$GF(p)$와 $GF(2^m)$ 상의 다중 타원곡선을 지원하는 면적 효율적인 ECC 프로세서 설계

이상현 · 신경욱*

금오공과대학교

An Area-efficient Design of ECC Processor Supporting Multiple Elliptic Curves over $GF(p)$ and $GF(2^m)$

Sang-Hyun Lee · Kyung-Wook Shin*

Kumoh National Institute of Technology

E-mail : lpp1124@kumoh.ac.kr

요 약

소수체 $GF(p)$와 이진체 $GF(2^m)$ 상의 다중 타원곡선을 지원하는 듀얼 필드 ECC (DF-ECC) 프로세서를 설계하였다. DF-ECC 프로세서의 저면적 설와 다양한 타원곡선의 지원이 가능하도록 워드 기반 몽고메리 곱셈 알고리듬을 적용한 유한체 곱셈기를 저면적으로 설계하였으며, 페르마의 소정리 (Fermat's little theorem)를 유한체 곱셈기에 적용하여 유한체 나눗셈을 구현하였다. 설계된 DF-ECC 프로세서는 스칼라 곱셈과 점 연산, 그리고 모듈러 연산 기능을 가져 다양한 공개키 암호 프로토콜에 응용이 가능하며, 유한체 및 모듈러 연산에 적용되는 파라미터를 내부 연산으로 생성하여 다양한 표준의 타원곡선을 지원하도록 하였다. 설계된 DF-ECC는 FPGA 구현을 하드웨어 동작을 검증하였으며, 0.18-um CMOS 셀 라이브러리로 합성한 결과 22,262 GEs (gate equivalences)와 11 kbit RAM으로 구현되었으며, 최대 100 MHz의 동작 주파수를 갖는다. 설계된 DF-ECC 프로세서의 연산성능은 B-163 Koblitz 타원곡선의 경우 스칼라 곱셈 연산에 885,044 클록 사이클이 소요되며, B-571 슈도랜덤 타원곡선의 스칼라 곱셈에는 25,040,625 사이클이 소요된다.

키워드

ECC, dual-field ECC, public-key cryptography, information security, word-based Montgomery multiplication

Ⅰ. 서 론

정보통신기술의 발전에 따라 정보보안 응용분야가 급속히 확대되면서, 키 관리 및 인증에 유용한 공개키 암호의 중요성이 대두되고 있다. 기술의 발전으로 인해 더 높은 암호 강도가 요구됨에 따라 키 길이가 증가되며, 키 길이의 증가는 메모리와 하드웨어의 증가를 의미한다. 사물인터넷 (IoT)과 같이 제한적인 하드웨어 자원을 갖는 응용분야의 경우 공개키 암호에서 RSA [1]에 비해 짧은 키 길이로 유사한 안전성을 얻는 타원곡선 암호 (ECC) [2]가 적합한 것으로 평가되고 있다.

타원곡선 암호는 Koblitz와 Miler에 의해 1985년에 제안되었으며, 실수에서의 정의된 타원곡선상의 연산은 느리고 반올림에 따른 오차로 연산이 부정확하기 때문에 유한체를 사용한다. 타원곡선 암호에서 사용하는 유한체는 소수체 (prime field)와 이진체 (binary field)로 구분되며, 유한체의 종류와 길이에 따라 타원곡선 파라미터인 타원곡선 계수와 생성점, 생성점의 위수 (order) 등이 SEC2 [3]에 정의되어 있다.

본 논문에서는 소수체와 이진체 상의 다중 타원곡선을 지원하는 DF-ECC 프로세서를 저면적으로 설계하고, FPGA 구현을 통해 하드웨어 동작을 확인하였다.

Ⅱ. DF-ECC 프로세서 설계

본 논문에서 설계한 DF-ECC 프로세서의 구조는 그림 1과 같으며, Data_MEM 블록, DF_ALU 블록, REGs 블록 그리고 Control_FSM으로 구성된다.

* corresponding author

Data_MEM 블록은 스칼라 곱셈연산을 위한 데이터를 저장하는 싱글포트 RAM이고, DF_ALU 블록은 유한체 연산을 수행하는 듀얼필드 연산회로이며, REGs 블록은 유한체 연산을 위한 데이터를 저장하는 레지스터 블록이다. Control_FSM은 전체적인 동작을 제어하는 제어블록이다.

DF_ALU 내부의 ASX_32-b 블록은 유한체 덧셈/뺄셈기, XOR 연산과 유한체 곱셈 결과 값에 대한 모듈러 연산을 수행하며, 덧셈기와 캐리 레지스터, 멀티플렉서로 구성된다. 캐리에 의한 지연을 줄이기 위해 캐리선택 가산기 (carry-select adder)를 사용하였으며, 유한체 덧셈/뺄셈 결과 값과 XOR 값을 선택하여 출력하도록 멀티플렉서를 추가하여 덧셈기를 설계하였으며, 캐리 레지스터를 통해 연산 결과 값이 모듈러 값보다 크거나 0보다 작을 경우 모듈러 연산을 수행하여 소수체와 이진체 상의 연산이 가능하도록 설계하였다.

유한체 곱셈기(WMM_32-b)는 모듈러 합동을 이용한 워드 기반 몽고메리 곱셈 알고리듬을 적용하여 설계되었으며, 그림 2와 같이 덧셈기 2개와 곱셈기 1개로 구성된다. 유한체 나눗셈은 페르마의 소정리 수식인 $a^{N-2} \equiv a^{-1} \pmod{N}$를 이용하여 회로 추가 없이 유한체 곱셈기에 의해 연산되도록 하였다.

워드 기반 몽고메리 곱셈 알고리듬을 구현하기 위해서는 피연산자를 몽고메리 도메인으로 변환하기 위한 R^2 값과 모듈러 합동 연산을 위한 $n_0^* = -n_0^{-1} \pmod{2^{32}}$ 값이 필요하다. n_0^*는 모듈로 최하위 워드 n_0의 역원을 마이너스 한 값이며, 본 논문에서는 오일러의 정리를 적용하여 유한체 곱셈기 내부의 곱셈기를 이용하여 역원을 구한 뒤, 유한체 덧셈/뺄셈기를 통해 마이너스 값을 구하여 생성되도록 설계하였다. 몽고메리 도메인 변환 데이터 $R^2 = (2^{w*m})^2$는 1을 $2 \times w \times m$번 왼쪽 시프트하고 유한체 덧셈/뺄셈기를 통해 모듈러 연산으로 생성되며, w은 워드의 비트수이고, m은 워드 개수를 나타낸다.

Ⅲ. 기능 검증

설계된 DF-ECC 프로세서는 ModelSim을 통해

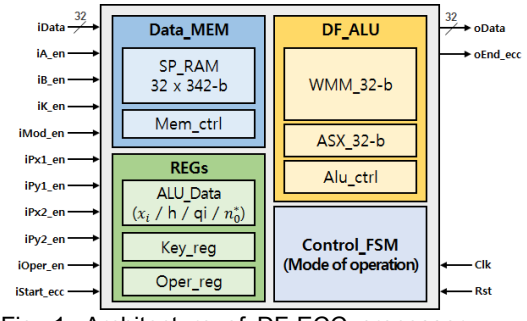


Fig. 1. Architecture of DF-ECC processor

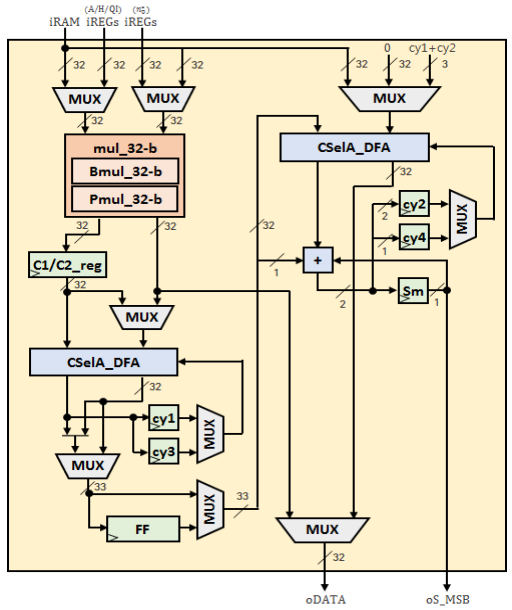


Fig. 2. WMM_32-b block

RTL 기능검증을 하였으며, FPGA 구현을 통해 하드웨어 동작을 검증하였다. SEC2에서 타원곡선의 종류에 따라 권장하는 파라미터 값인 타원곡선의 계수, 타원곡선의 생성점 등을 사용하였다.

그림 3은 B-283 Koblitz 타원곡선에 대한 시뮬레이션 결과이며 개인키 k “135899F D45B49A1 F88 5C464 FA10DFE7 B86BB9F0 C5F41FE3 9D2BEEA 7 1419B491 C3D2AEE7”를 최하위 워드부터 입력하여 스칼라 곱셈한 결과로 x좌표 “78A6ACD D5 F779F2 5E8AB413 965E217F E6B1E63D 4717EEF5 0DC8C59D F7B1A095 BC3027AE”와 y좌표 “7B6D 962 5F2D9DDF 516B5037 E1E7B115 26E12AC4 E 65AD498 CD85D65A 9E915D58 6976C00F”가 최하위 워드부터 출력되며, 스칼라 곱셈 연산에 1,999,481 클록 사이클이 소요된다.

그림 3의 시뮬레이션 결과 값과 문헌 [4]의 참조 구현 값이 정확히 일치하여 올바로 동작함을 확인하였다.

DF-ECC를 FPGA에 구현하고, EC-ElGamal 프로

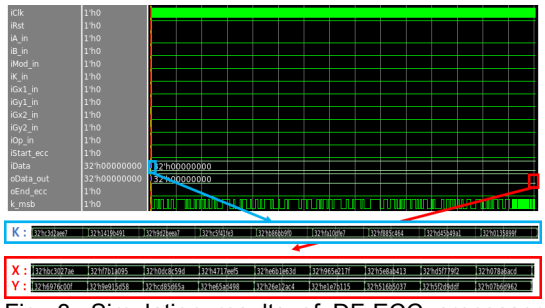
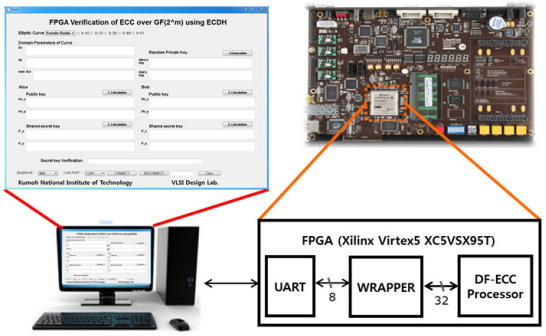
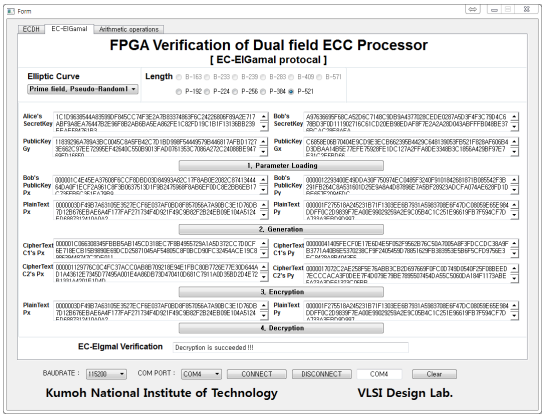


Fig. 3. Simulation results of DF-ECC processor over B-283 Koblitz curve

토콜을 통해 하드웨어 동작을 검증하였다. FPGA 검증 플랫폼은 그림 4-(a)와 같으며, FPGA 보드, uart 인터페이스, Python 기반 구동 및 GUI 소프트웨어로 구성되고, FPGA 소자는 Xilinx Virtex5 XC5VSX-95T 디바이스가 사용되었다. 그림 4-(b)는 P-521 슈도랜덤 타원곡선에 대한 EC-ElGamal 암/복호 프로토콜의 동작결과이다. EC-ElGamal 프로토콜은 스칼라 곱셈, 점 덧셈, 점 뺄셈을 사용하여 데이터를 암/복호하며, 다음의 과정으로 검증이 진행된다. 1.Paramter loading 버튼을 눌러 소프트웨어를 통해 생성점과 개인키를 생성하고, 2.Generation 버튼을 눌러 DF-ECC 프로세서에서 생성점과 Bob의 개인키를 스칼라 곱셈을 하여 Bob의 공개키를 생성하며, 소프트웨어로 평문을 생성한다. 3.Encryption 버튼을 누르면 암호화 과정이 진행된다. DF-ECC 프로세서에서 생성점과 Alice의 개인키를 스칼라 곱셈하여 암호문 C1을 생성하고, Bob의 공개키와 Alice의 개인키를 스칼라 곱셈한 뒤, 평문과 점 덧셈하여 암호문 C2를 생성한다. 4.Decryption 버튼을 누르면 복호화 과정이 진행된다. DF-ECC 프로세서에서 암호문 C2에서 암호문 C1과 Bob의 개인키를 스칼라 곱셈한 결과 값을 점 뺄셈하여 복호된 평문이 생성된다. 소프트웨어로 계산된 결과 값과 비교하여 DF-ECC 프로세서의 정상 동작을 확인하였다.



(a) FPGA verification setup



(b) EC-ElGamal (P-521 Pseudo-random curve)

Fig. 4. FPGA verification results of DF-ECC processor

Ⅳ. 결 론

타원곡선 암호 프로세서를 위한 다양한 설계기법을 적용하여 듀얼 필드 ECC 프로세서를 저면적으로 설계하였다. 유한체 곱셈에 사용되는 파라미터가 내부의 연산기를 통해 생성되도록 하여 다양한 타원곡선을 지원할 수 있도록 설계되었으며, 스칼라 곱셈, 점 연산 및 모듈러 연산 등 9가지 동작 모드를 지원하여 다양한 공개키 암호 프로토콜 구현에 응용할 수 있다. 설계된 DF-ECC 프로세서의 연산성능은 B-163 Koblitz 타원곡선의 경우 스칼라 곱셈 연산에 885,044 클록 사이클이 소요되며, B-571 슈도랜덤 타원곡선의 스칼라 곱셈에는 25,040,625 사이클이 소요된다. 설계된 DF-ECC 프로세서를 FPGA에 구현하여 하드웨어 동작을 검증하였으며, 0.18-um CMOS 셀 라이브러리로 합성한 결과, 100 MHz 동작 주파수에서 22,262 GEs와 11 kbit의 싱글포트 RAM으로 구현되었다.

Acknowledgement

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).

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] Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, September 2000.

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