Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.3, Jun. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.3.509

OP-Amp를 적용한 향상된 부채널 전력분석 방법*

김 진 배,[1,2†] 지 재 덕,[1] 조 종 원,[1] 김 민 구,[1] 한 동 국[2‡]
[1]한국기계전기전자시험연구원, [2]국민대학교

An Improved Side Channel Power Analysis with OP-Amp*

JinBae Kim,[1,2†] JaeDeok Ji,[1] Jong-Won Cho,[1] MinKu Kim,[1] Dong-Guk Han[2‡]
[1]Korea Testing Certification, [2]Kookmin University

요 약

전력소비를 이용한 부채널 분석은 Chip 기반의 보안디바이스의 키를 해독하는 효과적인 방법으로 알려져 있다. 기존의 전력소비정보는 저항의 직렬연결을 이용한 전압분배 방식을 사용한다. 이 방법은 디바이스에 인가되는 전압의 크기에 종속적이며. 그 크기가 작은 경우 노이즈의 영향을 크게 받아 신호 왜곡이 발생되고, 일부 신호 손실이 발생된다. 이와 같은 이유는 부채널 분석의 성능을 저하 시킨다. 본 논문에서는 OP-Amp를 이용한 전류-전압 변환방식을 적용하여 전력소비 정보를 계측함으로써 부채널 분석의 성능을 향상시킬 수 있는 방법을 제시한다. OP-Amp를 이용한 전류-전압 변환방식을 사용하여 전력소비 정보에 포함되는 노이즈의 영향을 줄일 수 있다. 따라서 부채널 분석의 성능을 향상됨을 실험을 통해 검증한다.

ABSTRACT

Side Channel Analysis of applying the power-consumption was known as effective method to analyze the key of security device based on chip. The precedential information of power-consumption was measured by the voltage distribution method using by series connection of resistor. This method was dependent on the strength of the voltage. If the voltage cannot be acquired much information which is involved with the key, the information of power-consumption significantly might be influenced by noise. If so, some of the information of power-consumption might be lost and distorted. Then, this loss can reduce the performance of the analysis. For the first time, this paper will be introduced the better way of the improvement with using the method of Current to Voltage Converter with OP-Amp. The suggested method can reduce the effect of the noise which is included in the side channel information. Therefore we can verify the result of our experiments which is provided with the improvement of the performance of side channel analysis.

Keywords: Side Channel Analysis, OP-amp, Voltage distribution, Current to Voltage converter with OP-Amp

I. 서 론

부채널 분석은 비밀정보를 포함하는 보안디바이스가 보안 알고리즘 등의 연산을 수행 하면서 발생되는 시간정보, 전력소비정보, 전자파정보 등을 이용하여 보안디바이스에 포함된 비밀정보를 분석하는 방법을 말한다.

전력소비 정보를 이용한 부채널 분석은 단순전력분석(Simple Power Analysis, SPA), 차분전력분석(Differential Power Analysis, DPA), 상관전

접수일(2015년 1월 9일), 수정일(2015년 3월 10일), 게재확정일(2015년 4월 28일)
* 본 연구는 2014년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임.(NRF-2013R1A1A2A10062137)
† 주저자, jbkim@ktc.re.kr
‡ 교신저자, christa@kookmin.ac.kr(Corresponding author)

력분석(Correlation Power Analysis, CPA) 등이 있다[1,2,3].

전력 분석(Power Analysis)방법은 디바이스에서 발생되는 전력소비정보를 통해 비밀키를 분석하므로 전력소비정보의 수집이 중요하다. 전력소비정보를 수집하는 과정에서 리더기, 계측기, 케이블 등의 장비에서 발생되는 노이즈가 포함되는데, 이러한 노이즈는 비밀키를 분석하는 것에 있어서 성능을 저해시키는 요인이 된다. 비밀정보에 대한 분석성능을 향상시키기 위해 필터를 이용한 노이즈 제거, 주파수 변환 등의 기법을 통해 수집된 전력소비정보에서 노이즈의 영향을 줄일 수 있지만, 수집된 전력소비정보에서 노이즈를 구별하기 힘들거나, 전력소비정보에서 비밀키와 관련된 정보가 노이즈 정보에 비해 상대적으로 적게 포함되어 있을 경우, 수집된 전력소비정보를 통해 비밀키가 얻어질 수 있는 분석효율을 기대하기 어렵다. 만일 전력소비정보에서 비밀키와 관련된 정보가 노이즈 정보의 영향이 미비할 정도로 포함되어 있다면 분석효율이 증가될 수 있다.

일반적으로 암호 알고리즘이 보안 디바이스에서 수행되면서 발생하는 전력신호나 전자파신호 등의 부채널 신호 수집은 저항의 직렬연결을 이용한 전압분배방식(이하 저항분압방식)을 사용하여 전위차를 생성하고, 전위차로 인한 전압 신호를 측정함으로써 이루어진다.[5] 이러한 방법은 저항의 크기가 커질수록 측정되는 부채널 신호의 크기가 커지지만, 저항값이 일정한 값보다 커지면 안정적으로 보안 디바이스가 동작할 수 없게 된다. 따라서, 저항분압방식을 사용한 방법은 저항의 값을 가변적으로 적용하여 부채널 신호를 수집하여야 하며, 한정된 저항의 값을 사용하기 때문에 일정 크기 이상의 부채널 신호를 계측 할 수 없다. 또한, 저항이 추가된 보안 디바이스에 인가되는 전압의 크기와 보안디바이스가 동작하기 위한 전압의 크기가 비슷한 경우에는 측정되는 부채널 신호의 스펙트럼이 좁아질 수밖에 없다. 부채널 신호의 스펙트럼이 좁아진다는 것은 노이즈에 더 큰 영향을 받을 수 있다는 것이며, 이로 인하여 신호 왜곡이 발생되거나, 일부 신호의 손실이 발생되어 결과적으로는 부채널 분석의 효율이 저하될 수 있다.

이러한 한계점을 개선하고자 본 논문에서는 OP-Amp를 이용한 전류-전압 변환방식을 사용하여 측정할 수 있는 전압의 범위를 증폭시켜, 노이즈 신호가 제거된 것과 같은 효율을 가지는 전력소비정보를 측정하는 방법을 제안하고자 한다.

OP-Amp는 아날로그 계산기용으로 개발되어, 증폭회로, 비교 회로 등 아날로그 전자회로에서 널리 쓰이고 있으며, 고성능 범용 증폭기이다. OP-Amp는 저항을 추가하여도 전압강하 현상이 일어나지 않은 특징을 가지기 때문에 측정 할 수 있는 전압의 범위가 증폭된다. 이러한 특징을 갖는 OP-Amp를 이용한 전류-전압 변환방식으로 전력소비정보를 수집하면, 저항분압방식을 사용한 전력정보에 비해 신호 왜곡이나 손실에 의한 비밀키 분석효율이 저하되는 문제점을 해소시킬 수 있다.

본 논문의 구성은 다음과 같다. Ⅱ장에서 저항분압방식을 통한 전력소비정보의 측정 방법을 설명하고, Ⅲ장에서 우리가 제안한 OP-Amp를 이용한 전류-전압 변환방식을 사용한 전력소비정보의 측정 방법에 대해 설명하여, OP-Amp를 이용한 전류-전압 변환방식을 사용한 방법이 기존의 저항분압방식을 통한 측정방법과 어떻게 다른지 서술한다. Ⅳ장에서는 Ⅲ장에서 설명한 OP-Amp의 특징을 실험하기 위해서 OP-Amp를 이용한 전류-전압 변환방식을 통해 수집된 파형과 저항분압방식을 통해 수집된 파형을 비교, 분석한다. 이를 통해 OP-Amp를 이용한 전류-전압 변환방식을 사용해 수집된 파형의 분석효율이 높은 것을 검증한다. 마지막 Ⅴ장에서는 실험 결과를 토대로 제시된 방법의 효용성에 대해 논한다.

Ⅱ. 저항분압방식의 계측방법

전력 정보를 이용한 부채널 분석을 수행하기 위해서는 보안디바이스에서 발생되는 전력소비정보가 필요하다. 보안디바이스에서 발생되는 전력소비정보는 전력량 P를 이용하여 측정한다. 전력량은 보안디바이스에 인가된 전압 V와 전류 I을 측정하여 다음의 옴의 법칙을 이용하여 계산할 수 있다.

$$P = V \circ I \quad (1)$$

공급되는 V는 항상 일정하기 때문에 전류 I의 변화량이 전력의 변화로 대응된다. 하지만 시간의 변화에 따른 전류의 변화를 계측하기는 어렵기 때문에 등가적으로 측정할 수 있는 추가적인 방법이 필요하다.

가장 쉽게 접근할 수 있는 방법은 키르히호프의 전압법칙을 이용하는 것이다. 보안디바이스의 전원 입력 또는 출력단에 계측을 위한 추가적인 저항을 삽입하면 키르히호프의 전압법칙에 의해 전력의 변화 즉 전류의

변화를 전압의 변화로 계측할 수 있다. 이것은 일종의 전류-전압 변환장치로 볼 수 있다. 추가된 저항을 일반적으로 가변 저항을 사용하지만 시간적인 관점에서는 고정된 값을 지니고 있다고 할 수 있다.

추가된 저항에서의 전압값을 측정하여 보안디바이스에서 사용하는 전력량을 간접적으로 계산할 수 있다. 전압값은 전류I와 저항R을 이용하여 옴의 법칙을 통해 계산할 수 있다. 옴의 법칙은 다음과 같다.

$$V = I \circ R \tag{2}$$

보안디바이스(R_1)와 추가저항 R_2가 연결된 전기회로는 Fig. 1과 같다. Fig. 1은 저항R_2의 전압을 측정하는 것을 나타낸다.

키르히호프의 전압법칙에 의해 공급되는 전압은 보안디바이스와 추가저항 부분으로 식(3)과 같이 나타낼 수 있다.

$$V = V_1 + V_2 \tag{3}$$

Fig. 1의 전기회로에 흐르는 전류I는 키르히호프의 전류법칙에 의해 저항 R_1, R_2에서 일정하므로 다음 식(4)와 같이 표현된다.

$$I = I_1 = I_2 \tag{4}$$

따라서 식(2)의 옴의 법칙을 이용하여 식(4) 변형하면 식(5)를 얻을 수 있다.

$$I = \frac{V_1}{R_1} = \frac{V_2}{R_2} \tag{5}$$

식(5)를 전압과 저항으로 표현하면 식(6)과 같이 나타낼 수 있다.

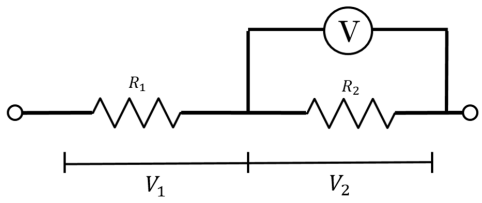


Fig. 1.Typical voltage measurement

$$R_1 = \frac{V_1}{V_2} \circ R_2 \tag{6}$$

보안디바이스는 보안알고리즘이 수행되면서 내부에서 수행되는 연산이나 데이터 등에 의해 저항 값이 달라진다. 따라서 고정된 저항값 R_2와 변화하는 저항값 R_1의 비율에 따라서 전압 V_1, V_2의 비율이 변하게 된다. 즉, 보안디바이스의 저항(R_1)이 높아지면 식(3)과 식(6)에 의해 V_1의 값이 커지고 V_2의 값이 줄어들게 된다. 이러한 전압 변화량은 Fig. 1과 같이 계측하여 전력소비량을 계산할 수 있다.

접촉식 스마트카드 표준문서인 ISO/IEC 7816-3을 보면 스마트카드의 경우 공급되는 전압에 따라 class A, class B, class C로 나누어지며, 각각의 class에서 인가 돼야 하는 전압은 $5V, 3V, 1.8V$이다. class A의 스마트카드가 정상동작하기 위해서는 $4.5V \sim 5.5V$의 전압이 인가되어야 하는데, $5V$의 전압이 인가된 경우 스마트카드에는 $4.5V \sim 5V$의 전압이 인가되어야 한다. 즉, V_2에 $0.5V$ 이상의 전압이 사용되면 스마트카드가 필요로 하는 전압이 인가되지 않아 스마트카드의 작동이 중지될 수 있다. 따라서 저항 R_2에서는 $0V \sim 0.5V$의 전압만을 계측할 수 있게 된다.

또한, ISO/IEC 7816-3에 규정된 소비전류의 최대값은 class A인 경우 $60mA$이다. 따라서 보안디바이스의 정상 동작을 위한 최소전압이 $4.5V$이므로 R_2 에 인가되는 최대 전압 $0.5V$로, 옴의 법칙을 이용하면 R_2의 크기는 약 8.333Ω 이내에서 결정해야 함을 알 수 있다.

키르히호프의 전압법칙인 식(3)식에 입력 전압을 class A, 즉, 5V로 하여 식(6)에 적용하면 식(7)을 얻을 수 있다.

$$R_1 = (\frac{5}{V_2} - 1) \times R_2 \tag{7}$$

식(7)에서 R_2는 고정된 값이므로 R_1의 변화에 의해 V_2도 반비례하여 변화됨을 알 수 있다. 이것은 동일한 소비전력의 크기변화가 기본적인 전력소비가 작은 디바이스일수록 전력소비가 큰 디바이스 보다 V_2가 작게 검출됨을 의미한다.

R_1에 대한 V_2값의 변화는 아래의 식(8)과 같이

나타낼 수 있다.

$$\frac{\Delta R_1}{\Delta V_2} = -\frac{5 \times R_2}{(V_2)^2} \tag{8}$$

이것은 저전력으로 설계된 보안 디바이스일수록 계측되는 크기가 작아진다는 것을 뜻한다.

저항분압방식을 이용하여 전력을 측정하는 방법은 R_2 의 값의 조정에 따라 보안디바이스에 인가되는 전압이 달라져, R_2 의 값에 따라 보안디바이스가 정상동작을 하지 않을 수 있으며, R_2 에 인가되는 전압의 크기 또한 특정전압 이상으로 계측하기는 힘들다. 또한, 저전력으로 설계된 보안디바이스일수록 전력의 변화에 비해 계측되는 전압의 변화가 더욱 작아진다. 이것은 전압측정에 사용되는 케이블이나 스마트카드 리더기, 계측 장비 등의 외부적인 요인에 의해 미약하지만 의미가 있는 신호가 손실되거나 왜곡될 수 있음을 추정할 수 있으며 보안디바이스에 따라 계측한계가 명확할 수밖에 없다.

III. OP-Amp를 이용한 전류-전압 변환방식

이상적인 OP-Amp는 전압 이득이 ∞, 입력 임피던스가 ∞, 출력 임피던스가 0, 주파수 대역이 ∞인 특성을 가진 것으로 정의한다. OP-Amp의 입력단 구성과 피드백 회로 구성에 따라 입력 신호가 반전되어 출력되는 반전 증폭과 반전되지 않는 비반전 증폭으로 주로 쓰인다.

Fig. 2.는 전형적인 OP-Amp의 회로구성을 나타낸 것으로 $V_+ = 0$ 이고 전압이득 $\alpha = V_{out}/V_-$ 이다. 이것을 다르게 표현하면 $V_- = V_{out}/\alpha$ 인데, 전압 이득 α가 ∞이므로 $V_- \cong 0$이 된다. 즉, 반전입력의 전위는 거의 0이 되는데, Fig. 2의 반전입력 S점을 virtual ground라고 한다.

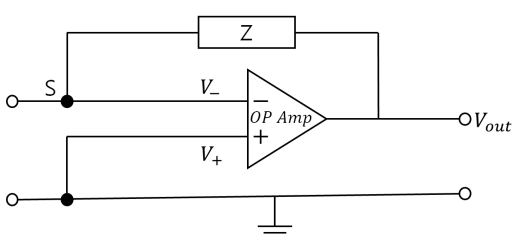


Fig. 2. Typical OP-Amp circuit

Fig. 3은 일반적인 반전 증폭회로로 OP-Amp를 통해 구성된 것이다.

Fig. 3의 전류 I_1은 키르히호프의 전류법칙에 의해 식(9)와 같다.

$$I_1 = I_S + I_2 \tag{9}$$

여기서 입력 임피던스가 ∞이므로 $I_s \cong 0$이 되고 $I_1 = I_2$ 가 되므로, 옴의 법칙을 적용하면 식(10)과 같이 나타낼 수 있다.

$$\frac{V_{in} - V_S}{R_1} = \frac{V_S - V_{out}}{R_2} \tag{10}$$

Fig. 3에서 virtual ground인 S점의 전위 $V_S \cong 0$ 이므로 식(10)을 변형하면 식(11)과 같이 된다.

$$V_{out} = -\frac{R_2}{R_1} V_{in} \tag{11}$$

식(11)을 통해 OP-Amp의 R_2와 R_1의 비에 의해 증폭도가 조절됨을 알 수 있다.

일반적으로 OP-Amp를 통해 증폭하고자 하는 신호원은 R_1 앞단에서 입력된다. R_1의 값이 없다면 증폭도가 ∞가 되기 때문에 R_2와의 비율로 증폭을 결정하기 위한 값이 정해진다. R_1 자리에 단순히 증폭도를 결정하기 위한 고정된 저항이 아닌 측정하고자 하는 보안디바이스를 위치할 경우를 생각해 볼 수 있다. 이 경우 V_{in}이 변하지 않는 고정된 값, 즉, 보안 디바이스에 공급되는 전압이고 R_1은 보안디바이스가 될 것이다. 보안디바이스의 동작에 의해 R_1는 가변적일 것이다. 따라서 전압증폭의 개념으로만 해석하기는 다소 거리가 있다.

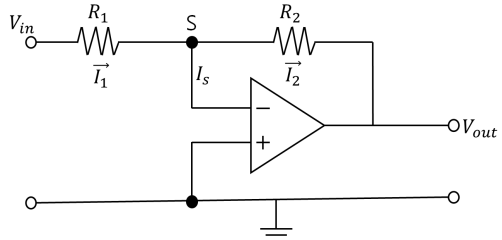


Fig. 3. Typical inverting amplifier circuit

옴의 법칙에 의해 전류 I_1은 식(12)와 같이 나타낼 수 있다.

$$I_1 = \frac{V_{in}}{R_1} \tag{12}$$

식(12)를 식(11)에 대입하면 식(13)을 얻을 수 있다.

$$V_{out} = -R_2 \circ I_1 \tag{13}$$

식(1)의 $P = V \circ I$에 의해 입력 전압이 일정하므로 전력의 변화는 곧 전류의 변화와 비례하게 되는 것을 알 수 있으며, 식(12)에 의해 R_2의 크기만큼 전류가 전압으로 반전증폭되어 출력된다는 것을 알 수 있다.

본 논문에서 제안하는 방법은 입력전압을 증폭하는 것이 아닌, OP-Amp의 반전입력단의 저항 자리에 보안디바이스를 위치시킴으로써 전류를 전압으로 변환하는 방식을 사용하였다. 아래 Fig. 4는 전체적인 전류의 흐름을 도식화 한 것이다.

Fig. 4는 본 논문에서 제안한 OP-Amp를 이용한 전류-전압 변환방식을 이용하여 보안디바이스의 전력 변화량을 계측하는 방법을 나타낸 것이다. Fig. 4와 같이 구성된 회로는 virtual ground의 특성과 R_2를 통해 전류-전압으로 변환, 반전증폭되어 계측된다. OP-Amp를 계측된 신호를 증폭하는 것에 사용한 것이 아닌 OP-Amp를 전류-전압 변환하는데 사용한 것이다.

Fig. 4에 사용되는 OP-Amp를 이용한 전류-전압 변환방식은 출력되는 전압이 반전되기 때문에 단전원 OP-Amp가 아닌 추가적으로 음전원을 생성하여 OP-Amp에 공급할 수 있는 회로를 필요로 한다. 본 실험에서는 -12V까지 보드 내에서 자체적으로 생성하여 공급할 수 있는 회로를 구성하였다. OP-Amp를 통해 출력될 수 있는 전압은 OP-Amp 칩에 공급되는

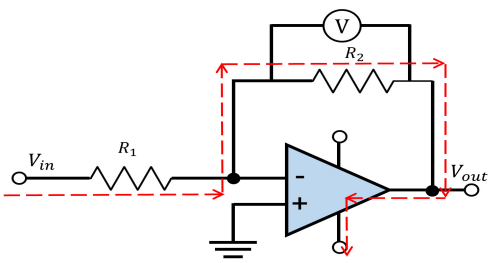


Fig. 4 Measurement by the OP-Amp converter

+전원과 -전원의 범위 내에서만 가능하다. 따라서 보다 크게 증폭된 신호를 출력하고자 한다면 사용전압 범위가 큰 OP-Amp 칩을 선택하고 공급되는 전압 또한 그에 맞게 조절하면 된다. 이상적인 OP-Amp는 전압이득, 입력임피던스가 ∞이고 출력 임피던스가 0이지만 실제 제조되고 있는 칩들은 각각 일정한 한계치를 가지고 있으며, 주파수 특성 또한 다르다. 따라서, OP-Amp의 제조사, 모델 등 해당 실험을 위해 충분한 사양을 가진 칩의 선정이 무엇 보다 중요하다고 할 수 있다. 본 실험에서는 200MHz급 ±16V 지원가능 칩을 적용했다. 하지만 OP-Amp에 공급되는 전압이 ±12V 이므로 계측 가능한 전압은 ±12V 이내이다.

본 논문에서 제안한 OP-Amp를 이용한 전류-전압 변환방식은 소비전력의 변화가 계측되는 전압으로 선형적으로 대응하여 보안디바이스의 소비전력의 크기에 따라 영향을 받지 않고 전압의 증폭도 OP-Amp에 공급되는 전압의 범위내에서 충분히 증폭시킬 수 있어 미세한 소비전력의 변화도 계측가능하고 외부적인 장비에 의한 노이즈의 영향을 거의 받지 않는다고 할 수 있다. 따라서, 기존의 계측방법보다 높은 효율의 부채널 분석 성능을 가지는 전력소비정보를 계측한다고 할 수 있다. Ⅳ에서는 OP-Amp와 기존 방법을 사용하여 계측된 파형을 분석함으로써 제안한 방법이 부채널 분석 성능을 향상시켰음을 보일 것이다.

Ⅳ. 실험 결과

4.1 실험 환경

본 장에서는 OP-Amp를 이용한 전류-전압 변환방식으로 계측한 전력소비정보와 저항분압방식으로 계측한 소비전력을 대조군으로 부채널 분석에 대한 성능을 실험하였다.

실험 환경은 ARIA 알고리즘이 포팅된 스마트카드와 스마트카드로부터 소비전력을 계측하기 위한 계측보드 계측된 파형을 디지털 정보로 변환하기 위한 Oscilloscope(LeCroy 610Zi), 변환된 파형을 수집하고 스마트카드를 동작시키기 위한 APDU를 전송하는 PC로 구성하였다.

Fig. 5의 좌측은 저항분배방식을 적용한 계측보드로 실험환경을 구성하였고, 우측은 OP-Amp를 이용한 전류-전압 변환방식을 적용한 보드로 실험 환경을 구성하였다.

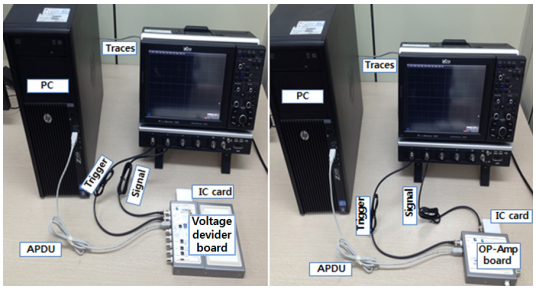


Fig. 5. Experimental environment

소비전력을 계측하기 위해 Oscilloscope의 Sampling rate를 250MS/s로 설정하였으며, 파형을 각각 20,000개씩 수집하였다. 수집된 파형은 파형에 대한 정렬과 파형압축(250MS/s → 25MS/s) 전처리 기법을 동일하게 적용하여 후처리 하였다.

4.2 SPA 실험 결과

Fig. 6과 Fig. 7은 ARIA 암호알고리즘 1 round를 수집한 것으로, Fig. 6은 저항분압방식으로 측정한 전력소비정보이고, Fig. 7은 OP-Amp를 이용한 전류-전압 변환방식으로 측정한 전력소비정보이다. Fig. 6, 7 모두 ARIA 암호알고리즘의 1 round와 1 round에서 수행되는 치환계층연산과 확산계층연산을 확인할 수 있으며, OP-Amp를 이용한 전류-전압 변환방식으로 계측된 Fig. 7의 파형이 저항분압방식으로 계측된 Fig. 6보다 ARIA 1 round 연산의 치환계층과 확산계층의 구분이 명확하다.

Fig. 8은 ARIA 암호알고리즘 1 round의 확산계층을 확대한 것으로, CPA 실험의 공격위치가 되는 부분이다.

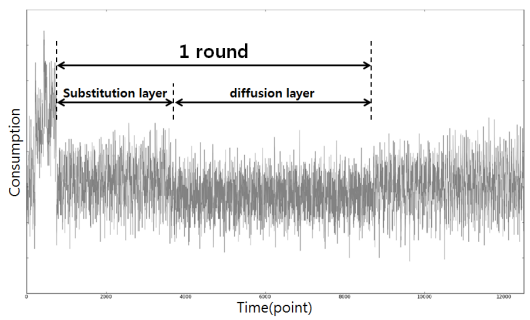


Fig. 6 The Power-consumption with resistor of the voltage-drop

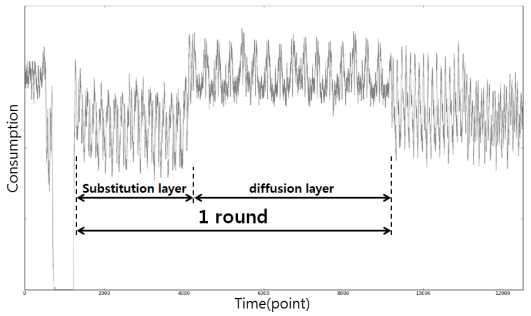


Fig. 7. The Power-consumption with OP-Amp

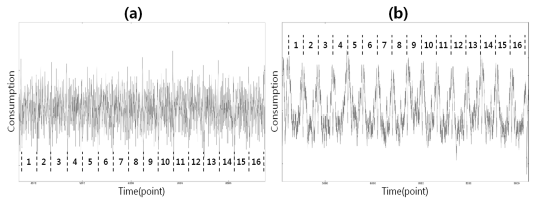


Fig. 8. Compare the Diffusion-layer

(a)는 저항분압방식으로 계측된 전력소비정보이며, (b)는 (a)와 동일한 연산 위치로 OP-Amp를 이용한 전류-전압 변환방식으로 계측된 전력소비정보이다.

Fig. 6, 7을 통해 저항분압방식과 OP-Amp를 이용한 전류-전압 변환방식을 이용한 두 가지 방법 모두 치환계층과 확산계층의 연산이 구분이 되는 것을 볼 수 있다. 하지만, Fig. 8.를 통해 (a)는 확산 계층의 16번 연산의 구분이 명확하지 않은 것을 확인할 수 있는 반면, (b)는 16번의 연산이 명확하게 구분되는 것을 확인 할 수 있다. Fig. 6, 7, 8을 통해 저항분압방식보다 OP-Amp를 이용한 전류-전압 변환방식을 사용한 방법이 파형을 더 명확하게 구분하는 것을 확인함으로써, OP-Amp를 이용한 전류-전압 변환방식을 적용한 전력소비정보에 대해 SPA 분석을 시도하는 것이 더 효율적이라고 할 수 있다.

수집된 파형의 패턴이 더 명확하게 구분되어 SPA 분석에 더 효율적이라는 것은 부채널 분석에 소비되는 시간, 데이터 등 자원에 대한 소비를 감소시킬 수 있다는 것을 말한다.

4.3 CPA 실험결과

Table. 1은 OP-Amp를 이용한 전류-전압 변환방식과 저항분압방식을 사용한 파형을 실험환경에 따라 각 20,000개씩 수집하여 CPA분석을 수행한 것이다.

Table. 1. Compare the result

Right Key	Voltage Divider		OP-Amp Converter	
	Key	ratio	Key	ratio
1st 0xD4	0x35	0.86	0xD4	1.50
2nd 0x15	0x15	1.05	0x15	2.59
3rd 0xA7	0x36	0.99	0xA7	1.44
4th 0x5C	0xDF	0.88	0x5C	1.56
5th 0x79	0x4F	0.88	0x79	1.80
6th 0x4B	0x4B	1.14	0x4B	1.90
7th 0x85	0x47	0.91	0x85	1.74
8th 0xC5	0x3B	0.82	0xC5	1.85
9th 0xE0	0x36	0.75	0xE0	1.65
10th 0xD2	0xD2	1.17	0xD2	1.53
11th 0xA0	0xF0	0.98	0xA0	1.97
12th 0xB3	0xB3	1.04	0xB3	1.80
13th 0xCB	0x96	0.95	0xCB	1.55
14th 0x79	0x62	0.78	0x79	1.71
15th 0x3B	0x3B	1.17	0x3B	1.12
16th 0xF6	0xF6	1.03	0xF6	1.57

CPA 분석지점은 ARIA 암호알고리즘 1 Round 치환계층의 출력값을 대상으로 하였다.

Table. 1에서 'Right Key' 값은 ARIA 1 Round의 치환계층에서 사용되는 16개의 부분키이며, 'ratio'는 실제 Right Key와 Right Key를 제외하고 상관계수가 가장 높게 나온 Guessing key의 상관계수 값의 비율이다.

저항분압방식과 OP-Amp를 이용한 전류-전압 변환방식의 Key에 해당하는 값은 분석 결과 키로 추정되는 값을 나타낸 것으로, ratio가 1을 초과하게 된다면 키를 분석한 것이라 할 수 있다. Table. 1에서 키가 분석된 경우 회색으로 채색하여 표시하였다.

저항분압방식으로 수집된 전력소비정보에 대한 CPA 결과를 보면 16개의 ARIA 1 Round 부분키 중에서 6개의 키만을 분석해 낼 수 있었다. 반면, 본 논문에서 제안한 OP-Amp를 이용한 전류-전압 변환방식을 적용하여 수집한 전력소비정보에 대한 CPA 결과를 보면, 16개의 키 모두 분석에 성공하였다.

15번째 Key의 경우 저항분압방식이 OP-Amp를 이용한 전류-전압 변환방식보다 높은 ratio를 가진다. 이것은 Table. 1에서 저항분압방식 분석결과에서 Key에 대한 ratio가 가장 높은 것이 10번째, 15번째 Key로 1.17이고 가장 낮은 것이 9번째 Key로 0.75 이듯이, OP-Amp를 이용한 전류-전압 변환방식에서는 가장 높은 ratio가 2번째 Key로 2.59이고 가장 낮은 것이 15번째 Key로 1.12이다. 즉, 저항분압방식에서 분석된 Key 중 가장 높은 ratio가 나온 부분과 OP-Amp를 이용한 전류-전압 변환방식에서 분석된 Key 중 가장 낮은 ratio가 비교된 것이다. 같은 스마트카드로 실험하였지만 계측방법이 다르기 때문에 다른 시간 위치에서 최대, 최소의 ratio가 나온 것이다. Fig. 9는 15번째 키의 분석을 명확하게 보이기 위해 15번째 키의 상관계수값을 나타낸 그림이다.

Fig. 9는 저항분압방식(a)과 OP-Amp를 이용한 전류-전압 변환방식(b)의 적용으로 수집된 파형에 대해 15번째 Key를 분석한 것으로, 0x00 ~ 0xFF까지의 Guessing key가 중간값으로 사용되어 얻어진 상관계수값을 그림으로 나타낸 것이다. (a)와 (b)에서 가장 높은 상관계수 값을 가지는 Guessing key는 0x3B로 Right Key가 분석된 것을 확인할 수 있다. (a)에서 0x3B의 상관계수는 0.0399이며, (b)에서 0x3B의 상관계수는 0.0452로 (b)에서 얻어진 상관계수가 높은 것을 확인할 수 있다. ratio의 경우 Right Key를 제외한 가장 높은 상관계수를 가지는 Guessing key에 의해 값의 차이가 있을 수 있기 때문에 15번째 Key와 같이 Right Key의 상관계수가 높음에도 Ratio가 낮게 나오는 경우가 발생하게 된다.

Fig. 10은 Table. 1에서 보인 두 방식의 차이를 사용된 파형수에 따라 나타낸 것으로 100개의 파형부터 20,000개의 파형까지 100개 단위로 키를 분석한 결과를 나타낸 것이다. 가로 축은 분석에 사용한 파형의 개수를, 세로축은 Right Key를 찾아낸 개수를 표시하였다. (a)는 저항분압방식으로 계측된 파형을 분석한 결과를 나타낸 그래프이고, (b)는 OP-Amp를 이용한 전류-전압 변환방식으로 계측된 파형을 분석한

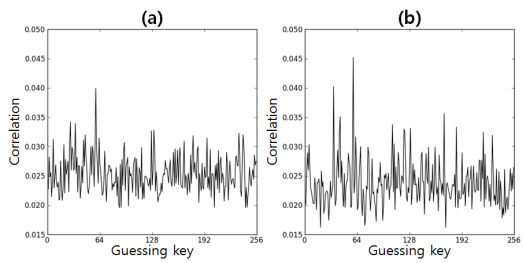


Fig. 9. 15th key analysis

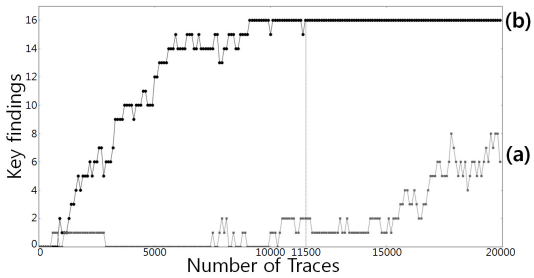


Fig. 10. Compare the Key findings

결과를 나타낸 그래프이다. Fig. 10에서 (b)는 11,500개의 파형부터 16개의 키를 모두 찾은 것을 확인할 수 있다. 반면, (a)는 11,500개의 파형에서 1개의 키만을 분석했으며, 20,000개까지 파형을 사용함에도 최대 8개의 키만이 분석된 것을 확인할 수 있다.

V. 결 론

본 논문에서는 OP-Amp를 이용한 전류-전압 변환방식을 적용하여 보안디바이스에서 소비되는 전력정보를 측정하는 방법을 소개 하였다. OP-Amp를 이용한 전류-전압 변환방식은 기존의 전압강하 방법을 사용하여 수집된 정보에 대한 부채널 분석보다 성능이 향상된다는 것을 실험을 통해 확인할 수 있었다. OP-Amp를 이용한 전류-전압 변환방식은 전압을 증폭시켜 저항분압방식 보다 전력 신호의 왜곡이나 손실 등에 영향을 덜 받으며, 전력 분석인 SPA와 CPA의 성능을 향상시키는 것 또한 확인할 수 있었다.

OP-Amp를 이용한 전류-전압 변환방식이 적용된 계측장비를 통해 파형을 수집하는 것은 기존의 방법보다 더 향상된 결과를 가져올 수 있다는 것을 확인한 것이며, 이는 전력분석 공격에 대한 전반적인 분석효율의 향상을 기대할 수 있다고 생각된다.

향후, ARIA만이 아닌 공개키 알고리즘 등 다양한 암호 알고리즘의 분석과 대응법이 적용된 알고리즘에 대해서도 OP-Amp를 이용한 전류-전압 변환방식이 적용된 계측장비의 효율을 연구할 것이다.

References

[1] E.Brier, C.Clavier, and F.Olivier, "Correlation power analysis whit a leakage model", CHES 2004, LNCS 3156, pp16-29, 2004.

[2] P.Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," CRYPTO 96, LNCS 1109, pp. 104-113, 1996.

[3] P.Kocher, J.Jaffe, and B.Jun, "Differential power analysis", CRYPTO 1999, LNCS 1666, pp. 388-397, 1999.

[4] JinBae Kim, JaeDeok Ji, Jong-Won Cho, MinKu Kim and Dong-Guk Han, "An Improved Side Channel Power Analysis with OP-Amp," CISC-S'14, pp. 105, June. 2014.

[5] YongJe Choi, DooHo Choi, JeaCheol Ryou, "Implementing Side Channel Analysis Evaluation Boards of KLA-SCARF system," Journal of The Korea Institute of Information Security & Cryptology, 24(1), pp. 229-240, Feb. 2014.

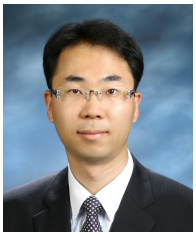
〈저자소개〉

김 진 배 (Jinbae Kim) 정회원
2002년 2월: 경희대학교 전자공학과 졸업
2014년 3월~현재: 국민대학교 일반대학원 석박사 통합과정
2002년 4월~2011년 8월:(주)듀얼아이 책임연구원
2011년 10월~현재: 한국기계전기전자시험연구원 선임연구원
〈관심분야〉 정보보호, 부채널 분석, IoT 정보보호 기술

지 재 덕 (Jae-Deok Ji) 정회원
1996년 2월: 고려대학교 금속공학과 졸업
1998년 2월: 고려대학교 금속공학과 석사
2012년 8월: 고려대학교 정보보호대학원 박사
2000년 9월 ~2006년 12월: 포스데이타 기술연구원 선임연구원
2007년 1월 ~2011년 10월: 한국인터넷진흥원 보안성평가팀 책임연구원
2011년 11월~현재: 한국기계전기전자시험연구원 정보보안평가팀 팀장
〈관심분야〉 부채널 분석, 광학 및 전자기파 오류주입 공격, IoT 정보보호 기술

조 종 원 (Jong-Won Cho) 정회원
2010년 2월: 국민대학교 수학과 졸업
2012년 2월: 국민대학교 일반대학원 수학과 석사
2014년 3월~현재: 한국기계전기전자시험연구원 연구원
〈관심분야〉 부채널 분석, IoT 정보보호 기술,

김 민 구 (Minku Kim) 정회원
2011년 2월: 국민대학교 수학과 졸업
2013년 2월: 국민대학교 일반대학원 수학과 석사
2014년 3월~현재: 한국기계전기전자시험연구원 연구원
〈관심분야〉 부채널 분석, IoT 정보보호 기술, 프라이버시 보호



한 동 국 (Dong-Guk Han) 종신회원
1999년 2월: 고려대학교 수학과 졸업
2002년 2월: 고려대학교 수학과 석사
2005년 2월: 고려대학교 정보보호대학원 박사
2004년 4월~2005년 4월: 일본 Kyushu Univ. 방문연구원
2005년 4월~2006년 4월: 일본 Future Univ.-Hakodate Post.Doc.
2006년 6월~2009년 2월: 한국전자통신연구원 정보보호연구단 선임연구원
2009년 3월~현재: 국민대학교 수학과 부교수
〈관심분야〉 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석 및 대응법 설계, IoT 정보보호 기술