情報保護學會論文誌
第17卷 第5號, 2007. 10

FPGA 기반 ARIA에 대한 차분부채널분석 공격

김 창 균,[1†‡] 유 형 소,[2] 박 일 환[1]
[1]국가보안기술연구소, [2]경북대학교

Differential Side Channel Analysis Attacks on FPGA Implementations of ARIA

ChangKyun Kim,[1† ‡] HyungSo Yoo,[2] IlHwan Park[1]
[1]National Security Research Institute, [2]Kyungpook National University

요 약

본 논문에서는 하드웨어 기반 블록 암호알고리즘에 대한 부채널분석 공격 취약성을 살펴보았다. 분석을 위해 ARIA 알고리즘을 FPGA에 구현하였으며 다양한 분석을 위해 두 가지 형태의 S-box로 나누어 구현하였다. 각각의 구현형태에 대해 DPA 공격, 근거리 DEMA 공격 및 원거리 DEMA 공격을 실험하였다. 기존에 발표된 소프트웨어 기반 스마트카드에 대한 DPA 공격결과와 비교했을 때 하드웨어(FPGA) 기반 암호알고리즘이 병렬처리 및 기타 이유로 인해 좀 더 많은 수의 수집신호가 필요하였지만 S-box의 구현형태에 상관없이 모든 부채널분석 공격에 취약함을 실험적으로 확인하였다.

ABSTRACT

This paper has investigated the susceptibility of an FPGA implementation of a block cipher against side channel analysis attacks. We have performed DPA attacks and DEMA attacks (in the near and far field) on an FPGA implementation of ARIA which has been implemented into two architectures of S-box. Although the number of needed traces for a successful attack is increased when compared with existing results on smart cards, we have shown that ARIA without countermeasures is indeed very susceptible to side channel analysis attacks regardless of an architecture of S-box.

Keywords : *ARIA, FPGA, DPA, DEMA*

Ⅰ. 서 론

부채널분석 공격은 지금까지 다양한 연구결과와 함께 하드웨어 암호장치에 대한 새로운 분석기법으로 자리잡고 있다. 특히 하드웨어 암호장치에 대한 전력분석 공격[1] 및 전자기분석 공격[2]은 기존의 수학적 이론에 기반을 둔 암호분석기법보다 훨씬 현실적인 분석기법이며 강력한 공격기법으로 여겨지고 있다. 최근까지 발표된 부채널분석 공격의 결과를 보면 제약된 환경을 가진 스마트카드[3-7]나 단순한 마이크로컨트롤러에 소프트웨어로 구현된 암호알고리즘에 대한 실험이 대부분이며 하드웨어[8]나 FPGA[9,10]에 대한 실험결과는 많지 않다. 하지만, 하드웨어기술 및 통신환경의 발전에 따라 암호알고리즘의 빠른 처리가 요구되고 있으며 이에 따라 FPGA 및 ASIC을 이용한 암호알고리즘의 하드웨어 구현이 보편화 되고 있다. 하드웨어로 구현된 암호알고리즘의 경우 소프트웨어와는 달리 병렬처리가 가능하여 수행속도가 매우 빠르다. 따라서 순차적으로 연산을 처리하는 소프트웨어와는 달리 여러 연산이 동시에 처리

접수일: 2007년 5월 16일; 채택일: 2007년 8월 23일
† 주저자, kimck@ensec.re.kr
‡ 교신저자, kimck@ensec.re.kr

되기 때문에 하드웨어로 구현된 암호알고리즘에 대한 부채널분석 공격이 다소 까다롭기 때문에 이에 대한 연구가 필요하다.

본 논문은 부채널분석 공격에 대한 하드웨어 기반 암호알고리즘의 취약성을 알아보기 위해 ARIA 알고리즘을 FPGA로 구현하였다. 하드웨어 구현환경은 Verilog HDL을 이용하여 ALTERA사의 APEX20KE 계열인 EP20K- 300EQC240-3 칩에 구현하였으며 블록 암호알고리즘의 핵심이라 할 수 있는 S-box를 테이블 룩업 방식(table look-up)과 곱셈 역원기(multiplicative inverter)로 나누어 구현하였다. 각각의 S-box에 대해 전력분석 공격과 전자기분석 공격을 실험하였으며 그 중에서 전자기분석 공격은 근거리 전자기분석 공격과 원거리 전자기분석 공격으로 나누어 실험하였다. 실험결과, 기존에 발표된 스마트카드에 대한 전력분석 공격보다 많은 수의 수집신호를 필요로 하였으나 대응방안이 없이 구현된 하드웨어 기반 암호알고리즘 역시 모든 공격에 취약함을 실험적으로 검증하였다.

본 논문의 구성은 다음과 같다. II장에서 ARIA의 구조 및 FPGA 구현에 대해 설명하고, III장과 IV에서는 각각 전력분석 공격과 전자기분석 공격에 대한 실험결과를 기술하였다. 전력분석 공격과 전자기분석 공격에 대한 비교 및 분석을 V장에서 서술하였으며 VI장에서 논문의 결론을 맺었다.

Ⅱ. ARIA 알고리즘에 대한 FPGA 구현

2.1. ARIA 개요

ARIA는 경량 환경 및 하드웨어 구현을 위해 개발된 블록 암호알고리즘으로써 SEED와 함께 국내를 대표하는 표준 블록 알고리즘이다[11]. Involutional SPN 구조로 되어 있으며 128비트 블록크기와 가변키(128, 192, 256비트)크기에 따라 라운드 수(12, 14, 16)가 결정되는 구조이다. ARIA는 하드웨어 구현 및 8비트 환경에서 뛰어난 효율성을 가지고 있어 스마트카드 등 저전력, 저성능의 플랫폼 및 ASIC은 물론 32비트 프로세서 등의 고성능 플랫폼에도 적용이 가능하도록 개발되었다.

ARIA의 라운드 함수는 다음과 같이 세 부분으로 구성되어 있으며, 마지막 라운드에서는 Diffusion layer가 생략되며, AddRoundKey가 수행된다.

- **AddRoundKey** : 128비트 라운드 키를 128비트 라운드 입력과 XOR한다.
- **Substitution layer** : 두 종류의 8비트 입출력 S-box와 그들의 역변환으로 구성된다.
- **Diffusion layer** : 16×16이진 행렬을 사용하여 S-box 출력을 확산하는 함수로 구성되어 있다.

2.1.1. Substitution Layer(치환 계층)

ARIA의 S-box는 S_1, S_2, S_1^{-1}, S_2^{-1}로 이루어져 있다. 각각의 S-box는 8비트 입출력을 가지며 다음과 같은 함수에 의해 연산이 이루어진다.

$$S_i : GF(2^8) \rightarrow GF(2^8)$$

$$S_1 : x \rightarrow A \cdot x^{-1} \oplus a,\ S_2 : x \rightarrow B \cdot x^{247} \oplus b$$

$$A = \begin{pmatrix} 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{pmatrix} \text{ and } a = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix},$$

$$B = \begin{pmatrix} 01011110 \\ 00111101 \\ 11010111 \\ 10011101 \\ 00101100 \\ 10000001 \\ 01011101 \\ 11010011 \end{pmatrix} \text{ and } b = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

일반적으로 S-box 연산은 사전 계산된 테이블을 참조하여 계산되며 $S_3 = S_1^{-1}$와 $S_4 = S_2^{-1}$ 역시 사전 계산된 테이블을 이용하여 계산된다. 하지만 S-box의 하드웨어 구현 시 곱셈 역원기를 사용하여 구현되기도 한다.

2.1.2. Diffusion Layer(확산 계층)

확산 계층은 ARIA와 다른 블록 암호를 구별 짓는 주요 부분으로 16×16 이진 행렬로 구성되어 있으며 S-box 출력(바이트)을 확산시키는 효과를 가진다. 확산 계층의 수식 및 행렬은 다음과 같다.

$$D : GF(2^8)^{16} \rightarrow GF(2^8)^{16}$$

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{pmatrix} = \begin{pmatrix} 0&0&0&1&1&0&1&0&1&1&0&0&0&1&1&0 \\ 0&0&1&0&0&1&0&1&1&1&0&0&1&0&0&1 \\ 0&1&0&0&1&0&1&0&0&0&1&1&1&0&0&1 \\ 1&0&0&0&0&1&0&1&0&0&1&1&0&1&1&0 \\ 1&0&1&0&0&1&0&0&1&0&0&1&0&0&1&1 \\ 0&1&0&1&1&0&0&0&0&1&1&0&0&0&1&1 \\ 1&0&1&0&0&0&0&1&0&1&1&0&1&1&0&0 \\ 0&1&0&1&0&0&1&0&1&0&0&1&1&1&0&0 \\ 1&1&0&0&1&0&0&1&0&0&1&0&0&1&0&1 \\ 1&1&0&0&0&1&1&0&0&0&0&1&1&0&1&0 \\ 0&0&1&1&0&1&1&0&1&0&0&0&0&1&0&0 \\ 0&0&1&1&1&0&0&1&0&1&0&0&1&0&1&0 \\ 0&1&1&0&0&0&1&1&0&1&0&1&1&0&0&0 \\ 1&0&0&1&0&0&1&1&1&0&1&0&0&1&0&0 \\ 1&0&0&1&1&1&0&0&0&1&0&1&0&0&1&0 \\ 0&1&1&0&1&1&0&0&1&0&1&0&0&0&0&1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{pmatrix}$$

2.1.3. 라운드 키 생성

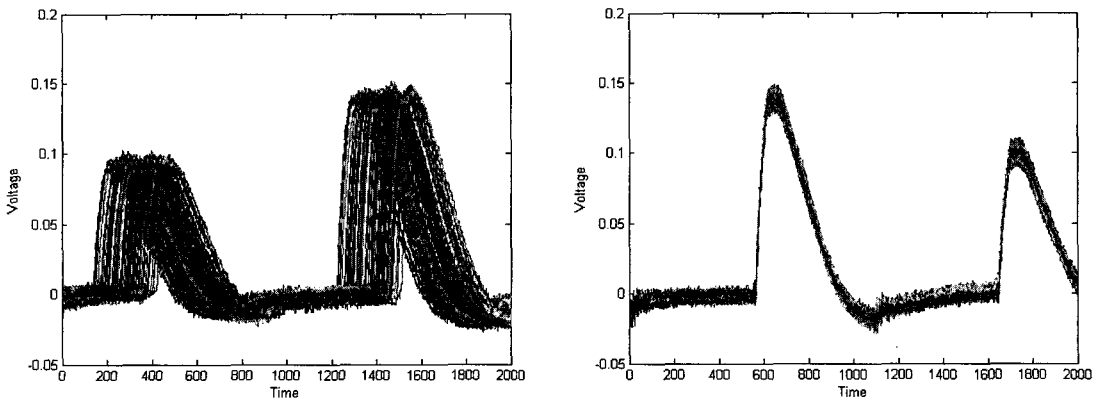
ARIA의 라운드 키 생성을 위해서는 256비트 입출력 3라운드 Feistal 구조를 가진 초기화 과정을 먼저 거쳐야 한다. 각 라운드의 키는 초기화 과정으로부터 얻은 4개의 128비트 값을 적절한 순환이동과 XOR 연산을 통해 얻을 수 있다. 복호화 라운드 키는 암호화 라운드 키와 다르며 암호화 라운드 키로부터 유도된다.

2.2. FPGA 구현

일반적으로 블록 암호알고리즘을 하드웨어로 구현할 때 구조에 따라 비반복적 구조(unrooled architecture)와 반복구조(rolled architecture)로 나눈다. 반복구조는 작은 면적으로 구현할 수 있으므로 스마트카드와 같은 제약적인 환경에 적합한 방식이다. 반면에 비반복적 구조는 데이터의 여러 블록을 동시에 처리할 수 있으므로 높은 처리율이 필요한 환경에 적합한 방식이다.

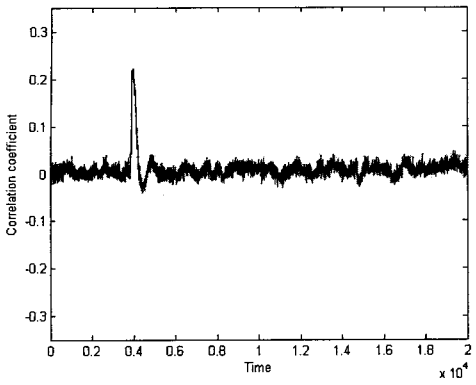
본 논문에서는 한 라운드 반복구조를 가지도록 ARIA을 구현하였다. 또한 S-box 구조에 따른 차분부채널분석 공격을 알아보기 위해 테이블 룩업 방식과 곱셈 역원기 방식으로 나누어 구현하였다. 앞서 이야기한 바와 같이 S-box 구현에는 크게 두 가지 방식이 이용된다. 첫 번째 방식은 미리 계산된 테이블을 메모리에 저장한 후 연산 시 마다 해당 값을 불러오는 테이블 룩업 방식이다. 비록 구현이 단순하며 일반적인 방식이기는 하나 차지하는 면적이 크다는 단점이 있다. 두 번째 방식은 메모리를 사용하는 첫 번째 방식을 개선하여 $GF(2^8)$ 역함수와 비트의 선형 부울함수를 이용하는 방식으로써 경량 구현에 많이 사용된다[12]. ARIA의 경우 4개의 서로 다른 4개의 S-box S_1, S_2, S_1^{-1}, S_2^{-1}를 사용하지만 S_2의 경우 $S_2 : x \rightarrow D \cdot x^{-1} \oplus b$와 같이 변형이 가능하므로 약간의 변형으로 곱셈 역원기를 공유하여 사용하였다[13,14]. 또한 [14]에서 제안한 바와 같이 두 개의 아핀 변환 A, D을 동형사상 함수(isomorphism function)와 결합이 가능하기 때문에 XOR 게이트의 수를 줄였다. 위 방식을 기반으로 각각의 S-box 구현방식에 대해 4개의 S-box S_1, S_2, S_1^{-1}, S_2^{-1}를 한 블록으로 구성하였다. 따라서 AddRoundKey의 결과 값 128비트를 4클록에 걸쳐 처리하도록 구현하였다.

마지막으로 라운드키 생성은 메모리 효율성을 높이기 위해 각 라운드가 수행될 때마다 해당 라운드키가 출력되는 on-the-fly 방식으로 구현하였다.

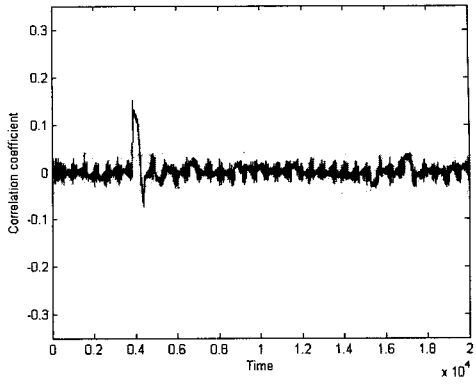


(a) 범용 함수 발생기를 이용한 경우 (b) F4100 시리즈를 이용한 경우

〔그림 1〕 클록 발생기에 따른 수집신호의 정렬화 정도



〔그림 2〕 룩업 테이블 기반 S-box에 대한 DPA 공격



〔그림 3〕 곱셈 역원기 기반 S-box에 대한 DPA 공격

Ⅲ. 차분전력분석 공격

3.1. 전력신호 측정을 위한 환경설정

FPGA기반 ARIA에 대한 차분전력분석(DPA) 공격을 수행하기 위하여 다음과 같이 실험환경을 구축하였다. 먼저 FPGA 칩의 전력을 측정하기 위하여 Vcc단에 저항(1Ω)을 연결하여 차동프로브(differential probe)로 측정하였으며 LeCroy사의 LC584 디지털 오실로스코프를 이용하였다. FPGA 보드와 PC간 통신은 RS-232를 이용하였으며 동일한 PC로 오실로스코프를 제어하도록 하였다.

FPGA 보드에 주파수를 공급하기 위하여 일반적으로 사용되는 범용 함수 발생기가 아닌 FOX electronics사의 F4100(3.6864MHz 전용) 시리즈 클록 발생기를 사용하였다. 이는 범용 함수 발생기를 사용했을 경우 함수 발생기의 클록 드리프트(clock drift)로 인하여 수집된 신호의 동기가 맞지 않을 수 있다. 〔그림 1〕은 랜덤하게 수집된 수십 개의 신호를 중첩시켜 그린 그래프이다. 〔그림 1〕(a)은 함수 발생기의 클록 드리프트에 의해 수집된 신호가 비정렬(misalignment)화되어 있음을 알 수 있다. 반면 〔그림 1〕(b)는 3.6864MHz 전용 클록 발생기를 사용한 경우로 수집된 신호가 잘 정렬되었음을 알 수 있다.

3.2. DPA 공격 실험 결과

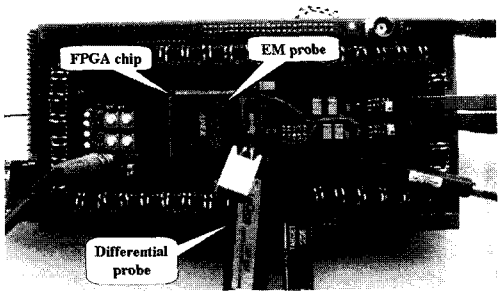
위에서 설명한 실험환경을 이용하여 10000개의 랜덤 입력평문과 고정된 키를 이용하여 전력신호를 수집하였다. 또한 근거리 DEMA 공격과 비교하기 위해 전력신호와 함께 전자기신호를 동시에 수집하였다. 공격에 앞서 우선 공격대상의 보드가 어떤 소비전력모델을 따르는지를 알아야 한다. 통상 전력분석 공격에 사용되는 소비전력 모델에는 처리되는 값의 해밍웨이트(Hamming weight)를 고려하는 해밍웨이트모델과 상태천이를 고려하는 해밍디스턴스모델(Hamming distance model)이 있다. 우리는 간단한 실험을 통하여 공격대상의 FPGA 보드의 소비전력이 해밍디스턴스모델를 따름을 알 수 있었다.

ARIA에 구현된 S-box는 4클록에 걸쳐 128비트를 처리하는 구조이다. 따라서 i번째 바이트의 S-box 출력과 $(i+4)$번째 바이트의 S-box 출력이 동일한 메모리에 저장되는 구조를 가지고 있으므로 공격자는 다음과 같은 추정모델을 설정할 수 있다.

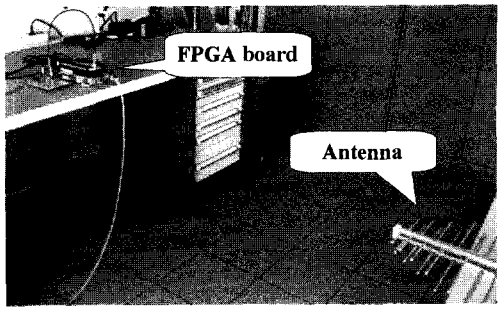
$$HD = HW(S(P_i \oplus K_i) \oplus S(P_{i+4} \oplus K_{i+4})) \quad (1)$$

여기서 P_i와 K_i는 각각 i번째 평문 바이트와 i번째 라운드키 바이트를 뜻한다. 결국 공격자는 두 개의 라운드키 바이트를 모두 고려해야 하므로 65536 경우를 고려해야 한다.

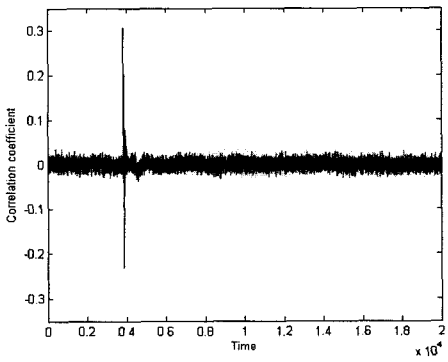
식 (1)와 같이 추정모델을 설정하여 S-box에 대한 DPA 공격을 실험하였다. 〔그림 2〕와 〔그림 3〕은 각각 다르게 구현된 S-box에 대한 DPA 공격 결과로써 모든 라운드키(2^{16})에 대한 상관계수를 나타낸 그래프이다. 〔그림 2〕와 〔그림 3〕에서 회색 그래프는 라운드 키를 잘못 추측한 경우의 상관계수를 나타내었으며 검은색 그래프는 올바른 키를 추측한 경우의 상관계수를 나타내었다. 두 가지 공격 모두에서 올바른 키를 추측한 경우 약 3800에서 피크신호를 볼 수 있다.



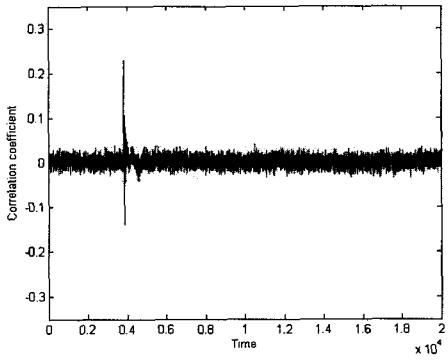
〔그림 4〕 전력분석공격 및 근거리 전자기분석 공격 실험환경



〔그림 5〕 원거리 전자기분석 공격 실험환경



〔그림 6〕 룩업 테이블 기반 S-box에 대한 DEMA 공격



〔그림 7〕 곱셈 역원기 기반 S-box에 대한 DEMA 공격

〔그림 2〕와 〔그림 3〕을 비교해 보았을 때 올바른 키 추측 시 룩업 테이블 기반의 S-box에 대한 DPA 공격에서 더 높은 상관계수를 얻을 수 있었다. 단정적으로 말하기 힘들지만 소비전력 측면에서 바라볼 때 복잡한 조합논리회로(combinational logic circuit)가 잡음으로 작용하는 곱셈 역원기와는 달리 룩업 테이블은 비교적 연산절차가 단순하기 때문에 높은 상관계수를 얻을 수 있다고 추측된다. 하지만 두 경우 모두 DPA 공격에 취약함을 알 수 있다.

Ⅳ. 차분전자기분석 공격

4.1. 전자기신호 측정을 위한 환경설정

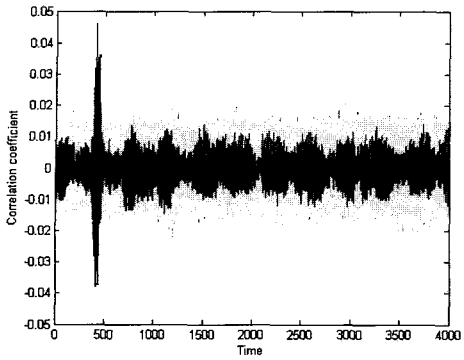
전자기분석 공격은 부채널 정보로써 전자기신호를 이용하는 것을 제외하면 전력분석 공격과 거의 흡사하다. 물론 다른 점도 있다. 전력분석 공격의 경우 회로의 모든 소비전력을 측정하는 반면 전자기분석 공격은 회로의 작고 특정한 부분에서 발생하는 신호를 측정할 수 있다. 그래서 공격적인 측면에서 보면 전력분석 공격에 비해 높은 신호대 잡음비를 가지는 부채널 신호를 측정할 수 있는 장점을 가진다.

〔그림 4〕와 〔그림 5〕는 각각 근거리 및 원거리 전자기신호 측정을 위한 실험환경이다. 근거리 전자기분석 공격과 원거리 전자기분석 공격을 실험하기 위해 신호원과 측정원의 거리에 따라 각각 다른 실험환경을 설정하였다. 근거리 전자기신호 측정을 위해서 근거리 전자기신호전용 프로브를 이용하였으며 전자기신호 증폭을 위한 광대역 증폭기를 오실로스코프와 프로브사이에 연결하였다. 원거리 전자기신호 측정을 위해서는 200MHz~1GHz 대역을 가지는 방향성안테나를 사용하였으며 근거리 측정과 동일하게 전자기신호 증폭을 위한 광대역 증폭기를 사용하였다. 안테나는 FPGA 보드에서 약 0.5미터와 1미터에 두고 두 번에 걸쳐 실험하였다. 모든 전자기신호의 측정은 신호측정을 위한 장비 외에도 다른 실험을 위한 PC 및 실험장비가 가동되고 있는 일반 실험실에서 이루어졌다.

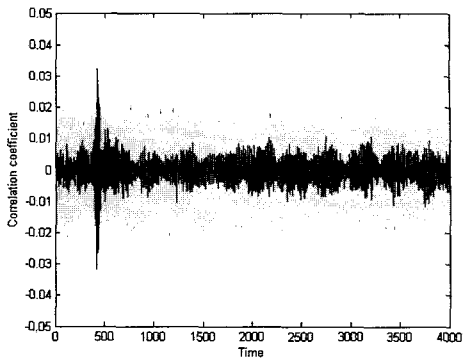
4.2. DEMA 공격 실험 결과

4.1.1. 근거리 DEMA 공격

근거리 차분전자기분석(DEMA)공격을 위해 DPA 공



〔그림 8〕 원거리 DEMA 공격 (0.5미터)



〔그림 9〕 원거리 DEMA 공격 (1미터)

격과 동일한 10000개의 랜덤 입력평문과 고정된 키를 이용하였으며 추정모델 또한 DPA 공격에서 사용된 식 (1)을 이용하였다.

〔그림 6〕과 〔그림 7〕은 각각 다르게 구현된 S-box에 대한 DEMA 공격 결과로써 모든 라운드키(2^{16})에 대한 상관계수를 나타낸 그래프이다. DPA 공격과 동일하게 올바른 키를 추측한 경우 약 3800에서 피크신호를 볼 수 있다. 올바른 키 추측 시 상관계수의 크기 또한 룩업 테이블 기반 S-box의 공격에서 더 크게 나왔다. 또한 두 가지 S-box에 대한 DEMA 공격 모두에서 DPA 공격보다 더 큰 상관계수를 얻을 수 있었다. 앞서 간단하게 언급하였지만 이에 대한 이유는 여러 가지 요인이 있을 수 있으므로 추후 연구가 더 필요할 것으로 생각된다. 하지만 DPA 공격과 마찬가지로 대응기법이 없이 구현된 두 가지 모두 DEMA 공격에 취약함을 알 수 있다.

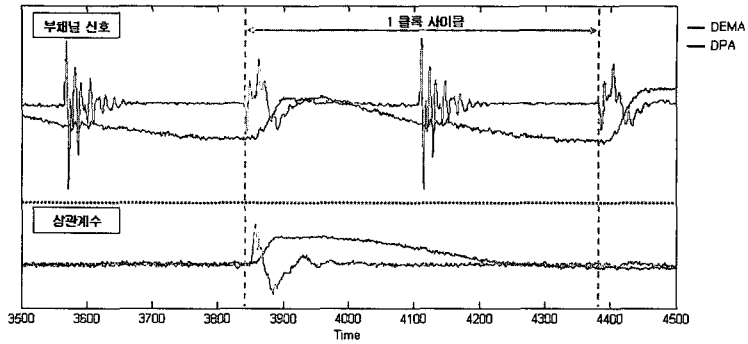
4.1.2. 원거리 DEMA 공격

전자기신호는 안테나 등을 이용하여 원거리에서도 측정이 가능하다. 하지만 원거리 전자기분석 공격은 라디오 신호 및 주위 전자장비에서 방출되는 원하지 않는 신호 등 매우 많은 잡음신호로 인하여 근거리 전자기분석 공격에 비해 매우 어렵다. 이러한 이유 때문에 원거리 전자기신호 측정에 앞서 성공적인 공격을 위해 ARIA 알고리즘의 S-box를 제외한 모든 부분을 생략하고 구현하였다. 다른 공격과의 비교를 위해 먼저 단순하게 구현된 S-box에 대해 DPA 공격과 DEMA 공격을 실험하였다. 그 결과 DPA 공격의 경우 약 0.6의 상관계수가 측정되었고 근거리 DEMA 공격의 경우 약 0.8의 상관계수가 측정되었다.

〔그림 8〕과 〔그림 9〕는 각각 0.5미터와 1미터 거리에서 30000개의 전자기신호를 이용한 원거리 DEMA 공격 결과이다. 비록 DPA나 근거리 DEMA에 비해 상관계수가 현저히 낮지만 공격이 가능함을 알 수 있다. 높은 상관계수를 얻기 위해 쉴딩룸을 이용하거나 스펙트럼 분석기나 기타 신호처리 등을 이용할 수도 있다[15].

V. DPA & DEMA 결과 비교

DPA 공격과 근거리 DEMA 공격의 실험결과를 비교/분석하기 우해 먼저 한 클록 주기 동안 피크신호가 어디에서 가장 높이 발생하는지를 살펴보았다. 〔그림 10〕은 한 클록 주기 동안의 전력신호, 전자기신호 및 각각의 상관계수를 나타낸 그림이다. 전력신호의 경우 클록이 시작되는 클록상승부분(rising edge)을 약간 지난 지점에서 가장 많은 전력을 소비하였으며 이를 정점으로 클록이 끝날 때 까지 점차 감소하는 패턴을 나타내고 있다. 그에 따른 DPA 상관계수 역시 전력신호와 유사한 패턴을 따르고 있다. 반면에 전자기신호는 클록상승부근과 클록하강부근(falling edge)에서 신호의 변동 폭이 크다. 하지만 DEMA 상관계수는 클록상승부근의 전자기신호와 유사한 패턴을 나타낼 뿐 클록하강부근에서는 거의 0이다. 즉 FPGA 보드가 클록상승에 동작하도록 설계되어 있기 때문에 클록상승부근에서 가장 많은 부채널 정보가 측정됨을 알 수 있다. 또한 이러한 사실을 바탕으로, 신호처리 시간을 줄이기 위해 사용되는 부채널 신호압축 시 클록상승부근의 샘플데이터를 중심으로 처리하면 효과적임을 알 수 있다.

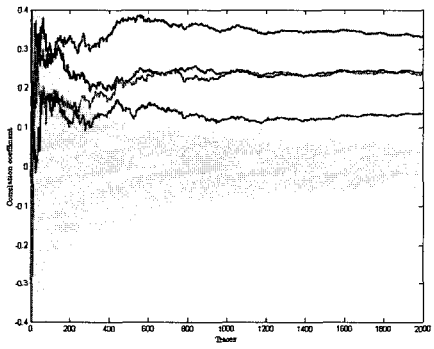


〔그림 10〕 DPA & 근거리 DEMA 비교

〔표 1〕 공격에 필요한 신호개수

공격 형태	S-box 구현 방법	ρ_{max}	N
DPA	룩업 테이블 (파란색)	0.2222	545
	곱셈 역원기 (녹색)	0.1521	1180
근거리 DEMA	룩업 테이블 (붉은색)	0.3068	278
	곱셈 역원기 (황토색)	0.2289	512

※ 그림 2, 3, 6, 7 참조



〔그림 11〕 수집신호개수에 따른 상관계수

부채널분석 공격 시 공격에 필요한 신호의 개수는 매우 중요한 정보 중 하나이다. 논문 〔16〕에서는 최대 상관계수와 공격에 필요한 전력파형 개수(N)의 관계를 다음과 같이 정의하였다.

$$N = 3 + 8\left(\frac{Z_\alpha}{\ln\left(\frac{1+\rho_{max}}{1-\rho_{max}}\right)}\right)^2 \quad (2)$$

여기서 Z_α는 $\rho=0$와 $\rho=\rho_{max}$간 거리를 결정짓는 항이다. 본 논문에서는 부채널분석 공격에 필요한 신호의 개수를 계산하기 위하여 $Z_{0.9999}=3.719$로 두고 계산하였다. 〔표 1〕은 각각의 부채널분석 공격에 따른 공격에 필요한 신호개수를 보여주고 있다. 〔그림 11〕은 수집신호개수에 따른 상관계수의 변화를 나타낸 것이다. 〔그림 11〕에서 붉은색, 파란색, 녹색, 황토색 그래프는 올바른 키 추측 시 수집신호개수에 따른 상관계수의 변화를 뜻하며 회색 그래프는 틀린 키 추측 시 상관계수를 뜻한다. 공격에 필요한 신호개수에 대한 〔표 1〕의 결과와 〔그림 11〕의 결과가 서로 일치함을 알 수 있다. 각 색깔에 따른 공격은 〔표 1〕의 'S-box 구현 방법'을 참조하기 바란다.

Ⅵ. 결 론

본 논문에서는 FPGA 기반 ARIA에 대한 부채널분석 공격 취약성을 살펴보기 위해 각각 다르게 구현된 S-box를 대상으로 DPA 공격, 근거리 DEMA 공격 및 원거리 DEMA 공격 등 다양한 부채널분석 공격을 실험하였다. 기존에 발표된 소프트웨어 기반 스마트카드에 대한 DPA 공격결과와 비교했을 때 하드웨어(FPGA) 기반 암호알고리즘이 병렬처리 및 기타 이유로 인해 좀 더 많은 수의 수집신호가 필요하였지만 S-box의 구현 형태에 상관없이 모든 부채널분석 공격에 취약함을 실험적으로 확인하였다.

비록 ARIA라는 단일 모듈의 FPGA에 대한 제한적인 실험결과이지만 소프트웨어 기반의 암호알고리즘 구

현과 마찬가지로 ASIC이나 FPGA를 이용한 암호알고리즘 구현 시에도 부채널분석 공격을 고려해야 할 것으로 판단된다. 아울러 마스킹 기법[4,6,7]과 같은 대응기법을 하드웨어에 적용할 경우 하드웨어의 특성을 잘 고려하여 구현해야 할 것이며 본 논문과 같은 기본적인 실험을 통하여 부채널분석 공격에 대한 취약성을 반드시 검증해야 할 것이다.

참고문헌

[1] P. Kocher, J. Jaffe and B.Jun, "Differential Power Analysis," CRYPTO'99, LNCS 1666, pp.388-397, Springer-Verlag, 1999.

[2] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis : Concrete Results," CHES'01, LNCS 2162, pp. 251-261, Springer-Verlag, 2001.

[3] J. Ha, C. Kim, S. Moon, I. Park, and H. Yoo, "Differential Power Analysis on Block Cipher ARIA," HPCC'05, LNCS 3726, pp. 541-548, Springer-Verlag, 2005,

[4] H. Yoo, C. Herbst, S. Mangard, E. Oswald, and S. Moon, "Investigations of Power Analysis ARIA," WISA'06, LNCS 4298, Springer-Verlag, 2007.

[5] 서정갑, 김창균, 하재철, 문상재, 박일환, "블럭 암호 ARIA에 대한 차분전력분석공격," 한국정보보호학회논문지, vol.15, no.1, pp. 99-107, 2005.

[6] 유형소, 하재철, 김창균, 박일환, 문상재, "랜덤 마스킹 기법을 이용한 DPA 공격에 안전한 ARIA 구현," 한국정보보호학회논문지, vol.16, no.2, pp. 129-139, 2006.

[7] 유형소, 하재철, 김창균, 박일환, 문상재, "저메모리 환경에 적합한 마스킹기반의 ARIA 구현," 한국정보보호학회논문지, vol.16, no.3, pp. 143-155, 2006.

[8] S. Örs, F. Grkaynak, E. Oswald, and B. Preneel, "Power Analysis Attack on an ASIC AES Impelementation," ITCC, Vol.2, pp. 546-552, 2004.

[9] S. Örs, E. Oswald and B. Preneel, "Power-Analysis Attacks on an FPGA-First Experimental Results," CHES'03, LNCS 2779, pp. 35-50, Springer-Verlag, 2003,

[10] F. Standaert, S. Örs and B. Preneel, "Power Analysis of an FPGA Implementation of Rijndael : Is Pipelining a DPA Countermeasure," CHES'04, LNCS 3156, pp. 30-44, Springer-Verlag, 2004,

[11] Daesung Kwon et al., "New Block Cipher ARIA," ICISC'02, LNCS 2971, pp. 541-548, Springer-Verlag, 2002.

[12] A. Satoh, S. Morioka, K. Takano and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," ASIACRYPT'01, LNCS 2248, pp. 239-254, Springer-Verlag, 2001.

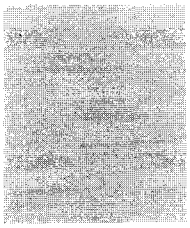
[13] A. Satoh and S. Morioka, "Unified Hardware Architecture for 128-bit Block Cipher AES and Camellia," CHES'03, LNCS 2779, pp. 304-318, Springer-Verlag, 2003.

[14] S. Yang, J. Park, and Y. You, "The Smallest ARIA Module with 16-Bit Architecture," ICISC'06, LNCS 4296, pp. 107-117, Springer-Verlag, 2006.

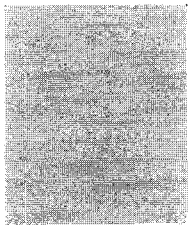
[15] M. Hutter, EM Side-Channel Attacks on Cryptographic Devices, Master thesis, Graz University of Technology, 2006.

[16] S. Mangard, "Hardware Counter- measures against DPA-A Statistical Analysis of Their Effectiveness," CT-RSA'04, LNCS 2964, pp. 222-235, Springer-Verlag, 2004.

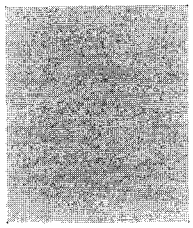
〈著者紹介〉



김 창 균 (ChangKyun Kim) 정회원
2001년 2월 : 경북대학교 전자전기공학부 졸업
2003년 2월 : 경북대학교 전자공학과 석사
2003년 3월~현재 : 경북대학교 전자공학과 박사과정
2004년 11월~현재 : 국가보안기술연구소
<관심분야> 정보보호기술



유 형 소 (HyungSo Yoo) 정회원
1997년 2월 : 경북대학교 전자공학과 졸업
1999년 2월 : 경북대학교 전자공학과 석사
2007년 2월 : 경북대학교 전자공학과 박사
<관심분야> 정보보호, 암호이론, 부채널공격



박 일 환 (IlHwan Park) 정회원
1988년 2월 : 고려대학교 수학과 졸업
1990년 2월 : 고려대학교 수학과 석사
1996년 2월 : 고려대학교 수학과 박사
1996년 5월~1999년 12월 : 한국전자통신연구원
2000년 1월~현재 : 국가보안기술연구소
<관심분야> 정보보호이론