通信情報保護學會論文誌
第 11 券 第 2 號, 2001. 4

# 타원곡선 암호 시스템에 효과적인 digit-serial 승산기 설계*

이 광 엽**, 위 사 혼**, 김 원 종***, 장 준 영***, 정 교 일***, 배 영 환***

# Design of an Efficient Digit-Serial Multiplier for Elliptic Curve Cryptosystems

Kwang-Youb Lee**, Sa-Heun Wie**, Won-Jong Kim***,
June-Young Chang***, Kyo-Il Chung***, Young-Hwan Bae***

요 약

본 논문에서는 유한체 연산을 바탕으로 하는 타원곡선 암호화 프로세서의 승산기를 효율적으로 구현할 수 있는 구조를 제안한다. 타원곡선 암호알고리즘에 적용된 비도는 193비트로 하드웨어 구현에 유리한 trinomial 다항식을 사용하였다. 제안된 승산기는 trinomial 다항식의 특성을 이용하여 기존의 193bit serial LFSR를 개선한 32bit digit serial 구조를 갖도록 설계하였다. 회로는 합성수준의 VHDL코드와 타원곡선 상에서 임의의 좌표의 가산식으로 부터 만들어진 테스트벡터를 적용하여 기능을 검증하고 회로의 규모를 측정하였다. 검증된 결과는 기존의 LFSR승산기의 30% 면적으로 승산기 구현이 가능하였다.

ABSTRACT

In this paper, an efficient architecture for the ECC multiplier in GF($2^m$) is proposed. We give a design example for the irreducible trinomials $x^{193}+x^{15}+1$. In hardware implementations, it is often desirable to use the irreducible trinomial equations. A digit-serial multiplier with a digit size of 32 is proposed, which has more advantages than the 193bit serial LFSR architecture. The proposed multiplier is verified with a VHDL description using an elliptic curve addition. The elliptic curve used in this implementation is defined by Weierstrass equations. The measured results show that the proposed multiplier is 0.3 times smaller than the bit-serial LFSR multiplier.

**keyword** : *Elliptic curve, Finite Field Multiplier, Cryptography, Digit-Serial, Smart card*

## Ⅰ. 서 론

암호알고리즘은 키의 특성에 따라 크게 암·복호화 키가 같은 대칭키 암호알고리즘과 암·복호화 키가 서로 다른 공개키 암호알고리즘으로 나눌 수 있다. 그러나 암호 사용자가 늘어나고, 또한 다양한 암호서비스에 대한 요구가 제기되면서 대칭키 암호알고리즘에서 발생된 키 관리 문제와 인증 문제를 해결하기 위한 알고리즘의 필요성 대두되었다. 1976년 W. Diffie와 M. E. Hellman이 위의 두 문제를 해결한 "New Directions in Cryptography"에서 공개키 암호의 개념을 처음 소개하였다. 이후 1978년

* 본 논문은 한국전자통신연구원의 지원으로 작성되었으며 회로구현에는 System IC 2010의 지원장비를 사용하였습니다.
** 서경대학교 컴퓨터공학과(kylee@skuniv.ac.kr)
*** 한국전자통신연구원

소인수분해의 어려움에 기반을 둔 RSA가 소개되어 지금까지 넓게 사용되고 있다. 그러나 RSA는 비도를 높이기 위해 1024 비트 이상으로 확장되는 추세로, 스마트카드와 같이 제한된 면적에 탑재되는데 어려움이 있다. 1987년 Koblitz와 Miller는 타원곡선(ECC) 을 공개키 암호시스템에 적용하였다.[1] ECC(Elliptic Curve Cryptography)는 적은 비트로 높은 비도를 보이기 때문에 최근 스마트 카드와 같은 IC카드의 암호화구현에 사용되는 추세에 있다.[2],[3]

본 논문에서는 유한체에서 타원곡선의 표현과 암호화에 적합한 타원곡선 알고리즘을 바탕으로 스마트카드와 같은 IC 카드의 암호화프로세서에 효과적으로 사용이 가능한 새로운 구조의 승산기를 제안한다.

Polynomial base 유한체상에서 일반적인 승산기구조는 bit-serial방식과 bit-parallel방식으로 구현된다.[4] Bit-parallel 경우 one clock으로 동작이 가능하지만 구현에 필요한 하드웨어면적 때문에 IC 카드에서는 사용될 수 없어 대부분 bit-serial 구조를 채택하고 있다.

Bit-serial 구조의 승산기는 LFSR(Linear Feedback Shift Register)를 주로 사용하여 설계되는데 암호비트수에 비례하여 증가하는 레지스터의 수를 감소시키는 방법으로 digit-serial방식이 사용된다. 본 논문에서는 digit-serial방식의 승산기를 설계하는데 새로운 구조를 제안한다. 첫 번째는 기약다항식 가운데 trinomial식의 특징을 이용하여 modular reduction을 위한 feedback이 발생하는 비트를 중심으로 digit shift register를 설계한다. 두 번째는 memory를 활용하여 digit-serial승산이 이루어질 때 데이터의 적절한 배치와 새로운 주소발생기구조로 제어와 신호를 절반으로 줄일 수 있도록 하였다.

제안된 구조의 검증을 위하여 원시다항식$p(x)=x^{193}+x^{15}+1$인 $GF(2^{193})$상에서 kP를 수행하는데 필요한 승산기를 설계하고 기존의 구조와 비교하여 IC카드에 적용할때 하드웨어 구현측면에서 우수함을 입증하였다.

## Ⅱ. 타원곡선 암호알고리즘

### 2.1 유한체에서 소체와 타원곡선의 비교

유한체(Galois field)란 암호 이론이나 부호 이론에서 주로 사용되는 원소의 개수가 유한인 체(0에 의한 나눗셈을 제외하고는 4칙연산에 대해 닫혀있는 군)를 말한다. p를 소수라 하면 p개의 원소로 되는 유한체가 존재한다. 이것을 GF(p)로 쓰고 소체(prime field)라 부른다. 표현방식은 {0, 1, …, p-1}이 된다. 이것으로부터 P(x)를 체 F위의 다항식이라고 하자. 이때 P(x)가 체 F 위에서 기약이면, P(x)를 모듈러로 하는 체 F 위의 다항식 환의 잉여류환은 체가 된다는 것이 증명되어 있다. 또 GF(2)위에서 $x^3+x+1$은 기약이다. 이와 같은 다항식을 기약 다항식(irreducible polynomial)이라 한다. 기약 다항식 P(x)의 차수를 n이라 하면, 같은 형태의 GF(p)에서 $p^n$개의 원소를 가지는 유한체를 만들 수 있다. 여기서 p=2로 놓으면 본 논문에서 논의되는 GF(2)가 되고 이것의 확장인 $GF(2^m)$이 되는 것이다. 이와 마찬가지로 유한체에서의 모듈러 p를 p(x)의 형태로 표현한다.(본 논문에서는 $GF(2^{193})$에서 $p(x)=x^{193}+x^{15}+1$를 대상으로 한다)[5]

〔표 1〕 유한체와 타원곡선의 비교

| 군 | $Z_p^*$ | $E(Z_p)$ |
|---|---|---|
| 원소 형태 | 정수 {1, 2, … , p-1} | E의 점 (x, y)과 $O$ |
| 연산 | 모듈러 p에서의 곱셈 | 점의 더하기 |
| 표기 | 원소 : g, h<br>곱하기 : $g^*h$<br>역원 : $g^{-1}$<br>나누기 : g/h<br>지수 : $g^a$ | 원소 : P, Q<br>더하기 : P + Q<br>역원 : - P<br>빼기 : P - Q<br>배수 : aP |
| 이산대수문제 | $Z_p^*$의 원소 g가 주어지고, $h=g^a \bmod p$일 때, a를 찾는 문제 | $E(Z_p)$의 원소 P가 주어지고, Q=aP일 때, a를 찾는 문제 |

〔표 1〕과 같이 타원곡선 암호시스템은 타원곡선 위의 점 $P$를 $x$번 더하는 계산이 주를 이룬다. 즉, $Q=xP$를 구하는 더하기 연산은 모듈러 곱셈을 통해 이루어진다. 주요 공개키 암호시스템은 효율적인 모듈러 곱셈에 의존하고 있으며, 타원곡선은 소수 $p$의 값이 다른 시스템보다 작기 때문에 그 효율성이 뛰어나다 할 수 있다. 즉, 타원곡선 암호시스템의 안전도는 타원곡선 이산대수문제에 의존하고 있으며, 그 효율성은 $xP$의 빠른 계산에 달려 있다. 위를 수행하는 알고리즘은 여러 가지로 변형될 수 있다.[6]

### 2.2 Polynomial Basis 구조

원소의 개수가 $2^m$개인 유한체 $GF(2^m)$상에서 다항

식 표현의 기본이 되는 basis는 NB(Normal Basis), PB(Polynomial Basis), 그리고 DB(dual Basis) 등 크게 3가지로 나눌 수 있다. 표현방식을 보면 NB의 경우 GF($2^m$)상에서 $\{\alpha, \alpha^2, \cdots, \alpha^{2^{m-1}}\}$이며 PB의 경우 GF($2^m$)상에서 $\{1, \alpha, \cdots, \alpha^{m-1}\}$이다. DB는 GF($2^m$)상에서 field generator P(x)의 근원인 $\alpha$로 이루어진 PB $\{1, \alpha, \cdots, \alpha^{m-1}\}$를 바탕으로 $\{1, \alpha, \cdots, \alpha_{m-1}\}$로 표현된다.

위 형식에서 볼 때 NB에서 원소 a의 제곱근은 한번의 순회치환으로 얻어지므로 승산의 이점이 있다. 그러나 이 표현에 사용되는 함수 f에 의존한다는 단점이 있다. 또한 DB 표현도 게이트 수는 줄일 수 있으나 속도가 감소한다. 이 표현에 의한 하드웨어 구현시 DB로부터 PB로 변환하는 회로로 인하여 회로규모가 증가하는 단점을 가진다. 이와 반대로 PB는 회로 구현시 구조가 간단하고 간단한 제어부를 요구한다. 또한 이 구조는 어떠한 field generator P(x)를 선택하더라도 동일한 구조를 사용할 수 있는 이점이 있다.

### 2.3 타원곡선 암호시스템의 장점

타원곡선 암호시스템은 유한체의 곱셈군에 근거한 시스템으로써 다음의 장점을 가진다.

① 군(Group)을 제공할 수 있는 다양한 타원곡선을 활용할 수 있다 (암호시스템 설계가 용이하다).
② (초특이 타원곡선을 피하면)이 군에서 subexponential time algorithms이 존재하지 않는다. 즉, 안전한 암호시스템을 설계하는 것이 용이하다.
③ 타원곡선 암호시스템은 존재하는 다른 공개키 스킴과 같은 안전도를 제공하는 데에 더 작은 키 길이를 가지고 가능하다(RSA 1024비트 키=ECC 160비트 키)
④ 타원곡선에서 가산은 유한체에서의 연산을 포함하므로, H/W와 S/W로 구현하기가 용이하다. 이 군에서의 이산대수 문제는 특히, 같은 크기의 유한체 K에서의 이산대수 문제보다 훨씬 어렵다.

### 2.4 Bit-serial 유한체 승산기 구조

N차의 다항식 A, B와 m차의 원시다항식 $\alpha$가 주어질 때 타원곡선에서 구현되는 유한체 승산의 표현식은 다음과 같다.

$$Z = A \cdot B = \sum_{i=0}^{m-1} b_i(A\alpha_i)$$
$$= [\cdots[[b_0(A) + b_1(A\alpha)] + b_2(A\alpha^2)] + \cdots] + b_{m-1}(A\alpha^{m-1}) \quad (1)$$

$\alpha$는 차수가 m인 원시다항식 $p(x)$를 이용 $\alpha^m = p_0 + p_1\alpha + \cdots + p_{m-1}\alpha^{m-1}$로 정리 후 식 (1)에 대입한다.

$$A\alpha = a_0\alpha + a_1\alpha^2 + \cdots + a_{m-1}\alpha^m = a_0\alpha + a_1\alpha^2 + \cdots + a_{m-1}(p_0\alpha + p_1\alpha_2 + \cdots + p_{m-1}\alpha^{m-1})$$
$$= a_{m-1}p_0 + (a_0 + a_{m-1}p_1)\alpha + (a_1 + a_{m-1}p_2)\alpha^2 + \cdots + (a_{m-2} + a_{m-1}p_{m-1})\alpha^{m-1} \quad (2)$$

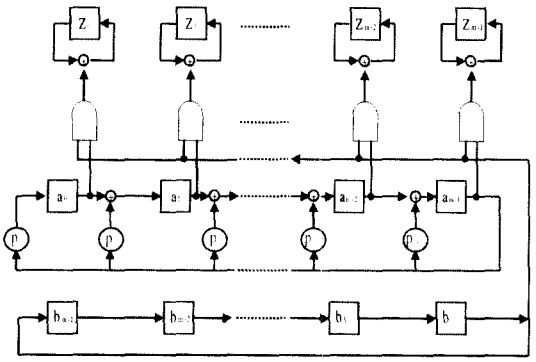
식 (2)를 레지스터와 논리게이트를 이용하여 회로로 구현하면 [그림 1]과 같은 bit-serial 승산기를 얻을 수 있다.[7,8]

식 (1)은 다음식 (3)과 같이 표현 할 수 있다.

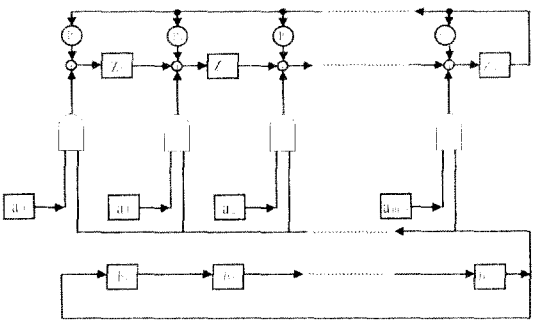
$$Z = A \cdot B = \sum_{i=0}^{m-1} b_i(A\alpha_i)$$
$$= (\cdots((b_{m-1}A)\alpha + b_{m-2}A)\alpha + \cdots)\alpha + b_0A \quad (3)$$

식 (3)을 [그림 1]과 같은 방식으로 회로를 설계하면 [그림 2]와 같은 다른 형태의 승산기를 얻게 된다.

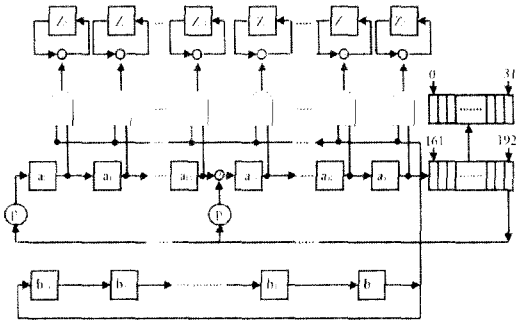
[그림 1]은 LSB(Least Significant Bit)부터 승산하는 회로이고 MSB(Most Significant Bit)부터 승산하도록 구현된 회로가 [그림 2]의 구조이다. 이 두가지 회로는 모두 LFSR(Linear Feedback Shift Register) 구조를 기본으로 한다. [그림 1, 2]



[그림 1] 순차회로를 이용한 승산기 I



〔그림 2〕 순차회로를 이용한 승산기 II



〔그림 3〕 m=193, d=32 bit digit-serial 승산기 구조

의 승산기 회로에서 A와 Z는 모든 bit들이 병렬적으로 처리가 되므로 키 길이와 상관없이 A · Bi mod P는 한 싸이클에 수행이 된다. 그러므로 순차적으로 곱해지는 B의 bit수로 전체시간을 계산한다.

이와같이 LFSR구조의 승산기는 multiplicand bit를 병렬로 연산하는 반면 multiplier는 bit단위의 직렬처리를 한다. 일반적인 LFSR구조의 승산기에서는 multiplicand가 m bits 병렬처리를 하기 때문에 3 · m레지스터, m XOR 게이트, m AND 게이트가 필요하다.

그러나 일반적인 LFSR구조의 승산기를 스마트카드와 같이 제한된 면적에서 활용하기 위해서는 보다 축소된 면적의 회로 설계가 요구된다.

## III. Digit-serial 유한체 승산기의 구조 및 회로 설계

### 3.1 메모리를 활용하는 Digit-serial 회로구조

LFSR구조 승산기에서 m bits길이의 연산 레지스터를 d bits 단위의 digit로 분할하면 레지스터의 수가 m/d 배 만큼 축소가 된다.

본 논문에서는 〔그림 3〕에서와 같이 d=32bit인 digit-serial 구조의 승산기를 제안한다. 원시다항식 $p(x)=x^{193}+x^{15}+1$인 $GF(2^{193})$상에서 임의의 두 원소 A, B간의 승산을 목적으로 설계된 승산기 이다.

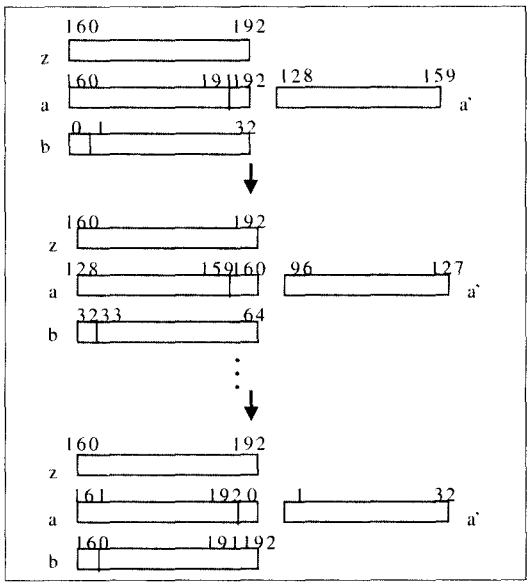
제안된 승산기는 그림 1의 승산기-I 구조를 바탕으로 하되 한 digit단위인 32bit길이의 레지스터들로 구성된다. 32bit로 분할된 A, B, Z레지스터 이외에 modular p(x)에 의하여 변형된 A레지스터의 32번 shift 결과가 저장되는 레지스터로 구성된다. 193bit multiplicand와 multiplier 그리고 변형된 A레지스터 값, 승산결과인 Z레지스터 값은 메모리에 저장된다. 메모리는 별도로 두지않고 스마트카드내의 메인 데이터 메모리를 공유하는 방식으로 한다. 따라서 메모리 access를 위한 주소발생장치가 설계되었다.

### 3.2 제안된 구조에서 승산방법

제안된 승산기에서 193bit 승산방법을 설명하면, 〔그림 4〕와 같이 초기상태에서는 multiplicand의 하위 32bit를 A 레지스터에 multiplier의 하위 32bit는 B 레지스터에 저장한다. A레지스터에 직렬로 연결되어 있는 A 레지스터 우측 32비트 레지스터에서는 A 레지스터로부터 shift right되어 밀려나온 bit들을 차례로 저장하게된다.

Multiplier 32bit는 multiplicand와 함께 bit-serial연산을 종료한 후, 다음 상위 32bit로 reload 된다. 새롭게 reload된 multiplier는 32bit bit-serial연산을 수행한다. 32bit단위로 수행되는 bit-serial연산 결과는 Z레지스터에 누적(accumulation)되고 $b_{193}$ bit의 연산이 완료될 때까지 반복되고 Z레지스터 값을 메모리에 저장한다. 이후 multiplicand의 다음 상위 32bit에 대한 연산을 위와 같은 방법으로 반복한다. 〔그림 5〕는 제안된 구조에서 m=193의 유한체 승산의 과정을 나타내고 있다.

A, B, Z레지스터 가운데 A 레지스터는 LFSR구조로 매 클럭마다 순환 shift right동작이 이루어진다. 그 결과 32 shift동작이 완료되면 좌측 digit값이 현재 digit의 32bit 레지스터와 교체된다. A레지스터에 현재 digit가 저장된다면 좌측 digit를 저장할 별도의 32bit 레지스터가 필요하다. 〔그림 4〕에서 $a_{192}$-$a_{161}$이 저장되어 있는 레지스터가 좌측 digit레지스터(그림에서는 우측에 나타나있다)이다. A레지스터에는 좌측레지스터 값인 $a_{192}$-$a_{161}$가 옮겨




〔그림 4〕 제안된구조에서 유한체 승산방법

오고 A레지스터 값인 $a_{31}$-$a_0$는 좌측 digit레지스터로 옮겨진다. 이때 옮겨진 $a_{31}$-$a_0$는 더 이상 초기값을 유지하지 못하고 modular p(x)에 의하여 변형된다. 따라서 변형된 값은 메모리에서 별도공간에 저장되어야 한다(A′ 레지스터). 이 변형된 값은 두 번째 digit인 $a_{63}$-$a_{32}$에서 연산이 이루어질 때 좌측 digit의 역할을 한다.

위와 같은 방법으로 digit 승산이 이루어질 때 m=193인 경우 6 digit와 1bit로 구성된다. 6 digit의 승산은 앞에서 설명한 바와 같이 32 shift를 6번 반복함으로써 수행이 완료된다. 그러나 남은 1 bit를 1 digit로 취급하여 처리하려면 32 cycle이 추가되기 때문에 마지막 digit에서는 남은 1bit를 포함하여 33bit로 처리되도록 설계하였다.

Multiplier $b_{192}$bit도 남은 1bit가 되며 〔그림 4〕의 맨 아래 블록에 표시된 것처럼 $b_{191}$-$b_{160}$과 더불어 마지막 digit를 형성하여 33bit digit로 승산을 수행한다.

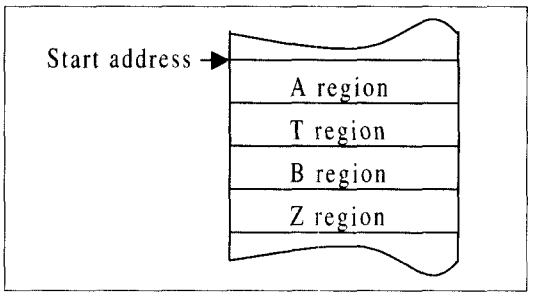
A, B 레지스터의 메모리 Load와 A′, Z 레지스터의 메모리 Load, Store를 임의의 주소영역에서도 가능하도록 주소 발생장치가 설계되었다.

### 3.3 제어FSM 및 주소발생장치 설계

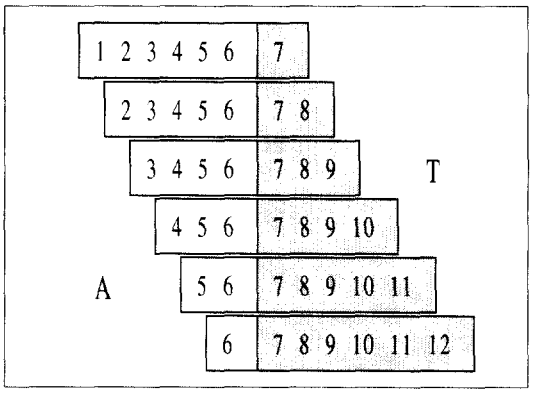
Digit-serial 승산기는 digit 단위로 연산이 이루어지기 때문에 32bit LFSR과 메모리간에 데이터교체가 자주 발생한다. 따라서 승산기 레지스터와 메모리간의 데이터교환을 위한 제어회로와 메모리 주소발생(address generation)이 복잡하게 이루어진다. 제어회로의 복잡도는 digit-serial 승산기의 장점을 상쇄할 수 있기 때문에 본 논문에서는 제어회로의 FSM(Finite State Machine)과 제어신호를 간략화할 수 있는 메모리 저장방법과 새로운 주소발생장치를 제안한다.

메모리에 저장되는 데이터는 승산입력데이터 A와 B, 승산결과값 Z, 그리고 modular reduction에 의하여 변형된 T의 영역으로 나누어진다. 〔그림 5〕는 메모리에서 A, B, Z, T영역의 배치순서이다. 본 논문에서는 승산기 FSM과 제어신호를 간략화하기 위한 방법으로 〔그림 5〕에서와같이 A영역과 T영역이 연속으로 이어지고 〔그림 6〕과 같은 구조의 계수기를 제안한다.

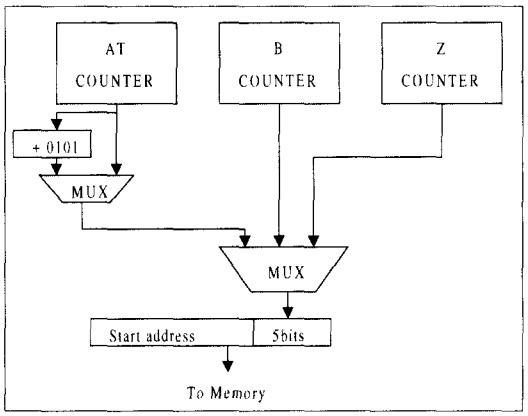
첫 번째 digit인 $a_0$-$a_{31}$의 승산에는 메모리 A1~6와 T7 영역에 저장되어 있는 digit가 사용된다. 두 번째 승산이 되는 digit는 $a_{160}$-$a_{191}$으로 메모리 A2~6와 T7~8 영역의 digit와 함께 승산이 이루어진다. 〔그림 4〕에 따라 여섯 번째 digit까지 승산



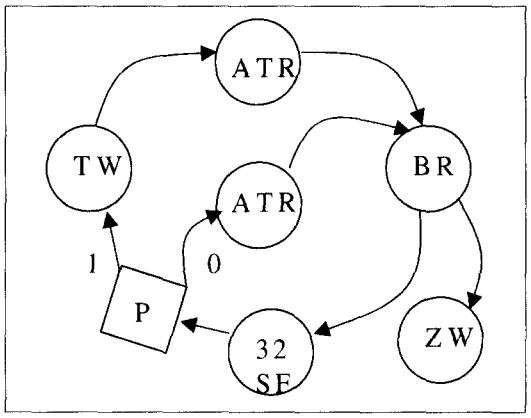

〔그림 5〕 메모리에서 데이터 영역




〔그림 6〕 AT counter의 상태변화도




〔그림 7〕 주소발생장치의 블록도




〔그림 8〕 승산기 제어FSM의 상태도

이 실행되며 이때 필요한 A의 영역과 T영역이 순서적으로 표시되어 있다. 〔그림 4〕에서와 같이 여섯개의 digit를 승산하는데 필요한 A영역의 digit주소와 T영역의 digit주소는 7-mode counter로써 시작주소(start address)가 1 씩 증가하는 구조의 counter에서 발생된다.

〔그림 6〕과 같이 A, T레지스터의 load를 위한 address를 발생하는 counter를 AT counter라하고 〔그림 7〕의 주소발생블록도에 나타내었다. 주소발생기는 3개의 counter와 이를 선택하는 멀티플렉서 그리고 counter값과 start address와 결합하여 메모리 주소를 만들기 위한 회로로 구성된다. 주소발생기의 동작을 간단히 설명하면 다음과 같다. A, T레지스터에 32bit multiplicand digit데이터를 load하기 위해서는 AT counter의 5bit출력값과 32bit start address의 상위 27bit를 연결하여 주소를 만들어낸다.

B레지스터에 32bit multiplier digit데이터를 load하는데는 B counter의 5bit가 같은 방법으로 사용된다. 승산 결과값 Z는 Z counter에 5bit를 더하여 만들고 이 주소값에 store한다.

제안된 AT counter의 장점은 주소발생회로에서 A counter와 T counter를 통합하여 회로 구현시 게이트수를 축소할 수 있고 승산기 제어 FSM에서 A counter와 T counter의 값을 증가하는 제어신호수를 반으로 줄일 수 있다. AT counter를 사용함으로써 간략화된 승산기 제어FSM의 상태도를 〔그림 8〕에 나타내었다. AT counter를 적용하지 않으면 A counter와 T counter가 각각 독립적으로 존재하여 각각의 제어 상태가 발생하여 AT counter에 비하여 2 state가 늘어난다. 〔그림 8〕의 상태도에서 ATR은 AT counter가 지정하는 주소의 digit를 read하는 동작이며 BR은 B영역의 digit의 read 동작이다. 그리고 ZW는 승산결과 digit의 저장동작을 TW는 modular reduction으로 변형된 A digit를 T영역에 저장하는 것을 의미한다. P는 reduced polynomial의 계수로 p=1인 부분에서는 A digit의 변형동작이 발생하기 때문에 변형된 값을 T영역에 저장하게되고 p=0인 부분에서는 A digit가 변형되지않고 원래값을 유지하면서 shift가 이루어지기 때문에 T영역에 저장하지 않고 승산이 진행된다.

## Ⅳ. 회로 검증 및 성능평가

제안된 회로는 하드웨어기술언어인 VHDL로 코딩되었다. 코딩 기술(description)의 수준(level)은 회로합성기(synthesizer) 툴로 합성가능한 수준으로 회로의 규모를 게이트단위로 정확하게 측정하는데 필수적인 방법이다. 합성가능한 VHDL코드는 구현된 회로의 크기 예측 뿐만아니라 정상적인 기능을 검증하는 수단으로 이용된다. 설계된 회로는 $p(x)=x^{193}+x^{15}+1$인 원시 다항식으로 다항식기저(polynomial basis) 유한체상에서 타원곡선 좌표의 덧셈연산에 사용된다.

회로의 기능을 검증하기 위하여 다음 식 (4), (5)를 이용한 타원곡선상의 좌표계산을 C언어로 프로그램 하여 승산검증을 위한 유효한 테스트벡터를 만들어 기능검증을 위한 입력프로그램으로 사용하였다.

〔표 2〕 VHDL과 SYNOPSYS로 구현된 결과

| 형태 | 게이트수 | cycle 수 |
|---|---|---|
| 193bit Bit-Serial 승산기 | 약 7120 | 210 cycle,6.93us@33MHz |
| Digit-Serial 승산기 | 약 2050 | 1200 cycle,39.6us@33MHz |

*게이트수는 합성결과로 Library에 따라 다소차이가 있음.

타원곡선 $y^2+xy=x^3+ax^2+b$

임의의 좌표 $P(x1, y1)$, $Q(x2, y2)$

$$R=P+Q, R(x3, y3) \quad (\text{if } P\neq Q) \tag{4}$$

$$x3=\frac{(y1-y2)}{(x1+x2)}^2+\frac{(y1-y2)}{(x1+x2)}+x1+x2+a$$

$$y3=\frac{(y1-y2)}{(x1+x2)}(x1+x3)+x3+y1$$

$$R=2P, R(x3, y3) \quad (\text{if } P=Q) \tag{5}$$

$$x3=\frac{(y1-y2)}{(x1+x2)}^2+\frac{(y1-y2)}{(x1+x2)}+a$$

$$y3=\frac{(y1-y2)}{(x1+x2)}x3+x3+y1$$

검증결과 〔표 2〕와 같이 기존의 LFSR구조를 193bit 에 적용한 경우에 비하여 면적에서 3.5배의 효율을 높일 수 있다. 반면 실행사이클 수는 6배 가량 증가하여 33MHz 클럭에서 193비트 승산에 39.6usec가 소요된다. EC(Elliptic Curve)를 projective coordinate에서 정의하면 EC의 point double에 12회의 승산이 point add에 14회의 승산이 요구된다. 이것을 EC의 point multiplication에 적용하면 대략 90msec의 시간이 소요된다. 스마트카드에 적용하여 보면 기존의 MC68HC05SC49, P83C858 등 스마트카드칩[3]과 비교할수 있다. 이들 칩은 5MHz 클럭에 RSA 1024비트를 적용할 때 signature time이 2 - 5.6초가 소요된다. 본 논문에서 제안된 구조와 비교하기 위하여 제안된 승산기를 5MHz로 맞추면 EC의 point multiplication이 약 600msec가 소요되어 비교대상의 스마트카드칩에 비하여 성능이 개선되었음을 검증할 수 있다.

## V. 결 론

본 논문에서는 스마트 카드 내에 탑재되는 암호화 프로세서 가운데 타원곡선(ECC)알고리즘 모듈을 구현하는데 필수적인 유한체 승산기를 설계하였다. 다항식기저(polynomial basis) 유한체상에서 다항식이 trinomial인 경우 기존의 bit-serial based LFSR구조의 승산기를 개선하여 digit-serial LFSR구조의 승산기로 구현하는 데 장점이 있으며 회로의 규모를 축소시켜 저전력, 소규모 회로구현에 적합하다는 것을 입증하였다.[9] 제안된 구조는 원시다항식이 $p(x)=x^{193}+x^{15}+1$인 타원곡선알고리즘을 사용한 암호화 프로세서에 적용하여 설계하였으며 이때 digit는 32bit단위로 하였다. 검증결과 기존의 방법을 사용한 193bit LFSR 승산기에 비하여 게이트 수가 70% 축소되었으며 스마트카드에 적용시 사용가능한 실행사이클을 보였다

## 참 고 문 헌


〔1〕 N. Koblitz, "Elliptic Curve Crypto systems", Mathematics of Computation, 48, pp. 203~209,1987.

〔2〕 G.B. Agnew, R.C. Mullin and S.A. Vanstone, "An Implementation of Elliptic Curve Cryptosystems Over $F_2^{155}$", IEEE journal on selected areas in communications, Vol. 11, No. 5, June 1993.

〔3〕 David Naccache David M'Raïhi, "Cryptographic Smart Cards", *IEEE MICRO*, Vol. 16, No. 3, pp. 14~23, June, 1996

〔4〕 Lijun Gao, Sarvesh Shrivastava and Gerald E. Sobelman, "Elliptic Curve Scalar Multiplier Design Using FPGAs", First International Workshop, CHES'99, Proceedings, pp. 257~268, Aug12-13,1999.

〔5〕 한국전자통신연구원, "*암호학의 기초*" 경문사, pp. 25~28, 3월, 1999.

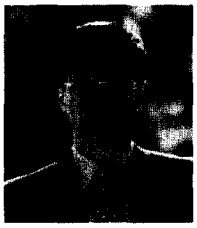
〔6〕 이인수, "타원곡선 암호시스템에 관한 연구", 연세대학교 대학원 석사 논문, pp. 3~28, 12월, 1996.

〔7〕 Edoardo D. Mastrovito, "VLSI Architectures for Computations in Galois Fields", *Linköping Studies in Science and Technologz. Dissertations*, No. 242, pp. 35~54, 1991

〔8〕 이만영, "*BCH부호와 Reed-Solomon 부호*", 민음사, pp. 21~54

〔9〕 B. Sunar and C.K. Koc, "Mastrovito Multiplier for All Trinomials", *IEEE Tran. Computers*, Vol. 48, No. 5, pp. 522~527, May, 1999.

## 〈著者紹介〉

**이 광 엽(Kwang-Youb Lee) 정회원**
1985년 : 서강대학교 전자공학과 학사
1987년 : 연세대학원 전자공학과 석사
1994년 : 연세대학원 전자공학과 박사
1989~1995년 : 현대전자 시스템IC연구소 선임연구원
1995년~현재 : 서경대학교 전자통신컴퓨터공학부 조교수
〈관심분야〉 마이크로 프로세서, 암호프로세서, 컴퓨터구조

**위 사 흔(sa-heun Wie) 회원**
1999년 2월 : 서경대학교 컴퓨터공학과 졸업
1999년 3월 : 서경대학원 컴퓨터과학과 석사 입학
1999년 3월~현재 : 서경대학원 컴퓨터과학과 석사과정
〈관심분야〉 VLSI, 마이크로 프로세서, 암호이론

**김 원 종(won-jong Kim) 정회원**
1989년 2월 전남대학교 전자공학과 공학사
1982년 2월 한양대학교 전자공학과 석사
1999년 2월 한양대학교 전자공학과 박사
1999년 3월~2000년 3월 한양대학교 공학기술 연구소 선임연구원
2000년 4월~현재 한국전자통신연구원 회로소자기술연구소 선임연구원
〈관심분야〉 VLSI CAD, Embedded System 설계,SoC 설계 등

**장 준 영(june-young Chang) 정회원**
1985년 2월 전남대학교 전산학과 학사
1987년 2월 중앙대학교 전산학과 석사
1996년 3월 전남대학교 전산학과 박사
1998년 대불대학교 컴퓨터 공학과 전임강사
1997년~현재 전자통신연구원 회로소자연구소 선임연구원
〈관심분야〉 CAD/VLSI, 논리합성, Codesign, Embadded System, SOC 설계

**정 교 일(kyo-il Chung) 정회원**
1981년 2월 한양대학교 전자공학과 석사
1983년 8월 한양대학교 산업대학원 전자계산학과 석사
1997년 8월 한양대학원 전자공학과 박사
1981년 12월~현재 : 한국전자통신연구원 정보보호기술연구본부
부장/책임연구원
〈관심분야〉 IC Card, Security , Biometry, 정보전, 신호처리

**배 영 환(young-whan Bae) 정회원**
1985년 2월 한양대학교 전자공학과 학사
1987년 2월 한양대학원 전자공학과 석사
1987년 2월~현재 한국전자통신연구원 회로소자연구소 선임연구원 시스템설계자동화팀 팀장
〈관심분야〉 VLSI CAD, 하드웨어/소프트웨어 통합설계, Embedded System설계,
Embedded 프로세서설계 등