情報保護學會論文誌
第15券 第1號, 2005. 2

블럭 암호 ARIA에 대한 차분전력분석공격*

서 정 갑,[1†] 김 창 균,[2] 하 재 철,[3‡] 문 상 재,[1] 박 일 환[2]
[1]경북대학교, [2]국가보안기술연구소, [3]나사렛대학교

Differential Power Analysis Attack of a Block Cipher ARIA

JungKab Seo,[1†] ChangKyun Kim,[2] JaeCheol Ha,[3‡] SangJae Moon,[1] IlHwan Park[2]
[1]Kyungpook National University, [2]National Security Research Institute,
[3]Korea Nazarene University

요 약

ARIA는 128비트 블록 암호 알고리즘으로 128, 192, 256 비트 암호키를 사용한다. 또한 SPN (Substitution and Permutation encryption Network) 구조와 Involution 이진 행렬을 사용하여 초경량 환경 및 하드웨어 구현에 최적으로 개발되었다. 본 논문에서는 실제 스마트카드에 부주의한 ARIA 구현이 차분 전력 분석 공격 (Differential Power Analysis)에 취약함을 보이고자 한다. ARIA에 적용된 공격시점은 S-box 출력에 대한 소비 전력이며 이는 매우 현실적이며 위협적이다. 또한 두 개의 라운드 키만을 이용하여 ARIA의 master key (MK)를 얻을 수 있다.

ABSTRACT

ARIA is a 128-bit block cipher having 128-bit, 192-bit, or 256-bit key length. The cipher is a substitution and permutation encryption network (SPN) and uses an involutional binary matrix. This structure was efficiently developed into light weight environments or hardware implementations. This paper shows that a careless implementation of an ARIA on smartcards is vulnerable to a differential power analysis attack. This attack is realistic because we can measure power consumption signals at two kinds of S-boxes and two types of substitution layers. By using the two round key, we extracted the master key (MK).

Keywords : *ARIA, Differential Power Analysis(DPA), Smartcards.*

Ⅰ. 서 론

1998년 Kocher[1]에 의해 전력 분석 공격이 소개된 후, 현재까지 많은 실험과 대응 방법이 제시되었다. 전력 분석 공격 (Power Analysis Attack)은 암호 장치내의 암호 알고리즘이 수행되는 동안에 부가 채널을 통해서 유출되는 소비 전력을 측정하여 비밀정보를 알아내는 방법이다. 전력 분석 공격은 크게 두 가지로 분류될 수 있다. 그중 SPA는 한번의 power trace를 측정하여 비밀정보와 관련된 연산을 구분하는 방법이며, 이와 달리 DPA는 비밀키에 따라 처리되는 데이터와 그에 따른 소비 전력간의 상관관계를 높여서 비밀키를 알아내는 공격방법이다. 따라서 DPA가 일반적으로 SPA보다 강력한 공격방법으로 알려져 있다.[2-6]

실제로 공개키 암호시스템 뿐만 아니라 대칭키 암호시스템 모두 DPA에 취약하다는 사실이 많은 논

접수일 : 2004년 12월 13일 ; 채택일 : 2005년 2월 2일
* 본 연구는 정보통신부 ITRC 육성지원사업의 연구지원에 의해 수행되었습니다.
† 주저자, jkseo5@palgong.knu.ac.kr
‡ 교신저자, jcha@kornu.ac.kr

문들을 통해 발표되었다.[7-10]

본 논문에서는 블록 암호가 부주의하게 구현될 때, 전력 분석 공격에 취약함을 ARIA (Academy, Research Institute, and Agency)을 통해 검증하고자 한다.[11,12] 본 논문은 크게 두 부분으로 나누어진다. 첫 번째는 ARIA가 동작될 때, DPA를 이용하여 모든 라운드 키를 구하는 공격 방법을 제시한다. 두 번째는 두개의 라운드 키 쌍으로부터 MK를 구하는 하이브리드 (Hybrid) 공격 방법을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 ARIA의 기본 구조를 살펴본다. 3장에서는 DPA를 이용한 ARIA의 공격방법을 제시한다. 4장에서는 두 개의 라운드 키를 이용하여 MK를 구하는 하이브리드 공격 방법을 제시한다. 5장에서 DPA 공격에 대한 실험결과를 살펴보고, 결론을 맺는다.

Ⅱ. ARIA 알고리즘

ARIA는 128비트 블록 암호 알고리즘으로써, 128, 196, 256비트의 3종류의 키 사용을 제공하며, 각각의 라운드 수는 12, 14, 16이다. 먼저 본 논문에서 사용하는 표기들은 다음과 같다.

- $S_i(x)$: 입력 x에 대한 S-box 의 출력
- $A(x)$: 입력 x에 대한 확산함수의 출력
- $\oplus$: 배타적 논리합 연산(XOR)
- $\lll n$: 각 비트를 왼쪽으로 n비트씩 순환이동
- $\ggg n$: 각 비트를 오른쪽으로 n비트씩 순환이동
- ||: 두 비트열 혹은 바이트열 간의 연접

2.1 ARIA 구조

ARIA는 다음과 같은 세 부분으로 구성되어 그림 1과 같다.

- 라운드 키 덧셈: 128비트 라운드 키와의 XOR
- 치환 계층: 두 유형의 치환 계층
- 확산 계층: 간단한 16×16 involution 이진행렬을 사용한 바이트 간의 확산 함수로 구성

2.1.1 치환 계층

치환계층은 두 종류의 8비트 입·출력 S-box들로 구성되며 S_1, S_2는 다음과 같다.

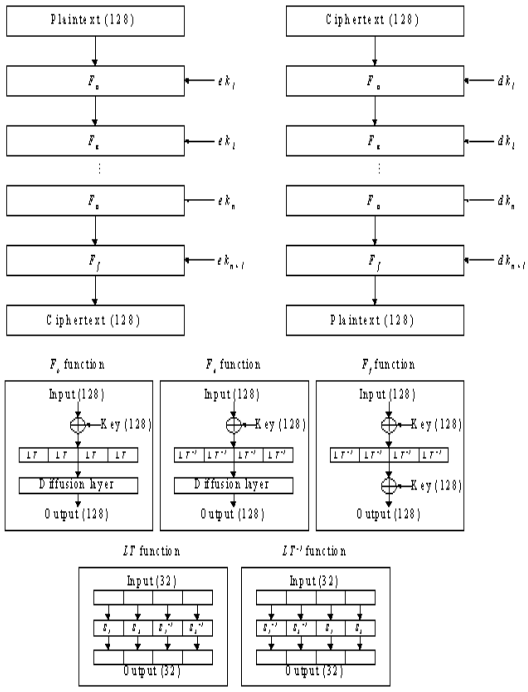


그림 1. ARIA 구조

$$S_1(x) = Bx^{-1} \oplus b,\ S_2(x) = Cx^{247} \oplus c$$

여기서 B, C는 8×8 정칙 행렬(non-singular matrix)이며, b, c는 8×1 행렬이다. ARIA는 위에서 생성한 S_1, S_2와 그 역치환 S_1^{-1}, S_2^{-1}가 사용되며 구체적인 값이 표현된 lookup table을 이용할 수 있다.

2.1.2 확산 계층

확산 계층은 ARIA와 다른 블록 암호를 구별짓는 주요 부분으로 16×16 involution 이진 행렬을 사용한다. ARIA의 확산함수 A : $GF(2^8)^{16} \mapsto GF(2^8)^{16}$는 입력을 $(x_0, x_1, \cdots, x_{15})$라 하고 출력을 $(y_0, y_1, \cdots, y_{15})$라 하면 다음과 같은 행렬 곱으로 표현된다.

2.2 Key Scheduling

ARIA의 key schedule는 초기화 과정과 라운드 키 생성 과정으로 나누어진다.

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

2.2.1 초기화 과정

초기화 과정에서는 암·복호화 한 라운드를 F함수로 하는 256비트 입·출력 3라운드 Feistel 암호를 이용하여, 암호기 MK로부터 4 개의 128비트 값 W_0, W_1, W_2, W_3을 생성한다. 암호기 MK의 길이는 128, 192 또는 256이므로 위 Feistel 암호의 입력에 필요한 256비트 (KL, KR)를 다음과 같이 구성한다.

- 128비트 KL은 MK의 상위 128비트를 취함.
- MK의 남은 비트를 이용하여 KR의 상위 비트를 채우고 나머지는 0으로 채움.

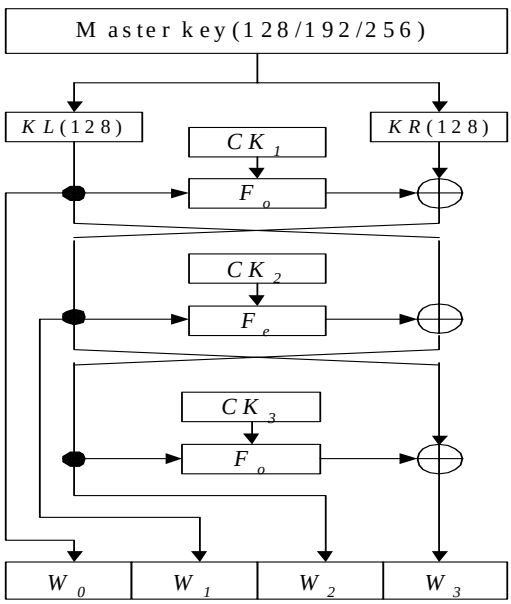


그림 2. 초기화 과정

F_o와 F_e을 각각 홀수, 짝수 라운드 함수라고 할 때, 다음과 같이 W_0, W_1, W_2, W_3을 생성한다.

$$W_0 = KL$$
$$W_1 = F_o(W_0, CK_1) \oplus KR$$
$$W_2 = F_e(W_1, CK_2) \oplus W_0$$
$$W_3 = F_o(W_2, CK_3) \oplus W_1$$

2.2.2 라운드 키 생성 과정

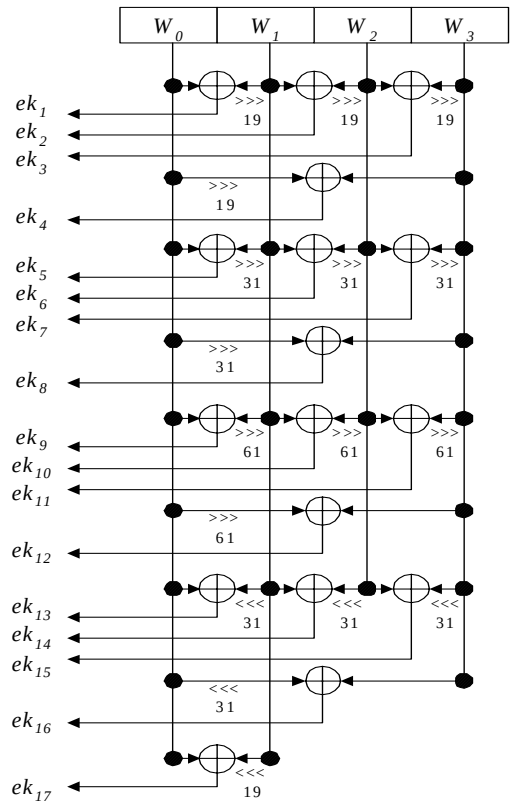


그림 3. 라운드 키 생성 부분

라운드 키 생성 과정에서는 4 개의 128비트 W_0, W_1, W_2, W_3을 조합하여 암호화 라운드 키 ek_i와 복호화 라운드 키 dk_i을 생성한다. 라운드 수는 암호키의 크기가 128, 192, 256비트인 경우 각각 12, 14, 16라운드이고 마지막 라운드에는 키 덧셈 계층이 두 번 있으므로 각각 13, 15, 17개의 라운드 키를 생성해야 한다.

복호화 라운드 키는 암호화 라운드 키로부터 유도

된다. 먼저 키의 순서가 바뀌고 처음과 마지막 라운드 키를 제외하고 암호키를 입력으로 하는 확산 함수 A의 출력이 복호화 라운드 키가 된다. 라운드 수가 n일 때, 복호화 라운드 키는 다음과 같다.

$$dk_1 = ek_{n+1}, dk_2 = A(ek_n), ..., dk_2 = A(ek_2), dk_2 = ek_1$$

Ⅲ. ARIA에 대한 DPA 공격

3.1 Differential Power Analysis (DPA)

3.1.1 부채널 공격 (Side Channel Attack)

최근 연구결과에 따르면 암호 알고리즘 및 프로토콜이 이론적으로 안전성을 제공한다 하더라도 실질적인 구현에 있어 추가적인 위험이 존재한다는 사실이 알려졌다. 즉, 수학적 이론에 기반을 둔 안전성 분석과는 별개로 물리적 공격 방법 (physical cryptanalysis)은 암호 알고리즘 혹은 프로토콜이 동작하는 기기의 소비 전력, 수행 시간, 전자기파 방사 등을 부채널이라는 추가적인 정보의 경로로 얻어 이들 정보를 분석한다. 이와 같이 부채널로 유출되는 정보들을 이용하는 공격법을 일컬어 부채널 공격 혹은 물리적 공격 (physical attack)이라고 한다.[13]

부채널 공격은 스마트카드와 같은 장치를 중심으로 진행되고 있는데 스마트카드는 CPU, ROM, EEPROM 그리고 RAM으로 구성되어 있으며 내부에 비밀키를 보관하고 있다 (카드에 따라 암호전용 프로세서인 Crypto-coprocessor를 장착한 것도 있음). 공격자의 주목표는 물리적인 방법을 이용하여 이 스마트카드내의 비밀키를 알아내는 것이다.

부채널 공격은 공격자의 형태에 따라 능동적 공격 방법과 수동적 공격 방법으로 분류할 수 있다. 능동적 공격으로는 암호 연산이 수행되는 기기에 오류를 주입하거나 자연적으로 발생한 오류가 암호문에 포함될 때 공격의 대상인 비밀키를 알아내는 오류 분석 공격 (fault analysis)이 대표적이다. 수동적 공격 방법에는 1998년 P. Kocher등이 제안한 전력 분석 공격이 대표적이다. 여기서는 가장 대표적인 전력 분석 공격인 DPA에 대해서 설명하기로 한다.

3.1.2 DPA

DPA는 한번의 power를 측정하여 비밀정보와 관련된 정보를 구분하는 SPA 공격 방법에 비밀키와 정확히 상관관계를 가지는 정보를 추출하기 위해 통계적인 분석과 에러 정정 기술을 덧붙여 사용한다.

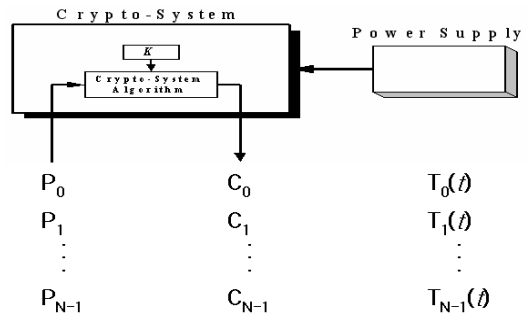


그림 4. DPA 공격을 위해 수집한 소비 전력 신호들

DPA 공격은 다음 두 단계로 나눌 수 있다. 먼저 데이터 수집 단계로서 암호 알고리즘이 수행될 때 소비되는 전력을 표본화 (sampling)하여 그 데이터를 수집한다. 다음은 수집한 데이터를 분석하는 단계로서 데이터의 잡음신호 감소와 차분 신호의 명확성을 위해 통계적인 방법을 이용한다.

그림 4는 DPA 공격을 위한 데이터 수집과정을 나타낸 것이다. N개의 평문 P_i를 스마트카드에 입력하고 비밀키 K를 이용하여 N개의 암호문과 소비 전력 신호 $T_i(t)$를 수집한다. 여기서 t는 샘플링 시간이다.

수집된 소비 전력 신호를 분석하기 위해서 공격자는 통계적인 분석 방법을 사용한다. 먼저 입력한 평문과 추측한 비밀키와의 반응을 알 수 있는 분류함수 (partitioning function) D를 정의해야 하며 다음과 같이 정의될 수 있다.

- $D(data, b, key)$: $data$와 key와의 연산 후 생성된 결과 값의 b번째 비트 값 ("0" or "1")

위의 분류함수를 이용하여 특정 해밍웨이트에 따라 수집한 소비 전력 신호를 분류한다. 그리고 분류한 신호는 각각 평균한 후에 차분 신호를 구하여 정확한 비밀키를 찾아낸다.

3.2 DPA를 이용한 라운드 키 공격

ARIA는 각 라운드마다 라운드 키와 XOR연산을 한 후 S-box lookup 연산을 수행한다. DPA 공격을 위해 공격자는 다음과 같은 분류함수 $D(P,b,rk_8)$

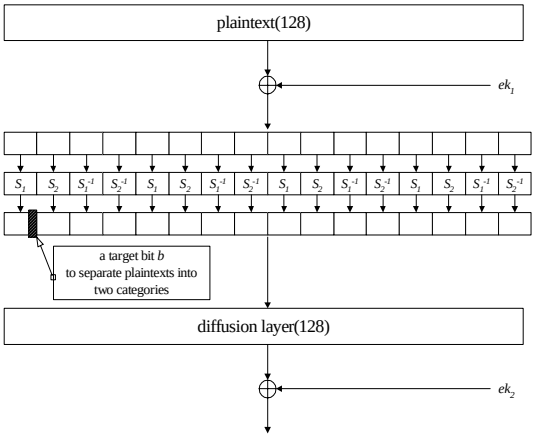


그림 5. 1라운드 ARIA에 대한 DPA 공격

을 정의한다. P와 rk_8는 그림 5에서 사용된 1라운드의 128비트 평문과 라운드 키 중 상위 8비트를 의미하며 이 값이 S_1-box의 입력으로 들어간다. b는 S_1-box의 출력 중 공격하고자 하는 특정 1비트 값이다.

공격자는 N개의 평문 P_i와 1라운드에 대한 소비 전력 신호 T_{it}을 구하고 값을 다음과 같이 나타낸다.

$$P_1, \cdots, P_N, \quad T_{1t}, \cdots, T_{Nt}$$

또한 공격자는 1라운드가 수행되는 동안 S_1-box의 출력 8비트 중 특정 1비트만을 고려하며 그 비트의 값을 b라고 하자. 그림 5에서 알 수 있듯이 b는 1라운드의 첫 8비트에만 관련이 있다. 따라서 공격자는 추측한 8비트 키와 소비 전력 데이터를 구할 때 사용한 평문을 입력으로 하여 생성된 S_1-box 출력을 분류함수를 이용하여 다음과 같이 소비 전력 파형을 두 가지로 분류를 할 수 있다.

$$T_0 = \{T_{it} \mid D(P, b, rk_8) = 0\}$$
$$T_1 = \{T_{it} \mid D(P, b, rk_8) = 1\}$$

다음 단계는 위에서 분류한 T_0, T_1의 평균을 구한다.

$$A_0[t] = \frac{1}{|T_0|} \sum_{T_{it} \in T_0} T_{it}$$
$$A_1[t] = \frac{1}{|T_1|} \sum_{T_{it} \in T_1} T_{it}$$

$A_0[t]$와 $A_1[t]$의 차분신호는 다음과 같다.

$$\Delta P[t] = A_1[t] - A_0[t]$$

만약 rk_8가 잘못된 키이면 분류함수를 통해 계산된 값이 실제 암호문의 값과 다를 것이다. 따라서 분류함수는 target device에 의해서 계산된 실제 값과 아무런 상관관계를 가지지 못하며 난수발생기 (random generator) 혹은 랜덤 함수 (random function)와 같은 기능을 가질 것이다. 결국 random function을 이용해서 두 가지로 분류를 하고 각각에 대해서 평균을 구하고 차분을 한 것이므로 $\triangle P[t]$는 N의 수가 커질수록 "0"으로 접근할 것이다.

만약 rk_8가 올바른 키라면, 분류함수를 통해서 계산된 값이 b와 일치하게 된다. 따라서 분류함수는 S_1-box후 레지스터에서 처리된 값과 상관이 있으며, 그 결과 power trace의 차분파형은 어떤 값 $\epsilon \neq 0$을 가지는 peak가 형성된다.

위의 과정을 반복하여 1라운드의 나머지 키를 모두 구할 수 있으며 결국 모든 라운드 키를 구할 수 있다.

제안하는 DPA 공격 방법은 2000개 정도의 power trace만 수집하면 한 라운드 키를 구할 수 있다. 따라서 12라운드 키를 모두 구하기 위해서는 12×2000개의 power trace가 필요하며, 이를 수집하는데 필요한 시간은 수십 시간이면 충분하다. 그러나 사전식으로 키를 구하려면 2^{128}번의 실행 시간이 필요하다. 이 사실로 볼 때 제안하는 아이디어는 이론적으로 구하기 어려운 비밀키를 공격하는데 매우 효과적인 방법이라 할 수 있다.

Ⅳ. 두 라운드 키를 이용한 MK 공격

우리는 전력 분석 공격을 이용하여 암호화 과정에서 1라운드 키를 구하였다. 마찬가지로 복호화 과정에서 전력 분석 공격을 이용하면 마지막 라운드 키를 구할 수 있다. 이 장에서는 1, 13라운드 키가 주어졌을 때, ARIA의 구조적 특성을 이용하여 MK를 찾는 방법 즉 두 공격이 합쳐진 하이브리드 형태의 공격 방법을 살펴본다.

$$ek_1 = W_0 \oplus W_1^{\gg 19}$$
$$ek_{13} = W_0 \oplus W_1^{\ll 31} = W_0 \oplus W_1^{\gg 97}$$

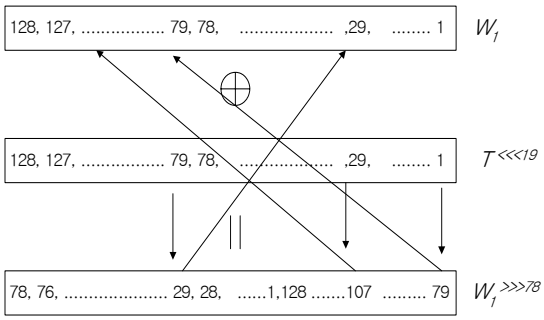


그림 6. 첫 번째 비트에 대한 연속적인 비트설정

위 식을 통해서 두개의 라운드 키만 알면 공격자는 다음과 같은 임시 값 T를 알 수 있다.

$$T = ek_1 \oplus ek_{13} = W_1^{\gg 19} \oplus W_1^{\gg 97}$$
$$W_1 = T^{\ll 19} \oplus W_1^{\gg 78}$$

위 그림 6에서 공격자가 W_1의 마지막 비트(MSB)를 0 혹은 1로 추측하면 $T^{\ll 19}$을 알고 있기 때문에 $W_{1,79}$을 결정할 수 있다. $W_{1,79}$가 결정되면 $W_{1,29}$ 또한 계산할 수 있다. 이런 방식으로 공격자는 홀수 위치에 있는 모든 비트들을 계산할 수 있다. 이와 유사하게 W_1의 마지막 전 비트를 0 혹은 1로 추측하면 공격자는 모든 짝수 비트를 계산할 수 있다.

따라서 공격자는 W_1의 마지막 두 비트만을 가정해서 4가지 경우의 W_1을 계산할 수 있다. 또한 공격자는 W_1과 $ek_1 = W_1 \oplus W_1^{\gg 19}$ 등과 같은 key generation 식을 이용해 나머지 W_0, W_2, W_3을 구할 수 있고, 이로부터 MK를 찾을 수 있다.

Ⅴ. 실험 결과

이 장에서는 스마트카드에서의 ARIA 구현에 대한 DPA공격을 실험으로 제시하며, 실험결과 ARIA가 DPA에 취약함을 보인다. 실험을 위해서 ARM 계열의 32비트 CPU core를 사용했으며, 128비트 키를 사용한 12라운드 ARIA를 구현하였다.

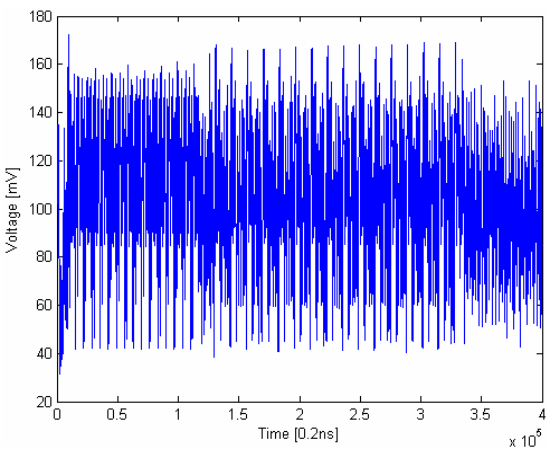
그림 7은 스마트카드가 연산을 수행하는 동안에 1, 12라운드에 해당하는 power trace를 샘플링한 것이다. 위 그림을 통해 공격자는 round key addition, S-box에 의한 치환 및 확산과정을 쉽게 확인할 수 있다.

ARIA의 공격시점은 치환함수 연산 시 발생하는 소비전력을 이용하였다. 또한 높은 peak를 얻기 위해서 S_1-box 출력 8비트 모두를 해밍웨이트 기반으로 분류하였다.

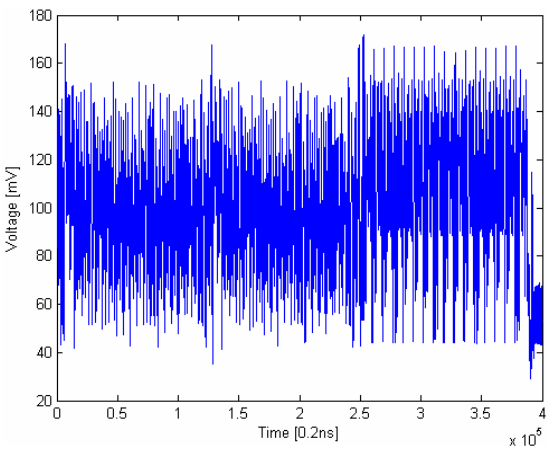
그림 8 (a), (b)는 올바른 키를 추측한 경우와 그렇지 않은 경우 얻을 수 있는 차분 전력 신호이다. 우리는 보다 분명한 peak를 위해 5000개의 power trace를 이용하였지만, 2000개의 power trace를 사용해도 공격이 가능함을 실험으로 확인할 수 있었다.

Ⅵ. 결 론

본 논문에서는 스마트카드에 구현된 ARIA가 차

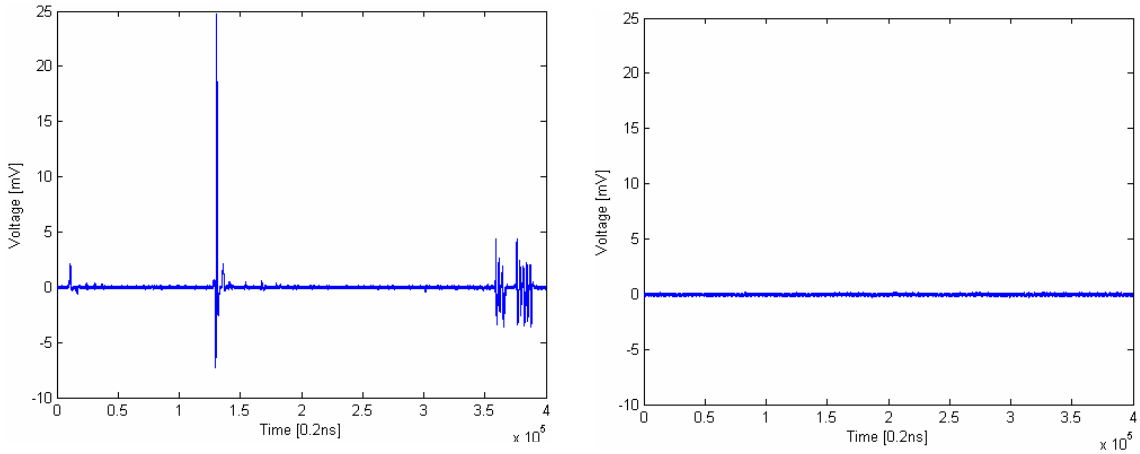


(a) 1라운드 power trace



(b) 12라운드 the power trace

그림 7. 암호화 과정에서 ARIA에 대한 single power trace



(a) 올바른 추측 (b) 잘못된 추측

그림 8. 차분 전력파형

분전력 분석 공격에 취약함을 보였다. 또한 실제 스마트카드를 통한 실험으로 검증하였다.

뿐만 아니라 구조적 특성을 이용하여 두 round key만을 조합함으로써 MK를 알아내는 하이브리드 형태의 공격을 보였으며 ARIA는 이런 공격에 취약한 특성을 지니고 있었다.

따라서 ARIA와 같은 암호시스템을 설계할 때는 전력 분석 공격 및 다른 부채널 공격이 결합된 하이브리드 형태의 공격에 대해서도 고려되어야 할 것이다.

참 고 문 헌

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

[2] B. Boer, K. Lemke, and G. Wieke, "A DPA attack against the modular reduction within a CRT implementation of RSA," *In CHES'02, LNCS 2523,* pp. 228-243, Springer-Verlag, 2002.

[3] J. Coron, "Resistance against differential power analysis for elliptic curve cryptosystems," *In CHES'99, LNCS 1717,* pp. 292-302, Springer-Verlag, 1999.

[4] L. Goubin and J. Patarin, "DES and differential power analysis," *In CHES'99, LNCS 1717,* pp. 158-172, Springer-Verlag, 1999.

[5] J.C. Ha and S.J. Moon, "Randomized signed-scalar multiplication of ECC to resist power attacks," *In CHES'02, LNCS 2523,* pp. 551-563, Springer-Verlag, 2002.

[6] C.D. Walter, "Some security aspacts of the MIST randomized exponentiation algorithm," *In CHES'02, LNCS 2523,* pp. 564-578, Springer-Verlag, 2002.

[7] Korea Information Security Agency, Block Cipher Algorithm SEED, Available from http://www.kisa.or.kr/seed/seed_eng.html.

[8] T. Messerges, E. Dabbish, and R. Sloan, "Power analysis attacks of modular exponentiation in smartcards," *In CHES'99, LNCS 1717,* pp. 144-157, Springer-Verlag, 1999.

[9] T. Messerges, "Securing the AES finalists against power analysis attacks," *In FSE'00, LNCS 1978,* pp. 150-164, Springer- Verlag, 2000.

[10] S.B. Örs, F. Grkaynak, E. Oswald, and B. Preneel, "Power-analysis at-

tack on an ASIC AES implementation," *In ITCC'04, Volume II,* pp. 546-552, 2004.

〔12〕 D. Kwon, J. Kim, S. Park, S. Sung, Y. Sohn, J. Song, Y. Yeom, E. Yoon, S. Lee, J.Lee, S. Chee, D. Han and J. Hong, "New Block Cipher : ARIA," *In ICISC'03, LNCS 2971,* pp. 432-445, Springer-Verlag, 2003.

〔13〕 J. Keley, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Cipher," in Proceedings of ESORICS '98, pp. 97-110, Springer-Verlag, Septemper 1998.

〈著者紹介〉

서 정 갑 (JungKab Seo) 학생회원
2004년 2월 : 경북대학교 전자전기공학부 졸업(학사)
2004년 3월~현재 : 경북대학교 전자공학과 석사 과정
〈관심분야〉 스마트카드 보안, 정보보호 기술

김 창 균 (ChangKyun Kim)
2001년 2월 : 경북대학교 전자전기공학부 졸업(학사)
2003년 2월 : 경북대학교 전자공학과(석사)
2003년 3월~2004년 10월 : 경북대학교 전자공학과 박사과정
2004년 11월~현재 : 국가보안기술연구소
〈관심분야〉 정보보호기술

하 재 철 (JaeCheol Ha) 종신회원
1989년 2월 : 경북대학교 전자공학과 졸업(학사)
1993년 8월 : 경북대학교 대학원 전자공학과 졸업(석사)
1998년 2월 : 경북대학교 대학원 전자공학과 졸업(박사)
1998년 3월~2000년 2월 : 나사렛대학교 전자계산소장
1998년 9월~2002년 2월 : 나사렛대학교 학술정보관장
1998년 3월~현재 : 나사렛대학교 정보통신학과 부교수, 학생지원처장
2002년 3월~현재 : 한국정보보호학회 이사
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안

문 상 재 (SangJae Moon) 종신회원
1972년 2월 : 서울대학교 공업교육(전자)과 졸업(학사)
1974년 2월 : 서울대학교 대학원 전자공학과 졸업(석사)
1984년 6월 : 미국 UCLA 전자공학과 졸업(박사)
1984년 7월~1985 6월 : UCLA Postdoctoral 근무
1984년 7월~1985 6월 : 미국 OMNET 컨설턴트
1974년 12월~현재 : 경북대학교 공과대학 전자전기컴퓨터공학부 교수
2000년 8월~현재 : 경북대학교 이동네트워크 정보보호기술 연구센터 소장
2002년 2월~현재 : 한국정보보호학회 명예회장
〈관심분야〉 정보보호, 디지털 통신, 이동 네트워크

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