NIST B-233 타원곡선을 지원하는 233-비트 ECC 프로세서

박병관* · 신경욱*

*금오공과대학교

233-bit ECC processor supporting NIST B-233 elliptic curve

Byung-Gwan Park* · Kyung-Wook Shin*

*Kumoh National Institute of Technology

E-mail : bask369@kumoh.ac.kr

요 약

전자서명(ECDSA), 키 교환(ECDH) 등에 사용되는 233-비트 타원곡선 암호(Elliptic Curve Cryptography; ECC) 프로세서의 설계에 대해 기술한다. $GF(2^{233})$ 상의 덧셈, 곱셈, 나눗셈 등의 유한체 연산을 지원하며, 하드웨어 자원 소모가 적은 쉬프트 연산과 XOR 연산만을 이용하여 구현하였다. 스칼라 곱셈은 modified montgomery ladder 알고리듬을 이용하여 구현하였으며, 정수 k의 정보를 노출하지 않고, 단순 전력분석에 보다 안전하다. 스칼라 곱셈 연산은 최대 490,699 클록 사이클이 소요된다. 설계된 ECC 프로세서는 Xilinx ISim을 이용한 시뮬레이션 결과값과 한국인터넷진흥원(KISA)의 참조 구현 값을 비교하여 정상 동작함을 확인하였다. Xilinx Virtex5 XC5VSX95T FPGA 디바이스 합성결과 1,576 슬라이스로 구현되었으며, 189 MHz의 최대 동작주파수를 갖는다.

키워드

ECC, ECDSA, ECDH, Public key cryptography, Montgomery ladder

Ⅰ. 서 론

정보는 하나의 자산으로 비인가 된 불법적인 접근으로부터 보호되어야 한다. 이에 대칭 키 암호시스템과 서로 보완적인 역할을 하며 전자서명, 키 교환, 무결성 검증 등을 위한 비대칭 키 암호시스템(asymmetric key cryptography)의 중요성이 더욱 증가하고 있다.

타원곡선 암호(Elliptic Curve Cryptography; ECC)는 미국 국제표준기관과 IEEE에서 공개키 암호(public key cryptography) 표준으로 채택되었으며, 한국정보통신기술협회는 ECC를 이용한 인증서 기반 전자서명 알고리듬(EC-KCDSA)을 정보통신단체표준으로 제정하였다.[1]

ECC는 기존의 비대칭 키 암호시스템 RSA나 DSA보다 작은 길이의 키 값으로 높은 안정성을 보장한다. 특히, 160-비트의 키 길이를 지원하는 ECC는 1024-비트의 키 길이를 지원하는 RSA와 동일한 안정성을 보장한다.[2]

최근 ECC는 적은 양의 메모리 사용과 용이한 키 관리로 인하여 사물인터넷, 스마트카드, 무선통신 단말기 등과 같이 제한된 응용분야에 적합한 비대칭 키 암호시스템으로 제안되고 있다.

미국 표준기술연구소(NIST)에서 2011년을 기준으로 224-비트 이상의 키 길이를 지원하는 타원곡선 암호를 권고하고 있으며, 이러한 이유로 본 설계에서는 233-비트 키 길이를 지원하는 ECC 프로세서를 설계하고, Xilinx ISim을 이용하여 기능검증을 하였다.

Ⅱ. 타원곡선 암호 알고리듬

$GF(2^m)$ 상에서 타원곡선은 식 (1)과 같으며, ECC가 근간을 두고 있는 ECDLP(Elliptic Curve Discrete Logarithmic Problem)는 타원곡선 상의 임의의 한 점 P에서 정수 k를 곱한 결과값이 $Q=kP$일 때, 점 P와 Q를 알고 있어도 정수 k를 알아내기 어렵다는 것을 의미한다. 이때 정수 k가 사용자의 비밀키이며, 점 Q가 공개키이다. 위 연산을 타원곡선 상의 스칼라 곱셈이라고 하며, 스칼라 곱셈은 점 덧셈 연산과 점 두배 연산으로 계산될 수 있다.

$$y^2 + xy = x^3 + ax^2 + b \qquad (1)$$

점 덧셈 연산과 점 두배 연산의 수식은 표 1과 같으며, 각 연산들은 유한체 상의 덧셈, 곱셈, 제곱, 나눗셈 연산으로 구현된다.

Table 1. Point addition and point doubling for EC

점 덧셈 연산	점 두배 연산
$\lambda = \frac{y_1 + y_0}{x_1 + x_0}$	$\lambda = x_0 + \frac{y_0}{x_0}$
$x_2 = \lambda^2 + \lambda + x_0 + x_1 + a$	$x_2 = \lambda^2 + \lambda + a$
$y_2 = \lambda(x_0 + x_2) + x_2 + y_0$	$y_2 = x_0^2 + (\lambda + 1)x_2$

III. ECC 프로세서 하드웨어 설계

설계된 ECC 프로세서의 전체구조는 그림 1과 같으며, 스칼라 곱셈의 중간 결과값 저장과 덧셈 연산 등을 수행하는 Reg_Add 블록, 유한체 상의 곱셈, 제곱, 나눗셈 연산을 수행하는 Alu_GF233 블록, 그리고 제어블록으로 구성된다.

Reg_Add 블록은 생성점 $G(x, y)$의 x좌표, y좌표를 저장하는 레지스터, 정수 k 값을 저장하는 레지스터, 스칼라 곱셈의 중간 결과값을 저장하는 레지스터를 포함한 7개의 233-비트 레지스터를 가지고 있다. 또한, 유한체 상의 덧셈 연산은 단순 비트 단위의 XOR 게이트로 구현하였다.

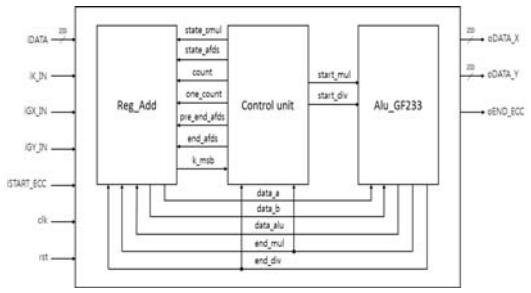


Fig. 1. Architecture of the ECC processor

스칼라 곱셈을 위한 제어블록은 Modified Montgomery ladder 알고리듬을 이용하여 구현하였으며, 정수 k의 최상위 비트가 1의 값을 갖는 경우만을 고려한 기존 Montgomery ladder 알고리듬[3]의 제약조건을 해결하였다.

또한, Double-and-Add 알고리듬과 비교하여 정수 k의 정보를 노출하지 않고, 단순전력분석에 보다 안전하다.[4]

Alu_GF233 블록은 유한체 상의 곱셈기와 나눗셈기로 이루어져 있다. 실제 점 덧셈 연산 또는 점 두배 연산에서 제곱 연산을 필요로 하지만 본 설계에서는 제곱 연산기를 곱셈 연산기로 대체함으로써 하드웨어 자원소모를 절감하였다.

그림 2는 제어블록을 제외한 곱셈기의 내부 구조를 나타낸다. 곱셈기는 자원소모가 큰 곱셈 연산과 모듈러 연산을 사용하지 않고, 오직 쉬프트 연산과 XOR 연산만을 이용하는 Shift-and-Add 방법을 사용하여 구현하였다. 곱셈기는 233-비트 레지스터 3개와 XOR 게이트 등으로 구성되며, Shift_reg 레지스터에 저장되어 있는 데이터는 오른쪽으로 1비트씩 쉬프트하며 연산을 수행한다. Reg_Add 블록으로부터 2개의 233-비트 데이터를 입력받아 233 클록 후에 end_mul 신호와 함께 C_reg 레지스터로부터 곱셈 결과값이 출력된다.

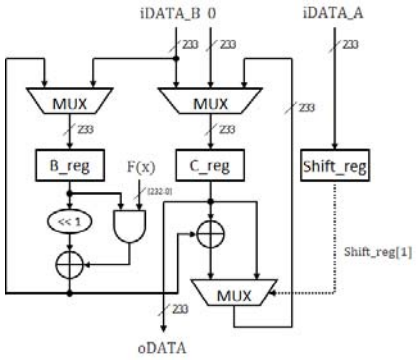


Fig. 2. Multiplication block

유한체 상에서의 나눗셈은 곱셈의 역원을 구하고, 그 역원을 곱하는 것으로 계산된다. 하지만 본 설계에서는 확장 유클리드 알고리듬을 이용하여 역원 연산과 곱셈 연산을 동시에 처리하도록 하였으며, $2m$ 사이클 만에 나눗셈 연산을 완료하도록 하였다. 유클리드 알고리듬과 비교하여 약간의 하드웨어 자원이 추가되었지만, 타원곡선 상의 스칼라 곱셈에 소요되는 전체 클록 수는 상당히 줄어들 것으로 예상한다. 그림 3은 나눗셈기의 간략한 내부 구조를 나타낸다.[5]

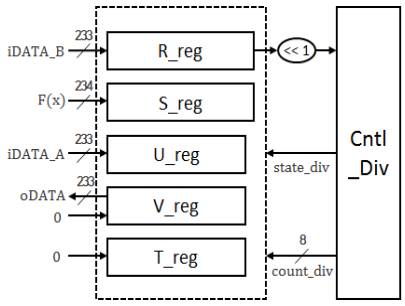
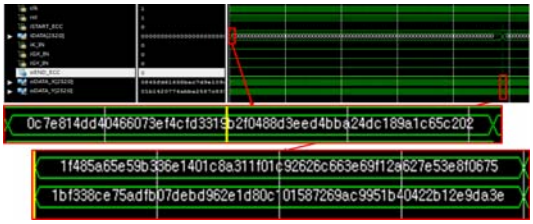


Fig. 3. Division block

나눗셈기는 233-비트 레지스터 3개, 234-비트 레지스터 2개, XOR 게이트 등으로 구성된다. R_reg 레지스터에서 출력되는 데이터를 왼쪽으로 1비트 쉬프트 하였을 때의 최상위 비트 값과 추가적인 2개의 제어신호를 이용하여 전체적인 연산을 제어하게 된다. Reg_Add 블록으로부터 2개의 233-비트 데이터를 입력받아 466 클록 후에 end_div 신호와 함께 V_reg 레지스터로부터 나눗셈 결과값이 출력된다.

Ⅳ. 기능검증

설계된 ECC 프로세서는 Xilinx ISim을 이용한 시뮬레이션 결과값과 한국인터넷진흥원의 참조 구현 값을 비교하여 정상 동작함을 확인하였다. 그림 4는 ECC 프로세서의 시뮬레이션 결과값과 참조 구현 값을 보여준다. NIST FIPS 186-2에 정의되어 있는 Curve B-233 타원곡선 파라미터를 사용하였으며, 233-비트 정수 k "0c7 e814dd40 466073ef 4cfd3319 b2f0488d 3eed4bba 24dc189a 1c65c202"를 생성점 $G(x,y)$에 스칼라 곱셈하였다. 그림 4-(a)에서 oEND_ECC 신호와 함께 스칼라 곱셈이 완료된 x좌표 "1f4 85a65e59 b336e140 1c8a311f 01c92626 c663e69f 12a627e5 3e8f0675", y좌표 "1bf 338ce75a dfb07deb d962e1d8 0c101587 269ac995 1b40422b 12e9da3e"가 출력됨을 확인할 수 있다. 이는 그림 4-(b)의 참조 구현 값과 정확히 일치함을 확인할 수 있다.



(a) ECC processor

$d^{-1} \bmod n$ = 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. 4. Functional simulation results of ECC processor

Ⅴ. 결 론

NIST FIPS 186-2 표준안에 정의되어 있는 타원곡선 B-233을 지원하는 타원곡선 암호 프로세서를 설계하였다. Xilinx Virtex5 XC5VSX95T FPGA 디바이스 합성결과 1,576 슬라이스로 구현되었으며, 최대 189 MHz로 동작하여 스칼라 곱셈에 최대 2.6 ms가 소요될 것으로 평가된다.

ACKNOWLEDGMENTS

- This work was supported by the Industrial Core Technology Development Program (1004 9009, Development of Main IPs for IoT and Image-Based Security Low-Power SoC) funded by the Ministry of Trade, Industry & Energy.
- The authors are thankful to IDEC for EDA software support.

참고문헌

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

[2] Kumar, Sandeep S. Elliptic curve cryptography for constrained devices. Diss.Ruhr University Bochum, 2006.

[3] Parrilla, L., et al. "Hardware implementation of a new ECC key distribution protocol for securing Wireless Sensor Networks." Design of Circuits and Integrated Systems (DCIS), 2015 Conference on. IEEE, 2015.

[4] Selma, Haichour Amina, and Hamadouche M'hamed. "Elliptic curve cryptographic processor design using FPGAs." Control, Engineering &Information Technology (CEIT), 2015 3rd International Conference on. IEEE, 2015.

[5] Guo, J-H., and C-L. Wang. "Hardware-efficient systolic architecture for inversion and division in GF (2 m)." IEE Proceedings-Computers and Digital Techniques 145.4 (1998): 272-278.