ECDSA 하드웨어 암호모듈의 구현방법과 암호모듈의 SCA 분석 방법 연구

김용성*, 김영효, 방민지
한국전자기술연구원

yskim@keti.re.kr*, jun1014@keti.re.kr, alswl1216@keti.re.kr

Implementation method of ECDSA hardware cryptographic module and Research on SCA method of cryptographic module

Kim Yong Seong*, Kim Yeong Hyo, Bang Min Ji
Korea Electronics Technology Institute.

요 약

NIST 는 CMVP(ptographic Module Validation Program)를 통해 암호화 장비 검증을 하고 있다. 한국에서도 KCMVP(Korea CMVP)를 통해 검증필을 받은 암호 장비만 국가와 공공기관에서 사용 가능하다. ECDSA 의 경우 NIST 표준 암호 알고리즘임과 동시에 KCMVP 검증 대상 암호화 알고리즘으로 국내외에서 사용 가능하다. 1996 년 P.Kocher 에 의해 암호 알고리즘의 안전성 뿐 아니라 암호모듈의 소비 전력량, 방출하는 전자파 등을 통해 암호를 해독하는 방법이 제안되었다. 본 논문은 KCMVP 암호 알고리즘 탑재 암호 모듈의 동작 속도 및 clock 수를 통한 SPA 가능성을 분석하였다.

Ⅰ. 서 론

국내에서 국가와 공공기관 등에서 암호화 장비를 사용하기 위해서는 KCMVP 검증필을 받아야한다. 또한 NIST 에서도 CMVP 검증 프로그램을 통해 암호 모듈의 검증을 진행하고 있다. ECDSA 의 경우 국내 KCMVP. 검증대상 암호 알고리즘임과 동시에 NIST 표준 암호알고리즘으로 국내외에서 사용 가능하다.

KCMVP 검증필 암호모듈 목록 암호 알고리즘 종류에 관계없이 하드웨어 구현물은 총 12 종이면 이중 효력 2 종은 효력이 만료된 상태로 현재 10 종이 존재하여 소프트웨어 69 종에 비하면 많이 부족한 상황이다[3].

1996 년 P.Kocher 가 암호 알고리즘의 안전성이 아닌 암호 모듈 등 암호 구현물의 구현 과정 및 동작 정보를 이용하여 암호 모듈을 해독하는 방법을 제안하였다[2].

본논문에서는 타원곡선기반 전자서명 알고리즘의 ECDSA 구현 결과물의 동작과정을 제시한다. 또한 이 암호모듈의 동작시간과 clock cycle 을 측정을 통하여 ECDSA 의 키 정보의 추측가능성을 확인하여 암호모듈의 부채널 분석 가능성을 확인한다.

Ⅱ. ECDSA

ECDSA 의 경우 타원곡선 군 상의 이산대수문제 기반 전자 서명 알고리즘이다[1]. 타원곡선 군 정의 시 정수체 또는 이진체를 이용하여 구현 가능하다. 본논문에서는 정수체 기반의 타원곡선 연산을 이용하여 ECDSA 를 구현하였으며, 사용 해시함수는 SHA-2 series 중 SHA-224/256 이다. [표 1]은 하드웨어 암호모듈 구현에 사용된 타원곡선 파라미터와 해시함수 종류이다.

ECDSA 키 길이	224-bit	256-bit
타원곡선 파라미터	Secp224r1	Secp256r1
해시함수	SHA-224	SHA-256

[표 1] 타원곡선 파라미터 및 해시함수

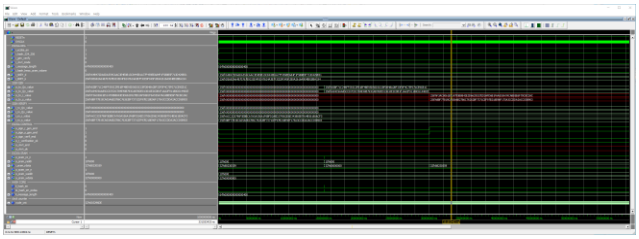
타원곡선 상의 점 스칼라 배 연산의 경우 Left-to-Right 알고리즘을 이용하여 고속 구현이 가능하다. 하지만 이 알고리즘의 경우 스칼라 값의 헤밍웨이트 등에 따라 동작 속도가 달라질 수 있다. 이는 부채널 분석을 통하여 스칼라 값의 헤밍웨이트 등의 정보가 노출될 가능성이 있다.

Ⅲ. Modelsim 시뮬레이션

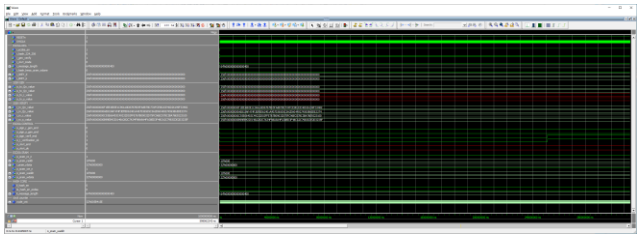
하드웨어 구현 결과물의 구현 정확성 검증 및 clock 수 측정을 위해 Modlesim Simulator 을 사용하였다.

시뮬레이션 환경: ModelSim SE-64 10.5

[그림 1, 2]는 정수체 기반 ECDSA 의 키 길이 별 서명 생성과정의 Modelsim 시뮬레이션 결과이다.



[그림 1] ECDSA-224 서명생성 시뮬레이션



[그림 2] ECDSA-256 서명생성 시뮬레이션

Ⅳ. Clock cycle 및 동작시간 측정 결과

본 장은 ECDSA-224/256 의 서명 생성 및 검증에 대한 NIST 제공 Test Vestor 별 clock cycle 수와 펌웨어를 이용하여 측정한 알고리즘 동작 시간을 제시한다. [표 2]는 알고리즘 동작 시간 측정 환경이다.

외부 클록 수	10MHz
Emulator	CortexM3 emulator ARM KEIL ULINK2
prescale	256

[표 2] 펌웨어 시간 측정 환경

[표 3, 4]는 ECDSA 키길이별 서명 생성 과정의 클록수와 동작 시간 측정결과이다. 해시함수의 동작 속도를 동일하게 하기 위해 모든 메시지 길이는 1024-bit 로 통일하였다.

case	1	2	3
Cycle 수(회)	2,554,092	2,481,274	2,543,138
동작 시간	255.158	247.888	254.058
case	4	5	6
Cycle 수(회)	2,547,535	2,428,741	2,509,135
동작 시간	254.493	242.640	250.678
case	7	8	9
Cycle 수(회)	2,584,890	2,576,026	2,588,905
동작 시간	258.230	257.360	258.640
case	10	11	12
Cycle 수(회)	2,599,429	2,537,557	2,578,999
동작 시간	259.715	253.520	257.642
case	13	14	15
Cycle 수(회)	2,527,909	2,528,812	2,580,869
동작 시간	252.573	252.650	257.846

[표 3] ECDSA-224 클록 수 및 동작 시간

동일한 길이의 키, 서명난수를 이용하여 서명을 생성한 경우에도 clock 수와 서명 생성 시간은 입력 값에 따라 달랐으며 가장 차이가 ECDSA-224 의 경우 약 5%, ECDSA-256 의 경우 약 4%의 클록 수, 시간 차이를 확인할 수 있다.

Ⅴ. SCA 분석 가능성

ECDSA 의 경우 서명키와 서명 난수를 비밀 값으로 관리하여야 안전성을 보장받을 수 있다. 하지만 4 장의 결과에 Left-to-Right 알고리즘을 이용하여 타원곡선 점

case	1	2	3
Cycle 수(회)	3,005,848	2,929,683	2,998,510
동작 시간	300.343	292.714	299.601
case	4	5	6
Cycle 수(회)	3,018,385	2,989,499	2,987,485
동작 시간	301.597	298.705	298.500
case	7	8	9
Cycle 수(회)	2,954,392	2,987,893	3,010,337
동작 시간	295.197	298.551	300.778
case	10	11	12
Cycle 수(회)	2,989,117	3,042,929	3,046,770
동작 시간	298.679	304.029	304.439
case	13	14	15
Cycle 수(회)	3,012,236	3,014,268	3,017,821
동작 시간	300.957	301.162	301.521

[표 4] ECDSA-256 클록 수 및 동작 시간

스칼라배 연산을 구현한 경우 서명 생성 시간만 확인하여도 비밀 값의 일부 정보가 노출됨을 알 수 있다.

Ⅵ. 결론

ECDSA 의 하드웨어 구현물의 시뮬레이션 결과와 동작 클록 수 및 서명 생성 시간을 확인함에 따라 비밀값의 정보를 알 수 있다. 공격자가 암호 모듈에 접근 가능 한 경우에는 SPA 등을 이용하여 정확한 비밀값을 알 수도 있다. 이를 막기 위해 부채널 분석 내성 알고리즘을 이용한 암호 모듈 구현이 필요하다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2022-0-00973, CCTV 에 적합한 AI 가속기와 보안모듈이 적용된 인공지능반도체와 응용시스템 개발).

참 고 문 헌

[1] Diffie, Whitfield, and Martin E. Hellman. "New directions in cryptography." Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman. 2022. 365-390.

[2] Kocher, P. C. (1996, August). Timing attacks onimplementations of Diffie-Hellman, RSA, DSS, and other systems. In Annual International Cryptology Conference (pp. 104-113).

[3] NCSC. "On the security of DES," Advances in Cryptology, Proc.Crypto '85, pp. 280-285, Aug. 1985.