GF(2^m)상에서 효율적인 Power-Sum 연산을 위한 시스톨릭 구조의 설계

김남연*, 김현성*, 이원호*, 김기원*, 유기영*

*경북대학교, 컴퓨터공학과

Systolic Architecture for Efficient Power-Sum Operation in GF(2^m)

Nam-Yeun Kim*, Hyun-Sung Kim*, Won-Ho Lee*, Kee-Won Kim*, Kee-Young Yoo

*Department of Computer Engineering KyungPook National Univ.

요 약

본 논문은 GF(2^m)상에서 파워썸 연산을 수행하는데 필요한 새로운 알고리즘과 그에 따른 병렬 입/출력 구조를 제안한다. 새로운 알고리즘은 최상위 비트 우선 구조를 기반으로 하고, 제안된 구조는 기존의 구조에 비해 낮은 하드웨어 복잡도와 적은 지연을 가진다. 이는 역원과 나눗셈 연산을 위한 기본 구조로 사용될 수 있으며 암호 프로세서 칩 디자인의 기본 구조로 이용될 수 있고, 또한 단순성, 규칙성과 병렬성으로 인해 VLSI 구현에 적합하다.

I. 서론

최근 유한 필드 상의 연산은 에러-교정 코드[1], 암호학[2, 3, 4], 디지 시그널 프로세싱[5] 등의 분야에서 주목을 받고 있다. 그리고 공개키 암호 시스템[3, 4, 6]에서의 기본 연산인 GF(2^m)상에서의 많은 구조들은 기저들을 달리하여 개발되어져 왔는데, 그 예로 정규기저(normal), 이원기저(dual basis), 다항식기저(polynomial basis) 타입이 있다. 그 중 정규기저와 이원기저 타입의 구조들은 각각의 장점을 가진 반면에 기저 변환을 해야한다는 단점을 지닌다. 반면에 다항식기저 구조는 기저 변환을 필요로 하지 않는다.

파워썸(AB^2+C)은 GF(2^m)상에서 공개키 암호 시스템[3, 4, 6]을 위한 효율적인 연산이다. 예를들면, 고속 회로를 디자인할 때 파워썸 연산은 곱셈과 곱셈의 역원($A/B=AB^{-1}$)을 이용한 나눗셈 연산을 수행하는데 효과적으로 쓰인다. 이 때 역원 연산은 $B^{-1} = B^{2^m-1} = (B(B(B\cdots(B(B)^2)^2\cdots)^2)^2)^2$과 같이 지수의 계산을 통해 얻어질 수 있다. 따라서 본 논문에서는 다항식기저를 사용하여 GF(2^m)상에서 파워썸 연산을 하는데 중점을 두겠다.

GF(2^m)상에서 파워썸 연산을 수행하기 위한 다항식 기저 시스톨릭 어레이에 대한 연구가 이미 이루어져 왔다[6, 7, 8]. Wei[6]는 파워썸 시스톨릭 구조에 MUX와 DEMUX를 하나씩 덧붙여 여덟 가지 다른 타입의 연산을 할 수 있도록 하였고, [7]에서는 [6]을 바탕으로 역원과 나눗셈을 위한 구조를 제안하고 있다. 그러나 이러한 시스톨릭 파워썸 구조들은 하드웨어 복잡도가 높고 지연 시간이 길어 암호 시스템의 응용에는 적합하지 못하다. 그러므로 효율적인 파워썸 연산에 대한 연구가 필요하다.

따라서 본 논문에서는 표준 기저를 사용한 GF(2^m)상에서의 파워썸 연산에 대한 새로운 알고리즘을 제안하고, 이 알고리즘을 통해 병렬 입/출력 구조를 유도한다. 제안된 알고리즘은 병렬성을 제공하기 위해 최상위 비트 우선(MSB-first) 구조를 사용하였고 하드웨어 복잡도는 m^2(3AND+3XOR)-m(2AND+2XOR)+($9m^2$-$6m$-1)Latches이고, 지연시간은 $3m$-1로 전통적인 구조들에 비해 효율적이다. 덧붙여 이 구조는 VLSI 구현에 적합하고 역원 구조에 쉽게 적용이 가능하다.

II. 제안된 곱셈기

1. 알고리즘

유한필드 GF(2^m)은 2^m개의 원소를 가진다. 본 논문에서는 GF(2^m)상의 모든 (2^m-1)개의 0이 아닌 원소들을 다항식 기저 방식으로 표현한다. GF(2^m)상의 두 원소 A와 B가 있다고 가정하고 이를 다항식 x로 나타내면 다음과 같다. $A = \sum_{i=0}^{m-1} a_i x^i$, $B = \sum_{i=0}^{m-1} b_i x^i$, 이 때 a_i, $b_i \in$ GF(2) ($0 \le i \le m-1$). GF(2^m)상의 유한 필드 원소들은 GF(2)상의 m 차수의 원시 다항식으로 표현되고, 연산 후 연산 결과를 필드의 원소로 만들기 위해서는 차수 m의 기약 다항식이 필요하다. $F(x)$를 기약 다항식으로 표현하면 다음과 같은데, $F(x) = x^m + f_{m-1}x^{m-1} + \cdots + f_1 x + f_0$의 근을 α라고 놓으면 $F(\alpha) = 0$ 이고, 다음과 같이 표현할 수 있다.

$$F(\alpha) \equiv \alpha^m = f_{m-1}\alpha^{m-1} + \cdots + f_1\alpha + f_0$$

$F'(\alpha) \equiv \alpha^{m+1} = f'_{m-1}x^{m-1} + \cdots + f'_1 x + f'_0$ 이 때 f_i, $f'_i \in$ GF(2), ($0 \le i \le m-1$). AB^2+C 연산을 하기 위해 다음과 같은 식을 제안하였다.

$$\begin{aligned} P &= AB^2 + C \\ &= A(b_{m-1}\alpha^{2m-2} + b_{m-2}\alpha^{2m-4} + \Lambda + b_1\alpha^2 + b_0) \\ &= (Ab_{m-1}\alpha^{2m-2} + Ab_{m-2}\alpha^{2m-4} + \Lambda + Ab_1\alpha^2 + Ab_0) \\ &= (\Lambda\ (\Lambda\ ((Ab_{m-1})\alpha^2 + Ab_{m-2})\alpha^2 + \Lambda + Ab_1)\alpha^2 + Ab_0 \quad (1) \end{aligned}$$

이 때, $c_i = 0$ ($0 \le i \le m-1$)이고, 이 알고리즘은 최상위 비트 우선 구조에 기반을 두고 있다. 새로운 순환식은 효율적인 파워썸 시스톨릭 어레이 구현에 효율적으로 적용될 수 있을 것이다. 식(1)에서 첫 번째 항은 Ab_{m-1}이고 식(2)와 같이 표현할 수 있다.

$$\begin{aligned} P_1 &= Ab_{m-1} \\ P_2 &= P_1\alpha^2 + Ab_2 \\ P_3 &= P_2\alpha^2 + Ab_1 \\ P_4 &= P_3\alpha^2 + Ab_0 \end{aligned} \quad (2)$$

새로운 알고리즘은 다음과 같다.

먼저, 첫째 항을 살펴보자.

$$\begin{aligned} P_1 &= Ab_{m-1} \\ &= \sum_{k=0}^{m-1} a_k b_{m-1}\alpha^k \end{aligned}$$

이 때,

$$p_k^1 = a_k b_{m-1}$$

을 유도할 수 있다.

일반적인 경우의 항은

$$\begin{aligned} P_i &= P_{i-1}\alpha^2 + Ab_{m-i} \\ &= \sum_{k=0}^{m-1} p_k^{i-1}\alpha^k\alpha^2 + \sum_{k=0}^{m-1} a_k b_{m-i}\alpha^k \\ &= \sum_{k=0}^{m-1} p_k^{i-1}\alpha^{k+2} + \sum_{k=0}^{m-1} a_k b_{m-i}\alpha^k \\ &= p_{m-1}^{i-1}\alpha^{m+1} + p_{m-2}^{i-1}\alpha^m + \Lambda + p_0^{i-1}\alpha^2 \\ &\quad + a_{m-1}b_{m-i}\alpha^{m-1} + a_{m-2}b_{m-i}\alpha^{m-2} + \Lambda \\ &\quad + a_1 b_{m-i}\alpha + a_0 b_{m-i} \\ &= p_{m-1}^{i-1}(f'_{m-1}\alpha^{m-1} + f'_{m-2}\alpha^{m-2} + \Lambda + f'_1\alpha + f'_0) \\ &\quad + p_{m-2}^{i-1}(f_{m-1}\alpha^{m-1} + f_{m-2}\alpha^{m-2} + \Lambda + f_1\alpha + f_0) + \Lambda \\ &\quad + p_0^{i-1}\alpha^2 + a_{m-1}b_{m-i}\alpha^{m-1} + a_{m-2}b_{m-i}\alpha^{m-2} + \Lambda \\ &\quad + a_1 b_{m-i}\alpha + a_0 b_{m-i} \\ &= (p_{m-1}^{i-1}f'_{m-1} + p_{m-2}^{i-1}f_{m-1} + a_{m-1}b_{m-i} + p_{m-3}^{i-1})\alpha^{m-1} \\ &\quad + (p_{m-1}^{i-1}f'_{m-2} + p_{m-2}^{i-1}f_{m-2} + a_{m-2}b_{m-i} + p_{m-4}^{i-1})\alpha^{m-2} + \Lambda \\ &\quad + (p_{m-1}^{i-1}f'_1 + p_{m-2}^{i-1}f_1 + a_1 b_{m-i})\alpha \\ &\quad + p_{m-1}^{i-1}f'_0 + p_{m-2}^{i-1}f_0 + a_0 b_{m-i} \end{aligned}$$

와 같은데, 이 때 식(3)과 같은 일반식을 유도해 낼 수 있다.

$$p_k^i = p_{m-1}^{i-1}f'_k + p_{m-2}^{i-1}f_k + p_{k-2}^{i-1} + a_k b_{m-i} \quad (3)$$

이처럼 AB^2+C의 합 P는 위의 알고리즘을 사용하여 효과적으로 구할 수 있으며, 이 때 P는 $\sum_{i=0}^{m-1} P_i$와 같다.

3. 시스톨릭 어레이 설계

새로운 파워썸 알고리즘으로부터, 병렬 입/출력 시스톨릭 어레이 구조를 얻을 수 있다[10, 11]. 그림 1은 GF(2^m) 상에서 제안된 시스톨릭 파워썸 구조를 보여준다. D^n은 n-유닛 지연 요소를 말한다. A, F와 F'는 위로부터 병렬로 입력이 되고, B는 가장 왼쪽 행으로부터 입력이 된다. 결과 P는 병렬로 행렬의 아래쪽으로 산출된다. 입력 A와 B는 둘 다 최상위 비트 우선 구조로 입력이 되고 출력도 같은 구조를 가진다. 이 때 최상위 비트 우선 구조는 최하위 비트 우선 구조에 비해 지수, 나눗셈, 역원 연산처럼 반복 연산을 필요로 하는 회로에 병렬성을 제공한다는 점에서 유리하다. 그림 1에서 (i, k) 셀을 지나는 선이 있다. 이 선은 (i-1, k-1)셀에서 (i, k+1)셀로 p_{k-1}^{i-1} 시그널을 전해주는 기능을 가진다. 셀이 첫 번째 열에 위치한 경우(k=m-1), p_k^{i-1}는 p_{m-1}^{i-1}과 연결하게 되고, p_{k-1}^{i-1}는 p_{m-2}^{i-1}와 연결하게 되어 그 값은 전달받는다.

그림 2의 PE1(Processing Element1)은 첫 번째 열에 위치한 셀들의 논리 회로를 표현하고, 그림 3의 PE2는 기본적인 셀들의 논리 회로를 보여준다. 만일 셀이 우측 두 행에 위치하면 (즉, k = 0, k = 1), p_{k-2}^{i-1}의 값은 0이다. 첫 번째 셀들은 오직 p_k^1만 계산된다는 사실은 주목할 만하다. 그림 2에서 보는 것처럼 처음 행에 위치한 셀들의 회로가 간단하기 때문에 이전의 구조들과 비교해 볼 때 전체 셀 복잡도를 줄일 수 있다. 첫 번째 행의 셀들을 제외하고 나머지 셀들의 수직 연결은 두 개씩의 지연을 필요로 하므로 전체 지연은 3m-2이다.

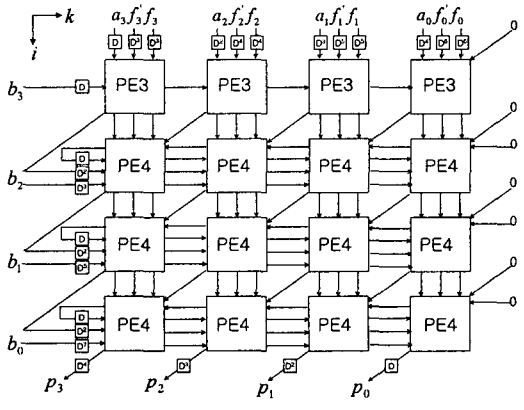

그림1:GF(2^m)상에서 AB^2+C을 위한 시스톨릭 구조

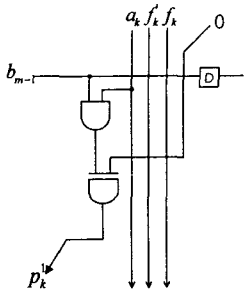

그림2:기본셀1(PE1)

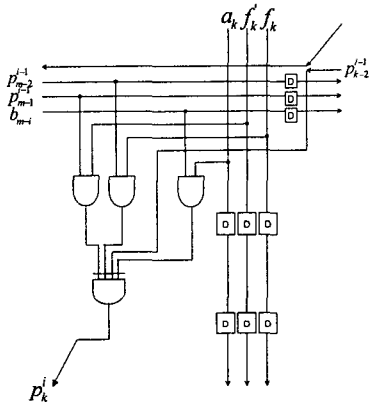

그림3:기본셀2(PE2)

Ⅲ. 분석

표1은 제안된 병렬 입/출력 구조와 그와 관련된 구조[6]를 비교하고 있다. Wang[8]의 논문에 따르면 Wei[6]의 논문은 정확하지 못한 부분이 있다. 즉, 회로의 각각의 셀에 세 개의 1비트 래치들을 추가해야 한다. 따라서 본 논문은 정확한 비교를 위해 Wang[8]의 가정을 따른다. 이 때, AND와 XOR는 2-input AND와 2-input XOR를 각기 지칭한다. 그리고 3-input XOR와 4-input XOR 게이트는 각각 두 개와 세 개의 2-input XOR 게이트로 수행될 수 있다.

Wei[6] 구조의 셀 복잡도는 m^2(3AND+3XOR+13Latches)인 반면, 제안된 병렬 구조는 m^2(3AND+3XOR)-m(2AND+2XOR)+(9m^2-6m-1)Latches의 셀 복잡도를 가진다. 이것은 제안된 구조가 m(2AND+2XOR)+(4m^2+6m+1)Latches 만큼의 셀 복잡도를 줄였음을 보여준다. 그리고 Wei 구조의 지연은 4m인데 반해, 제안된 구조는 3m-1의 지연을 가진다.

표 1: GF(2^m)상에서의 병렬 구조들 비교

Item \ Circuits	Wei[6]	제안된 구조	
No. of cells	m^2	m^2	
Function	AB^2+C	AB^2+C	
Throughput	1	1	
Latency	$4m$	$3m-1$	
Computation time per basic cell	$T_{AND}+T_{XOR3}$	$T_{AND}+T_{XOR4}$	
Cell complexity	3 2-input AND 1 2-input XOR 1 3-input XOR 13 1-bit latches	PE 1	1 2-input AND 1 2-input XOR 1 1-bit latch
		PE 2	3 2-input AND 1 4-input XOR 9 1-bit latches
Algorithm fashion	LSB	MSB	

Ⅳ. 결론

본 논문은 GF(2^m)상에서 파워썸 연산을 수행하는데 있어서 새로운 알고리즘과 병렬 입/출력 구조를 제안했다. 새로운 알고리즘은 최상위 비트 우선 구조를 기반으로 하고, 제안된 구조는 Wei[6]의 구조에 비해 낮은 하드웨어 복잡도와 적은 지연을 가진다.

따라서 본 논문에서 제안한 구조는 역원과 나눗셈 연산을 위한 기본 구조로 사용될 수 있으며 암호 프로세서 칩 디자인의 기본 구조로 이용될 수 있다. 또한 단순성, 규칙성과 병렬성으로 인해 VLSI 구현에 적합하다.

참고문헌

[1] W.W.Peterson and E.J.Weldon, *Error-correcting codes*, MIT Press, MA, 1972.

[2] D.E.R.Denning, *Cryptography and data security*, Addison-Wesley, MA, 1983.

[3] A.Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, Boston, 1993.

[4] T.ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Trans. on Info. Theory*, vol. 31(4). pp. 469-472, July 1985.

[5] I.S.Reed and T.K.Truong, The use of finite fields to compute convolutions, *IEEE Trans. Inform. Theory*, 21, pp.208-213, 1975.

[6] S.W.Wei, A Systolic Power-Sum Circuit for GF(2m), *IEEE Trans. Computers*, 43, pp.226-229, 1994.

[7] S.W.Wei, VLSI architectures for computing exponentiations, multiplicative inverses, and divisions in GF(2m), *Proc. IEEE Trans. Circuits and Systems*, 44, pp.847-855, 1997.

[8] C.L.Wang and J.H.Guo, New systolic arrays for C+AB2, inversion, and division in GF(2m), *IEEE Trans. Computers*, 49, pp.1120-1125, 2000.

[9] C.W.Wu and M.K.Chang, Bit-Level Systolic Arrays for Finite-Field Multiplications , *Journal of VLSI Signal Processing*, 10, pp. 85-92, 1995.

[10] S. Y. Kung, *VLSI Array Processors*, Prentice-Hall, 1987.

[11] K. Y. Yoo, *A Systolic Array Design Methodology for Sequential Loop Algorithms*, Ph.D. thesis, Rensselaer Polytechnic Institute, New York, 1992.