DOI: 10.3745/KIPSTA.2008.15-A.3.161

$GF(2^m)$상의 MSD 우선 알고리즘 기반 디지트-시리얼 곱셈기

김 창 훈[†] · 김 순 철[††]

요 약

본 논문에서는 유한체 $GF(2^m)$상의 다항식 기저를 이용한 디지트 시리얼 시스톨릭 곱셈기를 제안한다. 제안된 곱셈기는 MSD(Most Significant Digit) 우선 곱셈 알고리즘에 기반하며, 연속적인 입력 데이터에 대해 $\lceil m/D \rceil$ 클럭 사이클마다 곱셈 결과를 출력한다. 여기서 D는 선택된 디지트 크기이다. 기존에 제안된 구조들은 선형의존성 때문에 디지트 크기 D가 증가하면 최대 처리기 지연시간 역시 선형으로 증가하지만 제안된 곱셈기는 이진트리 형태의 내부 구조를 가지기 때문에 D에 대해 로그단위로 증가한다. 따라서 제안된 구조는 기존에 제안된 디지트 시리얼 시스톨릭 곱셈기에 비해 계산지연시간을 상당히 감소시킨다. 뿐만 아니라 제안된 곱셈기는 높은 규칙성, 모듈성, 단방향 신호 흐름의 특성을 가지기 때문에 VLSI 구현에 매우 적합하다.

키워드 : 유한체 곱셈, 디지트 시리얼 구조, 시스톨릭 어레이, VLSI

A Digit Serial Multiplier Over $GF(2^m)$ Based on the MSD-first Algorithm

Chang Hoon Kim[†] · Soon Cheol Kim[††]

ABSTRACT

In this paper, an efficient digit-serial systolic array is proposed for multiplication in finite field $GF(2^m)$ using the polynomial basis representation. The proposed systolic array is based on the most significant digit first (MSD-first) multiplication algorithm and produces multiplication results at a rate of one every $\lceil m/D \rceil$ clock cycles, where D is the selected digit size. Since the inner structure of the proposed multiplier is tree-type, critical path increases logarithmically proportional to D. Therefore, the computation delay of the proposed architecture is significantly less than previously proposed digit-serial systolic multipliers whose critical path increases proportional to D. Furthermore, since the new architecture has the features of a high regularity, modularity, and unidirectional data flow, it is well suited to VLSI implementation.

Keyword : Finite Field Multiplier, Digit-serial Architecture, Systolic Array, VLSI

1. 서 론

최근 유한 필드 $GF(2^m)$상의 연산들은 오류 제어 코딩, 암호응용 등 여러 분야에서 중요한 역할을 하고 있다[1,2]. $GF(2^m)$상에서 중요한 연산은 덧셈, 곱셈, 지수, 나눗셈이 있다. $GF(2^m)$상의 덧셈은 비트별 배타적 논리합(XOR) 연산으로 적은 비용의 고속 구현이 가능하지만 다른 연산들은 상당히 복잡할 뿐만 아니라 구현에 따른 비용이 크다. 곱셈 연산은 $GF(2^m)$ 응용분야에서 가장 많이 사용되는 연산일 뿐만 아니라 곱셈의 반복적인 연산을 통하여 지수 및 나눗셈을 수행할 수 있다. 따라서 본 논문은 $GF(2^m)$상의 고속 디지트 시리얼 곱셈기 설계에 초점을 맞춘다.

$GF(2^m)$상의 효율적인 곱셈기 구현에 대해 많은 연구가 이루어져 왔다[3-5,8,9]. 기존의 곱셈기들은 서로 다른 기저를 사용하였는데 가장 대표적인 $GF(2^m)$ 원소표기법에는 정규기저(normal basis)와 다항식기저(polynomial basis)가 있다. 각 기저 표기법은 장·단점을 가지는데, 정규기저 표기법을 사용할 경우 제곱연산이 쉽게 되는 반면 곱셈연산이 매우복잡하고 서로 다른 m에 대해 규칙적인 하드웨어 구조 설계가 어렵다. 이러한 이유로 $GF(2^m)$상의 곱셈에 대한 하드웨어 구현에는 다항식기저 표기법이 더 많이 사용된다.

다항식 기저를 사용할 경우, $GF(2^m)$상의 곱셈 알고리즘

※ 본 연구는 2005학년도 대구대학교 학술연구비 지원에 의해 수행되었음.
† 정 회 원 : 대구대학교 컴퓨터·IT 공학부 전임강사
†† 정 회 원 : 대구대학교 컴퓨터·IT 공학부 부교수(교신저자)
논문접수 : 2007년 9월 18일
수 정 일 : 2008년 4월 2일
심사완료 : 2008년 4월 14일

은 크게 LSB(Least Significant First) 우선 방식과 MSB(Least Significant First) 우선 방식이 있다[3]. LSB-우선 방식은 곱수의 LSB부터 처리되고, MSB-우선 방식은 MSB부터 처리된다. [4,8]의 연구결과는 MSB-우선 방식에 기반하고 [5,9]는 LSB-우선 방식을 사용하였다. 비트-시리얼 곱셈기의 경우 LSB-우선 방식을 사용할 경우 MSB-우선 기법보다 낮은(하나의 2-입력 XOR 게이트) 최대처리기 지연시간(critical path)을 보인다.

최근 Song 등[3]은 $GF(2^m)$상에서 특별한 기약다항식 ($G(x)=x^m+g_kx^k+\sum_{i=0}^{k-1}g_ix^i$, $D\le m-k$)을 사용한 고속의 저비용 디지트 시리얼/패러럴 곱셈기를 제안하였다. 위의 조건을 만족하는 기약다항식을 사용한다면 $A(x)x^D \bmod G(x)$ 연산은 비트별 AND 게이트와 XOR 게이트의 이진트리를 이용한 계산이 가능하다[3]. 여기서 $A(x)$는 $GF(2^m)$상의 원소이다. 일반적으로 Trinomial, Pentanomial, all one polynomial과 같은 특별한 기약다항식은 저면적 및 고속의 곱셈기 구현이 가능하지만 모든 m에 대하여 존재하지 않는다[7]. 이와 달리 Song 등이 사용한 기약다항식은 D를 적당하게 선택하면 모든 m에 대해 존재한다. 예를 들면, 타원곡선 암호 시스템을 위해 NIST[7]에서 권고하는 모든 기약다항식의 경우 D의 크기는 128까지 가능하다. 따라서 실제적인 응용에 있어서는 제약조건이 거의 없다 할 수 있다.

Song 등에 의해 제안된 곱셈기가 하드웨어 면적, 전력소모, 기약다항식의 선택등 많은 장점을 가지지만 많은 글로벌 신호의 브로드캐스팅을 포함하기 때문에 현저한 속도저하를 보인다.

본 논문에서는 암호 응용을 위한 $GF(2^m)$상의 새로운 디지트 시리얼 시스톨릭 곱셈기를 제안한다. MSD 우선 곱셈 알고리즘[3]으로부터 디지트-레벨의 새로운 자료의존 그래프를 유도하고 이에 기반한 새로운 디지트 시리얼 시스톨릭 어레이를 설계한다. 제안된 곱셈기는 연속적인 입력 데이터에 대해 매번 N 클럭 사이클마다 곱셈 결과를 출력한다. 또한 기존에 제안된 구조들은 선형의존성 때문에 디지트 크기 D가 증가하면 최대 처리기 지연시간 역시 선형으로 증가하지만 제안된 곱셈기는 이진-트리 형태의 내부 구조를 가지기 때문에 D에 대해 로그단위로 증가한다. 따라서 제안된 구조는 기존에 제안된 디지트 시리얼 시스톨릭 곱셈기에 비해 속도측면에서 상당한 개선을 보인다. 뿐만 아니라 제안된 구조는 높은 규칙성, 모듈성, 단방향 신호 흐름의 특성을 가지기 때문에 VLSI 구현에 매우 적합하다.

2. 디지트-레벨 자료의존 그래프

2.1 MSD 우선 곱셈 알고리즘

$A(x)=\sum_{i=0}^{m-1}a_ix^i$, $B(x)=\sum_{i=0}^{m-1}b_ix^i$를 $GF(2^m)$상의 두 원소라 하고 $G(x)=x^m\sum_{i=0}^{m-1}g_ix^i$를 유한체 $GF(2^m)\cong GF(2)[x]/G(x)$를 생성하는 기약다항식이라 하면, $A(x)B(x) \bmod G(x)$의 결과값은 $P(x)=\sum_{i=0}^{m-1}p_ix^i$로 나타낼 수 있고 아래의 식 (1)과 같이 계산할 수 있다. 여기서 D는 디지트 크기이다.

$$\begin{aligned}P(x)&=A(x)B(x) \bmod G(x)\\&=(\cdots(A(x)B_{N-1}x^D \bmod G(x)+A(x)B_{N-2})x^D \bmod G(x)\\&+\cdots+A(x)B_1)x^D \bmod G(x)+AB_0\end{aligned} \quad (1)$$

식 (1)의 MSD 우선 곱셈 방법으로부터 아래의 [알고리즘 1]을 유도할 수 있다[3]. 여기서 $N=\lceil m/D\rceil$은 디지트의 전체 개수이다.

[알고리즘 1] : $GF(2^m)$상의 MSD 우선 곱셈 알고리즘

Input : $G(x)$, $A(x)$, $B(x)$, $T(x)$
Output : $P(x)=A(x)B(x) \bmod G(x)$
Initialize : $A=A(x)$, $B=B(x)$, $G=G(x)$,
$T^{(0)}=T(x)=0$
1. for $i=1$ to N do
2. $\quad T^{(i)}=(T^{(i-1)} \bmod G)x^D+AB_{N-i}$
3. end for
4. $P=T^{(N)} \bmod G$

2.2 디지트-레벨 자료의존 그래프

[알고리즘 1]에서 주된 연산은 $T^{(i)}=T^{(i-1)}x^D \bmod G+AB_{N-i}$와 $P=T^{(N)} \bmod G$이다. 이 연산들의 최대 처리기 지연시간은 선택된 기약다항식에 따라 달라진다. 만약 일반적인 기약다항식을 이용하여 연산을 수행하면 최대 처리기 지연시간은 데이터 의존성 때문에 선택된 디지트 크기 D에 비례해서 증가한다[5]. 반면 [3]에서 사용한 특별한 기약다항식($G=x^m+g_kx^k+\sum_{i=0}^{k-1}g_ix^i$, $D\le m-k$)을 이용하면 최대 처리기 지연시간이 D에 로그단위로 증가하기 때문에 지연시간을 줄일 수 있다[3].

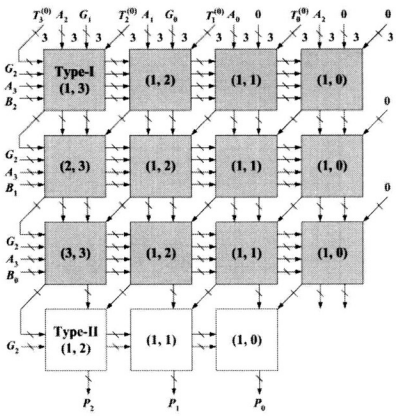
T_i'를 $T^{(i)}$의 계수라고 하면 $T^{(i)}=T^{(i-1)}x^D \bmod G+AB_{N-i}$는 다음 식과 같이 계산할 수 있다.

$$T_i'=\sum_{i=0}^{N}\sum_{j=0}^{D-1}\left(\sum_{k=1}^{D}(b_{D-k}a_{D(i-1)+j+k}+t_{m+D-k}^{(i-1)}g_{D(i-2)+j+k})+t_{D(i-1)+j}^{(i-1)}\right) \quad (2)$$

여기서 $A_N=G_{-1}=G_{-2}=0$이다. P'를 P의 계수라고 하면 $P=T^{(N)} \bmod G$를 계산하기 위한 식 (3)을 얻을 수 있다.

$$P'=\sum_{i=1}^{N}\sum_{j=0}^{D-1}\left(\sum_{k=1}^{D}(t_{m-k}^{(N)}g_{D(i-1)+j+k})+t_{D(i-1)+j}^{(N)}\right) \quad (3)$$

식 (2), (3)으로부터 그림 1과 같은 $GF(2^m)$상의 곱셈을 위한 새로운 자료 의존 그래프를 얻을 수 있다. 여기서 $m=9$, $D=3$으로 가정한다.

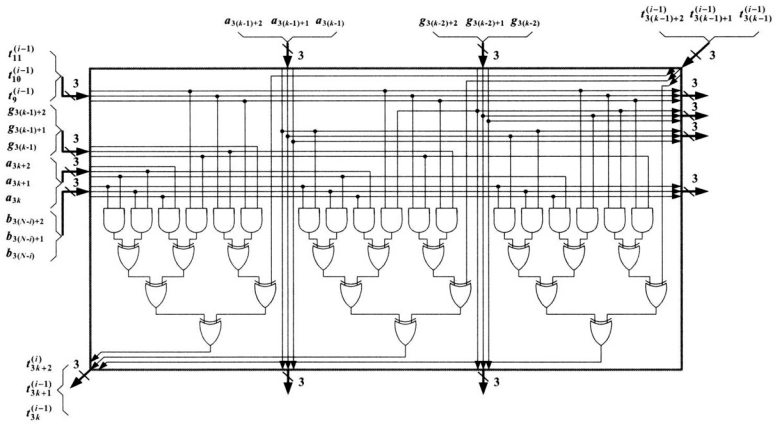


(그림 1) $GF(2^9)$상의 새로운 자료 의존 그래프

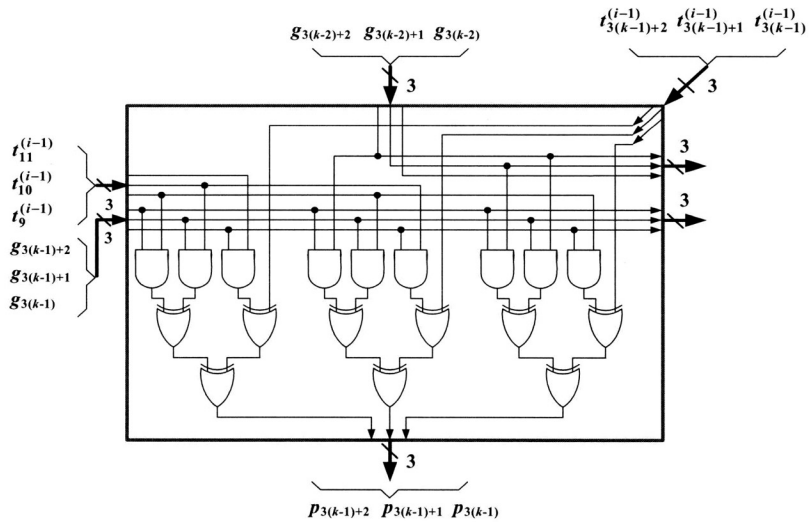
(그림 1)의 자료 의존 그래프는 디지트 레벨의 $N\times(N+1)$개의 Type-1 셀과 N개의 Type-2 셀로 구성된다. (그림 1)의 i번째 행 Type-1 셀은 $T^{(i)}=T_{i-1}x^D \bmod G+AB_{N-i}$를, Type-2 셀은 $P=T^{(N)} \bmod G$ 연산을 각각 수행한다. 디지트 계수 P_i는 $(N+1)$ 반복 후에 어레이의 최 하단 행에서 나타난다. (그림 2, 3)은 각각 Type-1과 Type-2 셀의 회로도를 나타낸다.

3. 디지트 시리얼 시스톨릭 곱셈기

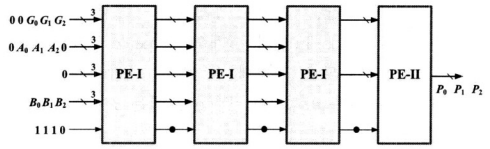
(그림 4)는 $GF(2^m)$상의 곱셈 계산을 위한 일차원 신호 흐름 그래프(Signal Flow Graph: SFG) 어레이를 나타낸다. 여기서 $m=9$이고 $D=3$이다. (그림 4)에 나타나듯이 처리기



(그림 2) (그림 1)의 Type-1 셀 회로도

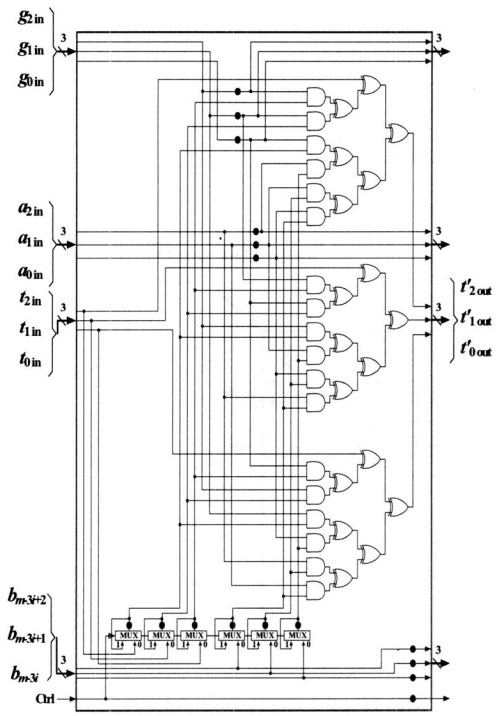


(그림 3) (그림 1)의 Type-2 셀 회로도

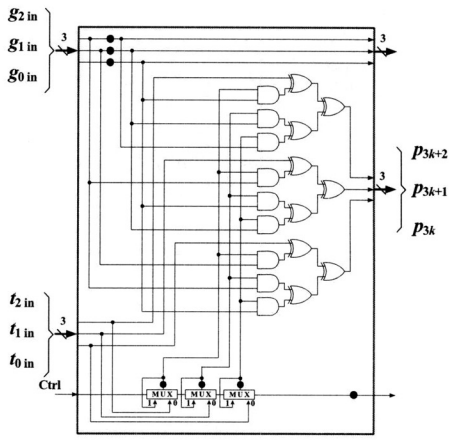


(그림 4) (그림 1)의 일차원 SFG 어레이

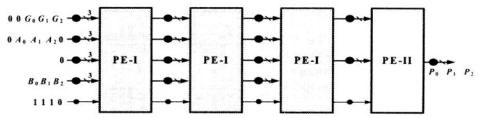
(Processing Element: PE)는 N개의 PE-I과 한 개의 PE-II로 구성되며 $N+1$ 길이의 컨트롤 시퀀스(011…1)에 의해 제어된다. (그림 5, 6)은 각각 PE-I과 PE-II의 회로도를 나타낸다. 여기서 '•'는 1-비트 1 사이클 지연 소자이다. 그림 1에 나타나듯이 $T_{N-1}^{(i-1)}$과 B_{N-i}의 계수는 자료 의존 그래프의 모든 기본 셀에 브로드캐스트 되어야한다. 이를 위해 각 PE-I에는 $2D$개의 멀티플렉서와 $2D$개의 1-비트 래치를, PE-II에는 D개의 멀티플렉서와 D개의 1-비트 래치를 추가한다. 컨트롤 신호가 0이면 데이터는 래치된다. (그림 4)에 컷 셋 시스톨릭화 기법(cut-set systolization technique)[6]을 적용하면 (그림 7)과 같은 $GF(2^m)$상의 곱셈을 위한 새로운 디지트 시리얼 시스톨릭 곱셈기를 얻을 수 있다. 이 곱셈기는 연속적인 입력 데이터에 대해 초기 $3N+2$ 클럭 지연시간 후 매번 N 클럭 사이클마다 곱셈결과를 출력한다.



(그림 5) (그림 4)의 PE-I 회로도



(그림 6) (그림 4)의 PE-II 회로도



(그림 7) $GF(2^m)$상의 새로운 MSD 우선 디지트 시리얼 곱셈기

4. 성능분석

(그림 7) 곱셈기의 기능 검증을 위해 VHDL로 회로를 기술하였고 Mentor Graphics사의 VHDL-ChipSim을 이용하여 시뮬레이션 하였다. 시뮬레이션을 위한 회로 합성은 Synopsis사의 FPGA-Express(버전 2000, 11-FE3.5)에서 이루어졌으며, 타겟 FPGA 디바이스로 Altera사의 EP2A70F1508C-7을 사용하였다. (그림 7) 곱셈기의 기능 검증 후, 동일한 입출력 형태를 가지는 기존의 곱셈기와 성능을 비교하였으며 일반화 된 결과를 <표 1>에 요약 하였다. 또한 <표 2>에 일반적인 디지트 크기를 지원하는 곱셈기 중 가장 낮은 최대처리기 지연시간을 갖는 구조[5]와 디지트 크기에 따른 최대처리기 지연시간을 비교하였다. <표 1>에서 3-입력 XOR 게이트와 4-입력 XOR 게이트는 두 개와 세 개의 2-입력 XOR 게이트로 구성된다고 가정하였다. 참고로 <표 1>에서 [9]의 구조는 D=2인 경우에만 적용 가능하다. <표 1>에 나타나듯이 기존에 제안된 구조들은 선형의 존성 때문에 디지트 크기 D가 증가하면 최대 처리기 지연시간 역시 선형으로 증가하지만 제안된 곱셈기는 이진트리 형태의 내부 구조를 가지기 때문에 D에 대해 로그단위로 증가한다. 보다 자세한 비교를 위해 <표 2>를 살펴보면 D=1인 경우 본 논문에서 제안한 구조는 [5]의 구조에 비해 T_{XOR2} 만큼 최대처리기 지연시간이 증가하지만 D가 크질 경우 속도 측면에서 상당한 성능 향상을 보인다.

〈표 1〉 $GF(2^m)$상의 디지트 시리얼 시스톨릭 곱셈기의 성능 비교

		[4]	[5]	[8]	[9]	그림 7
Throughput (1/cycles)		$1/N$	$1/N$	$1/N$	$1/\lceil \frac{m}{2} \rceil$	$1/N$
Latency (cycles)		$3N$	$3N$	$3N$	$3\lceil \frac{m}{2} \rceil$	$3N+2$
Circuit	AND2	$N(2D^2+D)$	$2ND^2$	$2ND^2+D$	$9\lceil \frac{m}{2} \rceil$	$N(2D^2+D)$
	XOR2	$2ND^2$	$2ND^2$	$2ND^2$	$8\lceil \frac{m}{2} \rceil$	$2ND^2$
	Latch	$10ND$	$8ND+4D$	$9ND+1$	$22\lceil \frac{m}{2} \rceil$	$10ND+2D$
	MUX2	$2ND$	$2ND$	$2ND$	$4\lceil \frac{m}{2} \rceil$	$2ND$
Critical Path		$T_{AND2}+3T_{XOR2}+(D-1)(T_{AND2}+2T_{XOR2}+T_{MUX2})$	$T_{AND2}+T_{XOR2}+(D-1)(T_{AND2}+T_{XOR2}+T_{MUX2})$	$(D-1)T_{MUX2}+D(T_{AND2}+2T_{XOR2})$	$T_{AND2}+T_{MUX2}+3T_{XOR2}$	$T_{AND2}+\log_2(2D+1)T_{XOR2}$
Control Signal		1	1	1	1	1

$N=\lceil m/D \rceil$
AND_2 : 2-input AND gate
XOR_2 : 2-input XOR gate
MUX_2 : 2-to-1 multiplexer
T_{AND2} : propagation delay through one AND_2 gate
T_{XOR2} : propagation delay through one XOR_2 gate
T_{MUX2} : propagation delay through one MUX_2 gate

5. 결 론

본 논문에서는 $GF(2^m)$상의 새로운 디지트 시리얼 시스톨릭 곱셈기를 제안하였다. 이를 위해 MSD 우선 곱셈 알고리즘으로부터 디지트-레벨의 자료의존 그래프를 얻은 후 투영 절차에 따라 일차원 SFG 어레이 및 PE를 유도하였고 컷셋 시스톨릭화 기법을 적용하여 $GF(2^m)$상의 완전한 디지트 시리얼 시스톨릭 곱셈기를 구성하였다.

제안된 곱셈기는 크게 다음과 같은 두 가지 특성을 가진다. 1) 기존에 제안된 구조에 비해 거의 동일한 하드웨어를 사용하지만 훨씬 적은 계산지연을 가진다. 2) 제안된 구조가 타원곡선 암호 시스템과 같은 암호 응용에 적용된다면 다양한 디지트 크기를 선택할 수 있다. 따라서 위의 두 가지 특징으로부터 본 논문에서 제안된 $GF(2^m)$상의 곱셈기는 적절한 디지트 크기의 선택에 따라 최소한의 하드웨어 사용으로 최대한의 처리율을 만족시킬 수 있다. 뿐만 아니라 제안된 곱셈기는 높은 규칙성, 모듈성, 단방향 신호 흐름을 가지기 때문에 VLSI 구현에 매우 적합하다.

〈표 2〉 디지트 크기에 따른 최대처리기 지연시간 비교

D	[5]	그림 7
1	$T_{AND2}+T_{XOR2}$	$T_{AND2}+2T_{XOR2}$
8	$7T_{MUX2}+8(T_{AND2}+T_{XOR2})$	$T_{AND2}+5T_{XOR2}$
16	$15T_{MUX2}+16(T_{AND2}+T_{XOR2})$	$T_{AND2}+6T_{XOR2}$
32	$31T_{MUX2}+32(T_{AND2}+T_{XOR2})$	$T_{AND2}+7T_{XOR2}$
64	$63T_{MUX2}+64(T_{AND2}+T_{XOR2})$	$T_{AND2}+8T_{XOR2}$

참 고 문 헌

[1] R.E. Blahut, *Theory and Practice of Error Control Codes*, Reading, MA: Addison-Wesley, 1983.

[2] I.F. Blake, G. Seroussi, and N.P. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

[3] L. Song and K.K. Parhi, "Low Energy Digit-Serial/Parallel Finite Field Multipliers," *J. VLSI Signal Processing*, vol.19, no.2, pp.149-166, June 1998.

[4] J.H. Guo and C. L. Wang, "Digit-Serial Systolic Multiplier for Finite Field $GF(2^m)$," *IEE Proc. Comput. Digit. Tech.*, vol.145, no.2, pp.143-148, Mar., 1998.

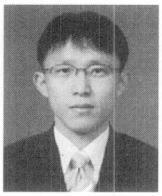
[5] C.H. Kim, C.P. Hong, and S. Kwon, "A Digit-Serial Multiplier for Finite Field $GF(2^m)$", IEEE Transactions on VLSI System, Vol.13, No.4, pp.476-483, April, 2005.

[6] S.Y. Kung, *VLSI Array Processors*, Englewood Cliffs, NJ: Prentice Hall, 1988.

[7] NIST, Recommended elliptic curves for federal government use, May, 1999. http://csrc.nist.gov

[8] 김창훈, 한상덕, 홍춘표, "유한 필드 $GF(2^m)$상의 MSB 우선 디지트 시리얼 곱셈기 설계", 한국통신학회논문지, 제 27권, 6C호, pp.625-607, 2002. 6.

[9] 김기원, 이건직, 유기영 "$GF(2^m)$상에서 2-디지트 시리얼 시스톨릭 곱셈기 설계 및 분석", 한국정보과학회 가을 학술발표논문집, 제 27권, 2호, pp.605-607, 2000. 10.



김 창 훈

e-mail : kimch@daegu.ac.kr
2001년 대구대학교 컴퓨터정보공학부 (학사)
2003년 대구대학교 컴퓨터정보공학과 (공학석사)
2006년 대구대학교 컴퓨터정보공학과 (공학박사)
2006년~2007년 대구대학교 정보통신공학부 BK21 연구교수
2007년-현 재 대구대학교 컴퓨터·IT 공학부 전임강사
관심분야 : 암호 시스템, 임베디드 시스템, RFID/USN 보안

김 순 철

e-mail : kimsc@daegu.ac.kr
1990년 서울대학교 컴퓨터공학과(학사)
1992년 서울대학교 대학원 컴퓨터공학과 (공학석사)
1998년 서울대학교 대학원 컴퓨터공학과 (공학박사)
1998년 서울대학교 컴퓨터신기술공동 연구소 특별연구원
2005년 University of Massachusetts Amherst 객원교수
1999년~현 재 대구대학교 컴퓨터·IT공학부 부교수
관심분야 : 임베디드시스템, 운영체제, 분산시스템