

유한체 GF(24)를 이용한 GF(216)의 직렬 곱셈기 설계와 이의 C언어 시뮬레이션

신 원 철* 이 명 호**

(Design of GF(216) Serial Multiplier Using GF(24) and its C Language Simulation

Won-Chul Shin* Myung-Ho Lee**

요 약

본 논문에서는 부분체(24)를 갖는 유한체 GF(216)의 곱셈기를 설계하였다. 이런 설계는 부분체를 이용한 비트 병렬 곱셈기를 사용한 순차 논리 곱셈기를 만들기 위해 사용된다. 부분체 상의 병렬연산기를 사용하여 유한체 GF(216)의 직렬 곱셈기를 설계하면 기존의 직렬 곱셈기 보다는 짧은 지연시간을 얻을 수 있으며, 병렬 곱셈기 보다는 적은 하드웨어로 구현할 수 있다. 이러한 설계는 유용한 특징을 갖는다. 여기서는 회로 복잡도와 지연시간의 특징을 비교하고 C언어를 이용하여 시뮬레이션결과를 보였다.

Abstract

In this paper, The GF(216) multiplier using its subfields GF(24) is designed. This design can be used to construct a sequential logic multiplier using a bit-parallel multiplier for its subfield. A finite field serial multiplier using parallel multiplier of subfield takes a less time than serial multiplier and a smaller complexity than parallel multiplier. It has an advatageous feature. A feature between circuit complexity and delay time is compared and simulated using C language.

* 주성대학 컴퓨터정보공학부 조교수

** 청주대학교 정보통신공학부 정교수

본 논문은 청주대학교 정보통신연구센터의 지원에 의한 논문입니다.

I. 서론

유한체(finite field or Galois field) 상의 연산은 오류정정 부호이론, 암호이론, 디지털 신호처리 등의 분야에서 널리 응용되고 있다. 특히 오류정정부호 중 BCH 부호나 Reed-Solomon 부호와 같은 블럭부호는 유한체 상에서 정의되며, 모든 연산이 유한체 상에서 이루어진다. 따라서 유한체 상의 연산은 이를 부호의 부호화 및 복호의 속도와 부/복호기의 하드웨어 량에 직접적으로 영향을 미치는 매우 중요한 요소이다.

유한체 GF(2m) 상의 곱셈기는 조합회로를 사용한 병렬 곱셈기와 순서회로를 사용한 직렬 곱셈기로 구현할 수 있다. 병렬 곱셈기는 연산속도는 빠른 반면에 회로가 복잡해지며, 직렬 곱셈기는 회로는 간단하지만 16 클릭 시간의 지연이 불가피 해진다.

본 논문에서는 이러한 문제점을 해결할 수 있는 한 가지 방법으로, 부분체(subfield)를 이용한 직렬 곱셈기를 제안한다. 유한체 GF(2m)의 차수 m이 1보다 큰 임의의 두 자연수의 곱으로 이루어진 경우 ($m = u \times v$), 유한체 GF(2m)은 GF(2u)와 GF(2v)를 부분체로 갖는다. 본 방법은 이러한 부분체 상의 병렬 연산기들을 이용하여 유한체 GF(2m) 상의 직렬 곱셈기를 구현하는 것이다. 이는 회로의 복잡도와 지연시간 사이에 적절한 절충을 꾀하는 것으로, 본 방법을 사용하면 기존의 직렬 곱셈기보다는 짧은 지연시간에 결과를 얻을 수 있으며, 병렬 곱셈기보다는 적은 하드웨어로 구현할 수 있다.

먼저 II에서 유한체 GF(2m)의 원소들을 그것의 부분체를 이용하여 표현하는 방법을 제시하고, III에서는 부분체를 이용한 유한체 GF(2m) 상의 곱셈기를 설계한다. 또한 실제 예로써 실용상 매우 중요한 유한체 GF(216)의 곱셈기를 그것의 부분체인 GF(24)를 이용하여 설계하고 이를 C언어를 이용하여 시뮬레이션하여 그 타당성을 입증하였고 병렬 곱셈기와 그 복잡도와 속도의 관계를 비교하였다.

II. 유한체 GF(2m)의 부분체 표현

α 를 유한체 GF(2m)의 원시원(primitive element)이라 할 때 영원(zero element)을 제외한 $2m-1$ 개의 모든 원소들은 α 의 럭(power)으로 표현할 수 있다. 또 이 α 를 식 (1)과 같은, 차수가 m 인 원시다항식(primitive polynomial)의 근(root)이라고 하면

$$f(x) = 1 + f_1x + \dots + f_{m-1}x^{m-1} + x^m, \quad (1)$$

$$f_i \in GF(2)$$

$f(\alpha) = 0$ 이므로 다음과 같이 된다.

$$\alpha^m = 1 + f_1\alpha + \dots + f_{m-1}\alpha^{m-1} \quad (2)$$

따라서 유한체 GF(2m)의 각 원소들은 차수가 $m-1$ 이하인 α 의 다항식으로 표현할 수 있다. 즉 유한체 GF(2m) 상의 임의의 한 원소 U 는 다음과 같이 쓸 수 있다.

$$U = u_0 + u_1\alpha + \dots + u_{m-1}\alpha^{m-1}$$

$$= \sum_{i=0}^{m-1} u_i\alpha^i, \quad u_i \in GF(2)$$

(3)

여기에서 다음과 같은 m 개의 서로 독립인 원소들을 유한체 GF(2m)의 표준기저(standard basis)라고 한다[2].

$$\{1, \alpha, \alpha^2, \dots, \alpha^{m-2}, \alpha^{m-1}\} \quad (4)$$

예를 들어 유한체 GF(28)의 GF(2) 상의 원시다항식이 다음과 같을 때

$$f(x) = 1 + x + x^3 + x^{12} + x^{16} \quad (5)$$

이 다항식의 근인 원시원을 α 라 하면 $f(\alpha) = 0$ 이므로

$$\alpha^{16} = 1 + \alpha + \alpha^3 + \alpha^{12} \quad (6)$$

가 되며, 따라서 유한체 GF(216)의 0이 아닌 65535개의 원소는 GF(2) 상의 15차 이하인 α 의 다항식으로 나타낼 수 있다.

또한 유한체 GF(24)의 GF(2) 상의 원시다항식을

$$f(x) = 1 + x + x^4 \quad (7)$$

이라 하고 원시원을 β 라 하면 $f(\beta) = 0$ 이므로

$$\beta^4 = 1 + \beta \quad (8)$$

가 되며, 따라서 유한체 GF(24)의 0이 아닌 15개의 원소는 GF(2) 상의 3차 이하인 β 의 다항식으로 나타낼 수 있다.

유한체 GF(2m)에서 위수 m 이 다음과 같이 1 보다 큰 임의의 두 자연수의 곱으로 이루어진 합성수(composite number)인 경우

$$m = u \cdot v, \quad u, v > 1 \quad (9)$$

유한체 GF(2m)은 GF(2u)와 GF(2v)를 부분체로 갖는다. 여기에서 u 와 v 은 1보다 큰 임의의 자연수이다. 이와 같은 경우 유한체 GF(2m)의 모든 원소는 부분체 GF(2u) 또는 GF(2v)의 원소들을 이용하여 표현할 수 있다. 예를 들어 식 (9)에서 $m = 16 = 4 \times 4$ 인 경우를 생각해보자. 유한체 GF(28)의 원시원 α 와 그것의 부분체인 GF(24)의 원시원 β 와의 사이에는 다음과 같은 관계가 성립한다.

$$\beta^{15} = 1 = \alpha^{65535} \quad (10)$$

그러므로 β 를 유한체 GF(216) 상의 원소로 나타내면

$$\beta = \alpha^{4369u} \quad (11)$$

가 된다. 여기에서 u 는 65535와 서로 소(relative prime)인 임의의 정수이다. $k = 1$ 을 선택하면 GF(24)

의 0이 아닌 15개의 원소 β^i ($0 \leq i \leq 14$)는 다음과 쓸 수 있다.

$$\beta^i = \alpha^{4369i}, \quad 0 \leq i \leq 14 \quad (12)$$

식 (1)에서 유한체 GF(2m)을 그것의 소체(prime field)인 GF(2) 상의 원시다항식을 이용하여 구성하였다. 이를 확장하면 유한체 GF(2m)은 그것의 부분체인 GF(2u) 또는 GF(2v) 상의 원시다항식을 이용하여 구성할 수 있다. 예를 들어 유한체 GF(216)은 GF(24) 상의 2차 원시다항식 또는 GF(24) 상의 4차 원시다항식을 이용하여 구성할 수 있다.

GF(216) 원시원 α 가 $f(x)$ 의 근이므로 α 의 공액(conjugate)인 $\alpha^{2^{m-1}}$, 즉 $\alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}, \alpha^{256}, \alpha^{512}, \alpha^{1024}, \alpha^{2048}, \alpha^{4096}, \alpha^{8192}, \alpha^{16384}, \alpha^{32768}$ 도 $f(x)$ 의 근이 된다. 따라서 GF(24) 상의 4차의 원시다항식 $f(x)$ 는 다음과 같이 구성할 수 있다.

$$f(x) = (x + \alpha)(x + \alpha^{16})(x + \alpha^{256})(x + \alpha^{4096}) \quad (13) \\ = x^4 + x^3 + x^4 + x + \alpha^{1369}$$

식 (12)로부터 $\beta = \alpha^{1369}$ 이므로 식 (13)의 $f(x)$ 를 GF(24) 상의 다항식으로 표현하면 다음과 같이 된다.

$$f(x) = x^4 + x^3 + x + \beta \quad (14)$$

또 $f(\alpha) = 0$ 이므로 다음과 같이 쓸 수 있다.

$$\alpha^4 = \beta + \alpha + \alpha^3 \quad (15)$$

그러므로 식 (15)를 이용하면 GF(216)의 0이 아닌 모든 원소는 다음과 같이 GF(24) 상의 3차 이하인 α 의 다항식으로 표현할 수 있다.

$$\alpha^0 = 1$$

$$\alpha^1 = \alpha$$

$$\alpha^2 = \alpha^2$$

$$\alpha^3 = \alpha^3$$

$$\alpha^4 = \beta + \alpha + \alpha^3 \quad (16)$$

$$\begin{aligned}\alpha^5 &= \beta\alpha + \alpha^2 + \alpha^4 \\ &= \beta + (1 + \beta)\alpha + \alpha^2 + \alpha^3 \\ &\quad \vdots \\ &\quad \vdots\end{aligned}$$

따라서 유한체 GF(216)의 임의의 한 원소 U 를 그것의 부분체인 GF(24)을 이용하여 표현하면 다음과 같이 된다.

$$U = U_0 + U_1\alpha + U_2\alpha^2 + U_3\alpha^3 \quad (17)$$

$$, \quad U_i \in GF(2^4) \quad \forall i = 0, 1, 2, 3$$

따라서 유한체 GF(216)의 임의의 한 원소 U 를 그것의 부분체인 GF(24)을 이용하여 표현하면 다음과 같다.

$$U = U_0 + U_1\alpha + U_2\alpha^2 + U_3\alpha^3 \quad (18)$$

$$, \quad U_i \in GF(2^4)$$

이상과 같이 유한체 GF(2m)에서 위수 m이 식 (9)와 같이 $m = u \cdot v$ 를 만족하는 경우, 유한체 GF(2m)의 임의의 한 원소 U 는 부분체 GF(2u) 또는 GF(2v)을 이용하여 다음과 같이 표현할 수 있다.

$$U = U_0 + U_1\alpha + \dots + U_{u-1}\alpha^{u-1} \quad (19)$$

$$, \quad U_i \in GF(2^v)$$

$$U = U_0' + U_1'\alpha + \dots + U_{v-1}'\alpha^{v-1} \quad (20)$$

$$, \quad U_i' \in GF(2^u)$$

III. 부분체 이용한 직렬 곱셈기 설계

유한체 GF(2m) 상의 임의의 두 원소 A 와 B 를 식 (19)과 같이 부분체로 표현하면 다음과 같다.

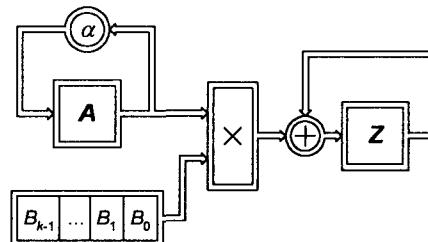
$$\begin{aligned}A &= A_0 + A_1\alpha + \dots + A_{u-1}\alpha^{u-1} \\ , \quad A_i &\in GF(2^v)\end{aligned} \quad (21)$$

$$\begin{aligned}B &= B_0 + B_1\alpha + \dots + B_{v-1}\alpha^{v-1} \\ , \quad B_i &\in GF(2^u)\end{aligned} \quad (22)$$

이 두 원소의 곱을 Z 라 하면 Z 는 다음과 같이 쓸 수 있다.

$$\begin{aligned}Z &= A \cdot B \\ &= A \cdot (B_0 + B_1\alpha + \dots + B_{v-1}\alpha^{v-1}) \\ &= (\cdots ((B_0 A) + B_1 A\alpha) + \cdots) + B_{v-1} A\alpha^{v-1}\end{aligned} \quad (23)$$

식 (23)을 살펴보면, 두 원소의 곱 Z 는 임의의 한 원소 A 에 α 를 곱해 가면서 B 의 계수들과 차례로 곱하여 계속 더하는 것이다. 따라서 식 (23)을 이용하면 그림 1과 같은 부분체를 이용한 직렬 곱셈기를 설계할 수 있다.



1. GF(24)의 병렬 곱셈기 설계

유한체 GF(24)의 0이 아닌 임의의 두원소 A와 B

$$\begin{aligned} A &= a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 \quad (24) \\ &= \sum_{i=0}^3 a_i\beta^i \quad a_i \in GF(2) \end{aligned}$$

$$\begin{aligned} B &= b_0 + b_1\beta + b_2\beta^2 + b_3\beta^3 \quad (25) \\ &= \sum_{i=0}^3 b_i\beta^i \quad b_i \in GF(2) \end{aligned}$$

로 표현할 수 있다.

두원소의 곱 Z는

$$\begin{aligned} Z &= A \cdot B = A \left(\sum_{i=0}^3 b_i\beta^i \right) = \sum_{i=0}^3 b_i(A\beta^i) \quad (26) \\ &= b_0A + b_1(A\beta) + b_2(A\beta^2) + b_3(A\beta^3) \end{aligned}$$

위의 식을 이용하면 유한체 GF(24)상에 승산기를 구성 할 수 있다. 먼저 임의의 한원소 A에 원시원 β 를 곱하면 식(24)과 같은 GF(24)의 임의 한원소 A에 β 를 곱하면

$$\begin{aligned} A\beta &= (a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3)\beta \\ &= a_3 + (a_0 + a_3)\beta + a_1\beta^2 + a_2\beta^3 \quad (27) \end{aligned}$$

A의 한원소에 $\beta 2$ 을 곱하면

$$\begin{aligned} A\beta^2 &= (a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3)\beta^2 \\ &= a_2 + (a_2 + a_3)\beta + (a_0 + a_3)\beta^2 + a_1\beta^3 \quad (28) \end{aligned}$$

A의 한원소에 $\beta 3$ 곱하면

$$\begin{aligned} A\beta^3 &= (a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3)\beta^3 \\ &= a_1 + (a_1 + a_2)\beta + (a_2 + a_3)\beta^2 + a_3\beta^3 \quad (29) \end{aligned}$$

식 26으로부터

$$\begin{aligned} Z &= (a_0b_0 + a_1b_3 + a_2b_2 + a_3b_1) \\ &\quad + (a_1b_0 + a_0b_1 + a_1b_3 + a_2b_2 + a_3b_1 + a_3b_2)\beta \\ &\quad + (a_0b_2 + a_1b_1 + a_2b_3 + a_2b_0 + a_3b_2 + a_3b_3)\beta^2 \\ &\quad + (a_1b_2 + a_2b_1 + a_3b_0 + a_3b_3)\beta^3 \quad (30) \end{aligned}$$

식 (27), (28), (29), (30)을 이용하면 그림 2과 같이 병렬 승산기를 설계할 수 있다.

식 18에서 GF(24)의 원소로 표현된 \bar{u}_i 를 GF(2)의 원소로 바꾸어 쓰면 β 는 α^{4369} 으로 다음과 같이 쓸

수 있다.

$$\begin{aligned} U &= \bar{u}_0 + \bar{u}_1\alpha + \bar{u}_2\alpha^2 + \bar{u}_3\alpha^3 \\ &= (\bar{u}_0 + \bar{u}_1\beta + \bar{u}_2\beta^2 + \bar{u}_3\beta^3) + \\ &= (\bar{u}_4 + \bar{u}_5\beta + \bar{u}_6\beta^2 + \bar{u}_7\beta^3)\alpha + \\ &= (\bar{u}_8 + \bar{u}_9\beta + \bar{u}_{10}\beta^2 + \bar{u}_{11}\beta^3)\alpha^2 + \\ &= (\bar{u}_{12} + \bar{u}_{13}\beta + \bar{u}_{14}\beta^2 + \bar{u}_{15}\beta^3)\alpha^3 \quad (31) \end{aligned}$$

$\beta^2 = \alpha^{8738}$ $\beta^3 = \alpha^{13107}$ 를 식(31)에 대입하여 정리하면 다음과 같다.

$$\begin{aligned} &= \bar{u}_0 + (\bar{u}_1 + \bar{u}_4)\alpha + (\bar{u}_2 + \bar{u}_5 + \bar{u}_8)\alpha^2 \\ &+ (\bar{u}_1 + \bar{u}_3 + \bar{u}_6 + \bar{u}_9 + \bar{u}_{12})\alpha^3 \\ &+ (\bar{u}_1 + \bar{u}_5 + \bar{u}_7 + \bar{u}_{10} + \bar{u}_{13})\alpha^4 \\ &+ (\bar{u}_3 + \bar{u}_5 + \bar{u}_9 + \bar{u}_{11} + \bar{u}_{14})\alpha^5 \\ &+ (\bar{u}_2 + \bar{u}_3 + \bar{u}_7 + \bar{u}_9 + \bar{u}_{13} + \bar{u}_{15})\alpha^6 \end{aligned}$$

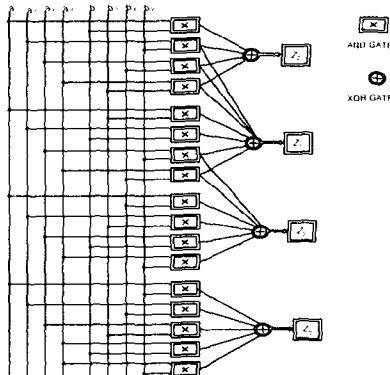


그림 2. GF(24) 상의 병렬 곱셈기

$$\begin{aligned} &+ (\bar{u}_3 + \bar{u}_6 + \bar{u}_7 + \bar{u}_{11} + \bar{u}_{13})\alpha^7 \\ &+ (\bar{u}_2 + \bar{u}_7 + \bar{u}_{10} + \bar{u}_{11} + \bar{u}_{15})\alpha^8 \\ &+ (\bar{u}_6 + \bar{u}_{11} + \bar{u}_{14} + \bar{u}_{15})\alpha^9 \\ &+ (\bar{u}_3 + \bar{u}_{10} + \bar{u}_{15})\alpha^{10} \\ &+ (\bar{u}_3 + \bar{u}_7 + \bar{u}_{14})\alpha^{11} \\ &+ (\bar{u}_3 + \bar{u}_7 + \bar{u}_{11})\alpha^{12} \\ &+ (\bar{u}_7 + \bar{u}_{11} + \bar{u}_{15})\alpha^{13} \\ &+ (\bar{u}_{11} + \bar{u}_{15})\alpha^{14} \\ &+ \bar{u}_{15}\alpha^{15} \quad (32) \end{aligned}$$

식 (32)에 근거하여 표준 기저로 표현된 GF(216)의 원소들을 GF(24) 상의 기저 표현으로 변환할 수 있다.

$$\begin{aligned}
 u_0 &= \overline{u_0} \\
 u_1 &= \overline{u_1} + \overline{u_4} \\
 u_2 &= \overline{u_2} + \overline{u_5} + \overline{u_8} \\
 u_3 &= \overline{u_1} + \overline{u_3} + \overline{u_6} + \overline{u_9} + \overline{u_{12}} \\
 u_4 &= \overline{u_1} + \overline{u_5} + \overline{u_7} + \overline{u_{10}} + \overline{u_{13}} \\
 u_5 &= \overline{u_3} + \overline{u_5} + \overline{u_9} + \overline{u_{11}} + \overline{u_{14}} \\
 u_6 &= \overline{u_2} + \overline{u_3} + \overline{u_7} + \overline{u_9} + \overline{u_{13}} + \overline{u_{15}} \\
 u_7 &= \overline{u_3} + \overline{u_6} + \overline{u_7} + \overline{u_{11}} + \overline{u_{13}} \\
 u_8 &= \overline{u_2} + \overline{u_7} + \overline{u_{10}} + \overline{u_{11}} + \overline{u_{14}} \\
 u_9 &= \overline{u_6} + \overline{u_{11}} + \overline{u_{14}} + \overline{u_{15}} \\
 u_{10} &= \overline{u_3} + \overline{u_7} + \overline{u_{14}} \\
 u_{11} &= \overline{u_3} + \overline{u_7} + \overline{u_{14}} \\
 u_{12} &= \overline{u_3} + \overline{u_7} + \overline{u_{11}} \\
 u_{13} &= \overline{u_7} + \overline{u_{11}} + \overline{u_{15}} \\
 u_{14} &= \overline{u_{11}} + \overline{u_{15}} \\
 u_{15} &= \overline{u_{15}}
 \end{aligned} \tag{33}$$

또한 식(33)을 선형 조합하면 역변환도 구할 수 있다.

$$\begin{aligned}
 \overline{u_0} &= u_0 \\
 \overline{u_1} &= u_4 + u_5 + u_6 + u_8 + u_{11} + u_{12} + u_{13} + u_{15} \\
 \overline{u_2} &= u_8 + u_{10} + u_{12} \\
 \overline{u_3} &= u_{12} + u_{13} + u_{15} \\
 \overline{u_4} &= u_1 + u_4 + u_5 + u_6 + u_8 + u_{11} + u_{12} + u_{13} + u_{15} \\
 \overline{u_5} &= u_5 + u_6 + u_7 + u_8 + u_9 + u_{10} + u_{13} + u_{14} \\
 \overline{u_6} &= u_9 + u_{11} + u_{12} + u_{15} \\
 \overline{u_7} &= u_{13} + u_{14} \\
 \overline{u_8} &= u_2 + u_5 + u_6 + u_7 + u_9 + u_{12} + u_{13} + u_{14} \\
 \overline{u_9} &= u_6 + u_7 + u_8 + u_9 + u_{10} + u_{11} + u_{14} + u_{15} \\
 \overline{u_{10}} &= u_{10} + u_{12} + u_{13} \\
 \overline{u_{11}} &= u_{14} + u_{15} \\
 \overline{u_{12}} &= u_3 + u_4 + u_5 + u_7 + u_{10} + u_{11} + u_{12} + u_{14} \\
 \overline{u_{13}} &= u_7 + u_9 + u_{11} + u_{15} \\
 \overline{u_{14}} &= u_{11} + u_{12} + u_{14} + u_{15} \\
 \overline{u_{15}} &= u_{15}
 \end{aligned} \tag{34}$$

2. GF(24)를 이용한 GF(216)의 직렬 곱셈기

유한체 GF(216)의 임의의 한 원소 A 를 부분체 GF(24)를 이용하여 표현하면 다음과 같이 쓸 수 있다.

$$A = A_0 + A_1\alpha + A_2\alpha^2 + A_3\alpha^3 \tag{35}$$

$$, A_i \in GF(2^4)$$

여기에서 GF(216)의 원시원 α 를 곱하고 식 (35)를 이

용하여 정리하면 다음과 같이 된다.

$$\begin{aligned}
 A \cdot \alpha &= A_0\alpha + A_1\alpha^2 + A_2\alpha^3 + A_3\alpha^4 \\
 &= A_0\alpha + A_1\alpha^2 + A_2\alpha^3 + A_{3(\beta)} + \alpha + \alpha^3 \\
 &= A_3\beta + (A_0 + A_3)\alpha + A_1\alpha^2 + (A_2 + A_3)\alpha^3
 \end{aligned} \tag{36}$$

그러므로 식 (36)를 이용하면 그림 3와 같이 GF(216)의 임의의 한 원소 A 에 원시원 α 를 곱하는 회로를 설계할 수 있다. 그림 2에서 모든 선은 4비트 버스이고 \square 는 4비트 레지스터를, \oplus 는 GF(24) 상의 병렬 덧셈기를, \boxed{B} 는 GF(24) 상의 임의의 한 원소에 GF(24)의 원시원 β 를 곱하는 회로를 나타내고 있다.

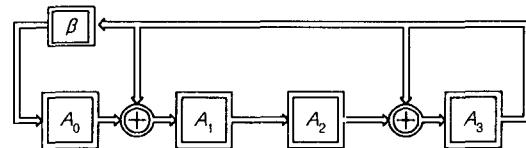


그림 3. GF(216) 상의 임의의 한 원소에 α 를 곱하는 회로

유한체 GF(24)의 임의의 한 원소 C 에 원시원 β 를 곱하고, 식 (19)를 이용하여 정리하면

$$\begin{aligned}
 C \cdot \beta &= (c_0 + c_1\beta + c_2\beta^2 + c_3\beta^3) \\
 &= c_3 + (c_0 + c_3)\beta + c_1\beta^2 + c_2\beta^3
 \end{aligned}$$

$$(37)$$

식(37)을 이용하면 그림 4과 같이 설계할 수 있다.

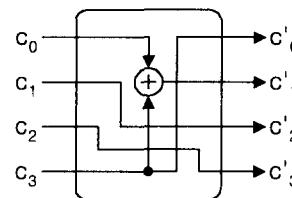


그림 4. GF(24) 상의 임의의 한 원소에 β 를 곱하는 회로

따라서 $\boxed{\beta}$ 는 1개의 2입력 XOR로 구현할 수 있다.

그림 1과 그림 3을 이용하면 그림 5과 같은 부분체 GF(24)를 이용한 GF(216) 상의 직렬 곱셈기를 설계할

곱셈의 시뮬레이션 결과		
	연산 A	연산 B
i=0	j=0	결과 C
i=0	j=0	0111011000110001
i=1	j=0	0111011000110001
i=2	j=0	0111011000110001
i=3	j=0	0111011000110001
i=4	j=1	1100011001100010
i=5	j=1	1100011001100010
i=6	j=1	1100011001100010
i=7	j=1	1100011001100010
i=8	j=1	1100011001100010
i=9	j=2	0001111001100100
i=10	j=2	0001111001100100
i=11	j=2	0001111001100100
i=12	j=3	0010010111000100
i=13	j=3	0010010111000100
i=14	j=3	0010010111000100
i=15	j=3	0010010111000100
i=16	j=3	0010010111000100
i=17	j=3	0010010111000100
i=18	j=3	0010010111000100
i=19	j=3	0010010111000100
i=20	j=3	0010010111000100
i=21	j=3	0010010111000100
i=22	j=3	0010010111000100
i=23	j=3	0010010111000100
i=24	j=3	0010010111000100
i=25	j=3	0010010111000100
i=26	j=3	0010010111000100
i=27	j=3	0010010111000100
i=28	j=3	0010010111000100
i=29	j=3	0010010111000100
i=30	j=3	0010010111000100
i=31	j=3	0010010111000100
i=32	j=3	0010010111000100
i=33	j=3	0010010111000100
i=34	j=3	0010010111000100
i=35	j=3	0010010111000100
i=36	j=3	0010010111000100
i=37	j=3	0010010111000100
i=38	j=3	0010010111000100
i=39	j=3	0010010111000100
i=40	j=3	0010010111000100
i=41	j=3	0010010111000100
i=42	j=3	0010010111000100
i=43	j=3	0010010111000100
i=44	j=3	0010010111000100
i=45	j=3	0010010111000100
i=46	j=3	0010010111000100
i=47	j=3	0010010111000100
i=48	j=3	0010010111000100
i=49	j=3	0010010111000100
i=50	j=3	0010010111000100
i=51	j=3	0010010111000100
i=52	j=3	0010010111000100
i=53	j=3	0010010111000100
i=54	j=3	0010010111000100
i=55	j=3	0010010111000100
i=56	j=3	0010010111000100
i=57	j=3	0010010111000100
i=58	j=3	0010010111000100
i=59	j=3	0010010111000100
i=60	j=3	0010010111000100
i=61	j=3	0010010111000100
i=62	j=3	0010010111000100
i=63	j=3	0010010111000100
i=64	j=3	0010010111000100
i=65	j=3	0010010111000100
i=66	j=3	0010010111000100
i=67	j=3	0010010111000100
i=68	j=3	0010010111000100
i=69	j=3	0010010111000100
i=70	j=3	0010010111000100
i=71	j=3	0010010111000100
i=72	j=3	0010010111000100
i=73	j=3	0010010111000100
i=74	j=3	0010010111000100
i=75	j=3	0010010111000100
i=76	j=3	0010010111000100
i=77	j=3	0010010111000100
i=78	j=3	0010010111000100
i=79	j=3	0010010111000100
i=80	j=3	0010010111000100
i=81	j=3	0010010111000100
i=82	j=3	0010010111000100
i=83	j=3	0010010111000100
i=84	j=3	0010010111000100
i=85	j=3	0010010111000100
i=86	j=3	0010010111000100
i=87	j=3	0010010111000100
i=88	j=3	0010010111000100
i=89	j=3	0010010111000100
i=90	j=3	0010010111000100
i=91	j=3	0010010111000100
i=92	j=3	0010010111000100
i=93	j=3	0010010111000100
i=94	j=3	0010010111000100
i=95	j=3	0010010111000100
i=96	j=3	0010010111000100
i=97	j=3	0010010111000100
i=98	j=3	0010010111000100
i=99	j=3	0010010111000100
i=100	j=3	0010010111000100
i=101	j=3	0010010111000100
i=102	j=3	0010010111000100
i=103	j=3	0010010111000100
i=104	j=3	0010010111000100
i=105	j=3	0010010111000100
i=106	j=3	0010010111000100
i=107	j=3	0010010111000100
i=108	j=3	0010010111000100
i=109	j=3	0010010111000100
i=110	j=3	0010010111000100
i=111	j=3	0010010111000100
i=112	j=3	0010010111000100
i=113	j=3	0010010111000100
i=114	j=3	0010010111000100
i=115	j=3	0010010111000100
i=116	j=3	0010010111000100
i=117	j=3	0010010111000100
i=118	j=3	0010010111000100
i=119	j=3	0010010111000100
i=120	j=3	0010010111000100
i=121	j=3	0010010111000100
i=122	j=3	0010010111000100
i=123	j=3	0010010111000100
i=124	j=3	0010010111000100
i=125	j=3	0010010111000100
i=126	j=3	0010010111000100
i=127	j=3	0010010111000100
i=128	j=3	0010010111000100
i=129	j=3	0010010111000100
i=130	j=3	0010010111000100
i=131	j=3	0010010111000100
i=132	j=3	0010010111000100
i=133	j=3	0010010111000100
i=134	j=3	0010010111000100
i=135	j=3	0010010111000100
i=136	j=3	0010010111000100
i=137	j=3	0010010111000100
i=138	j=3	0010010111000100
i=139	j=3	0010010111000100
i=140	j=3	0010010111000100
i=141	j=3	0010010111000100
i=142	j=3	0010010111000100
i=143	j=3	0010010111000100
i=144	j=3	0010010111000100
i=145	j=3	0010010111000100
i=146	j=3	0010010111000100
i=147	j=3	0010010111000100
i=148	j=3	0010010111000100
i=149	j=3	0010010111000100
i=150	j=3	0010010111000100
i=151	j=3	0010010111000100
i=152	j=3	0010010111000100
i=153	j=3	0010010111000100
i=154	j=3	0010010111000100
i=155	j=3	0010010111000100
i=156	j=3	0010010111000100
i=157	j=3	0010010111000100
i=158	j=3	0010010111000100
i=159	j=3	0010010111000100
i=160	j=3	0010010111000100
i=161	j=3	0010010111000100
i=162	j=3	0010010111000100
i=163	j=3	0010010111000100
i=164	j=3	0010010111000100
i=165	j=3	0010010111000100
i=166	j=3	0010010111000100
i=167	j=3	0010010111000100
i=168	j=3	0010010111000100
i=169	j=3	0010010111000100
i=170	j=3	0010010111000100
i=171	j=3	0010010111000100
i=172	j=3	0010010111000100
i=173	j=3	0010010111000100
i=174	j=3	0010010111000100
i=175	j=3	0010010111000100
i=176	j=3	0010010111000100
i=177	j=3	0010010111000100
i=178	j=3	0010010111000100
i=179	j=3	0010010111000100
i=180	j=3	0010010111000100
i=181	j=3	0010010111000100
i=182	j=3	0010010111000100
i=183	j=3	0010010111000100
i=184	j=3	0010010111000100
i=185	j=3	0010010111000100
i=186	j=3	0010010111000100
i=187	j=3	0010010111000100
i=188	j=3	0010010111000100
i=189	j=3	0010010111000100
i=190	j=3	0010010111000100
i=191	j=3	0010010111000100
i=192	j=3	0010010111000100
i=193	j=3	0010010111000100
i=194	j=3	0010010111000100
i=195	j=3	0010010111000100
i=196	j=3	0010010111000100
i=197	j=3	0010010111000100
i=198	j=3	0010010111000100
i=199	j=3	0010010111000100
i=200	j=3	0010010111000100
i=201	j=3	0010010111000100
i=202	j=3	0010010111000100
i=203	j=3	0010010111000100
i=204	j=3	0010010111000100
i=205	j=3	0010010111000100
i=206	j=3	0010010111000100
i=207	j=3	0010010111000100
i=208	j=3	0010010111000100
i=209	j=3	0010010111000100
i=210	j=3	0010010111000100
i=211	j=3	0010010111000100
i=212	j=3	0010010111000100
i=213	j=3	0010010111000100
i=214	j=3	0010010111000100
i=215	j=3	0010010111000100
i=216	j=3	0010010111000100

마지막 줄은 16회의 순차 연산이 수행된 최종결과이다.

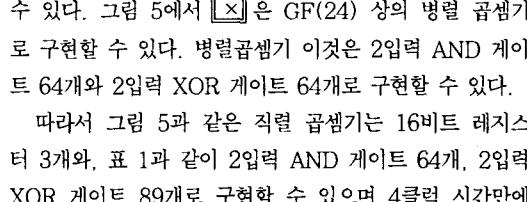


표 1. 그림 3과 같은 직렬 곱셈기의 회로 규모

GF(24) 상의 병렬 곱셈기	AND : $16 \times 4 = 64$ XOR : $16 \times 4 = 64$
GF(24) 상의 병렬 덧셈기	XOR : $4 \times 6 = 24$
β 곱셈기	XOR : $1 \times 1 = 1$
합 계	AND = 64 XOR = 89

본 논문에서는 표준기저 상에서 부분체를 이용한 GF(2m) 상의 곱셈기의 구성 방법을 제시하고, 실제 예로써 유한체 GF(216) 상의 곱셈기를 그것의 부분체인 GF(24)를 이용하여 설계하였다. 제안된 곱셈기는 직렬 곱셈기의 긴 지연시간과 병렬 곱셈기의 복잡한 회로 사이를 적절하게 절충함으로써, 직렬 곱셈기보다는 짧은 지연 시간에 결과를 얻을 수 있으며 병렬 곱셈기보다는 적은 회로로 구현할 수 있는 장점이 있다.

GF(216) 상의 병렬 곱셈기는 일반적으로 1클럭 시간 만에 결과를 얻을 수 있는 반면에 2입력 AND 901개와 2입력 XOR 870개가 소요된다. 본 논문에서 제안한 곱셈기는 회로규모와 지연시간에 대한 상대적인 관계를 적절히 절충한 것이다. GF(216)의 경우, GF(24)를 이용하여 설계한 그림 5과 같은 직렬 곱셈기는 표 1과 같이 2입력 AND 게이트 64개, 2입력 XOR 게이트 89개로 구현할 수 있으며 4클럭 시간만에 결과를 얻을 수 있다. 또 GF(24)를 이용하여 설계한 그림 6과 같은 직렬 곱셈기는 표 2와 같이 2입력 AND 게이트 32개, 2입력 XOR 게이트 44개로 구현할 수 있으며 2클럭 시간만에 결과를 얻을 수 있다.

IV. 결 론

저자 소개

참고문헌

- [1] 이만영, BCH 부호와 Reed-Solomon 부호, 민음사, 1988
- [2] C.Paar, "A New Architecture for a Parallel Finite Field Multiplier with Low Complexity Based on Composite Fields," IEEE Trans. Computers, Vol.45, No.7, pp.856~861, July 1996.
- [3] YongSuk Cho and SangKyu Park, "Design of GF(2^m) Multiplier using Its Subfields," Electronics Letters, Vol.34, No.7, pp.650~651, April 1998.
- [4] A. M. Patel, "On-the-fly decoder for multiple byte errors," IBM J. RES. DEVELOP., Vol. 30, No.3, pp.259~269, May 1986.



신 원 철

1990.2 청주대학교 대학원 전
자계산학과 졸업
(공학석사)
현재 : 청주대학교 대학원 전자
공학과 박사과정
현재 : 주성대학 컴퓨터 프로그
래밍과 조교수



이 명 호

1981.2 연세대학교 대학원 전
자공학과 졸업
(공학석사)
1991.8 연세대학교 대학원 전
자공학과 졸업
(공학박사)
현재 : 청주대학교 첨단공학부
교수