THE JOURNAL OF KOREAN INSTITUTE OF ELECTROMAGNETIC ENGINEERING AND SCIENCE. 2024 July; 35(7), 585～594.

http://dx.doi.org/10.5515/KJKIEES.2024.35.7.585
ISSN 1226-3133 (Print) · ISSN 2288-226X (Online)

암호 회로로부터 방출된 전자파 평가를 통한 오류 주입 위치 탐색

Finding Fault Injection Location via Evaluation of Electromagnetic Emission from Cryptographic ICs

최건희 · 김주환 · 한재승 · 한동국*

Keon-Hee Choi · Ju-Hwan Kim · Jaesueng Han · Dong-Guk Han*

요 약

전자파 오류 주입은 의도한 오류를 유발하기 위해 타이밍, 세기, 위치 등의 파라미터를 찾아야 한다. 기존에는 반복적인 전자파 오류 주입 실험을 통해 의도한 오류가 발생하는 파라미터를 찾아왔다. 하지만 이것은 상당한 시간을 요구하며 실험 중 발생하는 영구적 결함에 대비한 다수의 대상 기기가 필요하다. 본 논문은 대상 알고리즘이 동작할 때 방출되는 전자파로부터 취약한 회로의 위치를 파악하고, 전자파 오류 주입에 대한 관계성을 분석한다. 제안하는 기법은 세 종류의 공격자 가정에서 적용 가능한 기법이며, 각각은 암호에 의존한 전자파 강도 차분 분석, 전력과 전자파의 상관성 분석, 전자파와 암호 중간값의 상관성 분석이다. 검증 결과 제안한 모든 기법은 일관되게 칩의 특정 영역을 주요 위치로 식별하였다. 실제 전자파 오류 주입의 타이밍, 세기의 파라미터를 변경한 다수의 실험 결과도 동일한 영역이 취약함을 보여 제안한 기법의 타당성을 증명했다. 본 논문에서 제안하는 기법은 XMEGA128D4 대상 실험을 통해 칩의 최소 75 %의 영역을 전자파 오류 주입 위치 탐색에서 제거할 수 있음을 실험을 통해 증명하였다.

Abstract

EM(Electromagnetic) fault injection requires finding parameters such as timing, intensity, and location to cause the intended fault. Previously, iterative EM fault-injection experiments were conducted to determine the parameters that cause the intended error. However, this is time consuming and requires the replacement of several target devices owing to permanent faults during the experiment. This study identifies the location of vulnerable circuits from the EM emitted when the target algorithm is operating and analyzes their relationship with the EM fault injection. The proposed methods apply to three different attacker assumptions: differential analysis of the EM intensity, correlation analysis of the power and EM, and correlation analysis of the EM and the intermediate value of the cipher. In our validation, all the proposed methods consistently identified a specific region of the chip as the key location. The results of several experiments in which the timing and intensity parameters of the actual EM fault injection are changed also indicate the vulnerability of the same region, proving the validity of the proposed method. The methods proposed in this study are experimentally proven to exclude at least 75% of the chip area from the EM fault injection location searches through experiments conducted on XMEGA128D4.

Key words: Cryptography, Side Channel Analysis, Fault Injection, EMC

「이 논문은 2022년 정부(방위사업청)의 재원으로 국방기술진흥연구소의 지원을 받아 수행된 연구임(KRIT-CT-23-005).」

국민대학교 금융정보보안학과(Department of Financial Information Security, Kookmin University)

*국민대학교 정보보안암호수학과(Department of Information Security, Cryptology, and Mathematics, Kookmin University)

· Manuscript received June 27, 2024 ; Revised July 8, 2024 ; Accepted July 17, 2024. (ID No. 20240627-059)

· Corresponding Author: Dong-Guk Han (e-mail: christa@kookmin.ac.kr)

Ⅰ. 서 론

부채널 분석은 대상 기기에서 암호 알고리즘이 동작할 때 발생하는 부채널 정보(소비 전력, 방출 전자파, 연산 시간 등)를 활용하여 비밀 정보를 복구하는 공격 방법이다[1]. 부채널 분석에는 비침입 공격과 준침입 공격이 있다. 비침입 공격이란 동작하는 대상 기기에서 누출되는 정보를 이용해서 비밀 정보를 분석하는 방법이다[2]. 준침입 공격이란 대상 기기에 전자파, 레이저 등의 신호원을 통해 오류를 유도해서 비밀 정보를 분석하는 방법이다[3]. 전자파 오류 주입 공격이란 정상 동작을 수행하는 칩 표면의 국소적인 부위에 전자파 펄스(pulse)를 발생시켜 오류를 유도하고 이를 통해 비밀 정보를 분석하는 방법이다. 비밀 정보를 획득하기 위해서는 분석 논리에 맞는 의도한 오류를 유도할 수 있어야만 한다. 전자파 오류 주입을 수행하기 위해서는 타이밍, 세기, 위치 등의 파라미터를 고려해야 한다. 이를테면 오류를 유발하는 타이밍을 정확하게 선정해야 하고, 회로의 동작을 방해시킬 수 있으면서 고장을 피할 수 있는 세기를 찾아야 한다. 즉, 각각의 최적의 파라미터를 찾아야 의도한 오류를 유발할 수 있다.

오늘날 오류 주입 파라미터를 효율적으로 탐색하기 위한 연구가 활발히 수행되고 있다. 국소적인 위치를 찾기 위해 칩의 모든 부분을 스캔하면서 의도한 오류가 발생하는 위치를 탐색해 왔다[4]. 또한 주된 영역을 식별하고 해당 영역을 대상으로 영역을 좁혀 반복적인 실험을 통해 오류 발생 여부를 파악하는 방식의 연구가 수행되었다[5]. 이를 자동화하기 위해서 타이밍, 세기, 위치 변화에 따라 발생하는 오류를 평가하는 모델을 통해 최적의 파라미터를 찾는 방안이 연구되었다[6]. 하지만 전자파 오류 주입만을 이용해서 파라미터를 탐색하는 것은 반복적인 실험을 수행하며 이는 상당한 시간과 영구적 결함을 대비한 다수의 대상 기기 확보를 요구한다. 전자파 방출 세기와 열 방출 세기를 통해 위치 탐색을 시도한 연구가 있다[7]. 하지만 이때 전자파의 단순 세기만 관측했으며, 이는 전자파 자체에 대한 분석으로 볼 수 없다. 한편, 방출 전자파의 취약한 위치를 탐색하는 연구가 수행되었다[8],[9]. 하지만 이는 전자파 오류 주입과의 관련성을 보이지 않았다.

기존 연구에서는 반복적인 전자파 오류 주입을 통해 최적화된 파라미터 탐색을 시도하였으며, 이는 대상 기기의 영구적인 결함을 일으킬 수 있고 이에 따라 다수의 대상 기기를 요구한다. 또한 실험에 있어서 상당한 시간을 요구한다. 본 논문에서는 전자파 오류 주입만을 이용해 최적화된 3차원 파라미터를 탐색할 때 필요한 시도 횟수를 식으로 보인다. 본 논문은 방출 전자파를 이용해 전자파 오류 주입의 위치 파라미터를 탐색하는 방안을 제안한다. 이는 대상 기기에 영구적인 결함을 일으키지 않으며 비교적 빠른 시간 내에 주요 위치를 탐색할 수 있다. 또한 주요 위치를 식별한 상태에서 2차원 파라미터만을 탐색하는 전자파 오류 주입은 수 시간의 실험 시간을 단축할 수 있다.

본 논문에서는 전자파 오류 주입을 통한 비밀 정보 분석을 수행하며, 이를 위해서 현실적으로 사용 가능한 암호 칩의 취약한 위치 탐색 방법을 제안한다. 현실적인 전자파 오류 주입은 다양한 환경에서 수행될 수 있다. 본 논문에서는 다음의 세 종류의 공격자 모델을 가정하며 각각이 적용 가능한 탐색 방안을 제안한다. 첫 번째는 동작하는 암호를 모르지만 방출 전자파를 수집할 수 있는 공격자이다. 해당 공격자는 암호에 의존한 전자파 강도 차분 분석을 적용 가능하다. 두 번째는 첫번째 공격자 가정에 추가적으로 소비전력을 측정할 수 있는 공격자이다. 해당 공격자는 전력과 전자파의 상관분석이 가능하다. 세 번째는 동작하는 암호를 알고 방출 전자파를 수집할 수 있는 공격자이다. 해당 공격자는 전자파와 암호 중간값의 상관 분석이 가능하다.

본 논문은 XMEGA128D4 대상 실험을 통해 제안한 세 가지의 방법이 칩의 취약한 회로의 위치를 일관되게 탐색함을 보였다. 또한 전자파 오류 주입을 수행하여 해당 위치가 실제 오류 주입에 취약한 위치임을 밝혔다. 특히, 해당 위치는 전자파 오류 주입 파라미터를 다양하게 조정하여 실험하였음에도 공통되게 취약한 위치임을 보였다. 세 가지의 기법은 일관되게 칩의 특정 영역을 식별하고, 이는 오류 주입에 취약한 위치 탐색에 있어 75 % 이상의 위치를 제거할 수 있음을 보인다.

Ⅱ. 비밀 정보 분석

본 절에서는 방출 전자파를 통한 비밀 정보 분석 방법과 전자파 오류 주입을 통한 비밀 정보 분석 방법을 다룬다.

2-1 전자파 오류 주입

전자파 오류 주입을 통한 비밀 정보 분석[3]은 의도한 오류가 발생하였을 때 비밀 정보를 분석하는 논리와 의도한 오류를 발생시키는 검증 실험으로 나눌 수 있다. 본 장에서는 분석 논리를 설명하고 검증 실험에 있어서 한계점을 설명한다.

2-1-1 비밀 키 분석 논리

DFA(differential fault analysis)는 오류 암호문을 유도하여 정상 암호문과의 차분을 이용하여 비밀 정보를 분석한다. 본 논문에서는 AES 대상 DFA를 수행한다. 그림 1은 AES-128(advanced encryption standard)[10]암호 알고리즘이다.

AES는 전체 10라운드로 구성되며 한 라운드는 AddRoundKey, SubBytes, ShiftRows, MixColumns로 구성된다. 단, 마지막 라운드에는 MixColumns이 제외된다. 오류 주입은 9라운드 MixColumns 입력 값의 1 Byte를 변화시켜

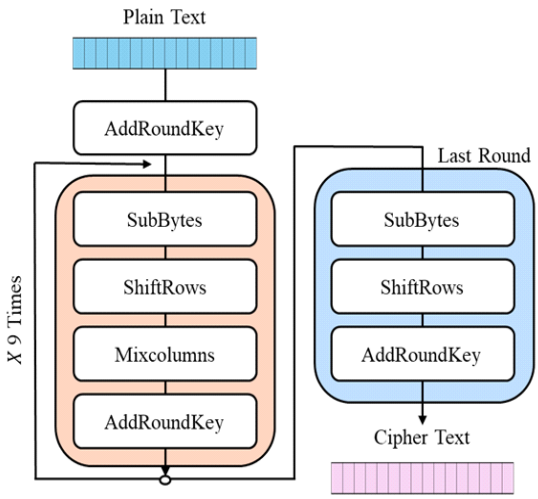


그림 1. AES-128 구조
Fig. 1. AES-128 structure.

오류 암호문을 획득하고 정상 암호문과의 차분을 통해 비밀 값을 복구한다[3]. 단 AES의 구조적 특성으로 Mixcolumns의 입력 값은 9라운드의 SubBytes의 출력 값으로 계산할 수 있다. 즉, SubBytes 연산의 1 Byte를 변화시켜도 동일하게 키 복구 논리를 적용 가능하다.

2-1-2 전자파 오류 주입 제한성

의도한 오류를 유발하기 위해서는 위치, 타이밍, 세기 등 파라미터를 조정해서 최적의 파라미터를 탐색해야만 한다. 기존 연구는 이러한 파라미터의 전수조사를 통해 조정하였고[3],[4], 이는 시간과 비용 측면에서 현실적이지 못한 제한이 있다. 전자파 오류 주입의 최적 파라미터를 전수조사를 통해 탐색하기 위한 시도 횟수는 식 (1)이다. 위치 탐색 횟수는 $N_{row} \times N_{col}$회의 탐색이 필요하다. 이때의 N_{row}는 분할한 칩의 행의 개수, N_{col}은 열의 개수를 의미한다. 의도한 오류가 발생하는 최적의 강도를 찾기 위해서는 $V_{max} - V_{min} + 1$회의 탐색이 필요하다. 이때의 V_{min}은 전자파 오류 주입 기기가 인가 가능한 최소 세기를 의미하고, V_{max}는 최대 세기를 의미한다. 의도한 오류가 발생 가능한 최적의 시간은 최대 $T_{max} - T_{min} + 1$회 탐색해야만 한다. 이때의 T_{min}은 공격 대상 함수의 시작 시점을 의미하고 T_{max}는 종료 시점을 의미한다. 즉, 오류가 발생하는 최적의 위치, 타이밍, 세기 파라미터를 찾기 위해 최대 횟수 NS는 식 (1)과 같다.

$$NS = (N_{row} \times N_{col}) \times (V_{max} - V_{min} + 1) \times (T_{max} - T_{min} + 1) \quad (1)$$

즉, 최적의 파라미터를 찾기 위해 방대한 시간이 요구되며 이를 개선할 연구가 필요하다.

2-2 상관 전자파 분석

CEMA(correlation electromagnetic analysis)[2]는 동작하는 암호 알고리즘을 알고 있을 때 방출 전자파의 비밀 정보 분석을 통해 수집된 신호에 포함된 암호의 정보량을 평가할 수 있다. 본 장에서는 상관 전자파 분석 방법과 그것의 변형을 설명한다. 이때의 전자파는 소비되는 전력 신호에 비례한다.

2-2-1 Hamming Weight 모델

암호 알고리즘이 동작할 때 소비되는 전력량 P는 연산되는 데이터를 이진수로 나타냈을 때의 1의 개수인 $HW(data)$와 비례한다[1]. 즉, 연산에 필요한 전체 전력량을 다음과 같이 나타낼 수 있다. 이때의 ε은 정보량 상수이고 P_{noise}는 잡음을 의미한다.

$$P_{\text{total}} = \varepsilon \cdot HW(\text{data}) + P_{\text{noise}} \tag{2}$$

2-2-2 피어슨 상관계수

피어슨 상관계수는 두 집합 간의 선형적인 관계를 평가하는 지표이다. n개의 샘플로 이루어진 두 집합 X, Y에 대하여 공분산과 표준편차를 이용해 상관계수 값 $corr_{XY}$를 계산한다. 식의 $\overline{X}, \overline{Y}$는 각각의 평균을 의미한다.

$$corr_{XY} = \frac{\sum_{i}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i}^{n}(X_i - \overline{X})^2}\sqrt{\sum_{i}^{n}(Y_i - \overline{Y})^2}} \tag{3}$$

2-2-3 상관 전자파 분석 및 변형

CEMA는 암호 알고리즘이 동작할 때 발생하는 전자파를 이용해서 비밀 정보인 키를 획득하는 방법이다. 식 (2)의 원리를 이용하여 알고 있는 데이터 정보와 추정하는 비밀 정보의 결합을 통해 생성한 중간값 집합 G_n과 동작 시간에 따른 세기를 n개 점으로 나타낸 m개의 집합 간의 상관도를 식 (3)을 통해 분석한다. 즉, 다음과 같은 절차를 통해 분석을 수행한다.

- 단계 1. i번째 비밀 정보 추정값에 대해 m개의 G_m^i 집합 생성
- 단계 2. n개의 점 중 j번째 점에 대한 m개의 실제 방출 전자파 세기 T_m^j 집합 저장
- 단계 3. $corr^j_{G_m^i, T_m^j}$ 계산
- 단계 4. n개의 점에 대해 반복 수행을 통해 최대 $corr^{max}_{G_m^i, T_m^{max}}$값을 계산하고 이를 G_m^i 을 나타내는 대푯값으로 지정
- 단계 5. 모든 추정 비밀 값에 대한 대푯값을 계산하고 이때의 가장 큰 상관계수를 갖는 추정값을 비밀키로 판단

CEMA를 변형하여 전력과 전자파 신호 간의 상관도를 분석할 수 있다. 분석은 n개의 점으로 이루어진 전력 파형을 T_m^{EL}이라 하고 전자파 파형을 T_m^{EM}이라 정의하면 위와 같이 각각의 시점에 대해 상관계수를 계산하고 전체 n번 반복하여 대푯값을 설정하여 수행할 수 있다. 이는 식 (2)에서 말한 AES에 대한 소비 전력의 변화를 기준으로 전자파 방출량의 변화의 상관도를 평가한다.

Ⅲ. 방출 전자파 기반 오류 주입 위치 탐색 기법

본 논문에서 제안하는 방법은 암호 동작 시 칩에서 방출되는 전자파 분석만을 통해 오류 주입 위치를 탐색한다. 이는 오류 주입만을 이용한 파라미터 탐색 대비 칩의 물리적 결함 가능성을 제거하고 소요 시간을 감소시킨다. 또한 현실적인 세 가지의 공격자 가정을 고려하여 제안하는 방법의 실효성을 보인다.

3-1 암호에 의존한 전자파 강도 차분 분석

기존에는[7] 암호 알고리즘이 동작할 때 강하게 발생하는 전자파 방출 위치를 대상으로 전자파 오류 주입을 시도하였다. 하지만 칩의 내부 회로 설계에 따라 암호 동작과 관계성이 낮은 영역이 전자파 방출이 많은 부근일 수 있다. 본 논문에서는 암호 동작 이전에 전자파 방출의 세기를 분석하고 암호 동작 시 전자파 방출 세기의 변화를 관찰한다. 이를 통해 암호 알고리즘이 동작하는 정보를 누출하는 취약한 위치를 식별한다.

3-2 전력과 전자파의 상관 분석

전자파 신호는 암호 알고리즘이 동작할 때 소비되는 전력과 비례한다. 즉, 암호 알고리즘의 동작 정보를 누출시키는 취약한 회로의 위치에서는 소비 전력과 유사한 전자파 신호의 관측이 가능하다. 만일 암호 알고리즘이 동작할 때 소비되는 전력을 측정할 수 있다면, 식 (3)을

이용한 CEMA의 변형을 통해 전력을 기준으로 전자파 신호를 평가할 수 있다. 본 논문에서는 위치별 전자파 신호와 소비 전력 신호와의 상관 분석을 통해 주요 위치를 식별한다.

3-3 전자파와 암호 중간값의 상관 분석

전자파 오류 주입을 수행하는 환경에 따라 소비전력을 수집하는 것이 용이하지 않을 수 있다. 본 논문은 전자파만을 분석하여 전자파 오류 주입에 취약한 위치를 탐색하는 방안을 제안한다. 데이터에 의존된 전자파 방출량의 변화량을 분석하는 CEMA는 옳은 키에 대한 상관계수를 계산하여 주요 위치를 식별할 수 있다. 하지만 이는 동작하는 알고리즘을 알고 중간값을 계산할 수 있어야 한다.

Ⅳ. 검증 실험

4-1 실험 환경

본 장은 실험에서 사용되는 AES 동작 여부에 따른 전자파 방출 수집 환경과 전자파 오류 주입 실험 환경을 다룬다. 실험은 칩의 표면을 10×10으로 나누어 수행된다.

4-1-1 전자파 수집 환경

전자파 신호는 AES가 동작하기 이전을 수집하고 AES가 동작할 때의 신호를 수집한다. 그림 2는 NewAE Technology 사의 CW308 UFO 보드에 탑재된 XMEGA128D4에서 AES가 동작할 때 방출되는 전자파를 CW-Lite (Chipwhisperer-Lite)를 통해 수집하였다. 이때 CW308 UFO보드는 부채널 분석에 용이하게 제작된 검증 보드이다. 또한 오른쪽 하단은 XMEGA128D4칩을 10×10으로 분할한 것을 확대한 그림이다. Chipwhisperer-Lite의 scope 변수에 대한 설정은 표 1이다. 이때의 scope.gain.db, scope.gain.gain은 기기의 저잡음 증폭기의 gain에 대한 파라미터이다. 또한 사용한 프로브는 EMV-Technik사의 LF B-3이며 증폭기는 Amplifier PA303을 사용했다.

4-1-2 전자파 오류 주입 환경

그림 3은 전자파 오류 주입 환경이다. Riscure[11]사의

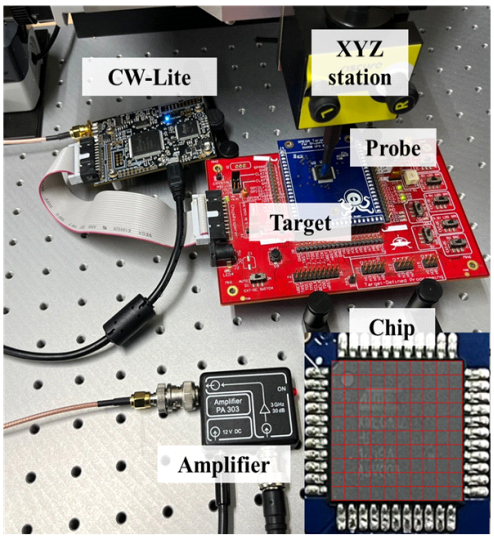


그림 2. 방출 전자파 수집 환경
Fig. 2. EM emission acquisition environment.

표 1. Chipwhisperer-lite 주요 파라미터
Table 1. Chipwhisperer-lite main parameters.

Clock frequency	7.38 MHz
Sampling rate	4-points per 1-clock
scope.gain.db	49.97
scope.gain.gain	69

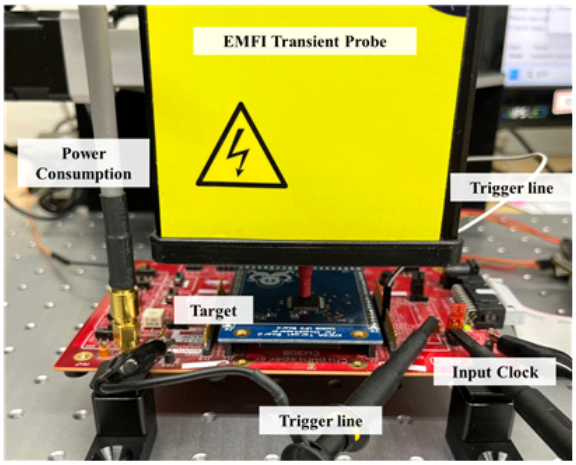
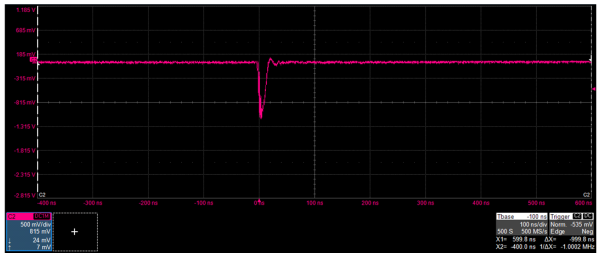
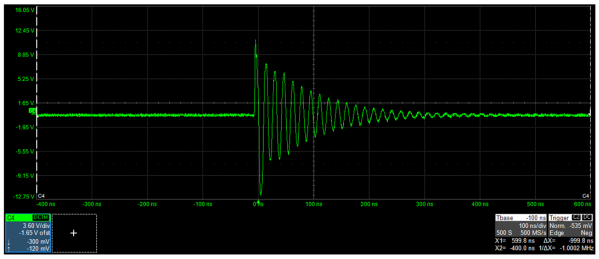


그림 3. 전자파 오류 주입 환경
Fig. 3. EM fault injection enviroment.

EMFI Transient Probe를 이용하여 펄스 신호를 Atmel XMEGA128D4에 주입한다. 또한 실험에서는 트리거 신



(a) 전류 관측
(a) Current monitor



(b) 방사 전자파 측정
(b) EM emission measurement

그림 4. 전자파 오류 주입 펄스 신호
Fig. 4. EM fault injection pulse signal.

호, 입력 clock, 주입 신호 등을 모니터링하기 위해 Oscilloscope WaveRunner 9000을 사용하였다.

이때 EMFI Transient Probe의 위치를 XYZ station으로 조정했다. 기기의 최대 방출 전압 V_{max}는 450 V이고, V_{min}은 24 V이다. 전자파 세기는 이에 비례하는 비율로 표기한다. 그림 4는 전자파 오류 주입에 사용되는 펄스 신호이다. 대상 기기는 암호 알고리즘이 동작할 때 발생하는 트리거를 통해 설정한 타이밍에 펄스를 발생시켜 오류를 유발한다.

4-2 검증 실험

본 장은 앞서 제안한 세 가지 방식에 대해 실험을 수행하였으며, 세 가지 모두 일관되게 칩의 특정 위치를 주요 위치로 식별하였다.

4-2-1 암호에 의존한 전자파 강도 차분 분석

본 논문에서는 AES의 동작을 정의하기 위해 칩을 제어하는 프로토콜을 조사하였다. 프로토콜은 3단계로 정의할 수 있다. 표 2는 초기 설정 과정, AES 코드를 Bootloader를 통해서 포팅하는 과정, AES 암호를 동작시키는 과정이다.

표 2. 제어 PC와 대상간의 프로토콜 정의
Table 2. Definition of the protocol between the control PC and the target.

Command	Contents
1. Setup	UART communication and digital clock manager (DCM) settings, etc.
2. Bootloader	Porting a target algorithm to a chip with Bootloader
3. AES Run	AES operation

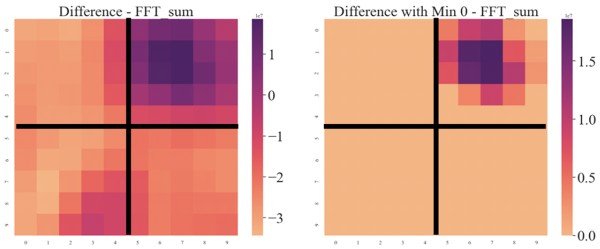
본 논문은 Bootloader 명령 이후를 암호 동작 이전으로 정의하였다. 이를 통해 암호 동작 이전 전자파 방출 세기와 암호 동작 시 전자파 방출 세기의 차이를 통해 전자파 오류 주입 영역을 식별할 수 있음을 실험을 통해 증명했다.

그림 5의 왼쪽은 위치별 암호 동작 이전 전자파 방출 세기와 암호 동작 시 전자파 방출 세기의 차이를 보이고, 오른쪽은 해당 결과에서 음수를 0으로 처리한 결과를 나타낸다. 이때의 차이는 암호 동작 시 방출되는 전자파와 암호 동작 시 방출되는 전자파의 위치별 대푯값의 차이를 의미한다. 대푯값을 나타내는 방법은 다음과 같다. 그림 5(a)는 FFT 변환한 신호를 대상으로 전체 주파수 대역의 모든 강도의 합을 이용한 방법이고, 그림 5(b)는 원신호를 대상으로 가장 강한 세기를 이용한 방법이고, 그림 5(c)는 절댓값이 적용된 원신호의 가장 강한 세기를 이용한 방법이다. 제안한 방법은 일관되게 칩을 사 등분하였을 때 우측 상단 영역을 주요 위치로 식별하였다. 이는 제안한 방법이 취약한 회로의 특정 위치를 식별할 수 있음을 의미한다.

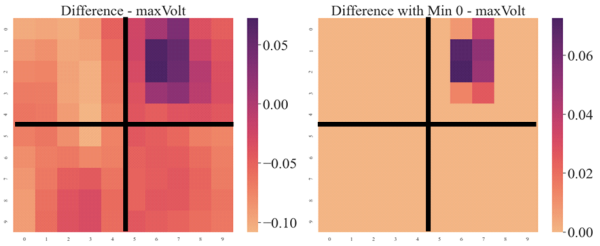
4-2-2 전력과 전자파의 상관 분석

본 논문은 피어슨 상관계수를 이용해 전력 파형의 변화량과 전자파 파형의 변화량의 유사성을 평가하여 주요 위치 식별 방법을 제안한다.

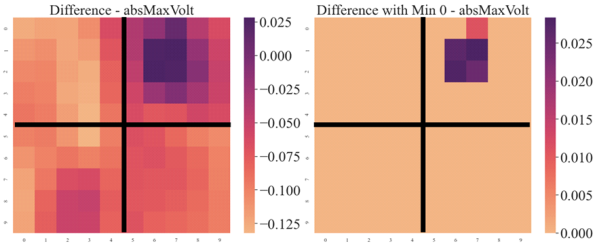
그림 6(a)는 암호가 동작할 때 소비되는 전력 파형이고, 그림 6(b)는 특정 위치에서의 방출되는 전자파 파형이다. 전력 신호는 잡음이 적고 AES의 함수별 개형이 눈으로



(a) 전체 주파수 강도의 합을 이용한 차분 분석
(a) Difference analysis using the sum of all frequency intensities



(b) 최대 강도를 이용한 차분 분석
(b) Difference analysis using maximum intensity



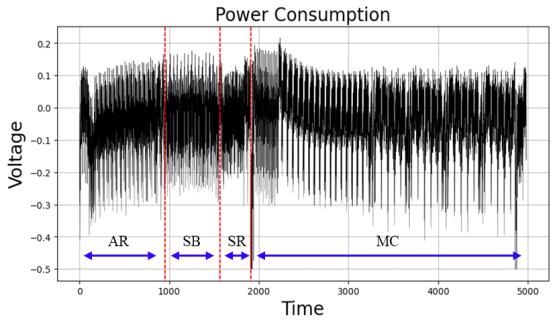
(c) 절댓값이 적용된 신호의 최대 강도를 이용한 차분 분석
(c) Difference analysis using maximum intensity of absolute value

그림 5. 전자파 강도 차분 분석 결과
Fig. 5. Results of EM intensity difference analysis.

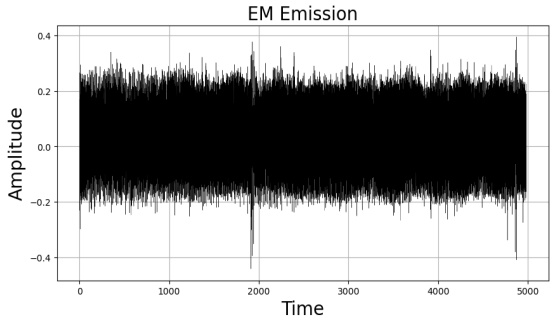
구분될 만큼 데이터에 따른 변화를 잘 나타내어 기준으로 선정할 수 있다. 구분은 순차적으로 9라운드의 AddRoundKey, SubBytes, ShiftRows, MixColumns에 해당한다.

본 논문은 이러한 특성을 이용하여 전력 신호를 기준으로 각 시점에서 방출되는 전자파 신호와 유사도를 식 (3)의 상관계수로 평가한다. 실험은 10,000개의 파형에 대해 SubBytes 연산 시점의 변화량을 기준으로 상관도를 평가하였다. 연산 구간 동안 평가된 상관도 중 가장 높은 상관도가 그 위치를 평가하는 대푯값이다.

그림 7은 각 위치별 상관도를 나타낸다. 0.8 이상의 상



(a) 소비 전력 파형(AR: AddRoundKey, SB: SubBytes, SR: ShiftRows, MC: MixColumns)
(a) Power consumption trace (AR: AddRoundKey, SB: SubBytes, SR: ShiftRows, MC: MixColumns)



(b) 방출 전자파 파형
(b) EM emission trace

그림 6. 소비 전력 파형(위)과 방출 전자파 파형(아래)
Fig. 6. Power consumption trace and emitted EM trace.

관도를 갖는 위치는 우측상단의 4개이고 0.75 이상의 상관도를 갖는 것은 전체 19개 중 10개가 우측상단이다. 이를 통해 칩의 우측상단이 AES가 동작하는 위치로 식별할 수 있다.

4-2-3 전자파와 암호 중간값의 상관 분석

그림 8은 칩의 위치마다 방출되는 전자파 신호에 대한 CEMA를 수행한 결과이다. 암호 알고리즘의 정보가 많이 담긴 신호가 방출될수록 CEMA의 성능이 높게 나타난다. 이때의 성능은 옳은 키의 상관계수 값을 의미한다. 옳은 키를 통해 만든 가상의 집합과 가장 상관도가 높은 지역은 우측상단이다. 또한 0.5 이상의 상관계수를 갖는 지역도 우측상단이다.

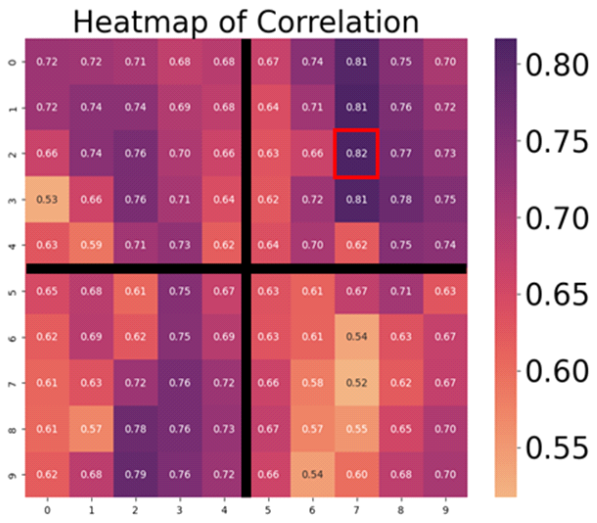


그림 7. 전자파 파형과 전력 파형의 상관 분석 결과
Fig. 7. Correlation analysis results of EM traces and power traces.

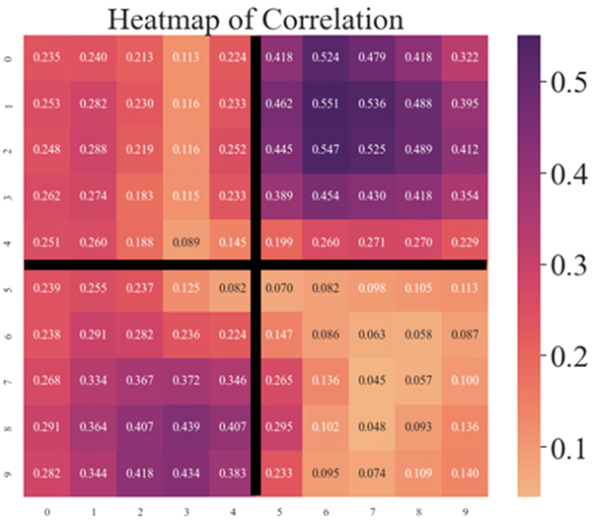
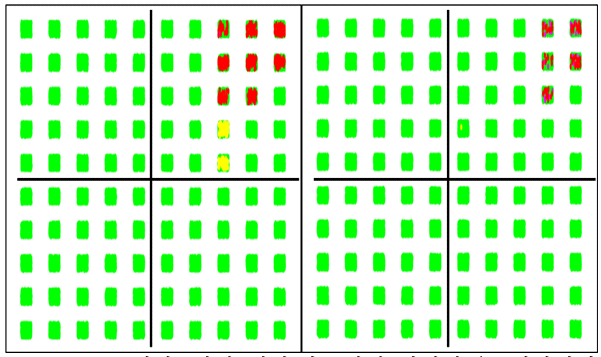


그림 8. CEMA 결과: 옳은 키에 대한 상관계수
Fig. 8. CEMA results: Correlation coefficient for the right key.

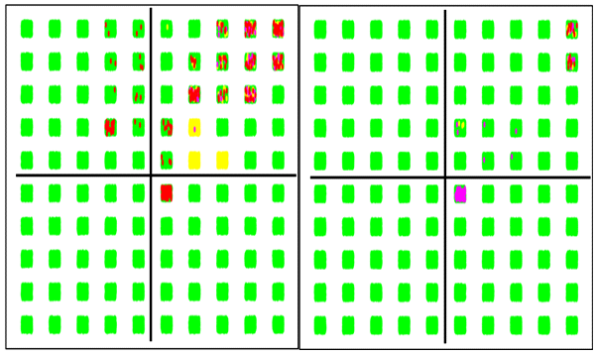
4-3 파라미터에 따른 전자파 오류 주입 실험 결과

전자파 오류 주입은 오류 주입 장비의 물리적 지연 및 오차로 인해 동일한 파라미터로 오류를 주입해도 다양한 영향을 미칠 수 있다. 본 논문은 타이밍 및 세기 파라미터 변경에 대한 결과를 파악하여 공통된 오류 주입 영역을 파악한다.

그림 9의 실험 결과는 SubBytes 함수와 MixColumns 함수가 동작할 때 첫 번째 바이트가 연산 되는 부분을 대상으로 전자파 오류 주입을 수행한 결과이다. 이때 녹색은 오류가 발생하지 않은 정상 암호문, 노란색은 응답이 돌아오지 않은 경우, 자홍색은 의도하지 않은 오류가 발생한 암호문, 빨간색은 의도한 오류가 발생한 암호문을 의



(a) SubBytes 대상: 가변 세기(좌), 가변 타이밍(우) 파라미터에 대한 오류 주입 결과
(a) SubBytes target: Fault injection results for variable strength (left) and variable strength (right) parameter



(b) MixColumns 대상: 서로 다른 가변 타이밍 파라미터에 대한 오류 주입 결과
(b) MixColumns target: Fault injection results for different variable timing parameters

그림 9. 파라미터 변경에 따른 위치별 오류 주입 결과 (녹색: 정상, 노랑색: 응답없음, 자홍색: 의도하지 않은 오류 발생, 빨강색: 의도한 오류 발생)
Fig. 9. Fault injection results by location based on parameter changes (Green: Normal, Yellow: No response, Magenta: Unintended fault occurred, Red: Intended fault occurred).

표 3. 파라미터에 따른 오류 주입 결과
Table 3. Fault injection results of each parameters.

Type	Green/Yellow/Magenta/Red
(a) Left	55,496/130/5/369
(a) Right	65,874/3/48/75
(b) Left	72,223/2,385/88/304
(c) Right	119,886/17/80/17

미한다. 그림은 칩을 10×10으로 나누어 각 위치에서 반복적인 오류 주입을 통해 얻은 결과를 보인다. 칩을 네 개의 영역으로 나누어 공통으로 의도한 오류가 발생한 위치를 전자파 오류 주입에 취약한 회로의 위치로 판단한다.

그림 9(a)는 SubBytes 함수, 그림 9(b)는 MixColumns 함수 대상 결과이다. 그림 9(a)의 왼쪽은 세기를 5~60 %로 1씩 증가시키면서 타이밍을 고정하고 20회씩 수행한 결과이다. 오른쪽은 세기를 52 %로 고정하고 1,100 ns 연산 구간을 34 ns 단위로 각각 20회씩 수행한 결과이다. 그림 9(b)의 왼쪽은 세기를 60 %로 고정하고 2,028 ns 연산 구간을 136 ns 단위로 50회씩 수행한 결과이다. 오른쪽은 세기를 60 %로 고정하고 34 ns 단위로 20회씩 수행한 결과이다. 각각의 결과는 표 3이다. 그림 9는 칩의 오른쪽 상단 부근이 세기, 타이밍의 파라미터가 변경되어도 오류 주입에 취약한 위치임을 보인다.

Ⅴ. 결 론

본 논문은 암호 알고리즘이 동작할 때 방출되는 전자파를 분석하여 전자파 오류 주입에 용이한 위치 탐색 방법을 제안하였다. 제안한 기법은 세 가지이며, 일관되게 칩의 특정 영역을 식별할 수 있음을 보였다. 실험을 통해 정보량 누출 관점에서 취약한 회로의 위치가 전자파 오류 주입에서도 취약한 위치임을 보였다. 이를 통해 제안한 방법이 75 % 이상 위치 탐색에 효율적임을 보였다. 또한 제안하는 방법들은 동작하는 암호 알고리즘을 모르는 상황 등 다양한 공격자 가정에 따라 적용이 가능하며 이를 통해 전자파 오류 주입에서의 위치 탐색에 효율적으로 사용할 수 있다. 본 논문은 전자파 방출 신호를 분석하여 전자파 오류 주입 위치를 탐색하는 기초 연구이다. 따라서 향후 연구는 방출되는 전자파 파형의 잡음을 제거하는 방식을 적용하고 프로브 등 전자파 오류 주입 파라미터를 변경하며 오류 주입 결과에 대한 위치 변화를 관측하여 향상된 방출 전자파와 전자파 오류 주입 위치의 관계해석 연구를 수행할 계획이다.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology - CRYPTO '99*, *LNCS*, Berlin, 1999, vol. 1666, pp. 388-397.

[2] E. Brier, C. Clavier, and F. Olivier "Correlation power analysis with a leakage model," in *Proceedings of Cryptographic Hardware and Embedded Systems - CHES 2004. Lecture Notes in Computer Science*, Berlin, 2004, vol. 3156, pp. 16-29.

[3] G. Piret, J. J. Quisquater, "A differential fault attack technique against SPN structures, with application to the AES and KHAZAD," in *Cryptographic Hardware and Embedded Systems*, *CHES 2003*, *LNCS*, Berlin, 2003, vol. 2779, pp. 77-88.

[4] M. Madau, "A methodology to localise EMFI areas on microcontrollers," Ph.D. dissertation, Université Montpellier University, Montpellier, 2019.

[5] S. Lim, J. Han, and D. G. Han, "Single-byte error-based practical differential fault attack on bit-sliced lightweight block cipher PIPO," *IEEE Access*, vol. 10, pp. 67802-67813, Jun. 2022.

[6] A. Maldini, N. Samwel, S. Picek, and L. Batina, "Genetic algorithm-based electromagnetic fault injection," in *Proceedings of 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography(FDTC)*, Amsterdam, Sep. 2018, pp. 35-42.

[7] H. Moon, J. Ji, and D. G. Han, "Electromagnetic and thermal information utilization system to improve the success rate of laser fault injection attack," *Journal of the Korea Institute of Information Security & Cryptology*, vol. 32, no. 5, pp. 965-973, Oct. 2022.

[8] J. Danial, D. Das, S. Ghosh, A. Raychowdhury, and S. Sen, "SCNIFFER: Low-cost, automated, efficient electromagnetic side-channel sniffing," *IEEE Access*, vol. 8, pp. 173414-173427, Sep. 2020.

[9] S. Wada, Y. Hayashi, D. Fujimoto, N. Homma, and Y. Kim, "Measurement and analysis of electromagnetic information leakage from printed circuit board power delivery network of cryptographic devices," *IEEE Transactions on Electromagnetic Compatibility*, vol. 63, no. 5, pp. 1322-1332, Mar. 2021.

[10] M. J. Dworkin, E. B. Barker, J. R. Nechvatal, J. Foti, L. E. Bassham, and E. Roback, et al., "Advanced encryption standard(AES)," *National Institute for Standards and Technology*(NIST), Report No. 197, Nov. 2001.

[11] Riscure, "EM-FI transient probe quick start guide," 2020. Available: https://support.riscure.com/en/support/solutions/articles/15000014311-em-fi-transient-probe

최 건 희 [국민대학교/석사과정]

https://orcid.org/0009-0007-2557-566X

2023년 2월: 국민대학교 정보보안암호수학과 (이학사)

2023년 3월~현재: 국민대학교 금융정보보안학과 석사과정

[주 관심분야] 암호 안전성 평가, 양자 내성 암호, 부채널 분석 및 대응기법, 오류 주입

김 주 환 [국민대학교/석·박사통합과정]

https://orcid.org/0000-0001-8762-5553

2021년 2월: 국민대학교 수학과 (이학사)

2023년 9월~현재: 국민대학교 금융정보보안학과 석·박사통합과정

[주 관심분야] 부채널 분석 및 대응법 설계, 딥러닝, 오류 주입 공격

한 재 승 [국민대학교/박사과정]

https://orcid.org/0000-0001-7111-2315

2020년 2월: 국민대학교 정보보안암호수학과 (이학사)

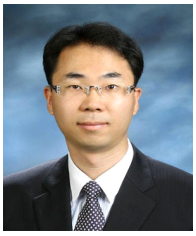
2022년 2월: 국민대학교 금융정보보안학과 (이학석사)

2022년 3월~현재: 국민대학교 금융정보보안학과 박사과정

[주 관심분야] 대칭키 암호, 양자 내성 암호, 부채널 분석 및 대응기법

한 동 국 [국민대학교/교수]

https://orcid.org/0000-0003-1695-5103



1999년 2월: 고려대학교 수학과 (이학사)

2002년 2월: 고려대학교 수학과 (이학석사)

2005년 2월: 고려대학교 정보보호대학원 (공학박사)

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 정보보안암호수학과 정교수

[주 관심분야] 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석 및 대응법 설계, IoT 정보보호 기술