정 보 보 호 학 회 지
제 30 권 제1호, 2020. 2

FPGA 기반 오픈소스(HDL) 암호화 로직 부채널 분석 시험 환경 연구

방 혁 준*

요 약

본 연구에서는 하드웨어 암호화 로직이 적용된 FPGA 암호 시험 평가 보드를 기반으로 구축한 부채널 분석 시험 환경과 이 환경에서의 부채널 취약성 시험 결과를 소개한다. 시험 대상은 2종의 RSA 암호화 로직 오픈소스가 적용된 FPGA 암호 시험 평가 보드이며, 암호화 과정을 수행 중에 전력 파형을 수집 분석하여 부채널 취약성을 검증하였다.

Ⅰ. 서 론

최근 IoT, 스마트 빌딩, 산업 자동화 등의 다양한 분야에서 오픈 플랫폼 사용이 증가하고 있다. 안드로이드, 리눅스와 같은 운영체제가 사용되는 오픈 플랫폼은 다양한 네트워크 기능과 하드웨어 인터페이스를 갖고 있다. 이러한 새로운 디바이스 환경은 공격자의 중요한 타겟이 되었고 민감한 자산 정보를 보호하는 것이 더욱 중요해지고 있다. 오픈 플랫폼에서 자산의 정보를 보호하는데 있어 가장 핵심적인 역할을 하는 것이 암호화 기능일 것이다. 하지만 서버사이드의 안전한 공간에서 암호키를 관리하는 것과는 달리 다양한 악성 사용자가 접근 가능한 하드웨어에서 암호 안전성을 확보하는 것은 매우 어려운 일이다.

부채널 공격은 이러한 하드웨어 암호화 공격에서 가장 널리 활용되는 공격 기법이다. 최근에는 사용자 디바이스 환경의 변화로 더욱 활발한 공격이 보고되고 있다. 부채널 공격은 저렴한 비용의 장비로 암호화를 공격할 수 있어 비용대비 공격의 효과가 매우 크다. 생체정보를 사용하는 홍채, 지문 인식 장비와 같은 오픈 하드웨어를 공격한다면 매우 치명적이다. 하지만 IoT 디바이스와 서비스를 개발하는 작은 규모의 중소업체 및 스타트업은 부채널 공격 대응을 위한 암호 안전성 평가를 수행하기가 현실적으로 어렵다.

한국 인터넷 진흥원에서 SEED, ARIA 등 국산 암호화 알고리즘을 개발하여 소스코드 형태로 제공하고 있으나 하드웨어 레벨에서 시험하기 위한 HDL 언어로 된 소스는 없는 실정이다. 과거에는 그러한 수요가 없었기 때문이다. 하지만 최근에는 RISC-V 와 같은 무료 개방형 ISA 표준이 대두되고 있다. 많은 스타트업이 RISC-V 기반의 아키텍처로 시스템을 개발하고 있으며 암호 모듈을 추가하여 개발이 가능하다. 무료 개방형 ISA를 활용하여 암호 시스템을 개발하는 중소 국내기업은 자체적으로 암호의 안전성을 시험하기 어렵다. 일본의 경우 정부 지원을 통해 부채널 공격 표준 평가 보드(SASEBO)와 표준 암호를 HDL 언어 소스코드와 함께 공개하고 있어 기업이 손쉽게 활용할 수 있다.

본 연구에서는 램버스사의 FPGA 암호 시험 평가 보드를 기반으로 구성한 암호화 로직 분석 시험 환경과 시험 환경 상에서 RSA 로직에 대해 부채널 분석을 시험한 사례를 소개한다.

Ⅱ. 전력 부채널 분석 시험 환경

집적회로가 동작하기 위해서는 전력이 소비되며, 집적회로가 동작할 때 흐르는 전류의 흐름은 전자기파를 방출한다. 이 때 집적회로에 의해 소비되는 전력은 집적회로 내부의 논리회로 구성요소들의 동작에 의해 결정되므로 소비 전력의 변화는 집적회로가 무엇을 하고 있는지에 대한 정보를 제공할 수 있다. 부채널 분석은 이러한 정보를 기반으로 암호키 등 내부 데이터를 유출하는 공격에 활용된다.

* 쿤텍 주식회사 (대표이사, joon@coontec.com)

본 연구에서 소개하는 부채널 분석 시험 환경은 다양한 암호화 알고리즘을 적용하여 시험할 수 있는 FPGA 암호 시험 평가 보드 기반으로 구성되어 있다. FPGA (Field Programmable Gate Array)는 사용자가 설계한 로직을 하드웨어로 구현할 수 있는 집적회로이다. 대표적으로 HDL 언어로 프로그래밍할 수 있는 하드웨어 로직 블록으로 구성되어 있어 사용자가 원하는 로직을 설계하여 하드웨어로 구현할 수 있다. 다른 하드웨어 로직과 동일하게 암호화 로직 또한 FPGA 상에서 개발할 수 있고 FPGA 또는 ASIC 형태로 활용된다.

2.1. DPAD FPGA 암호 시험 평가 보드

본 연구의 시험 환경에서 사용한 DPAD FPGA 암호 시험 평가 보드는 RAMBUS Cryptography Research 사의 DPA 평가 보드로 FPGA 암호 로직의 전력 특성을 모니터링하고 이를 인터페이스를 통해 외부에서 수집하여 부채널 취약성을 시험하는데 사용되는 보드이다. 평가 보드는 암호화 로직을 구현하여 수행할 수 있는 FPGA(Xilinx Kintex 7)와 제어 로직, 전력 파형 수집 및 트리거로 활용할 수 있는 BNC 타입의 다양한 시그널 탭을 갖추고 있다.

또한 암호화 과정을 제어할 수 있는 하드웨어 로직과 소프트웨어 인터페이스를 제공하기 때문에 암호화 알고리즘만을 교체하여 분석을 수행할 수 있다. 따라서 다양한 암호화 알고리즘 분석 시험 환경에서 활용이 가능하다.

〔그림 1〕 DPAD FPGA 암호 시험 평가 보드

2.2. 부채널 전력 분석 시험 환경

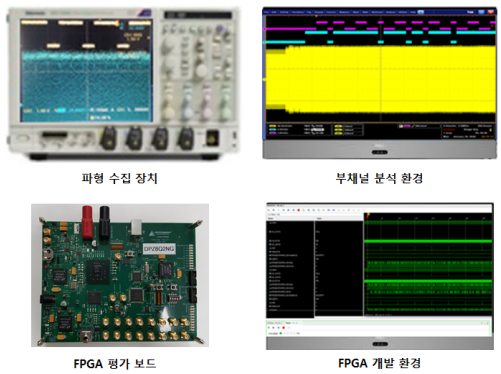
부채널 전력 분석 시험 환경은 FPGA 개발환경, DPAD FPGA 암호 시험 평가보드, 파형 수집 장치, 부채널 분석 환경으로 구성하였다.

FPGA 개발 환경은 Xilinx Vivado 도구 등을 활용하여 HDL 언어로 암호화 알고리즘을 구현하고 FPGA 평가보드에 다운로드할 수 있는 환경이다.

DPAD FPGA 암호 시험 평가 보드는 하드웨어 암호화 로직을 다운로드하고 실행할 수 있는 보드로 암호화 로직을 수행하는 FPGA와 암호화 과정을 제어할 수 있는 제어 로직으로 구성된다.

전력 파형 데이터는 통상 오실로스코프와 디지타이저 등과 같은 장치에서 수집할 수 있는데 본 환경에서는 파형 수집 장치로 대역폭 1GHz, 샘플링 속도 20GS/s를 지원하는 텍트로닉스 DPO 7104를 사용하였다.

부채널 분석 환경은 DPAD FPGA 평가보드의 암호화 로직을 소프트웨어로 제어하고 암호화 로직을 수행하면서 수집한 파형을 분석할 수 있는 환경으로 SPA, DPA, CPA 등 다양한 기법의 전력 분석을 수행할 수 있는 소프트웨어로 구성되어 있다.



〔그림 2〕 부채널 분석 시험 환경 구성

Ⅲ. RSA 로직 SPA 검증

본 연구에서는 대표적인 SPA 공격 사례 중의 하나인 RSA 로직에 대한 부채널 분석 시험 결과를 소개한다.

3.1. RSA 로직의 SPA 취약성

SPA(Simple Power Analysis)는 전력 소비를 시간의 흐름에 따라 수집해서 얻어낸 변화 그래프를 분석하여 암호화 시스템의 비밀 키를 얻어내는 공격 방법으로 하나의 파형 또는 수개, 수십 여개의 파형만으로도 내부 데이터를 유출할 수 있는 공격 방법이다.

RSA 암호와 알고리즘은 이러한 SPA 공격에 취약한 대표적인 알고리즘 중의 하나이다. RSA는 그림 3과 modular exponentiation 과정(지수 연산 이후 양의 정수로 나눈 나머지 값을 계산)을 거치게 되는데, 개인키와 관련된 입력 값은 그림 3에서 exponent(e)이다. 이 과정(modular exponentation)에서 개인키(e)의 한 비트가 0일 때 한 번의 지수 연산을, 1일 때는 한 번의 지수 연산과 한 번의 곱셈 연산을 수행하게 된다. 이것이 악용되면 전력 파형 분석을 통해 대상이 되는 암호화 시스템에서 사용된 RSA 알고리즘의 개인키가 유출될 수 있다.

본 연구에서는 2종의 오픈소스 기반의 RSA 알고리즘을 대상으로 실험하였다. 2종의 RSA 알고리즘에 사용된 그림 4의 modular exponentiation 곱셈 블록은 Montgomery 알고리즘을 기반으로 구현되어 있다. Montgomery modular 곱셈 알고리즘은 지수 연산을 빠르게 수행할 수 있어 자주 쓰이는 알고리즘 중의 하나이다.

Verilog 코드 기반의 RSA 알고리즘은 Xilinx Vivado를 사용하여 구현하였고 DPAD FPGA 보드에 기존 AES 암호화 로직을 교체하여 RSA 로직을 다운로드하여 실험하였다.

```
function mod_exp(exponent e, base b, mod n)
A =1
X = b mod n
k = e의 비트수
for i = k to 0, do     <- LOOP
 A = (A*A) mod n       <- 지수연산(Square)
 if(e[i] == 1), do     <- e[i]는 e의 i 번째 비트
  A = (A*X) mod n      <- 곱셈연산(Multiplication)
 Done
Done
```

〔그림 3〕 Moluar_exponentiation

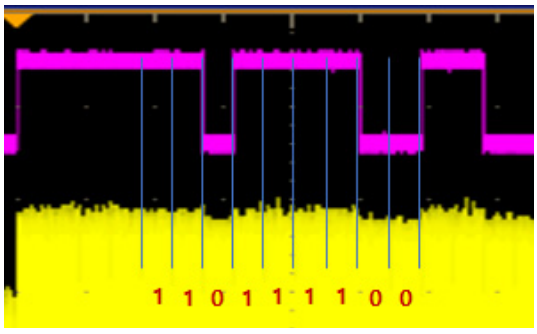
```
modular_exponentiation
입력 : X, N, E = (e_{k-1}, . . . e1, e0)2
출력 : Z = X^E mod N

W := InvN(N);
Y := MontRedc(X,N);
Z := X;
for i = k - 1 downto 0
 Z := MontMult(Z, Z, N, W);   <- 지수연산
 if(ei=1)then
  Z := MontMult(Z, Y, N, W);  <- 곱셈연산
 end if
end for
Z := MontMult(Z, 1, N, W);
```

〔그림 4〕 시험 대상 로직 modular exponentiation

3.2. 전력 소모량 차이에 의한 데이터 유출

그림 5은 2종의 알고리즘 중 첫 번째 알고리즘 수행 시 측정한 전력 파형이다. 파형 분석을 용이하게 할 수 있도록 e 비트의 값을 별도의 신호로 출력되게 하였다. 파형 분석을 통해 e 비트가 1인 경우 연산의 증가로 전력의 증가를 확인할 수 있었고 알고리즘 수행 시 측정된 전력 소모량 분석만으로 데이터 유출이 가능하여 부채널 공격에 매우 취약한 로직임을 알 수 있다. 전력 파형을 분석해 보면 modular exponentiation의 논리적 연산 구조를 기반으로 한 예상과 다르게 e 비트가 0인 경우와 1인 경우의 연산 사이클이 차이가 없음을 알 수 있다. 이는 FPGA 연산 구현상의 특성으로 성능을 높이기 위해 e 비트가 0 과 1 인 경우의 연산 사이클의 차이가 없는 구조로 구현되어 있다. 일반적인 FPGA

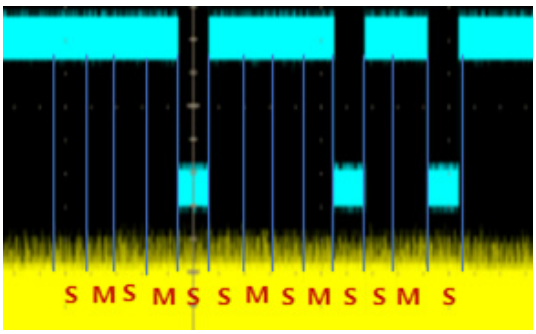


〔그림 5〕 전력 소모량 차이에 의한 데이터 유출

개발에서는 성능을 최대화하기 위해 선 연산, 후 적용의 구조로 구현을 많이 하게 되는데 첫 번째 알고리즘은 이 경우에 해당한다.

3.3. 수행 시간 차이에 의한 데이터 유출

그림 6는 두 번째 알고리즘 수행 시 전력 파형이다. 두 번째 알고리즘은 e 비트가 0인 경우 지수 연산(S)만을 수행하고 1인 경우 지수 연산(S) 후 곱셈 연산(M)을 추가로 수행하면서 연산 사이클이 증가하는 것을 확인할 수 있다. 저전력 시스템에서는 연산을 최대한 줄이는 방식으로 하드웨어 및 소프트웨어가 설계된다. 이 경우 e 비트가 1인 경우에만 연산 사이클이 늘어나는 것을 확인할 수 있다. 이는 타이밍 공격에 매우 취약한 경우로 데이터가 유출될 가능성이 크다고 볼 수 있다.



〔그림 6〕 수행 시간 차이에 의한 데이터 유출

Ⅳ. 결 론

이상으로 본 연구에서는 FPGA 평가 보드를 활용한 오픈소스 암호화 로직의 부채널 분석 환경과 전력 부채널 분석 사례를 소개하였다. 본 연구를 통해 다양한 국내 암호 알고리즘을 HDL 언어로 공개하면 암호화 알고리즘을 FPGA 에 적용해서 SPA, DPA 등 부채널 시험 및 분석이 가능하기 때문에 부채널 취약성 평가와 대응 방법(countermeasure) 개발에 활용하여 암호 안전성을 높일 수 있을 것으로 기대된다.

참 고 문 헌

[1] Kocher, Jaffer, Jun, “Differential Power Analysis”, www.paulKocher.com
[2] Mangard, Oswald, Popp, “Power Analysis Attacks Revealing the Secret of Smart Cards, Springer, 2007
[3] Miyamoto, Homma, Aoki, Satoh, “Chosen-Message SPA attacks against FPGA-based RSA Hardware Implementation”
[4] Rambus, https://www.rambus.com/security/dpa-countermeasures/dpa-workstation-platform
[5] Wikipedia, https://en.wikipedia.org/wiki/Field-programmable_gate_array
[6] CrypTech, https://trac.cryptech.is
[7] Hareware Security Project, http://satoh.cs.uec.ac.jp/SASEBO/en/index.html
[8] Xilinx,https://www.xilinx.com/products/design-tools/vivado.html

〈저 자 소 개〉

방 혁 준 (Joon Pang)
정회원
2004년~2008.5월 : ㈜엠브릿지
2008년~2015 12월 : 한컴 MDS
2016년~현재 : 쿤텍(주) 대표이사
<관심분야> 소프트웨어 공학, 정보보호