(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[5]
G06F 15/31

(11) 공개번호 특1994-0012170
(43) 공개일자 1994년06월22일

(21) 출원번호 특1992-0022937
(22) 출원일자 1992년11월30일

(71) 출원인 삼성전자 주식회사 윤종용
경기도 수원시 권선구 매탄동 416번지
(72) 발명자 이종환
서울특별시 동대문구 제기2동 892-66 한전아파트 다동 503호
(74) 대리인 이영필, 최덕용

심사청구 : 있음

(54) 유한체상의 역수 산출방법 및 장치

요약

본 발명은 유한체상에서 역수를 굿하는 방법 및 장치에 관한 것으로, 방법은 유한체GF(2^n)내에서 비트로 표현된 임의의 수 (a^k)를 이용하여 비트로 표현된 그의 역수(a^{-k})를 구하는 방법에 있어서, 상기 유한체GF(2^n)의 원시원을 a라할 때, 상기 a^k가 a^0인 경우에 a^0를 a^{-k}로서 구하는 과정과;$a^k \neq a^0$인 경우에는 A 및 A^{-1}에 a^0를 대입한 후 상기 A 값이 상기 a^k갑과 동일한 값을 가질때까지 상기 A 및 A^{-1}에 상기 유한체의 원시원 a및 a^{-1}을 각각 승산하는 과정과; 상기 A^{-1}의 값을 a^{-1}로서 구하는 과정을 포함하여 구성되며 이를 구현하기 위한 장치는 a곱셈기와 a^{-1}곱셈기와 비교기 및 랫치수단을 포함하여 구성되는 것으로, 특업테이블방식이 아닌 하드웨어로 구현할 수 있는 유한체상의 역수를 구하는 알고리즘을 새로이 제시함과 동시에 이를 수행할 수 있는 장치를 제공하며 종래의 유한체상의 역수를 구하는 장치보다 그 크기가 줄어드는 효과가 있다.

대표도

도2

명세서

[발명의 명칭]

유한체상의 역수 산출방법 및 장치

[도면의 간단한 설명]

제2도는 본 발명에 일실시예에 따른 유한체상의 역수 산출방법의 순서도이고,

제3도는 본 발명의 일실시예에 따른 유한체상의 역수 산출장치의 블럭도이고,

제4도는 a곱셈기 및 a^{-1}곱셈기의 일실시예에 따른 블럭도이다.

본 내용은 요부공개 건이므로 전문 내용을 수록하지 않았음

(57) 청구의 범위

청구항 1

유한체GF(2^n)내에서 비트로 표현된 임의의 수 (a^k)를 이용하여 비트로 표현된 그의 역수 (a^{-k})를 구하는 방법에 있어서, 상기 유한체GF(2^n) 의 원시원을 a라 할 때, 상기 a^k가 a^0인 경우에 a^0를 a^{-k}로서 구하는 과정과; $a^k \neq a^0$인 경우에는 A 및 A^{-1}에 a^0를 대입한 후 상기 A값이 상기 a^k값과 동일한 값을 가질때까지 상기 A 및 A^{-1}에 상기 유한체의 원시원 a 및 a^{-1}을 각각 승산하는 과정과; 상기 A^{-1}의 값을 a^k로서 구하는 과정을 구비하는 것을 특징으로 하는 유한체상의 역수 산출방법.

청구항 2

제1항에 있어서, 상기 A 및 A^{-1}에 상기 유한체의 원시원 a 및 a^{-1}을 각각 승산하는 과정은 상기 A값이 상기 a^{k}값과 동일한 값을 가지거나 또는 상기 A^{-1}의 값이 상기 a^{k}값과 동일한 값을 가질때까지 수행되며; A값이 a^{k}값과 동일한 경우에는 A^{-1}의 값을 a^{-k}로서 구하고, A^{-1}의 값이 a^{k}값과 동일한경우에는 A의 값을 a^{-k}로서 구하게 되는 것을 특징으로 하는 유한테상의 역수 산출방법.

청구항 3

유한체GF(2^{n})내에서 비트로 표현된 임의의 수 (a^{k})를 이용하여 비트로 표현된 그의 역수 (a^{-k})를 구하는 방법에 있어서, 상기 유한체GF(2^{n}) 의 원시원을 a라 할 때, 초기값으로 a^{0}를 로딩하고 클럭이 인가될 때마다 그 자시이 가지고 있는 값에 a를 곱셈하는 a곱셈기와; 초기값으로 a^{0}를 로딩하고 클럭이 인가될 때마다 그 자신이 가지고 있는 값에 a^{-1} 를 곱셈하는 a^{-1}곱셈기와; 상기 a^{k}와 상기 a 곱셈기의 출력을 비교하여 동일한 경우에 인에이블되는 신호를 출력하는 비교기; 및 상기 비교기의 출력이 인에이블되는 경우에 상기 a^{-1}곱셈기의 출력을 랫치하는 랫치수단을 구비하여 랫치수단의 울력이 a^{-k}가 되는것을 특징으로 하는 유한체상의 역수 산출장치.

청구항 4

유한체GF(2^{n})내에서 비트로 표현된 임의의 수 (a^{k})를 이용하여 비트로 표현된 그의 역수 (a^{-k})를 구하는 방법에 있어서, 상기 유한체 GF(2^{n})의 원시원을 a라 할 때, 초기값으로 a^{0}를 로딩하고 클럭이 인가될 때마다 그 자시이 가지고 있는 값에 a를 곱셈하는 a곱셈기와; 초기값으로 a^{0}를 로딩하고 클럭이 인가될 때마다 그 자신이 가지고 있는 값에 a^{-1} 를 곱셈하는 a^{-1}곱셈기와; 상기 a^{k}와 상기 a 곱셈기의 출력을 비교하여 동일한 경우에 인에이블되는 신호를 출력하는 제1비교기와; 상기 a^{k}와 상기 a^{-1}곱셈기의 출력을 비교여 동일한 경우에 인에이블되는 신호를 출력하는 제2비교기; 및 상기 제2비교기의 출력이 인에이블인 경우에는 상기 a 곱셈기의 출력을 선택하고 상기 제1비교기의 출력이 인에이블인 경우에는 상기 a^{-1}곱셈기의 출력을 선택하게 되는 선택기를 구비하여 선택기의 출력이 임의의 수 (a^{k})의 역수 (a^{-k})가 되는 것을 특징으로 하는 유한체상의 역수 산출장치.

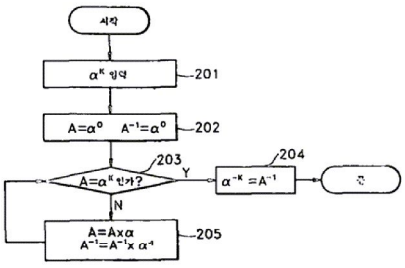
청구항 5

오류정정부호의 복호시, 유한체GF(2^{n})내에서 연산이 수행되며, 오류위치다항식의 계수를 구하기 위하여 n비트로 구성되는 오증들(S)을 이용하여 그의 역수(S^{-1})를 산출하기 위한 장치에 있어서, 상기 유한테GF(2^{n})의 원시원을 a라 할 때, 초기값으로 a^{0}(100…0)를 로딩하고 클럭이 인가될 때마다 그 자신이 가지고 있는 값에 a를 곱셈하는 a 곱셈기와; 초기값으로 a^{0}(100…0)를 로딩하고 클럭이 인가될 때마다 그 자신이 가지고 있는 값에 a^{-1}곱셈하는 a^{-1}곱셈기와; 상기 오중 S와 상기 a곱셈기의 출력을 비교하여 동일한 경우에 인에이블되는 신호를 출력하는 비교기; 및 상기 비교기의 출력이 인에이블되는 경우에 상기 a^{-1}곱셈기의 출력을 랫치하는 랫치수단을 구비하여 랫치수단의 출력이 오중의 역수 S^{-1}이 되는 것을 특징으로 하는 유한체상의 오증역수 산출장치.

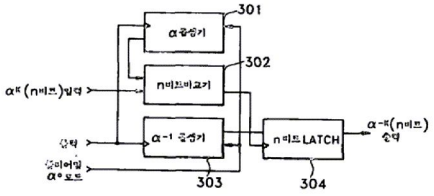
※ 참고사항 : 최초출원 내용에 의하여 공개하는 것임.

도면

도면2



도면3



도면4