ECC 코어가 내장된 보안 SoC를 이용한 EC-DSA 구현

양현준* · 신경욱

금오공과대학교

EC-DSA Implementation using Security SoC with built-in ECC Core

Hyeon-Jun Yang* · Kyung-Wook Shin

Kumoh National Institute of Technology

E-mail : 20206038@kumoh.ac.kr / kwshin@kumoh.ac.kr

요 약

보안 SoC (system-on-chip)를 이용한 타원곡선 디지털 서명 알고리듬 (elliptic curve digital signature algorithm; EC-DSA)의 H/W-S/W 통합 구현에 대해 기술한다. 보안 SoC는 Cortex-A53 APU를 CPU로 사용하며, 하드웨어 IP로 설계된 고성능 타원곡선 암호 (high-performance ellipitc curve cryptography; HP-ECC) 코어와 SHA3 (secure hash algorithm 3) 해시 함수 코어가 AXI4-Lite 버스 프로토콜로 연결된다. 고성능 ECC 코어는 12가지의 타원곡선을 지원하며, SHA3 코어는 4가지의 해시 함수를 지원한다. 보안 SoC를 Zynq UltraScale+ MPSoC 디바이스에 구현하여 EC-DSA에 의해 생성된 서명의 유효성을 검증하였다.

ABSTRACT

This paper describes an integrated H/W-S/W implementation of elliptic curve digital signature algorithm (EC-DSA) using a security system-on-chip (SoC). The security SoC uses the Cortex-A53 APU as CPU, and the hardware IPs of high-performance elliptic curve cryptography (HP-ECC) core and SHA3 (secure hash algorithm 3) hash function core are interfaced via AXI4-Lite bus protocol. The signature generation and verification processes of EC-DSA were verified by the implementation of the security SoC on a Zynq UltraScale+ MPSoC device.

키워드

EC-DSA, Security SoC, ECC, SHA3, MPSoC

Ⅰ. 서 론

디지털 서명 알고리듬 (digital signature algorithm; DSA)은 미국 표준기술연구소 (National Institute of Standards and Technology; NIST)에 의해 1991년 제안된 알고리듬이다. DSA는 정보가 서명된 후 수정 여부를 검증하는 곳에 사용될 수 있다. 즉, 서명된 정보의 무결성을 검증할 수 있다. 디지털 서명의 종류에는 RSA 기반의 디지털 서명 알고리듬, 타원곡선 기반의 디지털 서명 알고리듬 (Elliptic Curve-DSA; EC-DSA), 에드워즈 곡선 기반 디지털 서명 알고리듬 (Edwards Curve-DSA) 등이 있다 [1]. 본 논문에서는 고성능 ECC 코어와 SHA3 해시 함수 코어를 내장한 보안 SoC를 Zynq UltraScale+ MPSoC에 구현하고, EC-DSA 프로토콜의 서명생성과 서명검증 과정을 구현하였다. II장은 보안 SoC의 구조와 EC-DSA를 소개한다. III장에서는 보안 SoC를 통해 구현된 EC-DSA 서명 생성과 검증의 결과를 보이고, IV장에서 결론을 맺는다.

Ⅱ. 보안 SoC 및 EC-DSA

설계된 보안 SoC는 그림 1과 같이 Zynq UltraScale+ MPSoC 디바이스 PS 영역의 Cortex-A53 APU, 그리고 PL 영역에 구현된 12가

* speaker

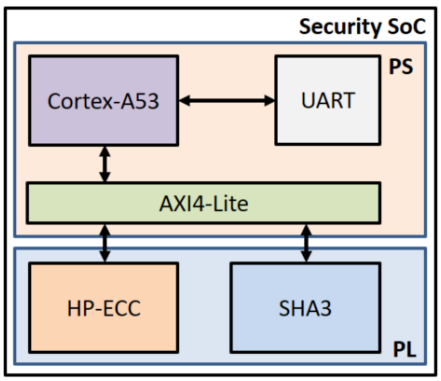

그림 1. 보안 SoC 구조

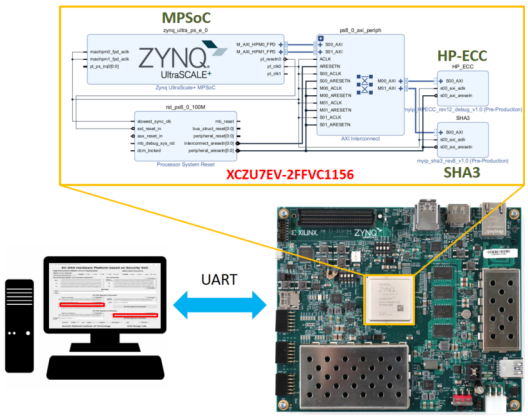

그림 2. 보안 SoC 기반 EC-DSA 하드웨어 플랫폼

지의 타원곡선을 지원하는 고성능 타원곡선 암호(high-performance ECC; HP-ECC) 코어 [2]와 4가지의 해시함수를 지원하는 SHA3 코어 [3]로 구성된다. 즉, 1개의 마스터와 2개의 슬레이브 IP (intellectual property)로 구성된다. 버스 프로토콜은 AXI4-Lite 프로토콜을 사용하였다. 개인키와 랜덤 정수 생성에 필요한 난수 발생기는 소프트웨어로 대체하였다.

EC-DSA는 타원곡선 암호 기반의 디지털 서명 알고리듬으로 서명생성과 서명검증 두 가지 알고리듬으로 구성된다. 서명 생성 과정에는 메시지, 해시 함수, 개인키와 타원곡선 도메인 파라미터가 사용된다. 먼저, 메시지를 해시함수의 입력으로 주어 다이제스트 e를 생성한다. 그 다음 랜덤 정수 k를 키 값으로 사용하여 타원 곡선 상의 점 스칼라 곱셈을 통해 서명 r을 생성한다. 마지막으로 e, r, k 그리고 개인키 d_a의 모듈러 연산으로 서명 s를 생성하며, 최종적으로는 서명 쌍 (r,s)가 출력된다. 수신자는 서명검증 과정을 통해 서명의 유효성을 검증한다. 서명검증에는 서명 쌍 (r,s)과 메시지 그리고 공개키와 타원곡선 도메인 파라미터가 사용된다. 공개키는 개인키를 점 스칼라 곱셈하여 생성된다. 수신된 메시지로 생성된 다이제스트와 서명 쌍 (r,s) 그리고 공개키를 모듈러 연산 및 점 연산을 통해 v를 생성한 뒤, 생성된 v값과 수신된 서명 r이 수식 $r=v(\mathrm{mod}n)$의 관계를 만족할 경우 수신된 서명은 유효하다. 여기서 n은 타원곡선 도메인 파라미터에 정의된 점의 위수 값이다.

III. EC-DSA 구현 결과

보안 SoC 기반의 EC-DSA 하드웨어 플랫폼은그림 2와 같으며, Zynq UltraScale+ MPSoC 디바이스를 기반으로 구성된다. 그림 2의 플랫폼을 이용하여 EC-DSA 서명생성 및 서명검증 프로토콜의 H/W-S/W 통합 검증을 하였다. 메시지는 'abcdefgh_abcdefgh_abcdefgh_abcdefgh_abcdefgh_abcdefgh_abcdefgh_abcdefgh_abcdefg'을 사용하였으며, 도메인 파라미터는 SP 800-186 [4] 문서의 데이터를 사용하였다. 서명생성 과정에 사용된 개인키와 랜덤 정수는 소프트웨어를 통해 생성하였다. EC-DSA 서명생성 및 서명검증 결과는 그림 3과 같으며, 서명생성 과정의 서명 r과 서명 검증 과정의 v가 일치하여 설계된 보안 SoC가 정상 동작함을 확인하였다.

IV. 결 론

Cortex-A53 APU와 HP-ECC 코어, SHA3 코어가 AXI4-Lite 버스 프로토콜로 연결된 보안 SoC 프로토타입을 구현하고, EC-DSA 서명생성과 서명검증 프로토콜이 정상 동작함을 확인하였다. 본 논문의 SoC 플랫폼에 난수생성 IP, 블록암호 IP등을 추가하여 ECC 기반의 다양한 공개키 암호 프로토콜의 구현이 가능하다.

Acknowledgement

- This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No. 2020R1I1A3A04038083)
- The authors are thankful to IDEC for EDA tool support.

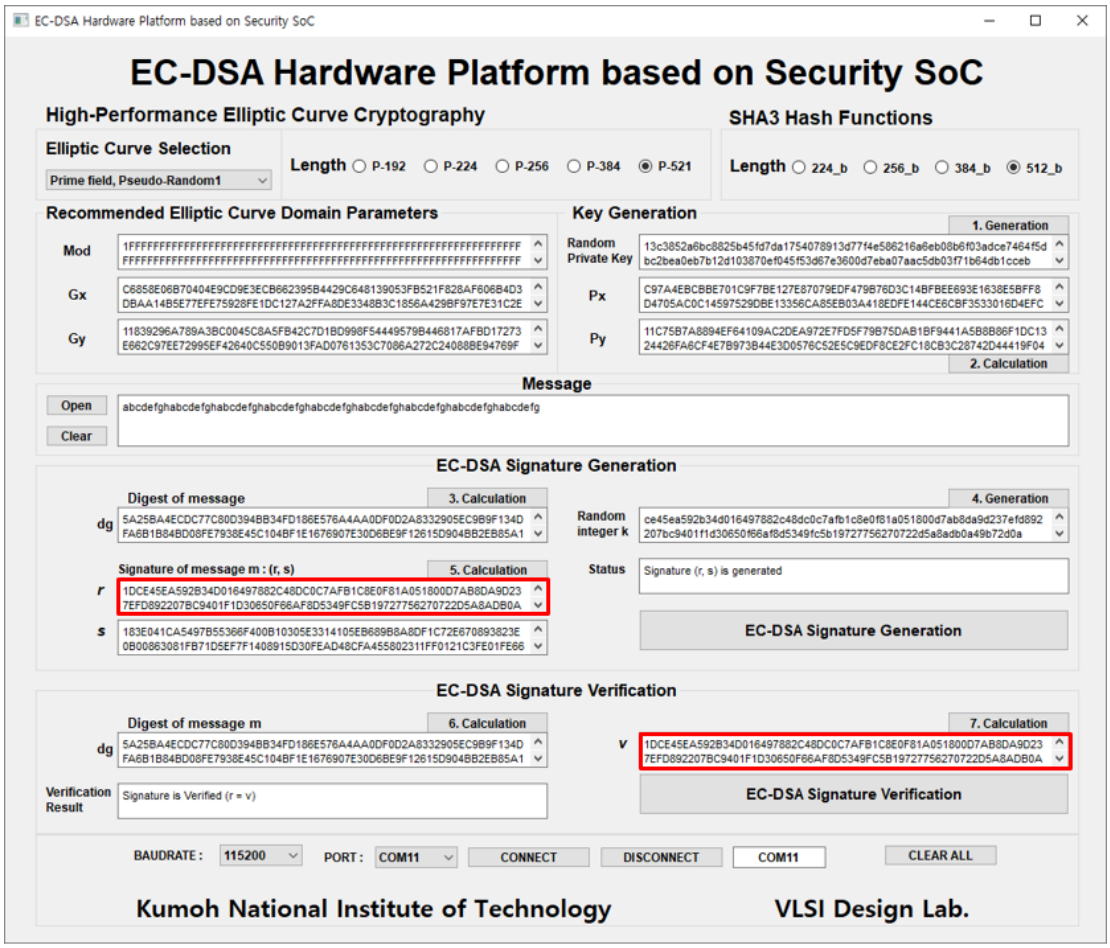

그림 3. 보안 SoC 기반 EC-DSA 검증 결과

References

[1] National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication (FIPS) 186-5 (Draft), Oct. 2019. https://doi.org/10.6028/NIST.FIPS.186-5-draft

[2] Jun-Yeong Choe, "A High Performance Elliptic Curve Cryptography Processor Supporting Multiple Field Sizes over GF(p)," Master Thesis, Kumoh national Institute of Technology, Dec. 2020.

[3] Dong-Seong Kim, Kyung-Wook-Shin, "An Optimized Hardware Implementation of SHA-3 Hash Functions," Journal of Institute of Korean Electrical and Electronics Engineers, vol. 22, no. 4, pp. 886-895, Dec. 2018.

[4] Lily Chen (NIST), Dustin Moody (NIST), Andrew Regenscheid (NIST), Karen Randall (Randall Consulting), "Recommendations for Discrete Logarithm-Based Cryptography: Elliptic Curve Domain Parameters," SP 800-186 (draft), October 2019.