 수 있다. 특히 逆元生成時 차수 m의 크기에 관계없이 m회의 乘算과 m−1회의 세제곱연산만으로 逆元을 구할 수 있다.

그러나 本 論文은 $GF(p^m)$上에서 p=3인 경우로 제어신호가 많이 필요하며 이에 대한 개선이 요구되며 제안한 乘算器와 逆元生成器를 토대로 $GF(3^m)$上의 算術演算器 시스템을 構成할 수 있으리라 展望되며 현재 硏究 진행중이다.

參 考 文 獻

[1] J.T. Butler, "Multiple-valued logic: guest editor's introduction and bibliography," *IEEE Comput. Mag.*, vol. 21, pp. 13-15, Apr. 1988.

[2] J.C. Muzio, "Introduction multiple-valued logic," *IEEE Trans. Comput.*, vol. C-35, pp. 97-98, Feb. 1986.

[3] Z.G. Vranesic, "Multiple-valued logic: an introduction and overview," *IEEE Trans. Comput.*, vol. C-26, pp. 1181-1182, Dec. 1977.

[4] S.L. Hurst, "Multiple-valued logic-it's status and it's future," *IEEE Trans. Comput., vol.* C-33, pp. 1160-1179, Dec. 1984.

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

[6] B.B. Zhou, "A new bit-serial systolic multiplier over $GF(2^m)$," *IEEE Trans. Comput.*, vol. C-37, pp. 749-751, Jun. 1988.

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

[8] 金興壽 外, "$GF(2^m)$상의 승법과 승법역 계산을 위한 가변형 산술 연산시스템의 설계," 전자공학회 논문지 제25권 제5호, pp. 528−535, 1988. 5.

[9] S. L. Hurst, "Two decades of multiple-valued logic-an invited tutorial," ISMVL 88, pp. 164-175, May 1988.

[10] 박춘명, 김홍수 外, "$GF(3^m)$상의 승산기 구성 이론," 전자공학회 추계종합학술대회논문집 제11권 제1호, pp. 329−333, 1988. 11.

[11] 박춘명, 김홍수 外, "$GF(3^m)$상의 역원생성기 구성이론," 전자공학회 하계종합 학술대회논문집 제12권 제1호, pp. 436−439, 1989. 7.

[12] H.S. Kim, "A construction of multiple-valued switching functions by Galois field," Ph.D. dissertation, Inha Univ., Incheon, Korea, Feb. 1979.

[13] Rudolf Lidi, Gunter PiZl, Applied abstract algebra, Springer-Verlag N.Y., 1984.

[14] X. Wu, P. Prosser, "Termary cmos. Sequential circuits," ISMVL 88, pp. 307-313, May. 1988.

著 者 紹 介

朴 春 明(正會員)

1955年 12月 4日生. 1983年 2月 인하대학교 전자공학과 졸업 (공학사). 1986年 2月 인하대학교 대학원 전자공학과 졸업(공학석사) 1986年 9月～현재 인하대학교 대학원 전자공학과 박사학위 과정 중. 주관심분야는 다치논리이론구성 및 회로설계, 컴퓨터구조 및 VLSI설계, Coding Theory, DSP & DIP 등임.

●

金 興 壽 (正會員) 第24卷 第5號 參照
현재 인하대학교 전자공학과 교수

金 泰 漢(準會員)

1965年 8月 12日生. 1988年 2月 인하대학교 전자공학과 졸업(공학사). 1990年 2月 인하대학교 대학원 전자공학과 졸업(공학석사). 1990年 1月～현재 런나이코리아 연구소 근무. 주관심분야는 VLSI설계, 컴퓨터 구조 등임.