GF(2^m) 상의 타원곡선 B-233을 지원하는 32-비트 WMM 기반 ECC 프로세서

이상현 · 신경욱

금오공과대학교

ECC Processor Supporting Elliptic Curve B-233 over GF(2^m) using 32-b WMM

Sang-Hyun Lee · Kyung-Wook Shin

Kumoh National Institute of Technology

E-mail : lpp1124@kumoh.ac.kr

요 약

이진체 상의 타원곡선 B-233을 지원하는 타원곡선 암호 프로세서를 32-비트 워드기반 몽고메리 곱셈기를 이용하여 설계하였다. 스칼라 곱셈을 위해 수정된 몽고메리 래더 (Modified montgomery ladder) 알고리즘을 적용하여 단순 전력분석에 내성을 갖도록 하였으며, Lopez-Dahab 투영 좌표계와 페르마의 소정리(Fermat's little theorem)를 적용하여 하드웨어 자원 소모가 큰 나눗셈과 역원 연산을 제거하여 저면적으로 설계하였다. 설계된 ECC 프로세서는 Xilinx ISim을 이용하여 기능검증을 하였으며, 0.18㎛ CMOS 셀 라이브러리로 합성한 결과 100 MHz의 동작 주파수에서 9,614 GEs와 4 Kbit RAM으로 구현되었으며, 최대 동작 주파수는 125 MHz로 예측되었다.

키워드

ECC, GF(2^m), Lopez-Dahab, Fermat's little theorem, Word-based montgomery multiplication

I. 서 론

정보통신기술의 발전에 따라 인터넷 기반인 사물인터넷(IoT; Internet of Things)이 빠르게 확산되며, 더불어 정보보안의 중요성이 증가하고 있다. 실생활과 밀접한 사물인터넷 디바이스들의 경우 하드웨어 자원이 제한적이므로 경량 보안기술이 필요하다. 개인정보 침해, 악성코드와 같은 보안 위협으로부터 정보를 안전하게 보호하기 위한 암호시스템으로 대칭키 암호, 공개키 암호, 해시함수 등 다양한 방법들이 사용된다.

공개키 암호 방식인 타원곡선 암호(Elliptic Curve Cryptography; ECC)는 1985년 Kobitz와 Miller에 의해 제안되었다[1,2]. 타원곡선 암호는 기존의 RSA 공개키 암호 방식에 비해 짧은 키 길이로 유사한 안전성을 얻어지는 장점이 있어 RSA를 빠르게 대체하고 있으며, IoT와 같이 제한된 자원을 갖는 디바이스에 적합한 공개키 암호 방식으로 응용분야가 확대되고 있다.

본 논문에서는 미국 국립표준기술국(NIST)에서 정의된 B-233 타원곡선[3]을 지원하는 ECC 프로세서를 저면적으로 설계하고, Xilinx ISim을 이용하여 검증하였다.

II. ECC 프로세서 설계

공개키 암호방식인 타원곡선 암호는 타원곡선 위의 한 점 P를 k번 가산하는 스칼라 곱셈을 기반으로 한다. 이 때 k는 개인 키이고, 연산결과로 생성된 점 $Q=kP$은 공개키로 사용된다. 스칼라 곱셈은 점 연산의 반복으로 계산되며, 타원곡선 상의 서로 다른 두 점을 더하는 점 덧셈 (point addition) 연산과 동일한 점에 대한 두 배 (point doubling) 연산으로 구성된다. 점 연산은 덧셈, 곱셈, 나눗셈 등의 유한체 연산으로 계산된다. 타원곡선 상의 점은 2차원 좌표로 구성된 아핀 (affine) 좌표, 3차원 좌표로 구성된 Lopez-Dahab, Jacobian 좌표 등으로 나타낼 수 있으며, 본 논문에서는 하드웨어 자원 소모가 큰 나눗셈 연산을 제거하기 위해 Lopez-Dahab 좌표를 사용하였다.

설계된 ECC 프로세서는 B-233 타원곡선 암호를 지원하며, 전체 구조는 그림 1과 같다. 스칼라 곱셈에 필요한 데이터를 저장하는 Smul_Reg 블록, XOR, 곱셈 연산을 하는 SAlu_GFb 블록, 스칼라 곱셈 연산을 제어하는 제어블록으로 구성된다.

Smul_Reg 블록은 정수 k, 생성점의 좌표 값, XOR, 곱셈연산 결과 값 등을 저장하는 112x32-비

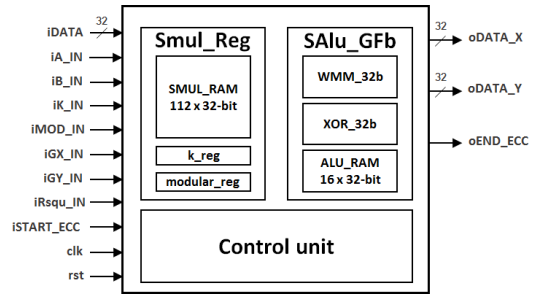


Fig. 1. Architecture of ECC processor.

트 메모리, 메모리에 저장된 정수 k를 32-비트씩 저장하며, 점 연산이 끝날 때마다 왼쪽으로 시프트하여 MSB 값을 통해 수정된 몽고메리 알고리즘을 적용하기 위한 k_reg, 유한체 연산에 필요한 기약다항식을 저장한 modular_reg로 구성된다.

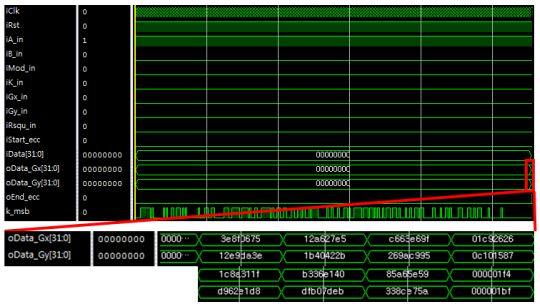
SAlu_GFb 블록은 곱셈 및 XOR 연산을 위한 WMM_32b, XOR_32b과 중간결과 값을 저장하기 위한 16x32-비트 메모리로 구성된다.

ECC 프로세서는 제어 블록을 통해 데이터 입력, 매핑, 스칼라 곱셈, 좌표 변환, 리매핑, 데이터 출력 순으로 진행된다. 매핑은 아핀 좌표 값으로 입력받은 데이터를 Lopez-Dahab 좌표로 변환하고, 몽고메리 도메인으로 변환한다. 스칼라 곱셈은 k_reg의 MSB 값을 통해 점 연산을 수행한다. 좌표 변환은 스칼라 곱셈의 출력 값을 아핀 좌표 값으로 변환하고, 리매핑은 몽고메리 도메인에서 일반 도메인으로 변환한다.

매핑 단계에서 Lopez-Dahab 좌표로 변환함으로써 아핀 좌표에서 사용되는 나눗셈 연산이 제거된다. 점 (x, y, z)를 점 $(x/z, y/z^2)$으로 변환하기 위해서는 역원 z^{-1}이 필요하다. 역원은 페르마의 소정리를 적용하여 워드 기반 몽고메리 곱셈기를 사용하여 구현하였다. 따라서 하드웨어 자원소모가 큰 나눗셈 및 역원 연산기를 사용하지 않음으로써 저면적으로 구현하였다.

III. 기능 검증

설계된 ECC 프로세서는 Xilinx ISim을 이용한 RTL 시뮬레이션 결과 값을 문헌 [4]의 참조 구현 값과 비교하여 검증하였다. 그림 2는 ECC 프로세서의 시뮬레이션 결과 값과 참조 구현 값을 보여준다. NIST FIPS 186-2에 정의된 B-233 타원곡선 파라미터를 사용하였으며, 233-비트의 정수 k "c7e814dd40 466073ef 4cfd3319 b2f0488d 3eed4bba 24dc189a 1c65c202"과 생성점을 스칼라 곱셈하였다. 시뮬레이션 결과 값은 하위비트부터 출력되며 그림 2-(a)에서 연산이 완료된 x좌표 "1f4 85a65e59 b336e140 1c8a311f 01c92626 c663e69f 12a627e5 3e8f0675", y좌표 "1bf 338ce75a dfb07deb d962e1d8 0c101587 269ac995 1b40422b 12e9da3e"로 그림 2-(b)의 참고 구현 값과 일치함을 확인하였다.



(a) Simulation result

$d^{-1} \bmod n$ = 00C7 E814DD40 466073EF 4CFD3319 B2F0488D 3EED4BBA 24DC189A 1C65C202

$Q = d^{-1}G = (x, y)$

x = 01F4 85A65E59 B336E140 1C8A311F 01C92626 C663E69F 12A627E5 3E8F0675

y = 01BF 338CE75A DFB07DEB D962E1D8 0C101587 269AC995 1B40422B 12E9DA3E

(b) Reference data

Fig. 2. Simulation results of ECC processor.

IV. 결 론

수정된 몽고메리 래더 알고리듬, Lopez-Dahab 투영 좌표계, 페르마의 소정리 등을 적용하여 ECC 프로세서를 저면적으로 설계하였다. ECC 프로세서는 0.18㎛ 공정의 CMOS 셀 라이브러리로 합성한 결과 100 MHz의 동작 주파수에서 9,614 GEs와 4 Kbit RAM으로 구현되었다.

ACKNOWLEDGMENTS

- This work was supported by KIAT(Korea Institute for Advancement of Technology) grant funded by the Korea Government(MOTIE : Ministry of Trade, Industry and Energy) (No.N0001883, HRD Program for Intelligent semiconductor Industry)
- This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education (No. 2017R1D1A3B03031677)

참고문헌

[1] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203-309, Jan. 1987.

[2] V. Miller, "Uses of Elliptic Curves in Cryptography," Advances in cryptography-CRYPTO 85', LNCS 218, pp. 417-426, 1986.

[3] NIST Std. FIPS PUB 186-2, *Digital Signature Standard (DSS)*, National Institute of Standard and Technology (NIST), Jan. 2000.

[4] EC-KCDSA : 부가형 전자 서명 방식 표준 - 제 3 부 : 타원곡선을 이용한 인증서 기반 전자 서명 알고리즘, TTA 정보통신표준, Dec. 2001.