(19) 대한민국특허청(KR)
(12) 특허공보(B1)

(51) Int. Cl.[4]
G06F 7/52

(45) 공고일자 1988년12월17일
(11) 공고번호 특1988-0002659

(21) 출원번호	특1985-0006167	(65) 공개번호	특1987-0002502
(22) 출원일자	1985년08월24일	(43) 공개일자	1987년03월31일

(71) 출원인 삼성전자주식회사 정재은
경기도 수원시 매탄동 416

(72) 발명자 정병국
경기도 수원시 원천동 아주아파트 나-106

(74) 대리인 이동모

심사관 : 고금영 (책자공보 제1493호)

(54) 유한 필드내의 곱셈 처리회로

요약

내용 없음.

대표도

도1

명세서

[발명의 명칭]

유한 필드내의 곱셈 처리회로

[도면의 간단한 설명]

제 1 도는 본 발명의 회로도.

제 2 도는 본 발명 회로도의 각부 파형도.

* 도면의 주요부분에 대한 부호의 설명

10 : 레지스터 20 : 병렬/직렬 변환기

AD_0~AD_7 : 앤드게이트 EX_0~EX_7 : 익스크루시버 오아게이트

FF_0~FF_7 : 플립플롭

[발명의 상세한 설명]

본 발명은 디지탈 신호 처리시에 두심볼(Symbol)을 곱셈 연산처리 할 수 있게한 유한 필드내의 곱셈 처리회로에 관한 것이다. 유한 필드(Galois field)내에서 곱셈 연산은 주어진 필드의 한계를 벗어나는 캐리(Carry : 자리올림)는 다시 필드내의 정의된 값으로 궤환되도록 함으로써 자리올림이 없는 일정한 디지탈 상태 신호로서 표시할 수가 있어 연산결과가 항상 필드내를 벗어나지 못하기 때문에 연산 처리시에 편리한 이점이 있다.

일예로서 유한 필드 GF(28)내에 8비트의 두심볼을 곱셈 연산 할때에는 FF(16진수)보다 큰 연산 결과는 정의된 값으로 궤환되어 다시 8비트의 디지탈 신호로서 표시할 수 있는 것이다. 따라서 종래에는 두 심볼을 A(A_0~A_7), B(B_0~B_7)이라할 때 각 비트(bit)끼리 앤드게이트 및 익스크루시버 오아게이트를 사용하여 8비트 대 8비트의 곱셈 연산시에 발생가능한 모든 디지탈 상태 신호를 1:1대응시켜 가며 게이트로 처리하기 때문에 곱셈 처리회로가 복잡하여질 뿐 아니라 높은 고주파의 클럭 신호가 필요하게 되는 단점이 있는 것이었다.

본 발명은 유한 필드내에서 주어진 필드의 한계를 벗어날때에 일정한 디지탈 상태 신호로 궤환되는 점을 감안하여 연산 곱셈되는 심볼을 직렬로 인가되게 구성하여 하나의 비트에 대하여 1:8의 연산이 되게하고 연산 결과가 궤환되도록 하되 캐리가 발생되는 것은 우한 필드내로 환원될 수 있는 유한 필드내의 곱셈 처리 회로를 제공하여 유한 필드내의 곱셈 연산회로의 단순화 및 연산속도를 증진시킬 수 있도록 한 것

으로 이를 첨부도면에 의하여 상세히 설명하면 다음과 같다.

제 1 도는 본 발명의 회로도로서 8비트의 두 심볼(A)(B)중에 한 심볼(A)은 레지스터(10)에 인가되게 구성시켜 병렬로 출력되어 앤드게이트(AD_0~AD_7)의 일측에 인가되게 구성하고 앤드게이트(AD_0~AD_7)의 타측에는 다른 심볼(B)의 8비트신호가 병렬/직렬 변환기(20)를 통하여 인가되게 구성시켜 앤드게이트(AD_0~AD_7)의 출력이 익스크루시버 오아게이트(EX_0~EX_7)를 통하여 플립플롭(FF_0~FF_7)에 인가되게 구성한후 플립플롭(FF_0~FF_7)의 출력이 순차적으로 익스크루시버 오아게이트(EX_0~EX_7)로 궤환되게 구성시켜된 것으로 여기서 사용되는 플립플롭(FF_0~FF_7)은 D-플립플롭으로서 D는 입력단자, Q는 출력단자「D」는 클럭입력단자를 나타낸다.

이와같이 구성된 본 발명에서 임의의 두수의 심볼이 각각 A,B라 하고 두수에 의한 곱셈 결과를 C라 하면 유한 필드(GF)내에서 다음의 식이 성립하게 된다.

$$C=A\otimes B=\sum_{i=0}^{n} Bi(A\alpha^{i})$$

그런데 GF(2^8)내에서의 연산이라면 i=0~i=7까지 변화되므로 위의 결과식을 다시 정리하면

$$C=\sum_{i=0}^{7} Bi(A\alpha^{i})$$

$=B_0(A\alpha^0)+B_1(A\alpha^1)+B_2(A\alpha^2)+\cdots+B_6(A\alpha^6)+B_7(A\alpha^7)$-①식이 된다.

따라서 A값을 α^0에서 α^7까지 순차적으로 곱하는 회로가 필요하며 $STEP_0$ ~$STEP_7$까지의 B값의 각 비트 B_0~B_7별로 더해주는 기능이 필요하게 된다. 즉 임의의 두 심벌 A,B를 유한 필드내에서 곱셈한 최종 결과의 값 C는 상기 ①식에서와 같이

$$C=\sum_{i=0}^{7} Bi(A\alpha^{i})$$

$=B_0((A\alpha^0)+B_1(A\alpha^1)+B_2(A\alpha^2)+B_3(A\alpha^3)+B_4(A\alpha^4)+B_5(A\alpha^5)+B_6(A\alpha^6)+B_7(A\alpha^7)$

단 $A=A_0\alpha^0+A_1\alpha+A_2\alpha^2+\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots+A_6\alpha^6+A_7\alpha^7$

$B=B_0\alpha^6+B_1\alpha^1+B_2\alpha^2+\ldots\ldots\ldots\ldots\ldots\ldots\ldots+B_6\alpha^6+B_7\alpha^7$이 된다.

따라서 상기 식을 만족시키기 위해서는 각 B_0~B_7과 $A\alpha^1$(i=0~7)과의 곱셈(Anding)을 위한 앤드게이트(AD_0~AD_7)와, $A\alpha^1$(i=0~7)자체의 연산을 위해 심벌 A(GF(2^8소)와 α를 곱하는 회로와, $B_0(A\alpha^0)$에서 $B_7(A\alpha^7)$까지의 각 연산 결과값을 더해줄 익스크루시버 오아게이트(EX_0~EX_7)가 필요하게 된다. 여기서 A와 α를 곱하는 회로는 유한필드의 개념상 8비트의 데이타를 넘는 캐리 발생시 유한 필드로 한정시켜주기 위하여 고정된 데이타(16진수로 1D=2진수로 00101101)를 인가시켜 주어야 하며 이를 위하여 플립플롭(FF_7)의 출력단자(Q)출력에서 캐리 발생시 이를 익 스크루시버 오아게이트(EX_4)(EX_3)(EX_2)(EX_0)의 입력측에 인가시켜 주게된다. 따라서 캐리 발생시 유한필드로 한정시켜 주기위한 데이타(00101101)가 익스크루시버 오아게이트(EX_4)(EX_3)(EX_2)(EX_0)에 인가되므로써 A와 α를 곱하는 연산이 유한 필드내에서 처리되게 하는 것이다.

이와같이 C=A⊗B의 연산은 데이타(B_7)과 심볼(A)를 앤드 연산하고 그 결과치에 α^7를 곱하고 여기에 데이타(B_6)와 심볼(A)를 앤드 연산한 값에 α^6를 곱한 값을 익스크루시버 해주는 방식으로 이를 순차적으로 B_0까지 연산하여 얻은 C_7 C_6~C_0의 값이 결과치가 되는 것으로 제 1 도의 회로와 같이 레지스터(10)에 심볼(A)의 데이타(A_7~A_0)가 인가된후 병렬/직렬 변환기(20)로 심볼(B)의 데이타(B_7~B_0)가 순차적으로 인가되어 앤드게이트(AD_0~AD_7), 익 스크루시버 오아게이트(EX_0~EX_7), 플립플롭(FF_0~FF_7)으로 순차적으로 연산하여 곱한 값이 심볼 C(C_0~C_7)을 얻을 수가 있는 것이다.

이를 계산에 의하여 살펴보면 A(α^{12})=11001101, B(α^7)=10000000이라 하면 C=A⊗B=$\alpha^{12}\otimes\alpha^7=\alpha^{19}$=01011010이 된다. 이 같은 계산에 의한 결과값이 본 발명에 의해 얻어질 수 있는 가를 살펴보면 다음과 같다. 먼저 각 심볼 A와 B의 연산값은 제 ① 식에서와 같이

$$C=\sum_{i=0}^{7} Bi(A\alpha^{i})$$

$=B_0((A\alpha^0)+B_1(A\alpha)+B_2(A\alpha^2)+B_3(A\alpha^3)+B_4(A\alpha^4)+B_5(A\alpha^5)+B_6(A\alpha^6)+B_7(A\alpha^7)$이 되며 이때 A,

$\alpha^0=\alpha^{12}$=11001101, A, $\alpha^1=\alpha^{13}$=10000111, A, $\alpha^2=\alpha^{14}$=00010011, A, $\alpha^3=\alpha^{15}$=00100110, A, $\alpha^4=\alpha^{16}$=01001100, A, $\alpha^5=\alpha^{17}$=10011000, A, $\alpha^6=\alpha^{18}$=00101101, A, $\alpha^7=\alpha^{19}$=01011010가 되고 $B_0,B_1,B_2,B_3,B_4,B_5,B_6$는 모두「0」이므로 결국 상기식은 $C=B_7A\alpha^7=\alpha^{19}$=01011010가 되는 것이다.

그러므로 본 발명에서는 유한 필드내에서의 두 심볼의 곱을 1비트 대 8비트로 연산한 결과값을 쉽게 얻을수가 있는 것이다. 이상에서와 같이 본 발명은 유한 필드내에 8비트의 두 개의 심볼을 연산 처리할 때에 연산결과가 펄드내에 정의된 값으로 환원되는 점을 이용하여 단순한 곱셈 회로를 제공할 수가 있어 연산 속도를 증진시킬 수 있는 이점이 있는 것이다.

(57) 청구의 범위

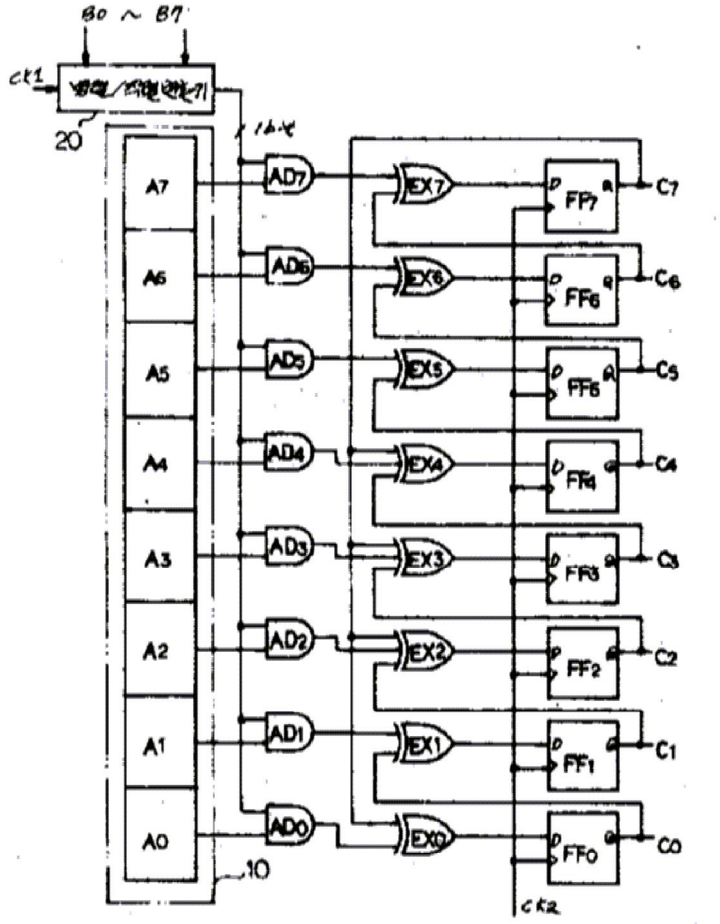
청구항 1

페지스터(10)에 인가된 값과 병렬/직렬변환기(20)를 통하여 인가되는 값을 유한필드내에서 곱셈처리시키는 회로에 있어서, 앤드게이트(AD_0~AD_7)의 울럭이 익스코쿠시 내오아게이트(EX_0~EX_7)를 통하여 플립플롭(FF_0~FF_7)에 인가되게 구성한 후 플립플롭(FF_0~FF_7)의 연산값이 순차적으로 익스코루시버오아게이트(EX_0~EX_7)로 궤환되개 구성한 유한핀트내의 곱셈처리회로.

※ 참고사항 : 최초출원 내용에 의하여 공개하는 것임.

도면

도면1



도면2