GF(2^m) 상의 NIST 타원곡선을 지원하는 ECC 프로세서

이상현 · 신경욱*

금오공과대학교

ECC Processor Supporting NIST Elliptic Curves over GF(2^m)

Sang-Hyun Lee · Kyung-Wook Shin*

Kumoh National Institute of Technology

E-mail : lpp1124@kumoh.ac.kr

요 약

NIST 표준으로 정의된 이진체 상의 5가지 pseudo-random 타원곡선과 5가지 Koblitz 타원곡선을 지원하는 타원곡선 암호 (Elliptic Curve Cryptography; ECC) 프로세서를 설계하였다. Lopez-Dahab 투영 좌표계를 적용하여 모듈러 곱셈과 XOR 연산으로 스칼라 곱셈 (scalar multiplication)이 연산되도록 하였으며, 32-비트x32-비트의 워드 기반 몽고메리 곱셈기를 이용한 고정 크기의 하드웨어로 다양한 키 길이의 ECC가 구현될 수 있도록 설계하였다. 설계된 ECC 프로세서는 FPGA 구현을 통해 하드웨어 동작을 검증하였으며, 0.18-um CMOS 셀 라이브러리로 합성한 결과 100 MHz의 동작 주파수에서 10,674 GEs와 9 킬로비트의 RAM으로 구현되었고, 최대 154 MHz의 동작 주파수를 갖는다.

ABSTRACT

This paper describes a design of an elliptic curve cryptography (ECC) processor that supports five pseudo-random curves and five Koblitz curves over binary field defined by the NIST standard. The ECC processor adopts the Lopez-Dahab projective coordinate system so that scalar multiplication is computed with modular multiplier and XORs. A word-based Montgomery multiplier of 32-b x 32-b was designed to implement ECCs of various key lengths using fixed-size hardware. The hardware operation of the ECC processor was verified by FPGA implementation. The ECC processor synthesized using a 0.18-um CMOS cell library occupies 10,674 gate equivalents (GEs) and 9 Kbits RAM at 100 MHz, and the estimated maximum clock frequency is 154 MHz.

키워드

ECC, binary field, pseduo-random curve, Koblitz curve, Lopez-Dahab, word-based Montgomery multiplication

Ⅰ. 서 론

사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술인 사물인터넷(Internet of Things; IoT)은 인터넷 기반인 기술이기 때문에 해킹과 같은 위협으로부터 정보 보안이 필수적이다. 또한 IoT의 빠른 성장에 따라 사이버 공간으로 한정된 보안 위협이 스마트홈, 의료, 교통과 같이 일상생활과 관련된 기기로 확대되어 하드웨어 자원이 제한적인 IoT 환경에 적합한 정보 보안 기술의 필요성이 강조된다. 정보 보안에 사용되는 암호 방식 중 하나로 공개키 암호 알고리듬이 있다.

* corresponding author

공개키 암호 알고리듬에서 대표적으로 RSA[1]와 ECC[2]가 사용되고 있다. ECC는 RSA와 비교하였을 때, 짧은 키 길이로 유사한 안전성을 얻을 수 있다는 장점이 있다. 따라서 ECC는 IoT 환경과 같이 하드웨어 자원이 제한적인 시스템에 적합한 공개키 암호 알고리듬으로 제안된다[3].

본 논문에서는 안정성이 높은 Pseudo-random 곡선과 연산 속도가 빠른 Koblitz 곡선을 지원하며, 각 곡선마다 이진체 상의 NIST 표준으로 정의된 5가지의 키 길이(163, 233, 283, 409, 571)를 지원하는 ECC 프로세서를 IoT 환경에 적합한 경량 하드웨어 설계하였다. 본 논문의 ECC 프로세서는 Lopez-Dahab 투영 좌표계[4]와 워드 기반 몽고메리 곱셈기[5]를 사용하여 설계되었다.

Ⅱ장에서는 ECC 프로세서의 하드웨어 설계에 대해 간략하게 설명한다. Ⅲ장에서는 ModelSim을 이용한 기능 검증과 FPGA 구현 결과에 대해 기술하고, Ⅳ장에서 결론을 맺는다.

Ⅱ. ECC 프로세서 설계

ECC 프로세서는 이진체 상의 NIST 표준으로 정의된 10가지의 타원곡선을 지원한다. 그림 1은 ECC 프로세서의 내부 구조이며, 스칼라 곱셈 연산에 필요한 데이터를 저장하는 SM_REG 블록, 스칼라 곱셈 연산의 하위 연산을 수행하는 SM_OP_GFB 블록 그리고 제어블록으로 구성된다.

SM_REG 블록에서는 타원곡선 계수 b, 개인키 k, 타원곡선 생성점의 좌표 값과 스칼라 곱셈 연산의 중간 결과 값 등을 저장하는 듀얼 포트 메모리 SM_RAM과 연산에 필요한 데이터를 입력하기 위한 레지스터들로 구성된다. SM_OP_GFB 블록은 32-비트 곱셈 및 XOR 연산을 위한 WMM_32-b, XOR_32-b로 구성된다. WMM_32-b는 워드기반 몽고메리 곱셈기 알고리즘을 사용하여 키 길이에 따라 연산 횟수가 달라짐에 따라 고정된 하드웨어 자원을 갖도록 설계하였다. XOR_32-b는 32-비트 단위로 XOR 연산이 수행된다.

SM_CTRL 블록에서는 스칼라 곱셈 연산을 하기 위한 제어기능을 수행한다. ECC 프로세서는 데이터 입력, 매핑, 스칼라 곱셈, 좌표 변환, 리매핑 그리고 데이터 출력 순으로 진행된다. 매핑은 워드기반 몽고메리 곱셈의 특성으로 인해 입력 데이터에 R이 곱해진 형태로 변환하는 과정이다. $R=2^{r\cdot n}$이며, r은 워드 기반 몽고메리 곱셈기의 연산 크기이고, n은 키 길이를 r로 나눈 값이다. 스칼라 곱셈에서는 몽고메리 래더 알고리즘을 적용하여 부채널 공격에 강인하도록 설계되었으며, 개인키 k의 MSB에 따라 XOR와 곱셈만으로 이루어진 Lopez-Dahab 좌표계에서 점 연산을 수행하고, 연산이 끝날 때마다 k 값을 왼쪽으로 시프트하며 반복한다. 좌표 변환에서는 Lopez-Dahab 좌표계 (x,y,z)로 출력된 값을 Affine 좌표계$(x/z,y/z^2)$로 변환한다. 설계된 WMM_32-b를 사용하여 페르마의 소정리를 통해 역원 z^{-1}을 구현하였다. 리매핑에서는 매핑의 반대 개념으로 몽고메리 도메인에서 일반 도메인으로 변환하는 과정이다.

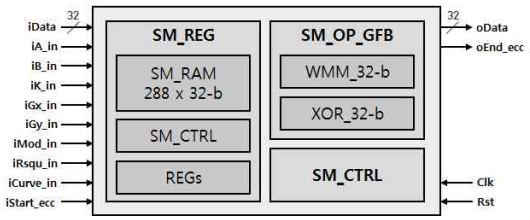


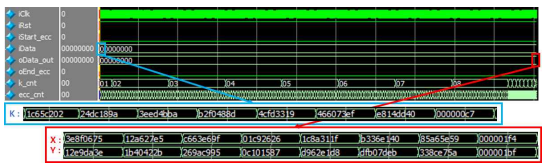
Fig. 1. Architecture of ECC processor

Ⅲ. 기능 검증

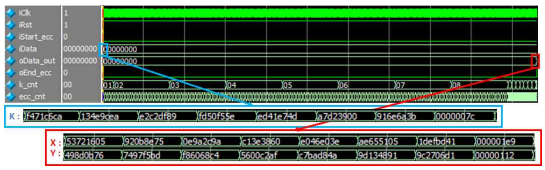
설계된 ECC 프로세서는 ModelSim을 이용한 기능검증과 FPGA 구현을 통한 하드웨어 동작을 확인하였다. NIST FIPS 186-2에 정의되어 있는 파라미터 타원곡선 계수, 생성점 등을 사용하였다.

그림 2-(a)는 키 길이 233-비트 Pseudo-random 곡선에서 시뮬레이션 결과 값이며 개인키 k "C7 E814DD40 466073EF 4CFD3319 B2F0488D 3EED4BBA 24DC189A 1C65C202"를 최하위 워드부터 입력하여 스칼라 곱셈한 결과 x좌표 "1f4 85a65e59 b336e140 1c8a311f 01c92626 c663e69f 12a627e5 3e8f0675", y좌표 "1bf338ce75a dfb07deb d962e1d8 0c101587 269ac995 1b40422b 12e9da3e"가 최하위 워드부터 출력된다. 그림 2-(b)는 키 길이 233-비트 Koblitz 곡선에서의 시뮬레이션 결과 값이며 개인키 k "7C 916E6A3B A7D23900 ED41E74D FD50F55E E2C2DF89 134E9CEA F471C6CA"를 최하위 워드부터 입력하여 스칼라 곱셈한 결과 x좌표 "1E9 1DEFBD41 AE655105 E046E03E C13E3860 0E9A2C9A 920B8E75 53721605", y좌표 "112 9C2706D1 9D134891 C7BAD84A 5600C2AF F86068C4 7497F5BD 498D0B76"가 최하위 워드부터 출력된다. 그림 2의 시뮬레이션 결과 값과 문헌 [6]의 참조 구현 값과 정확히 일치함으로써 정상 동작함을 확인하였다.

그림 3은 ECDH (Elliptic Curve Diffie-Hellman) 키교환 프로토콜을 사용한 FPGA 검증 결과이다. 타원곡선의 종류와 키 길이를 선택할 수 있도록 하였으며, 검증하고자 하는 타원곡선을 선택하면 NIST에서 정의된 타원곡선 파라미터 값이 표시된다. Alice와 Bob의 생성된 개인키와 생성점을 스칼라 곱셈하여 공개키를 생성하며 소프트웨어로 계산한 값과 비교하여 공개키가 올바르게 생성되었는지를 판단하였다. 이 후 생성된 공개키를 통해 개인키와 스칼라 곱셈하여 공유 비밀키를 생성하며 Alice와 Bob의 공유 비밀키를 비교하여 올바르게 생성되었는지를 판단하였다.

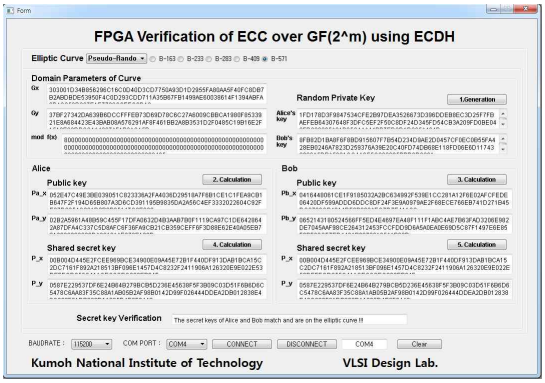


(a) Pseduo-random curve

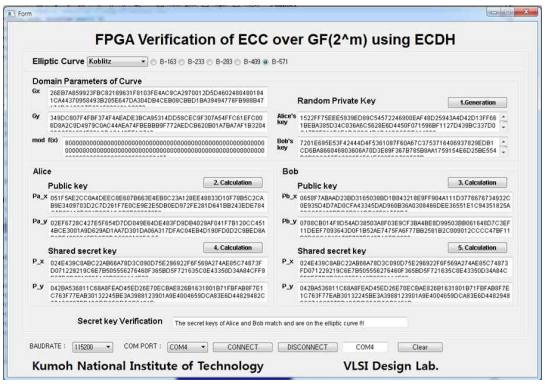


(b) Koblitz curve

Fig. 2. Simulation results of ECC processor over GF(2^{233})



(a) Pseduo-random curve



(b) Koblitz curve

Fig. 3. FPGA verification results of ECC processor over GF(2^{571}) using ECDH

그림 3-(a)는 키 길이 571-비트 Pseudo-random 곡선에서 FPGA 검증 결과이며, 그림 3-(b)는 키 길이 571-비트 Koblitz 곡선에서 FPGA 검증 결과이다. Alice와 Bob의 공유 비밀키가 동일하게 생성되는 것을 통해 정상 동작함을 확인하였다.

III. 결 론

NIST 표준에 정의된 이진체 상의 10가지의 키 길이를 지원하는 ECC 프로세서를 Lopez-Dahab 좌표계와 워드 기반 몽고메리 곱셈기를 통해 경량 하드웨어로 설계하였으며, ModelSim을 이용한 기능검증과 FPGA 구현을 통한 하드웨어 동작을 검증하였다. 설계된 ECC 프로세서는 0.18um 공정의 CMOS 셀 라이브러리로 합성한 결과 100MHz의 동작 주파수에서 10,674 GEs와 9-Kbit RAM으로 구현되었으며, 최대 154MHz의 동작 주파수를 갖는다. 본 논문에서 설계된 ECC 프로세서는 IoT와 같이 하드웨어가 제한적인 보안 시스템에 활용이 가능하다.

Acknowledgement

■ This research was supported by Kumoh National Institute of Technology(2018-104-072)

References

[1] R. Rivest, A. Shamir and L. Adleman, “A method for obtaining Digital Signatures and Public-Key Cryptosystems,” *Communications of Association for Computing Machinery (ACM)*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

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

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

[4] J. Lopez and R. Dahab, “Improved Algorithms for Elliptic Curve Arithmetic in GF (2^n),” In *International Workshop on Selected Areas in Cryptography Springer*, Berlin, Heidelberg, pp. 201-212, 1998.

[5] P. L. Montgomery, “Modular Multiplication Without Trial Division,”*Mathematics of Computation*, vol. 44, no. 170, pp. 519-521, Apr. 1985.

[6] TTA Std. TTAK.KO-12.0015/R3, Digital Signature Mechanism with Appendix(Part 3) Korean Certificate-based Digital Signature Algorithm using Elliptic Curves, 2016.