확장성에 유리한 병렬 알고리즘 방식에 기반한 GF(2^m) 나눗셈기의 VLSI 설계

문상국*

VLSI Design of an Improved Structure of a GF(2^m) Divider

San-Gook Moon*

요 약

본 연구에서 제안한 유한체 나눗셈기는 기존에 존재하는 알고리즘을 개선하여 병렬 처리가 가능하도록 개선하였고, 이를 위하여 n bit look-up table 참조 방식을 도입하여 division당 2m/n cycle의 연산 처리량을 가질 때, n의 증가에 따른 회로 면적의 증가, 동작 주파수의 감소가 적어지게 된다. 이에 따라, 높은 연산 처리량과 적은 회로 면적이라는 두 가지 목표를 모두 달성할 수 있는 나눗셈기의 구현이 가능해졌다. 이를 바탕으로, Reed-Solomon Code와 ECC (Elliptic Curve Cryptography) 암호화 알고리즘 등, 통신의 오류 정정 부호 분야와 암호화 분야에서 자주 응용되는 Galois Field에서의 나눗셈 연산을 수행하는 GF(2^m) 나눗셈기를 VHDL을 이용하여 설계하고 FPGA에 구현하여 기능을 검증하였다. 제안된 나눗셈기는 m=4, n=2의 경우에 대해 설계, 검증을 수행하였다. 회로의 구현은 Altera의 10만 게이트 급 FPGA EP20K30ETC144-1 Chip을 이용하여 77Mhz의 최대 동작 주파수상에서의 동작을 검증하였다.

ABSTRACT

In this contribution, we developed and improved an existing GF (Galois Field) dividing algorithm by suggesting a novel architecture for a finite field divider, which is frequently required for the error correction applications and the security-related applications such as the Reed-Solomon code, elliptic curve encryption/decryption, is proposed. We utilized the VHDL language to verify the design methodology, and implemented the architecture on an FPGA chip. We suggested the n-bit lookup table method to obtain the throughput of 2m/n cycles, where m is the order of the division polynomial and n is the number of the most significant lookup-bits. By doing this, we extracted the advantages in achieving both high-throughput and less cost of the gate areaon the chip. A pilot FPGA chip was implemented with the case of m=4, n=2. We successfully utilized the Altera's EP20K30ETC144-1 to exhibit the maximum operating clock frequency of 77 MHz.

키워드
Elliptic Curve Cryptography, GF divider, VHDL, FPGA

Ⅰ. 서 론

Galois Field GF(2^m)는 2^m 개의 원소를 가지는 다항식 전체 집합체로서, 원소들은 m보다 낮은 차수를 가지는 이진 다항식으로 표현할 수 있다 [1]. GF(2^m)에 대한 산술연산은 Reed-Solomon Code

*목원대학교
접수일자 : 2004. 12. 27

와 ECC(Elliptic Curve Cryptography) 암호화 알고리즘 등, 통신의 오류 정정 부호 분야와 암호화 분야 등, 광범위한 응용분야를 가지고 있다[2],[3].

GF(2^m)에서의 산술 연산은 덧셈, 뺄셈, 곱셈, 나눗셈이 있다. 이 중, 덧셈과 뺄셈은 다항식간의 덧셈, 뺄셈으로 정의되며 단순히 벡터간의 XOR 연산으로서 구현될 수 있다. 곱셈은 다항식 곱셈에 대한 원시원 F(x)에 의한 멱연산 A(x) · B(x) MOD F(x)으로 정의된다.

연산의 특성상, 덧셈, 뺄셈, 곱셈 연산의 경우 연산 빈도가 높고, 작은 회로 면적과 높은 연산 처리량을 가지기 때문에 많은 연구와 설계 결과가 발표되어 있는 반면, 나눗셈기는 연산 빈도가 가장 낮으면서, 많은 내부 연산이 필요하여 큰 회로 면적과 낮은 연산 처리량을 가지기 때문에 다른 연산기에 비해 연구의 질과 양적인 측면에서 열등한 상황이다[4],[5].

GF(2^m)에서의 피제수 A(x)와 제수 B(x)에 대한 나눗셈 연산은 A(x)와 B(x)의 역수의 곱 A(x) · B(x)-1으로 나타낼 수 있다. 이에 따라, B(x) 의 역수를 찾기 위한 몇 가지 방법이 제시되어 왔다 [6].

B(x)의 역수를 찾는 방법은 크게 목록 참조(table lookup) 방법과 알고리즘 근거 방법의 두 가지로 나눌 수 있다.

목록 참조 방법은 작은 m에 대해서는 가장 효율적인 방법이나, m에 지수 비례하여 커지는 목록의 크기 때문에 큰 m에 대해서는 회로 구현이 거의 불가능하다는 단점이 있다.

알고리즘 근거 방법은 B(x)의 역수를 여러 가지 수학적 이론을 이용하여 구하는 것으로 페르마의 정리, 유클리드의 알고리즘이 있다. 이 중, 페르마의 정리는 작은 m에 대해서만 적합하므로, m의 범위에 구애받지 않는 범용성을 가진 나눗셈기는 면적, 속도 면에서 효율적인 유클리드의 알고리즘을 GF(2^m)의 나눗셈 연산에 맞게 적용한 방식을 사용한다[7],[8].

본 논문에서는 유클리드의 알고리즘을 이용한 기존의 GF(2^m) 나눗셈기의 단점을 보완, 개량한 새로운 방식의 나눗셈기를 설계, 검증하였다. 알고리즘에 기반한 나눗셈기의 경우 회로 면적은 작지만, 연산 처리 속도가 낮으며, 목록 참조 방법은 연산 처리 속도는 높지만, 회로 면적이 크다는 단점을 가지고 있다. 따라서, 목록 참조 방법과 알고리즘 근거 방법의 두 가지 방법의 장점을 혼합하여, 기존의 나눗셈기의 문제점을 해결할 수 있는 해결책을 제시하였다. 설계된 나눗셈기는 n bit 참조(n bit lookup) 방식을 이용하여, division 당 2m/n cycle 의 연산 처리량을 가지면서, VLSI 구현에 적합한 면적을 가진다.

논문의 II 장에서는 유클리드의 알고리즘에 대한 개괄적인 설명과 설계된 나눗셈기에서 사용된 n bit 참조 방식에 대해 설명하고, III 장에서는 구현된 나눗셈기의 구조에 대해 설명한다. IV 장에서는 본 연구의 결과와 타 연구의 결과간의 비교, 고찰을 수행하고, V 장에서 연구에 대한 결론을 맺는다.

II. 유클리드의 알고리즘

유클리드의 알고리즘은 두 개의 수의 최대공약수를 구하는 것으로, Brunner의 연구에서는 불규칙적인 연산량을 가지는 원래의 알고리즘을 VLSI 구현에 맞게 규칙적인 연산량을 가지도록 개량하여, 다음과 같은 GF(2^m) 나눗셈 연산 알고리즘을 제안하였다.

Division Algorithm
Division:
F:=F(x);
S:=F(x); V:=0; (deg S = m)
R:=B(x); U:=A(x); (assume deg R = m)
delta:=0; (delta = deg S - deg R)
for i:=1 **to** 2m **do**
 if r_m = 0 **then**
  R:=x · R; U:=(x · U) MOD F;
  delta+=1 (deg R-=1)
 else (r_m = 1)
  if s_m = 1 **then**
   S:=S - R; V:=(V - U) MOD F;
  end;
  S:=x · S (deg S-=1)
  if delta = 0 **then**
   (deg S < deg R : division done)
  (R ↔ S); (U ↔ V);
  U:=(x · U) MOD F;
  delta:=1 (deg R - deg S)
  else
   U:=(U/x) MOD F;
   delta-=1;
  end
 end
end (A(x) · B^{-1}(x) = U)

이 알고리즘은 division당 2m cycle의 연산 처리량을 가지며, 각 R, S, U, V의 처리를 cell 단위로 구현한 설계 [7]와 시스톨릭 배열 방식을 이용하여

구현한 설계 [8]가 대표적인 구현 사례이다.

본 연구에서는 유클리드의 알고리즘을 이용한 나눗셈 연산 알고리즘에서 각 R, S, U, V의 값이 r_m, s_m, delta에 의해 처리되는 것에 착안, R, S의 최상위 비트를 2bit 씩 참조하여, r_m, r_{m-1}, s_m, s_{m-1}, zero의 5bit에 의한 목록 참조 방법을 이용하였다.

이 방식은, 25 = 32 가지의 경우의 수에 대하여, 원래의 알고리즘에서의 2 회의 iteration 후에 생성되는 결과를 대응시켜, 참조 목록으로부터 각 cell에서 처리해야할 연산에 대한 제어신호를 받도록 구성되어 있다. 이에 따라, 2m iteration이 필요한 기존의 알고리즘을 m iteration에 수행 가능하도록 재구성하였다.

III. 제안된 나눗셈기의 구조

제안된 나눗셈기의 전체 블록 다이어그램은 그림 1과 같다.

각 R, S, U, V에 대해 32개의 경우의 수에 대응되는 연산 회로를 구성하였다. 설계된 나눗셈기의 전체 블록 다이어그램은 그림 1과 같다.

전체 회로의 구성은, m+1 개의 R, S cell과 m 개의 U, V cell, 카운터, 그리고, 모듈에 대한 개별적인 연산처리에 대한 제어 신호 목록이 담겨있는 CTL_TABLE로 구성된다. 각 R, S, U, V cell에 대한 연산 목록은 표 1과 같다.

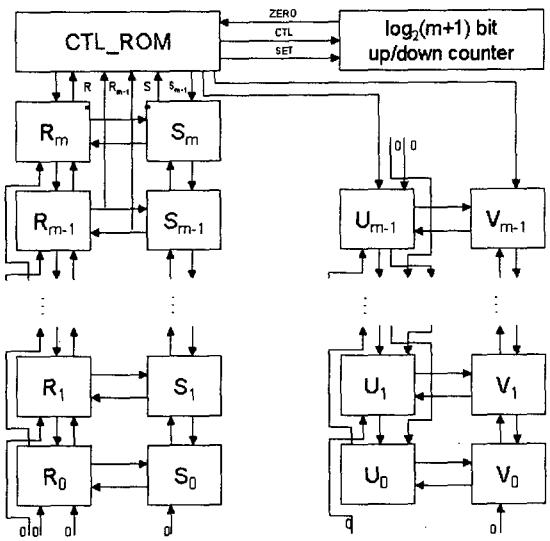

그림 1. 제안된 나눗셈기의 전체 블록도
Fig 1. Block diagram of suggested GF divider.

표 1. R, S, U, V 셀의 항상된 연산
Table 1. Functional description of R, S, U, V cells.

Module	Operation
R cell	R, xR, x^2R, xS, x^2S, x(S-R), x2(S-R)
S cell	S, xS, x^2S, R, x(S-xR), x^2(S-R), x(xS-R), x(R-x(S-R))
U cell	U, x^2U, U/x^2, V, x^2V, V-U, x^2(V-U)
V cell	V, U, V-U, V-xU, U-xV, V-U/x, U-x(V-U), V-U-U/x
Counter	delta, 0, delta+2, delta-2

제안된 나눗셈기의 동작은 다음과 같다.

1. 피제수 A(x), 제수 B(x)의 값을 각각 U cell, R cell에 입력한다.
2. 각 cell들은 r_m, r_{m-1}, s_m, s_{m-1}, zero의 5bit을 CTL_TABLE 에 입력, 제어신호를 받아, 연산처리를 수행한다.
3. m cycle 후, m번의 iteration을 거친 결과를 U cell에서 얻을 수 있다.

IV. 비교 및 성능평가

VLSI 설계에 있어서 가장 중요한 항목은 면적, 동작 cycle 수, 동작 주파수라고 할 수 있다.

설계된 나눗셈기를 유클리드의 알고리즘에 기반한 다른 나눗셈기와 비교한 결과를 표 2에 요약하였다.

Brunner의 연구는 division 당 2m cycle의 연산처리량을 가지는 가장 기본적인 연구 결과로서, O(m)의 면적을 가지며, 각 cell을 n번 중첩시킬 경우, division 당 2m/n cycle 의 연산 처리량을 얻을 수 있다. 그러나, n번 중첩 시, 임계 경로가 n 배 증가하고, 면적 면에서도 각 cell에서 플립플롭을 제외한 나머지 부분이 n배 증가하므로, 연산 처리량 증가를 기대하기 어려운 구조이다.

Guo의 연구는 시스톨릭 배열의 특징상 배열에 따라 division당 1 cycle의 높은 연산 처리량을 가지는 것이 가능하지만, cell의 개수가 많은 시스톨릭 배열의 특성 때문에, O(m^2)의 면적 복잡도를 가지게 되고, division당 1/m cycle의 결과를 얻기 위해서는 O(m$\log_2$m)의 면적 복잡도를 가지는 단점을 가지고 있다.

설계된 나눗셈기는 기본적으로 Brunner의 연구결과를 기반으로 하여, R, S의 MSB를 n bit 참조할

표 2. GF(2^m) 나눗셈기의 비교
Table 2. Comparison of GF dividers

Item \ Circuit	Brunner[7]	Guo[8]	Proposed
Throughput (1/cycles)	1/m	1/m	1/m
Latency (cycles)	3m	8m-1	3m
Area Complexity	O(m)	$O(m\log_2 m)$	O(m)

때 division 당 2m/n cycle의 처리량을 얻을 수 있도록 구성되었다. cell의 개수가 n에 비례하여 커지고, 임계경로 역시 n에 비례하는 Brunner의 연구와는 달리, n이 증가해도 각 cell에 대한 연산 처리의 종류가 늘어나 cell의 복잡도가 증가하고, 참조 목록인 CTL_TABLE의 면적이 n에 지수 비례하여 증가할 뿐, cell 개수에는 변화가 없으므로, 임계 경로나 회로의 면적 면에서 향상된 결과를 보인다. 따라서, 본 나눗셈기는 n이 커질수록, 즉, 높은 처리량을 가지는 나눗셈기의 구현에 적합한 구조임을 알 수 있다.

회로의 구현은 n=2, m=4인 경우에 대한 설계에 대해 Altera의 10만 게이트 급 FPGA chip EP20-K30ETC144-1을 이용, 검증을 수행하였으며, 77 Mhz의 최대 동작 주파수와 4 cycle 후, 나눗셈의 결과를 얻었다. 이에 대한 결과 파형은 그림 2와 같다.

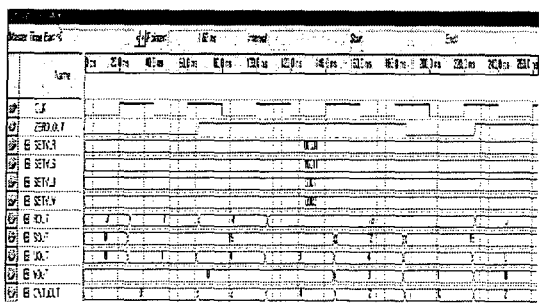

그림 2. 제안된 GF(2^m) 나눗셈기의 검증 결과
Fig 2. Waveform of the suggested GF divider.

V. 결 론

본 연구에서는 GF(2^m)에서의 나눗셈 연산을 기존의 연구에 비해 적은 cycle 내에 수행하면서, 실제 구현하기 적합한 면적을 가지는 나눗셈기를 설계, 구현하였다.

GF(2^m)에서의 연산기 구현은 나눗셈 연산이 빈도는 가장 낮으면서, 회로의 면적이 크고 연산 처리량이 낮다는 이유로 주로 곱셈기의 연구, 개량에만 치중해왔다. 본 연구에서 제안한 나눗셈기는 나눗셈 연산의 두 가지 방법인 목록 참조 방법과 알고리즘 근거 방법을 적절히 혼합한, n bit 목록 참조 방식을 이용하여, 높은 연산 처리량과 작은 회로 면적의 두 가지 목표를 동시에 달성할 수 있는 방법을 제시하였다. 제반 환경 변화에 따라 통신, 보안 분야에서 요구되는 정보 처리량이 급격히 늘어나면서 고속의 연산기가 요구되고 있다. 본 연구에서 제안한 n bit 목록 참조 방식을 이용할 경우, GF(2^m) 나눗셈 연산의 속도를 크게 향상시킬 수 있을 것으로 기대된다.

참고문헌

[1] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, CRC press, 1997.

[2] M. Rhee, Cryptography and Secure Communications, McGraw-Hill Book Co., 1994.

[3] B. Schneier, Applied Cryptography, second edition, John Wiley & Sons, Inc., 1996.

[4] G. L. Feng, "A VLSI Architecture for Fast Inversion in GF(2^m)," IEEE Trans. Computers, Vol. 38, no. 10, pp. 1383-1386, Oct. 1989.

[5] D. Hankerson, J. L. Hernandez, and A. Menezes, "Software Implementation of Elliptic Curve Cryptography over Binary Fields," Crypto95.

[6] G. B. Agnew, R. C. Mullin, and S. A. Vanstone, "An Implementation of Elliptic Curve Cryptosystems Over F2155," IEEE Journal on Selected Areas in Communications, Vol. 11, No. 5, Jun. 1993.

[7] H. Brunner, A. Cruiger, and M. Hofstetter : 'On Computing Multiplicative Inverses in GF(2^m)', IEEE Transactions on Computers, August 1993, Vol. 42, No. 8, pp. 1010-1015.

[8] Jyh-Huei Guo, Chin-Liang Wang : 'Systolic Array Implementation of Euclid's Algorithm for Inversion and Division in GF(2^m)', IEEE Transactions on Computers, October 1998,

Vol. 47, No. 10, pp.1161-1167.
[9] Edoardo D. Mastrovito, VLSI Architectures for Computations in Galois Fields, Linkoping Studies in Science and Technology, Dissertations, No.242, 1991.
[10] R. P. Brent and H. T. Kung, 'Systolic VLSI arrays for polynomial GCD computation', IEEE Transactions on Computers, August 1984, Vol. C-33, No. 8, pp.731-736.

저자소개

문상국 (Sangook Moon)

1995년 연세대학교 전자공학사
1997년 연세대학교 전자공학석사
2002년 연세대학교 전자공학박사
2002.2~2004.2 하이닉스반도체 선임연구원
2004.3 ~ 현재 목원대학교 정보전자영상공학부 전임강사
※ 관심분야 : 디지털 회로설계, 암호용 프로세서 VLSI 설계, 센서네트워크보안