NIST P-224 타원곡선을 지원하는 224-비트 ECC 프로세서

박병관* · 신경욱*

*금오공과대학교

224-bit ECC Processor supporting the NIST P-224 elliptic curve

Byung-Gwan Park* · Kyung-Wook Shin*

*Kumoh National Institute of Technology

E-mail : bask369@kumoh.ac.kr

요 약

투영(projective) 좌표계를 이용한 스칼라 곱셈(scalar multiplication) 연산을 지원하는 224-비트 타원곡선 암호(Elliptic Curve Cryptography; ECC) 프로세서의 설계에 대해 기술한다. 소수체 $GF(p)$ 상의 덧셈, 뺄셈, 곱셈 등의 유한체 연산을 지원하며, 연산량과 하드웨어 자원소모가 큰 나눗셈 연산을 제거함으로써 하드웨어 복잡도를 감소시켰다. 수정된 Montgomery ladder 알고리듬을 이용하여 스칼라 곱셈 연산을 제어하였으며, 단순 전력분석에 보다 안전하다. 스칼라 곱셈 연산은 최대 2,615,201 클록 사이클이 소요된다. 설계된 ECC-P224 프로세서는 Xilinx ISim을 이용한 기능검증을 하였다. Xilinx Virtex5 FPGA 디바이스 합성결과 7,078 슬라이스로 구현되었으며, 최대 79 MHz에서 동작하였다.

키워드

ECC, Modified Montgomery ladder, Projective coordinate, ECDH

Ⅰ. 서 론

사물인터넷(Internet of Things; IoT)은 사람과 사물 또는 사물과 사물 사이의 연결을 통하여 초연결 사회를 구축하고, 사용자 중심의 지능형 서비스를 제공한다. 하지만 기기 및 시스템에 대한 보안위협은 기존의 보안위협과 달리 시스템의 불법조작이 발생하게 되면 사용자의 신체나, 생명, 재산 등에 피해가 발생할 수 있다. 이러한 시점에서 AES(Advances Encryption Standard)[1]와 같은 대칭 키 암호시스템과 서로 보완적인 역할을 하며 키 교환, 전자서명, 무결성 검증 등에 사용되는 비대칭 키 암호시스템(asymmetric key cryptography)의 필요성이 증대되고 있다.

타원곡선 암호(Elliptic Curve Cryptography; ECC)는 비트 당 안전도가 RSA[2]와 비교하여 효율적이라는 것이 알려지면서 차세대 공개키 암호로 제안되고 있다. 한국정보통신기술협회는 ECC를 기반으로 한 전자서명 알고리듬(EC-KCDSA)을 정보통신단체 표준으로 제정하였다 [3].

타원곡선이 정의되는 유한체의 길이에 따라서 ECC는 다양한 보안 안전성을 제공하며, 미국 표준기술연구소(National Institute of Standards and Technology; NIST)에서 2011년을 기준으로 224-비트 이상의 키 길이를 지원하는 타원곡선 암호를 권고하고 있다.

본 설계에서는 224-비트 키 길이를 지원하는 ECC-P224 프로세서를 설계하고, Xilinx ISim을 이용하여 정상 동작함을 확인하였다.

Ⅱ. 타원곡선 암호 알고리듬

타원곡선 암호가 근간을 두고 있는 ECDLP (Elliptic Curve Discrete Logarithmic Problem)는 타원곡선 상의 스칼라 곱셈 연산 $Q=k*P$에서 점 P와 Q를 알고 있어도 정수 k를 알아내기 어렵다는 것을 의미한다. 이때 정수 k는 사용자의 비밀키이며, 점 Q는 사용자의 공개키이다. 소수체 $GF(p)$ 상의 타원곡선은 식 (1)과 같다. 계수 a, b가 $4a^3+27b^2 \neq 0$을 만족한다면 이 방정식은 실제 타원곡선 상에 존재하지 않는 무한원점 O와 함께 덧셈에 대해 닫혀 있는 군(group)을 형성하게 된다.

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

Table 1. Point addition and point doubling for EC over prime field using affine coordinate

점 덧셈 연산 (Q=A+B)	점 두배 연산 (Q=2A)
$\lambda = \frac{y_1 - y_0}{x_1 - x_0}$	$\lambda = \frac{3x_0^2 + a}{2y_0}$
$x_2 = \lambda^2 - x_0 - x_1$	$x_2 = \lambda^2 - 2x_0$
$y_2 = \lambda(x_0 - x_2) - y_0$	$y_2 = \lambda(x_0 - x_2) - y_0$

타원곡선 상의 스칼라 곱셈 연산은 점 덧셈 연산과 점 두배 연산으로 계산된다. Affine 좌표상에서 점 연산 수식은 표 1과 같이 정리될 수 있으며, 각 점 연산은 $GF(p)$ 상의 덧셈, 뺄셈, 곱셈, 제곱, 나눗셈 연산으로 구현된다. 본 설계에서는 소요 사이클이 크고, 하드웨어 복잡도가 높은 나눗셈 연산을 제거하기 위하여 투영 좌표계의 일종인 Jacobian 좌표[4]를 적용한 ECC 프로세서를 설계하였다. Jacobian 좌표에서 임의의 점은 좌표 (X, Y, Z)로 표현된다. 설계된 ECC-P224 프로세서의 스칼라 곱셈 결과값은 타 프로세서와의 상호 호환성을 위하여 $x = X/Z^2, y = Y/Z^3$와 같은 변환을 통해 다시 affine 좌표로 출력하도록 설계하였다.

III. ECC-P224 프로세서 하드웨어 설계

설계된 ECC-P224 프로세서의 전체 구조는 그림 1과 같다. 모듈러 연산을 위한 소수 p와 정수 k 등을 저장하는 Smul_Reg 블록, 소수체 상의 곱셈, 덧셈/뺄셈 연산을 수행하는 Alu_GFp224 블록, 그리고 제어블록으로 구성된다.

Smul_Reg 블록은 소수 p, 스칼라 곱셈을 위한 정수 k, 생성점의 X 좌표, Y 좌표, Z 좌표를 저장하는 레지스터, 스칼라 곱셈의 중간 결과값을 저장하는 레지스터를 포함한 12개의 224-비트 레지스터로 구성된다.

타원곡선 암호 프로세서의 연산을 위한 제어블록은 그림 2와 같은 FSM(Finite State Machine)을

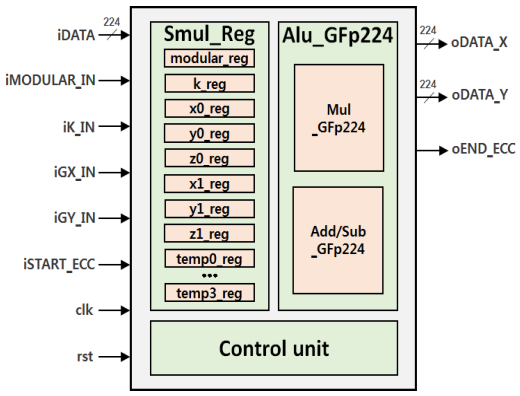


Fig. 1. Architecture of the ECC-P224 processor

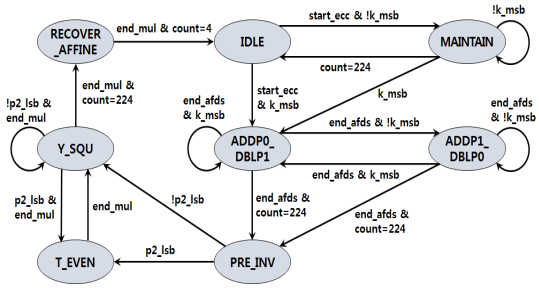


Fig. 2. FSM for ECC-P224 processor

이용하여 구현하였다. 설계된 FSM은 수정된 Montgomery ladder 알고리듬을 이용하여 스칼라 곱셈을 제어하는 부분, 연산이 완료된 Z 좌표의 역원을 구하는 부분, 투영 좌표계의 결과값을 affine 좌표로 변환하는 부분으로 구분된다. 수정된 Montgomery ladder 알고리듬을 이용한 스칼라 곱셈 연산을 통하여 정수 k의 hamming weight와 무관하게 점 연산을 수행함으로써 단순 전력분석에 보다 안전하다. 소수체 상의 역원 연산은 소수 p의 값에 따라 곱셈 연산을 반복하는 Fermat's 알고리듬을 이용하여 Z 좌표의 역원을 구하며, 이는 확장 유클리드 알고리듬이나 나눗셈 연산기를 필요로 하지 않기 때문에 하드웨어 자원소모를 절감하였다.

Alu_GFp224 블록은 그림 3과 같이 소수체 상의 곱셈기, 덧셈/뺄셈기로 이루어져 있다. 소수체 상의 곱셈기는 3개의 224-비트 레지스터를 포함하고 있으며, 하드웨어 자원소모가 큰 곱셈 연산자를 사용하지 않고, 단순 쉬프트 연산과 소수체 덧셈 연산을 이용하여 곱셈 연산이 수행되도록 설계하였다. 소수체 상의 덧셈/뺄셈기는 캐리에 의한 전파지연을 최소화하기 위하여 CSelA(Carry Select Adder)와 CSavA(Carry Save Adder)를 사용하여 구현하였다. 덧셈/뺄셈기는 Smul_Reg 블록으로부터 데이터를 입력받아 점 연산에 필요한 덧셈/뺄셈 연산을 수행한다. 또한, 곱셈기로부터 데이터를 입력받아 곱셈 연산에 필요한 소수체 상의 덧셈 연산을 수행한다. 본 설계에서는 소수체 상의 모듈러 연산에 필요한 비교기를 제거함으로써 하드웨어 자원소모를 절감하였다.

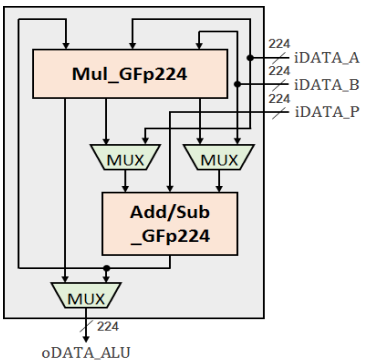
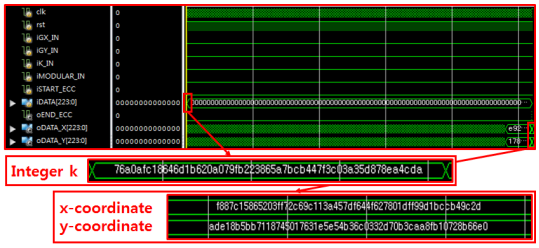


Fig. 3. Architecture of the Alu_GFp224



(a) Simulation results

k = 76A0AFC1 8646D1B6 20A079FB 223865A7 BCB447F3 C03A35D8 78EA4CDA

단계 2 $kG=(x_1, y_1)$의 계산 :

x_1 = F887C158 65203FF7 2C69C113 A457DF64 4F627801 DFF99D1B CCB49C2D

y_1 = ADE18B5B B7118745 017631E5 E54B36C0 332D70B3 CAA8FB10 728B66E0

(b) Reference data

Fig. 4. Functional simulation results of ECC processor

Ⅳ. 기능검증

설계된 ECC-P224 프로세서는 Xilinx ISim을 이용한 시뮬레이션 결과값과 한국인터넷진흥원의 참조 구현 값[5]을 비교하여 정상 동작함을 확인하였다. 그림 4는 ECC-P224 프로세서의 시뮬레이션 결과값과 참조 구현 값을 보여준다. NIST FIPS 186-2에 정의되어 있는 Curve P-224 타원곡선 파라미터를 사용하였으며, 224-비트 정수 k "76a0afc1 8646d1b6 20a079fb 223865a7 bcb447f3 c03a35d8 78ea4cda"를 생성점 $G(x, y)$에 스칼라 곱셈하였다. 그림 4-(a)에서 oEND_ECC 신호와 함께 스칼라 곱셈이 완료된 x 좌표 "f887c158 65203ff7 2c69c113 a457df64 4f627801 dff99d1b ccb49c2d", y 좌표 "ade18b5b b7118745 017631e5 e54b36c0 332d70b3 caa8fb10 728b66e0"가 출력됨을 확인할 수 있다. 이는 그림 4-(b)의 참조 구현 값과 정확히 일치함을 확인할 수 있다.

Ⅴ. 결 론

NIST FIPS 186-2 표준안에 정의되어 있는 타원곡선 P-224를 지원하는 타원곡선 암호 프로세서를 설계하였다. Xilinx Virtex5 XC5VSX95T FPGA 디바이스 합성결과 7,078 슬라이스로 구현되었으며, 최대 79 MHz의 클록 주파수에서 동작하였다. 스칼라 곱셈 연산에 최대 2,615,201 클록 사이클이 소요되며, 최대 동작 주파수에서 33.1 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] FIPS-197, Advanced Encryption Standard, National Institute of Standard and Technology(NIST), November, 2001.

[2] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining Digital Signatures and Public-Key Crypto- systems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[3] TTA Std. TTAK.KO-12.0015/R1, Digital Signature Mechanism with Appendix(Part 3) Korean Certificate-based Digital Signature Algorithm using Elliptic Curves, 2012.

[4] Izu, Tetsuya, Bodo Möller, and Tsuyoshi Takagi. "Improved elliptic curve multiplication methods resistant against side channel attacks." *International Conference on Cryptology in India*. Springer Berlin Heidelberg, 2002.

[5] KISA Std. KISA-WP-2011-0022, Development of Improved Korean Digital Signature Algorithm and Standard, 2011.