情報保護學會論文誌
第17卷 第5號, 2007. 10

# 하드웨어 마스킹 대응기법에 대한 고차 차분부채널분석 공격

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

# High-Order Differential Side Channel Analysis Attacks on Masked Hardware Implementations

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

요 약

본 논문에서는 기존에 제시된 다양한 고차 차분부채널분석 공격기법에 대해 살펴본다. 하드웨어로 구현된 마스킹 기법에서 두 개의 마스킹된 중간 값이 병렬로 처리되는 경우 기존의 공격기법에 문제가 있음을 실험적으로 보이고, 이를 해결하기 위해 효율적이며 간단한 사전처리함수를 제안한다. 제안된 사전처리함수를 이용한 2차 DPA 공격과 DEMA 공격 결과, 마스킹 대응기법에 대한 2차 차분부채널분석 공격이 매우 위협적인 공격임을 실험적으로 검증할 수 있었다.

ABSTRACT

In this paper, we investigate the several different types of higher-order differential side channel analysis (DSCA) attacks. We present that some of exiting higher-order DSCA attacks have some practical problem applying to two masked intermediate values being parallel processed. In order to solve this problem we propose a new higher-order DSCA attack using an efficient and simple preprocessing function. Using the proposed preprocessing function we clearly show that 2nd-order DSCA attacks are still a practical threat for masked hardware implementations.

**Keywords** : *High-order DSCA, ARIA, FPGA,*

## Ⅰ. 서 론

부채널분석 공격은 전통적인 암호분석 방법에 비해 매우 현실적이며 위협적인 공격이다. 실제로 부채널분석 공격이 등장한 이후, 대응방법이 없는 스마트카드[1]를 포함한 FPGA[2] 및 ASIC[3] 등으로 구현된 하드웨어 암호장치가 공격을 받았다. 더 나아가 부채널분석 공격에 대한 안전성 분석을 위한 전용 플랫폼까지 개발되고 있다. 한편, 부채널분석 공격에 안전한 암호장치를 구현하기 위한 대응기법 개발에도 활발한 연구가 진행되고 있다. 지금까지 연구된 대응기법은 암호장치에서 처리되는 데이터와 부채널 신호간의 상관관계를 제거하기 위한 방안이며 대표적인 기법에는 마스킹[4-9], 랜덤시간 삽입[10], 새로운 하드웨어 논리 회로[11-13] 등이 있다. 그 중에서 가장 활발히 연구되고 있는 분야는 마스킹을 이용한 대응방법 구현이다.

접수일: 2007년 6월 1일; 채택일: 2007년 8월 23일
† 주저자, kimck@ensec.re.kr
‡ 교신저자, kimck@ensec.re.kr

하지만 마스킹 기법의 가장 큰 결점은 고차 차분부채널분석(differential side channel analysis: DSCA) 공격에 취약하다는 점이며 이러한 사실은 지금까지 많은 논문에 의해 밝혀졌다[14-20]. 그 중 논문 [20]에서는 마스킹 기법이 적용된 스마트카드에 대한 보다 효율적인 고차 DSCA 공격을 제안하였으며 [15-19]에서는 하드웨어로 구현된 마스킹 기법에 대한 고차 DSCA 공격을 제안하였다.

본 논문에서는 하드웨어로 구현된 마스킹 기법에 대한 기존의 여러 가지 고차 DSCA 공격의 실질적인 위협성을 알아보고 구현환경에 따른 적절한 고차 DSCA 공격법을 제시하였다. 다양한 고차 DSCA 공격을 실험하기 위해 마스킹 기법이 적용된 ARIA를 FPGA에 구현하였다. 그리고 대표적인 고차 DSCA 공격법인 고차 차분전력분석(differential power analysis: DPA)과 고차 차분전자기분석(differential EM analysis: DEMA)을 위해 전력신호와 전자기신호를 동시에 측정하였다. 실험 결과, 공격자는 구현된 환경에 따라 적절한 사전처리함수(preprocessing function)를 선택적으로 사용해야 하며, 병렬로 처리되는 두 마스킹된 중간 값에 대한 고차 DSCA 공격의 경우 제안하는 사전처리함수를 이용한 공격방법이 기존 공격방법에 비해 효율적임을 실험적으로 검증하였다.

본 논문의 구성은 다음과 같다. II장에서는 마스킹 기법에 대한 간단한 소개와 함께 고차 DSCA 공격에 대해 설명하였다. III장에서는 하드웨어로 구현된 마스킹 기법에 대한 기존의 여러 가지 2차 DSCA 공격 뿐만 아니라 제안하는 사전처리함수를 이용한 2차 DSCA 공격에 대한 실험결과를 기술하였다. 마지막으로 IV장에서 논문의 결론을 맺었다.

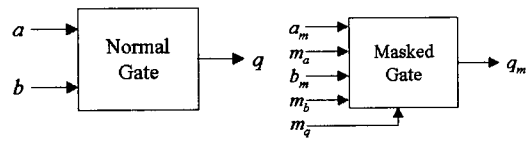
## Ⅱ. 마스킹 기법과 고차 DSCA 공격

### 2.1. 마스킹 기반 대응기법

마스킹 기법은 암호알고리즘의 연산중에 발생하는 중간 값을 공격자가 알 수 없도록, 즉 공격자의 입장에서 랜덤하게 보이도록 하는 방법으로 공격자가 추정하는 모델과 실제 발생하는 전력소모량(부채널 신호)간의 상관관계를 제거하는 방법이다. 마스킹은 가장 저렴한 비용으로 적용할 수 있어 대칭키 암호시스템에서 일반적으로 많이 사용된다. 마스킹은 구현하는 방법에 따라서, 암호알고리즘에 독립적으로 사용할 수 있는 게이트 수준의 마스킹[21,22]과, 암호알고리즘 자체를 변경하는 알고리즘 수준의 마스킹[5-9]으로 구분된다.

#### 2.1.1. 게이트 수준에서의 마스킹

게이트 수준의 마스킹은 회로에서 처리되는 실제 데이터 $a$를 두 개의 값 $a_m$, $m_a$로 표현하는 것이다. 따라서 디지털 회로에서 실제 처리되는 데이터와 전력소모량간의 상관관계가 존재하지 않는다. 이때 $m_a$는 $a$와는 통계적으로 독립적이고 균일한 분포를 가지는 랜덤 값으로 마스크라고 부르며, 마스킹된 값 $a_m$은 $a$와 $m_a$의 배타적 논리합 연산(XOR): $a_m = a \oplus m_a$을 통해 계산된다. 마스킹된 디지털회로에서, 논리 게이트는 $a$대신에 $a_m$, $m_a$를 입력으로 받아들인다. [그림 1]와 [그림 2]는 각각 일반 게이트와 마스킹된 게이트의 입출력을 보여준다.




[그림 1] 일반 게이트 [그림 2] 마스킹된 게이트

[그림 1]에서 일반 게이트는 두 개의 입력 $a$, $b$를 받아서 한 개의 출력 $q=f(a, b)$를 생성한다. 반면, [그림 2]의 마스킹된 게이트는 마스킹된 값 및 마스크 $a_m$, $m_a$, $b_m$, $m_b$, $m_q$를 입력으로 받아서 한 개의 마스킹된 출력 $q_m = f(a_m, m_a, b_m, m_b, m_q)$을 생성한다. 마스킹된 게이트에는 멀티플렉서와 크로스바 스위치를 이용하는 것[21], 일반 논리 게이트를 이용하는 것[22] 등 여러 형태가 있다. 게이트 수준의 마스킹은 알고리즘의 종류에 상관없이 일반적으로 적용할 수 있다는 장점이 있으나, 구현 면적의 증가 등 추가비용이 많이 드는 단점이 있다.

#### 2.1.2. 알고리즘 수준에서의 마스킹

알고리즘 수준의 마스킹은 DSCA 공격에 대한 대응방법으로 가장 활발히 연구되고 있는 분야이다. 이 기법의 기본 개념은 알고리즘의 중간 값을 랜덤화하는데 있다. 중간 값을 랜덤화하기 위해 지금까지 제안된 마스킹

기법에는 1차 DSCA 공격에 대응하기 위한 가산 마스킹[6], 곱셈 마스킹[5,7], 그리고 역원계산을 효율적으로 하는 방법[8,9] 등이 있으며, 2차 이상의 고차 DSCA 공격에 대응하기 위한 고차 마스킹[23]이 있다. 기존에 제안된 마스킹 기법 중 곱셈 마스킹[5]은 1차 DSCA 공격에도 취약함이 밝혀졌으며, 대수 연산을 변형하는 방법[8,9]은 소프트웨어 구현에는 적합하지 않다. 소프트웨어 구현에 가장 적합한 방법은 암호알고리즘 수행 시에 발생하는 중간 값 $i$를 랜덤 마스크 $m$을 이용하여 공격자가 알 수 없는 값 $r=i\oplus m$ 로 대체하는 가산 마스킹 방법이다. [그림 3]은 가산 마스킹을 이용한 마스킹된 Sbox 테이블 생성을 위한 일반적인 알고리즘코드이다.

입력 : $m$, $m'$
출력 : $MaskedSBOX(x\oplus m)=SBOX(x)\oplus m'$

```
1 : for i = 0 to 255 do
2 :     MaskedSBOX(x⊕m) = SBOX(x)⊕m'
3 : end
4 : Return(MaskedSBOX)
```

[그림 3] 마스킹된 Sbox 생성을 위한 알고리즘

## 2.2. 2차 DSCA 공격

P. Kocher는 전력분석 공격을 처음으로 제안한 그의 논문 [24]에서 고차 DSCA 공격에 대해서 언급하고 있지만 이를 실험적으로 처음 보여준 것은 T. Messerges 이다[15]. 그 후 많은 논문에서 소프트웨어 및 하드웨어로 구현된 마스킹 기법에 대한 고차 DSCA 공격 결과를 발표하였다[16-20].

1차 DSCA 공격은 측정한 부채널 신호의 한 시점 정보만 이용하지만 2차 이상의 고차 DCSA 공격은 두 시점 이상의 정보를 이용한다. 구체적으로 말하면 2차 DSCA 공격의 경우 $a_m$와 $m$에 해당하는 부채널 신호를 적절히 이용하여 마스크가 벗겨진 $a$값을 알아내는 공격법이다. 2차 DSCA 공격은 크게 사전처리단계와 분석단계로 나눌 수 있다. 사전처리단계는 수집한 부채널 신호에서 실제 $a_m$와 $b_m$가 처리되는 구간을 정한 후 사전처리함수를 이용하여 새로운 부채널 신호를 생성한다. 분석단계는 1차 DSCA 공격과 유사한데 사전처리단계에서 얻은 새로운 부채널 신호와 미리 설정한 추정모델을 이용하여 부채널 신호와 추정모델간의 상관관계를 계산한다. 실제 E. Oswald는 소프트웨어로 구현한 마스킹 기반 스마트카드에 대해 효율적인 2차 DSCA 공격 방법을 제안하였다[20]. 그는 다음과 같은 기본적인 가정을 바탕으로 2차 DSCA 공격을 수행하였다.

- **가정** : $a\in\{0,1\}^n$이고 $P(a)$를 $a$를 처리할 때의 소비전력 $HW(a)$를 $a$의 해밍웨이트라고 할 때, 소비전력은 $P(a)\sim HW(a)$를 따른다.

- **사실** : $a, b\in\{0,1\}$라 배타적 논리합 연산에 대해 $HW(a\oplus b)=|HW(a)-HW(b)|$의 관계가 확률 1로 성립한다.

예를 들어 동일한 마스크 $m$으로 마스킹된 $a_m$와 $b_m$에 대해 사전처리함수 $pre(HW(a_m), HW(b_m))$를 $|P(a_m)-P(b_m)|$라 할 때 위 가정과 사실을 기반으로 다음과 같은 관계가 성립함을 알 수 있다.

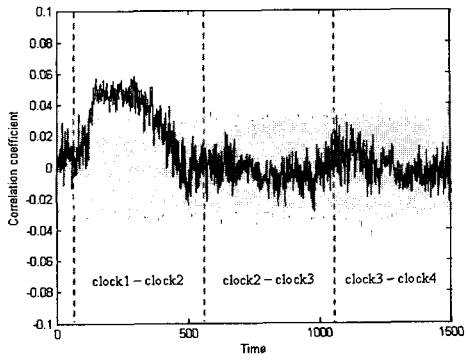
$$\begin{aligned}|P(a_m)-P(b_m)| &\approx |HW(a_m)-HW(b_m)| \\ &= HW(a_m\oplus b_m) \\ &= HW(a\oplus m\oplus b\oplus m) \\ &= HW(a\oplus b)\end{aligned} \quad (1)$$

따라서 공격자는 마스크에 상관없이 $a$와 $b$를 이용하여 공격을 수행할 수 있다.

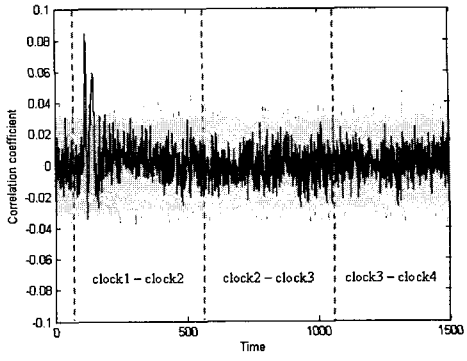
[표 1]은 서로 다른 사전처리함수에 따른 $HW(a\oplus b)$와의 상관계수를 보여주고 있다. 5개의 서로 다른 사전처리함수 중 2번 함수 $|HW(a_m)-HW(b_m)|$가 가장 높은 상관계수를 나타내고 있다. 하지만 하드웨어 환경에서는 $a_m$와 $b_m$가 동시에 병렬로 처리될 수 있기 때문에 1번과 2번 함수는 적합하지 않고 이 경우 3번 사전처리

[표 1] 사전처리함수에 따른 상관계수

| 사전처리함수 | | 값 | | | | 상관계수 |
|---|---|---|---|---|---|---|
| $a_m$ | | 0 | 0 | 1 | 1 | |
| $b_m$ | | 0 | 1 | 0 | 1 | |
| $HW(a_m\oplus b_m)$ | | 0 | 1 | 1 | 0 | |
| 1 [14] | $HW(a_m)\cdot HW(b_m)$ | 0 | 0 | 0 | 1 | -0.57 |
| 2 [15] | $\|HW(a_m)-HW(b_m)\|$ | 0 | 1 | 1 | 0 | 1 |
| 3 [16] | $(HW(a_m)+HW(b_m))^2$ | 0 | 1 | 1 | 4 | -0.33 |
| 4 | $HW(a_m)+HW(b_m)$ | 0 | 1 | 1 | 2 | 0 |
| 5 | $HW(a_m)-HW(b_m)$ | 0 | -1 | 1 | 0 | 0 |




〔그림 4〕 $|P1-P2|$를 이용한 2차 DPA 공격결과




〔그림 5〕 $|P1-P2|$를 이용한 2차 DEMA 공격결과

함수가 적절하게 이용될 수 있다. 논문 〔16-19〕에서는 FPGA로 구현한 마스킹 기법에 대해 3번 함수를 이용한 고차 DSCA 공격을 제안하였다.

위 결과를 살펴보면 공격자는 마스킹 대응기법의 구현환경에 따라 적절한 사전처리함수를 이용해야 함을 알 수 있다.

## Ⅲ. 마스킹 기반 하드웨어에 대한 2차 DSCA 공격

본 장에서는 〔표 1〕에 제시된 여러 가지 사전처리함수를 이용한 2차 DSCA 공격을 실험하기 위하여 두 가지 다른 환경을 가정하여 마스킹 기법을 구현하였다. 첫 번째 가정은 두 개의 마스킹된 중간 값 $a_m$와 $b_m$가 서로 다른 클록 사이클에서 처리되는 환경이고 나머지 가정은 두 값 모두가 동일한 클록 사이클에서 처리되는 환경이다. 실험을 위해 ARIA 알고리즘의 S-box를 〔그림 3〕을 이용하여 FPGA에 구현하였다. 하드웨어 구현을 위해 Verilog HDL을 이용하였으며 ALTERA사의 EP20K300EQC240-3 칩에 구현하였다.

### 3.1. 다른 클록 사이클에 대한 2차 DSCA 공격

먼저 두 개의 마스킹된 S-box 출력 $a_m = S_1(p_1 \oplus k_1) \oplus m$와 $b_m = S_2(p_2 \oplus k_2) \oplus m$를 서로 다른 클록 사이클에서 동작하도록 구현하였다. 마스크가 임의적으로 제거되는 것을 방지하기 위해 S-box의 출력이 저장되는 레지스터의 초기값은 '0'으로 설정하였다. 이 경우 첫 번째 S-box의 출력 $a_m$과 두 번째 S-box 출력 $b_m$에 따른 부채널 신호 $P1$, $P2$는 각각 식 (2)와 (3)을 따른다.

$$P1 \approx HW(S_1(p_1 \oplus k_1) \oplus m) \tag{2}$$

$$P2 \approx HW(S_2(p_2 \oplus k_2) \oplus m) \tag{3}$$

여기서 $p_i$는 한 바이트 평문이며 $k_i$는 그에 해당하는 한 바이트 라운드키이다. 따라서 공격자는 식 (1)과 같이 2차 DSCA 공격을 위한 추정모델을 다음과 같이 정의할 수 있다.

$$\begin{aligned} HW(a_m \oplus b_m) &= HW(S_1(p_1 \oplus k_1) \oplus m \oplus S_2(p_2 \oplus k_2) \oplus m) \\ &= HW(S_1(p_1 \oplus k_1) \oplus S_2(p_2 \oplus k_2)) \\ &= HW(a \oplus b) \end{aligned} \tag{4}$$

먼저 〔표 1〕의 여러 가지 사전처리함수 중 가장 높은 상관계수를 가지는 2번 함수 $|P1-P2|$를 이용하여 100,000개의 부채널 신호(전력신호와 전자기신호)를 처리하였다. $P1$은 $a_m$이 처리되는 사이클을 포함한 3 클록 사이클 동안의 부채널 신호이며 $P2$ 역시 $b_m$이 처리되는 사이클을 포함한 3 클럭 사이클 동안의 부채널 신호이다. 〔그림 4〕는 추정모델 (4)와 $|P1-P2|$간 상관계수를 계산한 2차 DPA 공격 결과이며 〔그림 5〕는 2차 DEMA 공격 결과이다. 〔그림 4〕와 〔그림 5〕에서 회색 그래프는 잘못 추측한 라운드 키에 대한 상관계수를 나타내며 검은색 그래프는 올바른 키를 추측한 경우의 상관계수를 뜻한다. 실제 $a_m$이 처리된 부채널 신호 $P1_{clock1}$와 $b_m$가 처리된 부채널 신호 $P2_{clock2}$에 의해 생성된 $|P1_{clock1} - P2_{clock2}|$에서 피크신호를 볼 수 있다.

본 논문에서는 〔20〕와 같이 사전처리함수 $|P1-P2|^{\beta}$에 서로 다른 $\beta$값을 적용하면서 최대 상관계수의 변화를 살펴보았다. 〔표 2〕는 $\beta$값에 따른 최대상관계수를 보여주고 있다. 2차 DPA 공격의 경우 $\beta=6$에서 최대

〔표 2〕 $\beta$값에 따른 최대상관계수

| $\beta$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 2nd-order DPA | 0.0547 | 0.0573 | 0.0592 | 0.0605 | 0.0614 |
| 2nd-order DEMA | 0.0791 | 0.0843 | 0.0864 | 0.0861 | 0.0839 |
| $\beta$ | 6 | 7 | 8 | 9 | 10 |
| 2nd-order DPA | 0.0618 | 0.0616 | 0.0611 | 0.0602 | 0.0589 |
| 2nd-order DEMA | 0.0801 | 0.0753 | 0.0698 | 0.0640 | 0.0581 |

상관계수가 측정된 반면 2차 DEMA 공격의 최대 상관계수는 $\beta=3$에서 측정되었다. [25]에서 제안한 방법을 기반으로 공격에 필요한 최소한의 부채널 신호수를 계산해 보면, 먼저 2차 DPA 공격의 경우 7,227개의 전력신호가 필요하며 2차 DEMA 공격은 3,690개의 전자기신호가 필요하다. 위에서 얻은 계산적 결과는 실험적으로 확인할 수 있었다.

마지막으로 [표 1]의 4번와 5번을 제외한 나머지 사전처리함수를 이용하여 상관계수를 계산하였다. 하지만 1번 함수 $\rho(P1\cdot P2, HW(a\oplus b))$, 3번 함수 $\rho((P1+P2)^2, HW(a\oplus b))$모두에서 의미있는 피크신호를 볼 수 없었다.

### 3.2. 동일 클록 사이클에 대한 2차 DSCA 공격

전 절에서는 같은 마스크로 마스킹된 두 중간 값 $a_m$와 $b_m$가 다른 클록 사이클에서 처리되는 경우를 살펴보았다. 하지만 하드웨어 구현에서는 두 중간 값이 동시에 병렬로 처리될 수 있다. 이 경우 두 중간 값은 서로 독립적으로 일어나지만 병렬처리에 의해 합쳐진 두 부채널 시호는 더 이상 독립적이지 않기 때문에 2차 DSCA 공격에 취약할 수 있다. 하지만 두 부채널 신호가 합쳐진 상태이기 때문에 앞서 살펴본 〔표 1〕의 1번과 2번 사전처리함수는 적용하기 힘들다. 그래서 논문 〔16-19〕에서는 〔표 1〕의 3번 사전처리함수를 이용한 2차 DSCA 공격을 제안하였다. 본 논문에서는 위 실험을 위해 동일한 마스크로 마스킹된 두 개의 S-box가 병렬로 처리되도록 구현하였다. 이 경우 두 S-box의 출력 $a_m$와 $b_m$은 한 클록 사이클에 처리되므로 이에 따른 부채널 신호는 식 (5)를 따를 것이다.

$$P=P1+P2\approx HW(a_m)+HW(b_m) \tag{5}$$

전술한 바와 같이 위 구현환경에 적절한 〔표 1〕의 3번 사전처리함수 $P^2$를 이용하여 상관계수 $\rho(P^2, HW(a\oplus b))$를 계산하였다. 하지만 100,000 부채널 신호를 이용했지만 의미있는 피크신호를 볼 수 없었다. 그래서 보다 효율적인 사전처리함수를 찾기 위해 사전처리함수에 부채널 신호의 평균을 오프셋 항으로 추가한 새로운 사전처리함수를 고려하였다. 식 (6)은 오프셋 항이 추가된 제안하는 사전처리함수이다.

$$pre(HW(a_m),HW(b_m))=|HW(a_m)+HW(b_m)-E| \tag{6}$$

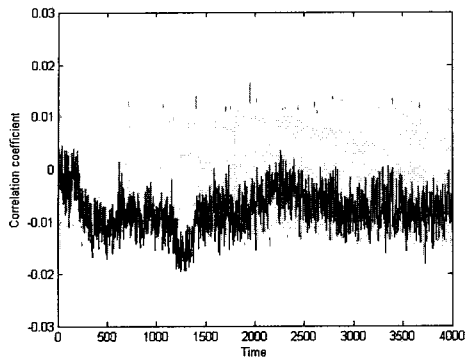
여기서 $E$는 모든 $a_m$와 $b_m$값에 대한 $HW(a_m)+HW(b_m)$의 평균값이다.

〔표 3〕 제안하는 사전처리함수에 대한 상관계수

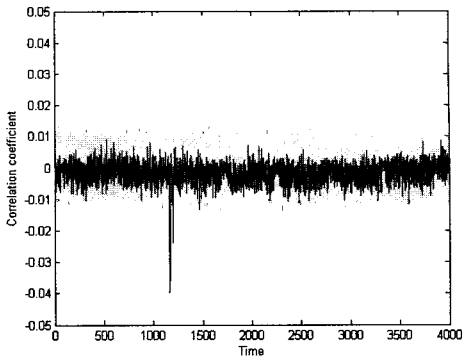
| 사전처리함수 | 값 | | | | 상관계수 |
|---|---|---|---|---|---|
| $a_m$ | 0 | 0 | 1 | 1 | |
| $b_m$ | 0 | 1 | 0 | 1 | |
| $HW(a_m\oplus b_m)$ | 0 | 1 | 1 | 0 | |
| $\lvert HW(a_m)+HW(b_m)-E\rvert$ | 1 | 0 | 0 | 1 | -1 |

〔표 3〕을 보면 제안하는 사전처리함수를 이용할 경우 단지 부호만 반대일 뿐 최대 상관계수를 얻을 수 있음을 알 수 있다. 우리는 제안한 사전처리함수 $|P-E(P)|$를 이용하여 상관계수 $\rho(|P-E(P)|, HW(a\oplus b))$를 계산하였다. 제안한 사전처리함수를 이용한 결과 성공적인 2차 DSCA 공격을 수행할 수 있었다. 〔그림 6〕과 〔그림 7〕은 제안하는 사전처리함수를 이용한 2차 DPA 공격과 2차 DEMA 공격에 대한 상관도 그래프이다. 두 그림에서와 같이 2차 DPA 공격의 경우 최대 상관계수는 -0.01963 이며 2차 DEMA 공격의 경우 최대 상관계수는 -0.03959이다. 그리고 최대 상관계수가 관측되는 시점의 전력신호의 평균은 $E(P_{power})_{\rho_{max}}=0.0045$이며 전자기신호의 평균은 $E(P_{EM})_{\rho_{max}}=4.16$이다.

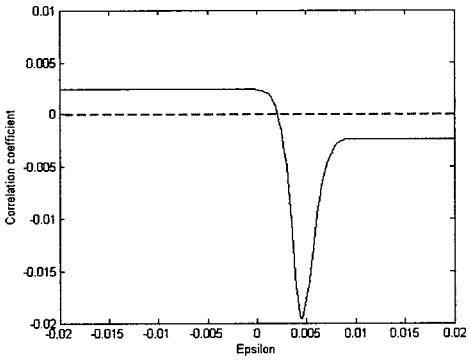
우리는 $|P-E(P)|$에서 $E(P)$를 $\varepsilon$로 대체한 후 $|P-\varepsilon|$에서 오프셋($\varepsilon$)값이 언제일 때 상관계수가 최대가 되는지 알아보았다. 〔그림 8〕과 〔그림 9〕는 $\varepsilon$값에 따른 상관계수 변화를 나타낸 그래프이다. 2차 DPA 공격의 경우 $\varepsilon_{\rho_{max}}=0.0045$에서 최대 상관계수가 측정되었으며 2차 DEMA의 경우 $\varepsilon_{\rho_{max}}=3.89$에서 최대 상관계수가 측정되었다. 비록 2차 DEMA 공격의 경우 앞서 측정된 $E(P_{EM})_{\rho_{max}}=4.16$와 약간의 오차가 발생하였지만 오프셋 값이 $\varepsilon=E(P)$일 때 최대 상관계수가 측정됨을 실험적으로 알 수 있으며 이는 제안하는 사전처리함수가 제



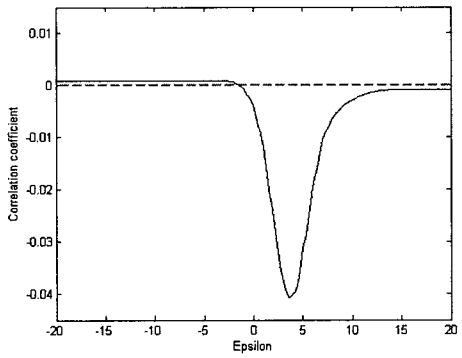

〔그림 6〕 $|P-E(P)|$를 이용한 2차 DPA 공격




〔그림 7〕 $|P-E(P)|$를 이용한 2차 DEMA 공격




〔그림 8〕 오프셋값(평균)에 따른 상관계수 변화
(2차 DPA 공격)




〔그림 9〕 오프셋값(평균)에 따른 상관계수 변화
(2차 DEMA 공격)

대로 동작함을 뒷받침해주고 있다.

덧붙여 제한적 환경에서 ARIA 알고리즘만으로 실험을 하였으나 SEED, AES, DES 등의 알고리즘도 동일한 메커니즘으로 마스킹 기법이 적용되기 때문에 제안하는 사전처리함수를 그대로 사용할 수 있다. 또한 기존에 제안되었던 3번 사전처리함수에 비해 제안하는 사전처리함수의 상관계수가 3배 크기 때문에 공격에 필요한 부채널신호도 현저하게 줄어든다. 위 실험결과를 볼 때, 동일한 실험환경에서 3번 사전처리함수를 이용해 의미있는 피크신호를 얻기 위해서는 각각 9배가 많은 158,822개의 전자기신호와 646,061개의 전력신호가 필요하다.

## Ⅳ. 결 론

마스킹 기법이 제안된 이 후 지금까지 마스킹 기법을 분석하기 위한 다양한 고차 DSCA 공격이 제안되었다. 하지만 마스킹 기법은 소프트웨어는 물론 하드웨어로도 구현될 수 있기 때문에 공격자는 구현환경을 고려하여 적절한 고차 DSCA 공격을 선택적으로 적용해야 한다. 본 논문에서는 하드웨어로 구현된 마스킹 기법에 대한 기존의 여러 가지 고차 DSCA 공격의 실질적인 위협성을 알아보고 구현환경에 따른 적절한 고차 DSCA 공격법을 제시하였다. 실험 결과, 두 개의 마스킹된 중간 값이 병렬로 처리되는 환경일 경우 기존의 공격기법에 문제가 있었으며 이를 해결하기 위해 새로운 사전처리함수를 사용하는 2차 DSCA 공격을 제안하였다. 제안하는 사전처리함수를 이용하여 성공적인 2차 DPA 공격과 DEMA 공격을 수행할 수 있었으며 마스킹 대응기법에 대한 2차 DSCA 공격이 매우 위협적인 공격임을 검증할 수 있었다.

## 참고문헌

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

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

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

[4] S. Örs, F. Gurkaynak, E. Oswald, and B. Preneel, "Power-Analysis Attack on an ASIC AES Implementation," In ITCC'04, Vol 2, pp. 546-553, IEEE Computer Society, 2004.

[5] M. L. Akkar and C. Giraud. "An Implementation of DES and AES, Secure against Some Attacks," In CHES2001, LNCS, vol. 2162, pp. 309-318, Springer-Verlag, 2001.

[6] J. D. Golic and C. Tymen. "Multiplicative masking and power analysis of AES," In CHES2002, LNCS, vol.2523, pp. 198-212, Springer-erlag, 2002.

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

[8] E. Trichina, D. D. Seta, and L. Germani. "Simplified adaptive multiplicative masking for AES," In CHES'02, LNCS 2535, pp. 187-197, Springer-Verlag, 2003.

[9] J. Blomer, J. Guajardo, and V. Krummel, "Provably secure masking of AES", in Proc. SAC'04, LNCS 3357, pp. 69-83, Springer-Verlag, 2004.

[10] E. Oswald, S. Mangard, and N. Pramstaller, and V. Rijmen, "A side-channel analysis resistant description of the AES S-box," In FSE'05, LNCS 3557, pp. 413-423, Springer-erlag, 2005.

[11] C. Clavier, J-S. Coron, and N. Dabbous. "Differential power analysis in the presence of hardware countermeasures", in Proc. CHES2000, LNCS, vol. 1965, pp. 252-263, Springer-Verlag, 2000.

[12] K. Tiri, M. Akmal and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," In ESSCIRC'02, 2002.

[13] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," In DATE'04, pp. 246-251, 2004.

[14] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic : DPA resistance without routing constraints," In CHES2005, LNCS 3659, pp. 157-171, Springer-Verlag, 2005.

[15] S. Chari, C. Jutla, J. Rao, and P. Rohatgi, "Towards Sound Approaches to Counteract Power-Analysis Attacks", "In CRYPTO'99, LNCS 1666, pp. 398-412. Springer-Verlag, 1999.

[16] T. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software," In CHES'00, LNCS 1965, pp. 238-251, Springer-Verlag, 2004.

[17] J. Waddle and D. Wagner, "Towards Efficient Second-Order Power Analysis," In CHES'04, LNCS 3156, pp. 1-15, Springer-Verlag, 2004.

[18] M. Joye, P. Paillier, and B. Schoenmakers, "On Second-Order Differential Power Analysis," In CHES'05, LNCS 3659, pp. 293-308, Springer-Verlag, 2005.

[19] E. Peeters, F.X. Standaert, N. Donckers, and J.J Quisquater, "Improved Higher Order Side-Channel Attacks with FPGA Experiments," In CHES'05, LNCS 3659, pp. 309-323, Springer-Verlag, 2005.

[20] F.X. Standaert, E. Peeters, and J.J. Quisquater, "On the Masking Countermeasure and Higher-Order Power Analysis Attacks," In ITCC'05, Vol1, pp. 562-567, IEEE Computer Society, 2005.

[21] E. Oswald, S. Mangard, C. Herbst, and S. Tillich, "Practical Second-Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers," In CT-RSA'06, LNCS 3860,

pp. 192-207, Springer-Verlag, 2006.

[22] T. Messerges, E. A. Dabbish and L. Puhl, "Method and appara- tus for preventing information leakage attacks on a micro-electronic assembly," U.S. Patent 6,295,606 B1, Sep. 2001.

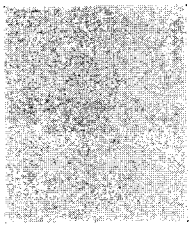
[23] E. Trichina, "Combinational logic design for AES subbyte transformation on masked data," Cryptology ePrint Archive, Report 2003/236, 2003.

[24] K. Schramm and C. Paar, "Higher order masking of the AES," In CT-RSA2006, LNCS, vol.3860, pp. 208-225, Springer-Verlag, 2006.

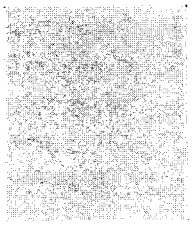
[25] P. Kocher, J. Jaffe and B.Jun, "Differential Power Analysis," In CRYPTO'99, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.

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

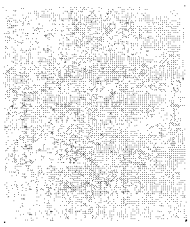
## 〈著者紹介〉



**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



**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



**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