가변 타원곡선 암호 프로세서의 FPGA 구현 및 전력분석 공격

장 수 혁, 이 동 호
경북대학교 전자공학과
전화 : 053-940-8857 / 핸드폰 : 016-507-9320

FPGA Implementation and Power Analysis Attack of Versatile Elliptic Curve Crypto-processor

Su Hyuk Jang, Dong Ho Lee
Dept. of Electronics Graduate School, Kyungpook National University
E-mail : guy3388@korea.com

Abstract

For implementation of Cryptographic algorithms, security against implementation attacks such as side-channel attacks as well as the speed and the size of the circuit is important. Power Analysis attacks are powerful techniques of side-channel attacks to exploit secret information of crypto-processors. In this thesis the FPGA implementation of versatile elliptic crypto-processor is described. Explain the analysis of power consumption of ALTERA FPGA(FLEX10KE) that is used in our hand made board. Conclusively this thesis presents clear proof that implementations of Elliptic Curve Crypto-systems are vulnerable to Differential Power Analysis attacks as well as Simple Power Analysis attacks.

I. 서론

무선 인터넷의 발전과 인터넷 결재, 무선기기에서의 결재가 널리 사용됨에 따라 정보 보안의 필요성이 크게 대두되었다. 타원곡선 암호(ECC)는 최근 표준화되고 있고, 그 사용 가능성은 점점 더 커지고 있다. ECC 알고리즘의 하드웨어 구현은 스마트카드와 저전력 무선 인터넷 정보기기의 보안을 위하여 널리 사용 될 예정이다. ECC 암호 알고리즘의 하드웨어 구현에 있어 크기, 속도, 전력 소모뿐만 아니라 보안적인 요소도 매우 중요하다.

본 논문은 Elliptic Curve Cryptography System의 Verilog HDL을 이용한 구현과 ALTERA FPGA (FLEX10KE)를 이용한 자체 제작 보드에서의 ECC 암호 알고리즘의 수행에 대한 SPA(Simple Power Analysis) attack과 DPA(Differential Power Analysis) attack 실험을 통하여 암호 알고리즘의 하드웨어 구현이 전력분석 공격에 상당히 취약함을 증명한다.

II. 타원곡선 알고리즘

유한체 $GF(2^m)$에서 정의된 nonsupersingular 타원곡선 E는 일반적으로 다음과 같은 Weierstrass식이라 불리는 방정식을 만족하는 근 집합으로 표현할 수 있고, 보통 $E(GF(2^m))$으로 나타낸다.

$$E(GF(2^m)) = \{(x,y) \in GF(2^m) | y^2+xy=x^3+ax^2+b, a,b(\neq 0) \in GF(2^m)\} \cup \{O\}$$

이러한 타원곡선 위의 점들은 무한원점 (infinity point) O를 포함하여 가환군(abelian group)을 이룬다.

타원 곡선 암호를 위한 보안 프로토콜의 수행에는

타원곡선 상의 한점 (P)를 자연수(n) 만큼 연속적으로 더하는 연산인 Scalar Multiplication이 가장 중요하다.

Scalar multiplication over ECC

$$Q = nP = \underbrace{P + P + \cdots + P}_{n}$$

그림 1과 그림 2는 scalar multiplication을 계산하는 Double and Addition 알고리즘과 Montgomery 알고리즘을 보인다.

1) Double and Addition Algorithm

Input : $P \in E(GF(2^m))$, n (integer)
Output : $Q = nP$

1. $n = \sum_{i=0}^{k-1} b_i 2^i$, $b_k = 1$ $\quad b_i \in 0, 1$
2. $A = P$
3. *For i from k-2 downto 0*
   $A = A + A$;
   If $b_i = 1$ *then* $A = A + P$;
4. Return A

그림 1. Double and Addition Algorithm

2) Montgomery Algorithm

INPUT : An integer $k > 0$ and a point P.
OUTPUT : $Q = kP$.

1. *set* $k \leftarrow (k_{l-1} k_{l-2} \cdots k_1 k_0)_2$.
2. *set* $P_1 \leftarrow P$, $P_2 \leftarrow 2P$.
3. *for i from l-2 downto 0 do*
   if $k_i = 1$ *then*
   set $P_1 \leftarrow P_1 + P_2$, $P_2 \leftarrow 2P_2$.
   else
   set $P_2 \leftarrow P_2 + P_1$, $P_1 \leftarrow 2P_1$.
4. Return $(Q = P_1)$

그림 2. Montgomery Algorithm

Scalar multiplication의 소프트웨어 구현의 경우 특히 나눗셈을 전혀 사용하지 않는 Projective 좌표계를 사용하는 알고리즘이 널리 사용되고 있다. 본 논문은 Projective 좌표계를 사용하여 Doubl and Addition 알고리즘과 Montgomery Scalar Multiplication 알고리즘을 구현하였다. 하드웨어 구현의 경우에도 Projective 좌표계를 사용하는 것이 효율적임이 널리 알려져 있다.

III. 타원곡선 암호 알고리즘의 구현

3.1 Verilog HDL Implementation

본 논문의 구현은 5개의 하위 모듈과 이를 불러오는 최상위 TOP 모듈로 구성되어 입력받은 타원곡선 상의 점 P와 정수 n과의 Scalar Multiplication 연산이 이루어진다. 연산의 기반이 되는 Primitive Polynomial, Field Size와 타원곡선의 여러 Parameter들은 변경이 가능하다. 입력값들의 Width는 8에서 32비트까지 변경할 수 있으며, $GF(2^m)$의 m값은 7에서 256까지 변경할 수 있다. 명령어 및 data는 먼저 host_int로 들어가게 되는데, host_int와 frontblock 모듈에 의해 각 Command에 따른 신호들이 생성된다. host_int 로 입력된 data 값들은 명령어가 지시하는 regfile의 지정된 번지의 메모리에 write 되거나, regfile의 메모리로부터 read된다. 타원곡선상의 Scalar Multiplication을 수행하기위한 알고리즘들은 control 모듈에 coding 되어진다. 여러 알고리즘의 구현을 위해 control 부분에 16bit 명령어들을 정의하고, 알고리즘이 바뀔 때마다 이 명령어들의 조합에 의해 연산과정을 바꿀 수 있게 구현하였다. 이 기능은 여러 알고리즘의 구현 및 검증에 매우 편리하다. 같은 입력 값을 주고 다른 알고리즘을 수행하였을 때 같은 결과 값이 나와야 되므로 두 알고리즘의 구현 확인 및 성능 비교를 위해서도 적합한 구조라 할 수 있다.

3.2 Verification of Implementation

구현한 ECC 암호 회로를 SoC Kit를 이용하여 검증하였다. 검증에 사용된 Kit는 Huins SoCMaster -XP400 Kit로써 100만 게이트 FPGA EPXA4F1020C3가 탑재되어있다. ARM992T 프로세서가 내장되어 있으며, Hyper Terminal을 통해 PC의 화면상에서 입력값에 대한 연산 결과 값을 확인 할 수 있다. 그림 3은 Kit와 동일한 동작을 하게 제작된 FPGA 보드를 위한 회로의 합성을 보이고 있다.

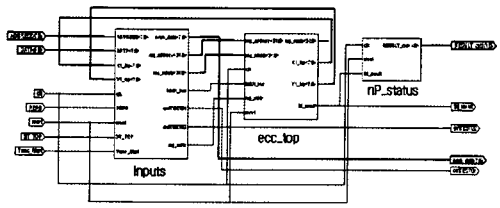


그림 3.자체 제작 보드 동작을 위한 회로의 합성도

표 1과 2는 각각 SoC Kit를 이용한 회로의 특성과 자체 제작된 보드의 FPGA 칩에 따른 특성을 나타내고 있다.

표 1. characteristics of ECC i
(Max. Field Size = 256 bits, AMBA BUS 포함)

Target Device	Logic Elements (LEs)	Total Memory bits	최대동작 주파수 (MHz)
EPXA10F1020C2	4,713	4,096	50.33

표 2. characteristics of ECC ii

Target Device	Maximum Field Size	Logic Elements (LEs)	Total Memory bits	최대동작 주파수 (MHz)
EP20K600 EBC652-3	256 bits	5,468	4096	29.68
EPF10K100 EQC240-2	128 bits	3,371	2048	25.06

Ⅳ. 전력분석 공격

Power Analysis Attack은 Side-Channel Attack의 매우 강력한 형태의 공격법이다.[4] 공격자는 예정된 사용 모드로 동작하는 디바이스를 이용하여, ECC 암호체계에서 가장 중요한 부분을 차지하는 kP 연산을 수행할 때 디바이스가 소모하는 전력을 측정하게 된다. 이 측정에 포함되어 있는 비밀키 k의 정보를 효과적으로 추출하기위해서 직접적 혹은 통계적인 방법을 사용하게 된다. 다음 그림 4는 전력분석 공격을 위해 자체 제작한 FPGA보드이다.

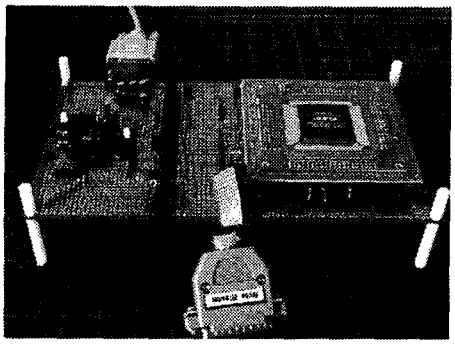


그림 4. 자체 제작 보드

4.1 Double and Addition 알고리즘의 SPA 공격

아래 그림 5와 그림 6은 Double and Addition 방식에 의한 scalar multiplication이 이루어질 때의 파형이다.

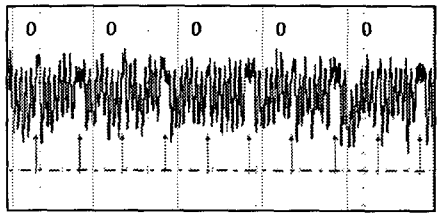


그림 5. Doubling and Addition Scalar Multiplication

위 그림 5에서 화살표로 표시된 눈에 쉽게 띄는 부분들이 계속 반복됨을 알 수 있다. 다음 그림 6은 Doubling 과 Addition이 섞여있는 파형이다.

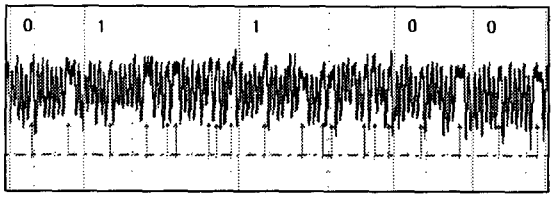


그림 6. Double and Addition Scalar Multiplication)

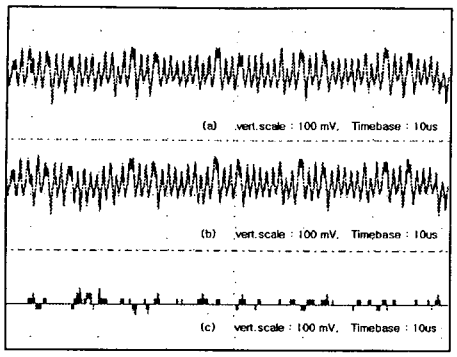
Doubling and Addition 방식으로 Scalar Multi-plication을 구현하였을 경우 위에서처럼 Simple Power Analysis attack으로 nP 연산에 사용되어지는 n 값을 쉽게 짐작을 할 수 있다. 또한 이 알고리즘의 경우 계산되어지는 bit가 0인지 1인지에 따라 Doubling 만 수행할 것인지 Doubling과 Addition을 함께 수행할 것인지 결정되므로, 연산 시간 또한 달라지므로 Timing Attack도 가능한 알고리즘이다. FPGA상에 구현된 암호 회로가 Simple Power Analysis attack에 상당히 취약함을 확인 할 수 있다.

4.2. Montgomery 알고리즘의 DPA 공격

비밀 키의 bit가 0과 1일 때 같은 동작을 수행하게 프로그램 되었을 경우 Simple Power Analysis 공격법으로 비밀 키를 찾아낼 수는 없다.

4.2.1 SEMD ATTACK

Montgomery 알고리즘에 대해 SEMD Attack을 실행한 결과는 다음 그림 7과 같다.



(a) : n = 110101 (b) : n = 100000 (c) : (a)-(b)
그림 7. nP 연산의 1,000번 평균과 Differential 파형

위 그림 7의 (c)파형에서 추측키의 값과 비밀키 값이 일치하는 부분과 일치하지 않는 부분을 구별할 수가 없다. 이는 현재 bit의 nP연산에서의 중간 결과값이 다음 bit의 nP 연산에 사용되어 전력 소모에 영향을 미치기 때문이다.

4.2.2 MESD ATTACK

성공적인 MESD Attack을 위해 최소 100번의 평균 작업이 필요하다.[4] 본 논문에서는 200번의 평균 파형들에 대해 MESD Attack을 수행하였다. MESD 공격으로 비밀키 k값을 추출하기 위해서는 한 비트씩 차례로 맞춰나가야 하며, 그 과정을 다음 그림 8에 나타내었다.

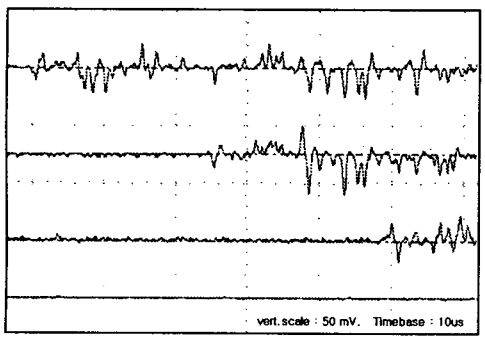


그림 8. 비밀 키 추측 과정의 differential 파형들

이로써 FPGA가 SPA 공격 뿐만 아니라 DPA 공격에도 상당히 취약함을 확인 할 수 있다.

V. 결론

Verilog HDL을 이용하여 ECC 암호 알고리즘을 구현하고 SoC 설계 검증 환경에서 속도 및 면적에 대한 결과를 보였다. 또한, FPGA가 Power Supply Line과 Ground를 통해 내부 연산 동작 시에 많은 중요한 정보를 누설함을 보이기 위해, Elliptic Curve Point Multiplication 연산을 수행하는 FPGA 보드를 제작하였다. SoC 환경에서 검증된 회로를 제작한 FPGA 보드에 맞게 수정하였고, 실제 하드웨어 상에서 ECC 암호 알고리즘의 수행에 대해 Simple Power Analysis Attack과 Differential Power Analysis Attack을 수행하였다.

앞에서의 실험 결과를 통해 FPGA의 전력소모 특성이 CMOS Technology에 기반한 ASIC의 전력 소모 특성과 비슷하며, Power Analysis Attack에 상당한 취약점을 갖고 있다는 결론을 내렸다. CMOS Technology에 기반 한 FPGA와 ASIC 은 전력소모 특성이 비슷하지만 FPGA를 프로그램 하는 것이 ASIC을 생산하는 것보다 가격이 훨씬 저렴하므로 연구실 환경에서 Power Analysis Attack을 적용하기에 최적이라 할 수 있다.

결론적으로, 우리는 싼 비용으로 아주 효과적인 실제 하드웨어 상에서의 Power Analysis Attack을 적용해보았다. 또한 Power Analysis Attack이 어렵다는 대표적인 타원곡선의 Scalar Multiplication 알고리즘인 Montgomery 알고리즘에 대한 Differential Power Analysis Attack을 수행하였다. FPGA상에 구현된 암호 회로가 Simple Power Analysis attack 뿐만 아니라 Differential Power Analysis attack 에도 상당한 취약점을 갖고 있다는 결론을 얻었다.

참고문헌(또는 Reference)

[1] M. Rosing, Implementing Elliptic Curve Cryptography, Manning Publications Co., 1999

[2] J. H. Kim and D. H. Lee, "A compact finite field processor over GF(2^m) processor," IEEE International Symposium on Circuits and Systems, 2002, Vol. 2, pp. 340-343

[3] J. Lopez and R. Dahab, "Fast Multiplication on Elliptic Curves over GF(2^m) without Precomputation," 1st International Workshop on CHES, Worcester, MA, U.S.A, August 12-13, 1999 pp. 316-327

[4] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcards," First International Workshop on Cryptographic Hard-ware and Embedded Systems, Worcester, MA, USA, August 12-13, 1999 pp. 144-157