Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.5, Oct. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.5.965

레이저 오류 주입 공격 성공률 향상을 위한 전자파 및 열 정보 활용 시스템*

문 혜 원,[1†] 지 재 덕,[3] 한 동 국[2‡]
[1,2]국민대학교 (대학원생, 교수), [3]한국기계전기전자시험연구원 (책임연구원)

Electromagnetic and Thermal Information Utilization System to Improve The Success Rate of Laser Fault Injection Attack*

HyeWon Mun,[1†] Jae-deok Ji,[3] Dong-Guk Han[2‡]
[1,2]Kookmin University (Graduate student, Professor),
[3]Korea Testing Certification (Senior Researcher)

요 약

IoT(Internet of Things) 기기가 보편화됨에 따라 사용자의 개인정보를 보호하기 위한 알고리즘들이 많이 개발되었다. 이를 위협하는 레이저 오류 주입 공격은 기기의 외부에 레이저 빔을 의도적으로 주입하여 시스템의 비밀 정보 또는 비정상 권한을 획득하는 부채널 분석이다. 필요한 오류 주입의 수를 감소시키기 위해 오류 주입의 타이밍을 결정하는 연구들은 많이 진행되었지만, 오류를 주입할 위치는 기기 전체에 대해 반복적으로 탐색하는 것에 그친다. 그러나 만약 공격자가 알고리즘과 무관한 영역에 레이저 오류 주입을 수행한다면 공격자는 의도한 오류문을 획득하거나 인증 우회를 시도할 수 없으므로, 오류 주입에 취약하여 공격을 수행할 영역을 탐색하는 것은 높은 공격 성공률을 달성하는 중요한 고려 사항이라고 할 수 있다. 본 논문에서는 기기의 칩에서 발생한 전자파와 열 정보를 활용하여 오류 주입 취약 영역을 판별하면 100%의 공격 성공률을 달성할 수 있음을 보이고, 이를 토대로 효율적인 오류 주입 공격 시스템을 제안한다.

ABSTRACT

As IoT(Internet of Things) devices become common, many algorithms have been developed to protect users' personal information. The laser fault injection attack that threatens those algorithms is a side-channel analysis that intentionally injects a laser beam to the outside of a device to acquire confidential information or abnormal privileges of the system. There are many studies to determine the timing of fault injection to reduce the number of necessary fault injections, but the location to inject faults is only repeatedly searched for the entire area of the device. However, when fault injection is performed in an algorithm-independent area, the attacker cannot obtain the intended faulted statement or attempt to bypass authentication, so finding areas vulnerable to fault injection and performing an attack is an important consideration in achieving a high attack success rate. In this paper, we show that a 100% attack success rate can be achieved by determining the vulnerable areas for fault injection by using electromagnetic and thermal information generated from the device's chip. Based on this, we propose an efficient fault injection attack system.

Keywords: Fault Injection Attack, System, Laser, Electromagnetic emission, Heat emission

Received(08. 17. 2022), Modified(09. 27. 2022), Accepted(09. 27. 2022)

* 본 연구는 고려대 암호기술 특화연구센터(UD210027XD)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.

† 주저자, qwerty25879@kookmin.ac.kr
‡ 교신저자, christa@kookmin.ac.kr(Corresponding author)

I. 서 론

부채널 분석은 기기에서 암호화 알고리즘이 동작할 때 소비 전력, 전자파, 소리, 열과 같이 부가적으로 누출되는 부채널 정보를 수집하고 가공하여 비밀 정보를 획득하는 공격 방법으로 폴 코쳐에 의해 처음으로 제시되었다[1]. 암호 알고리즘이 수학적으로 안전하게 설계되었더라도 부채널 분석을 고려하지 않고 구현한다면 그 안전성은 크게 저하된다. 지속적인 기술 발전에 따라 IoT(Internet of Things) 기기들이 많이 보급되었는데, 사용자의 특성 맞춤화를 위해 개인정보 데이터를 수집 및 이용한다. 이러한 민감 데이터의 기밀성을 유지하기 위하여 암호 기술이 필수적으로 요구되고, 따라서 부채널 분석으로 인한 위협이 꾸준히 제기되어 왔다. 더불어 IoT 기기에 대한 공격자들의 접근이 비교적 쉬워짐에 따라 하드웨어에 물리적인 동작 장애를 발생시켜 암호 기술에 사용된 비밀 키를 획득하는 부채널 분석도 강력한 공격 기법으로 고려되고 있다.

부채널 분석은 공격 장비에 가할 수 있는 수준에 따라 비침입, 준침입, 침입 공격으로 나뉘며, 그중 오류 주입 공격은 대표적인 준침입 공격에 속한다. 기기의 전원을 정상적으로 공급하지 않거나 전자파나 레이저 등을 칩의 외부에 인위적으로 노출하여 얻은 오류 값을 통해 비밀 정보를 도출한다[2]. 실제 오류 주입 공격을 수행할 때 오류를 주입할 타이밍과 위치를 결정하는 것은 중요한 문제이다. 알고리즘 구조에 의해 오류 주입 타이밍에 따라 얻을 수 있는 오류 값이 달라지므로, 공격자는 비밀 정보 복구에 필요한 오류 값을 얻기 위한 타이밍을 이론적으로 설정할 수 있다. 그러나 MCU(MicroController Unit)의 물리적 구조를 알지 못하는 공격자는 오류 값을 유도하기에 적합한 위치를 특정할 수 없으므로 오류 주입에 취약한 위치를 실험적으로 접근해야 한다. 알고리즘이 실동작하지 않는 영역에 공격을 수행할 경우 정상 결괏값만을 얻게 될 수 있기 때문이다. 그럼에도 불구하고 오류 주입 위치를 효율적으로 탐색하여 높은 공격 성공률을 달성하기 위한 방법론을 제시한 연구들은 미비하다.

Contribution: 본 논문에서는 레이저 오류 주입 공격 성공률을 향상시키기 위해 주입된 오류에 민감하게 반응하는 MCU의 취약 위치를 파악하는 방법론이 필요함을 주장한다. 또한, 알고리즘이 동작할 때 기기에서 발생하는 전자파와 열 정보가 레이저 오류 주입 공격에 효과적으로 활용될 수 있음을 보인다. 이를 기반으로 기존 레이저 오류 주입 공격에서 고려하지 않았던 성공률 향상을 위한 부채널 정보 활용 시스템을 제안한다.

II. 관련 연구

2.1 오류 주입 공격

기기에 인가되는 전압이 변경되거나, 외부가 전자파 등에 노출되고, 또는 비정상적인 온도 변화가 발생하면 데이터 손상을 초래할 수 있다. 오류 주입 공격은 공격자가 이를 의도적으로 이용하여 기기에서 동작하는 특정 알고리즘의 주요 정보를 추론하는 공격 기법이다. 주로 암호 알고리즘에 대한 오류 주입 공격이 많이 연구되었는데, 기기의 오동작으로 획득한 오류 주입 암호문과 정상적인 암호문 사이의 차분을 이용하여 비밀 키를 획득하는 차분 오류 공격[3,4]이 대표적이다. 그뿐만 아니라 비승인 사용자의 접근을 가능하게 하는 인증 우회 공격[5]에 대한 연구도 활발히 이루어지고 있다.

오류 주입 공격에 사용되는 주요 오류원은 전압 글리치, 클락(clock) 글리치, 전자파, 레이저 빔이다. 전압 글리치와 클락 글리치 공격은 기기에 공급되는 전압 또는 클락을 비정상적으로 변경하여 기기가 올바르게 동작하지 못하도록 유도한다. 전자파 오류 주입 공격은 유도 전력에 의해 생성된 전자기장을 기기의 MCU 표면에 노출하는 방법을 사용하여 올바른 데이터 출력을 방해한다[6,7]. 레이저 오류 주입 공격은 빛에 민감한 칩의 특성을 이용하여 표면 패키징을 제거(디캡핑)한 칩에 레이저 빔을 주입하여 기기의 오동작을 유도하며[8], 세밀하게 오류 주입 위치를 설정할 수 있다는 장점이 있다.

오류 주입 공격으로 실현 가능한 오류 모델은 한 비트가 플립되는 단일 비트 반전 모델, 바이트의 값이 바뀌는 무작위/다중 바이트 모델, 어셈블리 코드의 특정 명령어가 수행되지 않는 명령어 생략 오류 모델[9]이다. 오류 주입 공격을 수행하기 위한 오류원을 결정했다면 이러한 오류 모델을 고려하여 오류를 주입할 타이밍을 결정한다. 이때 공격자는 의도한 오류문을 얻기에 적합한 타이밍을 오류 모델과 함께 이론적으로 설정할 수 있다. 예를 들어, Piret 등이 제안한 AES(Advanced Encryption Standard)에 대한 차분 오류 공격[10]은 무작위 바이트 모델

을 고려했을 때, 9라운드 MixColumns 입력을 오류를 주입할 타이밍으로 설정하여 네 바이트에 오류가 확산된 암호문을 얻는 것을 목표로 한다.

이때 전자파 또는 레이저 오류 주입 공격은 칩 표면에 전자파 또는 레이저를 위치하여 공격을 수행하기 때문에 오류를 주입할 물리적 위치를 선택해야 한다. 그러나 어떤 위치가 오류 주입에 취약한지 알 수 없으므로, MCU 전체의 표면을 스캔하며 오류 주입을 반복적으로 수행하면서 원하는 오류가 유도되는 영역을 확인한다. 최종적으로 판별된 영역에 오류 주입 공격을 반복 수행하여 의도한 오류문을 획득하고 공격자의 목적을 달성한다.

2.2 부채널 정보 측정

기기에서 발생하는 부채널 정보는 대표적으로 전력, 전자파가 있고, 이 외에도 광자나 열, 소리 등이 있다. 이 절에서는 이러한 부채널 정보를 측정하는 방법을 소개한다.

전력 또는 전자파 신호를 이용하여 부채널 분석에 대한 시스템의 안전성을 검증하고자 하는 연구가 많이 진행됨에 따라, 많은 기업에서 부채널 분석을 수행하기 위한 다양한 시스템들을 개발하였다. 대표적으로 CRI 사의 DPA workstation[11], Brightsight 사의 Sideways[12], ETRI의 SCARF[13], Riscure 사의 Inspector[14] 등이 있다. 이 시스템들은 알고리즘이 동작하는 타겟 기기를 제어하고, 발생한 전력이나 전자파 신호를 수집하여 부채널 분석을 수행하는 소프트웨어를 제공한다.

전력 정보는 기기의 전원이나 그라운드에 작은 저항으로 인해 생기는 전압 차를 이용하여 측정되고, 전자파 신호는 Fig. 1.과 같이 EM(Electro Magnetic) 프로브를 통해 기기의 표면 위에서 측정된다. 측정된 전력 및 전자파 파형은 오실로스코프를 통해 수집되며, 기기에서 송신한 트리거 신호에 맞춰 전력 및 전자파 신호를 반복적으로 수집한다.

광자나 열 정보를 수집하여 부채널 분석을 진행하는 연구들[15]은 미비하며, 주로 시스템 내의 센서를 이용한다. 그러나 본 논문에서는 이러한 센서가 포함되지 않은 기기를 고려하여 기기 외부에서 광자 및 열 정보를 수집할 수 있는 기법을 소개한다.

기기 부품의 단선, 누설 등을 탐지하기 위해 기기의 전면 및 후면에 EMMI(EMission MIcroscopy)라는 비침입적 기법이 사용되는데, 그중 기기

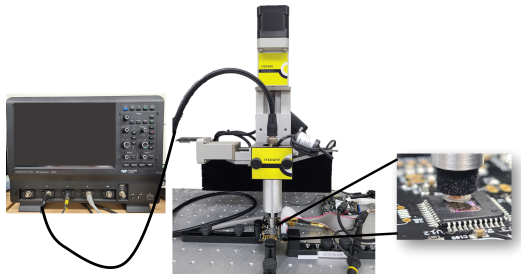


Fig. 1. EM measurement (left: Oscillo- scope, mid: EM probe)

Fig. 2. Heat measurement (THEMOS)

에 전기신호를 인가하여 불량 위치에서 빛, 열을 감지하는 시스템을 각각 PHEMOS(PHoton Emission MicrOScope), THEMOS(THermal Emission MicrOScope)라고 한다.

PHEMOS는 빛이 차단된 암실에서 전기적 신호를 인가한 기기가 동작할 때 발생하는 빛을 검출한다. InGaAs 카메라를 이용하여 빛 방출 이미지를 획득한다. Fig. 2.의 THEMOS는 전기적 신호를 인가한 기기가 동작할 때 발생하는 열을 검출한다[16]. InSb 카메라를 이용하여 칩의 열 이미지를 획득하고, 이를 칩의 패턴 이미지에 중첩해서 불량 위치를 탐지한다. 이때 기기의 칩 표면 패키징을 제거(디캡핑)한다면 불량 측정에 사용되는 THEMOS를 MCU에서 발생하는 열 정보를 관찰하는 목적으로 사용할 수 있다.

III. 부채널 정보 수집 및 분석을 통한 레이저 오류 주입 공격

오류 주입 공격을 수행할 때 의도한 오류문이나 상태를 유도하기 위해서 오류를 주입할 정확한 타이밍과 오류 주입할 위치를 찾는 것은 필수적으로 요구된다. 오류 주입 타이밍이나 수행 위치에 따라 공격 성공률이 좌우되기 때문이다. 오류가 주입되는 타이밍에 따라 오류가 전파되는 양상이 달라지거나 오류

상태가 크게 변화하므로 공격자는 알고리즘의 구조를 파악하여 정확한 타이밍을 설정할 필요가 있다. 그러나 타이밍을 정확히 판단하더라도 오류 주입 수행 위치가 올바르지 않다면 기기의 MCU가 오류 주입에 영향을 받지 않아 정상 동작하거나 의도치 않은 오류 상태만을 유도하여 공격 성공률이 감소하기 때문에, 위치 탐색 또한 중요한 공격 요소로 작용한다.

오류를 주입할 타이밍은 알고리즘의 수행 흐름에 따라 이론적으로 탐색하고, 트리거링을 통해 정확한 시점을 타겟할 수 있다. 그러나 오류를 주입할 영역을 탐색하는 것은 대상 MCU에 대한 하드웨어적 정보가 없다면 어려운 문제이다. 어느 영역이 오류 주입에 취약하여 의도한 암호문을 생성하는지 판단할 수 없기 때문이다. 기존 연구들은 전체 칩 영역에 대해 오류 주입을 반복적으로 수행하여 취약 영역을 탐색해왔다. 그로 인해 공격 성공률을 확보하기 위한 비용이 많이 소모되었지만 이를 개선하고자 하는 방법론이 연구되지 않았다. 본 논문에서는 MCU의 부채널 정보를 활용하여 레이저 오류 주입 공격 성공률을 향상시킬 수 있는 방안을 제안하고자 한다.

3.1 실험 환경

본 논문에서는 칩의 표면에서 비교적 쉽게 획득할 수 있는 전자파와 열 방출량을 레이저 오류 주입 공격을 수행할 때 활용할 부채널 정보로 고려하였다. 공격 실험 환경과 전자파 및 열 수집 환경은 Table 1과 같다.

본 논문에서는 ChipWhisperer-Lite에서 동작하는 AES-128의 비밀 키를 획득하는 차분 오류 공

Table 1. Experimental environment

Target Algorithm	AES-128
Target Device (MCU)	Decapsulated ChipWhisperer-Lite (Atmel XMEGA128D4)
Laser Fault Injection Attack	Laser Station (808nm laser : 75~85% power)
	FI Spotlight
EM Measurement	EM Probe
	Oscilloscope (Lecroy 8104)
Heat Measurement	THEMOS

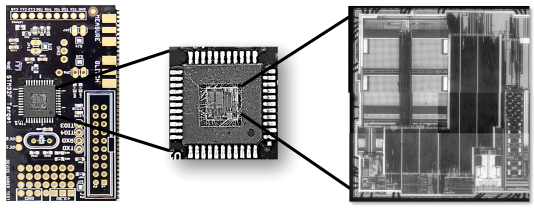


Fig. 3. Decapsulated ChipWhisperer-Lite MCU (Atmel XMEGA128D4)

Fig. 4. Riscure's Laser Station

격[10]을 수행한다. 레이저 빔을 오류원으로 사용하기 때문에 Fig. 3.과 같이 MCU는 디캡슐레이션을 진행한다. 레이저 오류 주입 공격은 Riscure 사의 Laser Station(Fig. 4.)으로 수행하며, 9라운드 MixColumns 입력에 대해 바이트 오류 모델을 가정했을 때 얻을 수 있는 오류 암호문을 획득한 경우 공격 성공으로 간주한다.

각 영역에 대한 전자파 방출량은 Fig. 1.과 같이 EM 프로브와 연결된 오실로스코프로 MCU의 전자파를 수집하여 계산한다. 열 정보는 THEMOS (Fig. 2.)로 측정하며, 디캡핑한 칩의 표면과 오버랩된 결과를 통해 정확한 열 방출 영역을 확인할 수 있다.

3.2 MCU의 부채널 정보 측정

3.2.1 MCU의 전자파 방출량

Fig. 5.의 왼쪽은 ChipWhisperer-Lite에서 AES-128이 동작할 때 디캡핑된 MCU에서의 전자파 방출량을 측정한 결과이다. 빨간색에 가까울수록 전자파 방출량이 많고, 파란색에 가까울수록 전자파 방출량이 적음을 나타낸다. 디캡핑한 MCU 표면과 전자파 방출량을 오버랩한 결과는 Fig. 5.의 오른쪽

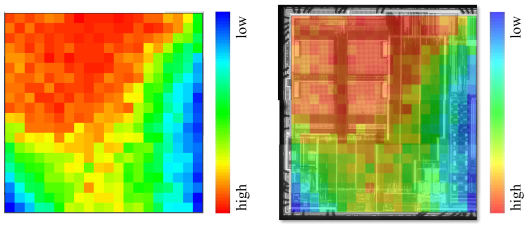


Fig. 5. left: EM emission, right: overlapping with the chip surface

과 같고, 좌측 상단에서 전자파가 많이 방출된 것을 확인할 수 있다.

3.2.2 MCU의 열 방출량

Fig. 6.은 THEMOS를 이용하여 AES-128이 동작할 때의 디캡핑된 MCU에 대한 열 방출량을 측정한 결과이다. 전자파 방출량과 마찬가지로 빨간색에 가까울수록 높은 열이 발생하고, 파란색에 가까울수록 적은 열이 발생했음을 나타낸다. 전자파 방출량과 달리 아주 적은 부분에서 높은 열이 방출됨을 알 수 있다.

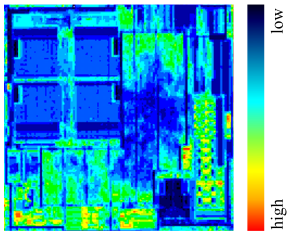


Fig. 6. Heat emission

3.3 전자파와 열 방출량 정보를 이용한 레이저 오류 주입 공격 수행

부채널 정보가 많이 발생한 밝은색 영역은 기기의 활발한 동작이 이루어지므로 오류 주입 성공률이 높고, 적게 발생한 어두운색 영역은 오류 주입 성공률이 낮을 것으로 기대한다. 이를 검증하기 위해 Fig. 7.과 같이 A, B, C, D, 네 영역에 대한 레이저 오류 주입 공격 결과를 대표적으로 보여준다. 각 영역에 대한 오류 주입 공격 결과는 Fig. 8.부터 Fig. 10.과 같이 FI Spotlight를 통해 확인하였으며, 각각의 점은 오류 주입 후 얻은 암호문의 유형을 나타낸다. 초록색 점은 정상 암호문, 빨간색 점은 의도한 오류 암호문, 노란색 점은 의도하지 않은 오류 암호문 또는 비정상 동작을 의미한다.

먼저, AES-128이 동작할 때 상대적으로 전자파 방출량이 많은 Fig. 7.의 A 영역에서의 오류 주입 공격을 수행한 결과는 Fig. 8.이다. 초록색, 빨간색, 노란색 점이 각각 30.14%, 0.14%, 69.72%의 비율로 나타났으며, 빨간색 점은 의도한 오류 암호문을 획득했음을 의미하므로 0.14%의 비율로 레이저 오류 주입 공격이 성공했음을 알 수 있다.

이때 전자파 방출량이 많은 Fig. 7.의 A 영역 중에서도 상대적으로 열 방출량이 높은 초록색과 하늘색 영역을 대상으로 레이저 오류 주입 공격을 수행하였다. Fig. 7.의 B 영역에서 Fig. 9.의 유효한 결과를 얻었다. 이는 Fig. 8.에서 빨간색 점이 나타난 영역을 타겟으로 레이저 오류 주입 공격을 수행했을 때의 결과이며, 모든 영역에서 빨간색 점이 관찰되었으므로 100%의 공격 성공률을 달성하였음을 알 수 있다.

그다음으로 열 방출량이 가장 높은 Fig. 7.의 C 영역에서의 오류 주입 공격을 수행한 결과는 Fig.

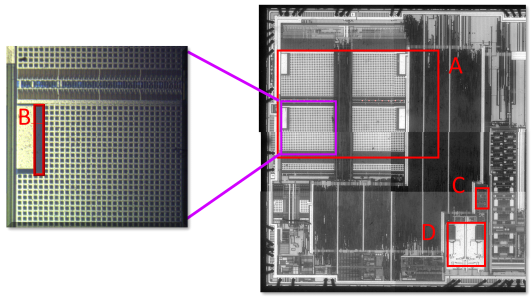


Fig. 7. Laser fault injection areas (A: high EM emission, B: relatively high heat emission in high EM emission, C: high heat emission, D: low EM, low heat emission)

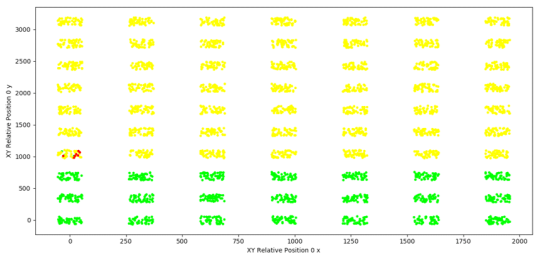


Fig. 8. Result of Laser fault injection attack in area A of Fig. 7.

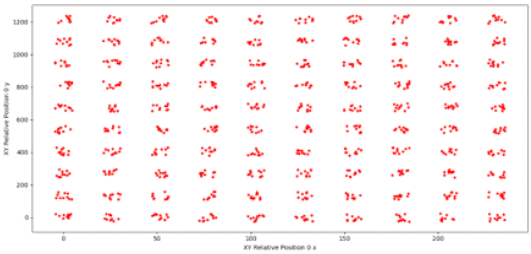


Fig. 9. Result of Laser fault injection attack in area B of Fig. 7.

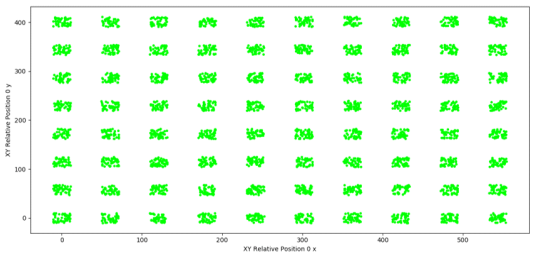


Fig. 10. Result of Laser fault injection attack in area C and D of Fig. 7.

10.이다. MCU가 활성화되는 영역임에도 불구하고 기기의 오동작이 유도되지 않아 공격 성공률이 0%임을 알 수 있다. 이 영역은 암호 알고리즘과 무관하게 기기에 인가되는 전원을 처리하는 등의 기타 동작으로 인해 많은 열이 발생한 것으로 추측할 수 있다.

마지막으로, 전자파 방출량과 열 방출량이 모두 적은 Fig. 7.의 D 영역에서의 오류 주입 공격을 수행한 결과는 Fig. 10.이다. 예상했던 것처럼 0%의 공격 성공률을 보이며, 암호 알고리즘이 동작하는 동안 전자파와 열 모두 적게 발생한 영역은 레이저 오류 주입 공격을 수행하기에 적합하지 않은 위치임을 확인할 수 있다.

IV. 레이저 오류 주입 공격 성공률을 향상시키는 전자파 및 열 정보 활용 시스템

3절은 수집한 전자파 방출량과 열 방출량을 관찰하고, 특징점이 있는 영역에 대해 레이저 오류 주입 공격을 수행하였다. 3.3절의 결과에 따라 전자파 방출량의 정보를 우선으로 하여 레이저 오류 주입 공격 시스템을 구성해야 함을 알 수 있다. Fig. 7.의 C 영역에 대한 공격과 같이 Fig. 6.의 열 방출량 정보를 우선으로 했을 경우 0%의 공격 성공률을 보였지만, Fig. 7.의 A 영역에 대한 공격과 같이 Fig. 5.의 전자파 방출량 정보를 우선으로 했을 경우 0.14%의 향상된 공격 성공률을 달성했기 때문이다. 더욱이 100%의 공격 성공률을 보인 Fig. 7.의 B 영역의 경우도 마찬가지로, 열 방출량보다 전자파 방출량이 많은 것을 확인할 수 있다. 이때 이 영역은 전자파 방출량이 많은 곳 중에서도 열 방출량이 상대적으로 많은 곳이라는 점에 주목하여, 단순히 전자파 방출량이 많은 영역을 모두 타겟하는 것보다 열 방출량 정보도 고려하여 유효한 공격 지점을 감소시킴으로써 더 높은 공격 성공률을 달성할 수 있음을 알 수 있다. 그러나 Fig. 7.의 D 영역과 같이 전자파 및 열 방출량이 모두 적은 곳은 알고리즘 동작과 무관하여 오류 주입 공격에 성공하지 못하므로 이러한 특징들을 토대로 레이저 오류 주입 공격 성공률 향상을 위한 전자파 및 열 활용 시스템(Fig. 11.)을 제안한다.

4.1 시스템 구성도

레이저 오류 주입 공격을 위한 전자파 및 열 활용 시스템(Fig. 11.)은 총 다섯 단계로 진행된다. 먼저, 레이저 오류 주입 공격을 수행할 알고리즘이 탑재된 기기를 선택한다. 알고리즘은 암호화 알고리즘 또는 인증 시스템 등이 될 수 있다.

그다음 레이저 오류 주입 공격을 수행하기 위한 환경을 구성한다. MCU의 전면부에 대해 디캡슐레이션을 진행하여 디캡핑된 영역에 레이저가 주입될 수 있도록 설치하고, 레이저를 주입할 타이밍을 알고리즘의 트리거링과 오실로스코프를 통해 설정한다.

이후, 알고리즘을 동작하는 동안의 전자파 방출량을 측정하고, 가능하다면 열 방출량도 추가로 측정한다. 열 방출량 기반으로 오류 주입 수행 위치를 판별하는 것은 정확도가 높지 않지만, 좀 더 세밀한 취약 영역 탐색을 위해 부가적인 정보로 사용할 수 있다. 예를 들어, 전자파 방출량이 많은 영역 중 상대적으로 열 방출량이 많은 Fig. 7.의 B 영역을 최종 오류 주입 공격 위치로 선택함으로써 단순히 전자파 방출량 정보만을 이용해 판별한 Fig. 7.의 A 영역에 대한 공격 범위가 감소하여 공격 수행 시간이 줄어 효율적이며, Fig. 9.와 같이 높은 공격 성공률을 달성할 수 있다. 이때 측정은 모두 디캡핑된 MCU에 대해 수행하여야 하고, 측정 결과를 MCU의 패턴과 중첩하여 더 정확한 정보를 획득한다.

앞서 수집한 전자파 또는 열 정보량을 토대로 레

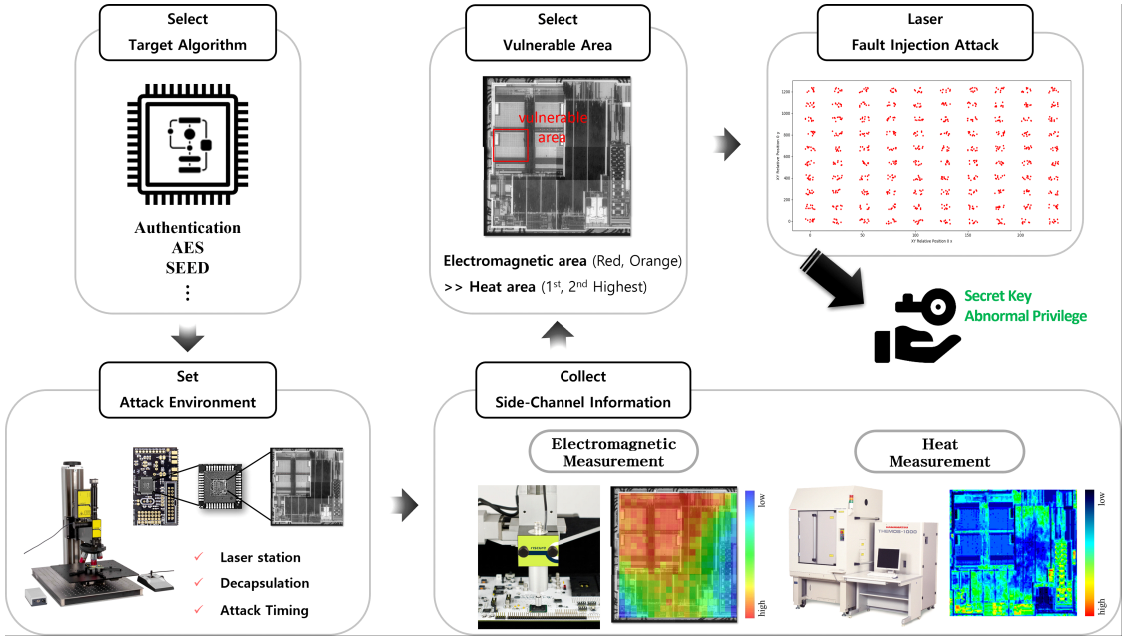


Fig. 11. Electromagnetic and thermal information utilization system to improve the success rate of laser fault injection attack

이저 오류에 민감하게 반응하는 취약 영역을 판별한다. 먼저 전자파 방출량이 많은 빨간색과 주황색 영역을 레이저 오류를 주입할 취약 영역으로 1차 선택한다. 그 이후 판별한 전자파 방출량에 따른 오류 주입 취약 영역 중 열 방출량을 고려하여 최종 레이저 오류 주입 영역을 선택한다. 주의할 점은 열 방출량이 절대적으로 높은 빨간색, 주황색 영역이 아닌 상대적으로 높은 열을 나타내는 영역을 고려하는 것이다. 즉 1차 선택된 영역 중 가장 높은 열과 두 번째로 높은 열을 방출하는 영역을 최종 오류 주입 공격 영역으로 선택한다.

마지막으로 식별한 오류 주입 영역을 대상으로 레이저 오류 주입 공격을 수행하여 높은 성공률로 공격자가 의도한 오류 암호문 또는 오류 상태를 획득한다. 획득한 오류 암호문을 분석하여 암호 알고리즘의 비밀 정보를 추출하거나 오류 상태를 통해 비정상 권한을 획득한다.

V. 결 론

본 논문에서는 레이저 오류 주입의 공격 성공률을 높이기 위한 MCU의 전자파 및 열 활용 시스템을 제안하였다. 기기에서 알고리즘이 수행되는 동안 발생하는 전자파와 열 정보를 획득하여 방출량이 많은 영역을 우선으로 오류 주입에 취약한 위치로 판단하였고, 그에 따라 레이저 오류 주입 공격을 수행한다. 그 결과 공격 성공률을 최대 100%까지 향상시킬 수 있음을 실험적으로 보였다. 본 논문에서는 대표적으로 ChipWhisperer-Lite에서 동작하는 AES-128을 대상으로 레이저 오류 주입 공격을 수행하였지만 다른 MCU의 다른 암호 알고리즘을 대상으로 이 시스템을 적용할 수 있다. 실제로 암호 알고리즘이 처리될 때 주로 사용되는 MCU의 특정 회로나 메모리가 존재하기 때문에, 전자파 및 열 정보와 같은 부채널 정보를 통해 이 영역을 판별할 수 있다. 따라서 레이저 오류 주입 공격을 수행하는 공격자가 디캡핑한 MCU의 물리적 구조에 대한 정보를 얻을 수 없다고 가정했을 때, 단순히 전자파와 열 정보를 획득함으로써 레이저 오류에 민감한 또는 취약한 영역을 특정할 수 있고, 그에 따라 오류 주입 공격 성공률을 높일 수 있을 것으로 기대하므로 기존 연구들이 수행한 오류 주입 공격보다 강력한 공격 기법으로 사용될 수 있다.

References

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

[2] Boneh, D., DeMillo, R. A., and Lipton, R. J., "On the importance of checking cryptographic protocols for faults," Advances in Cryptology, EUROCRYPT'97, LNCS 1233, pp. 37-51, May. 1997.

[3] Biham, E., and Shamir, A., "Differential fault analysis of secret key cryptosystems," Advances in Cryptology, CRYPTO'97, LNCS 1294, pp. 513-525, Aug. 1997.

[4] Giraud, C., "Dfa on aes," Advanced Encryption Standard, AES, LNCS 3373, pp. 27-41, May. 2004.

[5] Vasselle, A., Thiebeauld, H., Maouhoub, Q., Morisset, A., and Ermeneux, S, "Laser-induced fault injection on smartphone bypassing the secure boot-extended version," IEEE Transactions on Computers, vol.69, no.10, pp. 1449-1459, Oct. 2020.

[6] Schmidt, J. M., and Hutter, M., "Optical and em fault-attacks on crt-based rsa: Concrete results," Proceedings of the 15th Austrian Workshop on Microelectronics-Austrochip 2007, pp. 13-22, Oct. 2007.

[7] Elmohr, M. A., Liao, H., and Gebotys, C. H., "EM fault injection on ARM and RISC-V," Proceedings of the 2020 21st International Symposium on Quality Electronic Design (ISQED), pp. 206-212, Mar. 2020.

[8] Skorobogatov, S. P., and Anderson, R. J., "Optical fault induction attacks," Cryptographic Hardware and Embedded Systems, CHES 2002, LNCS 2523, pp. 2-12, Aug. 2002.

[9] Seonghyuck. L., "A Study on Differential Fault Attacks against ARX and Bit-Sliced Block Ciphers based on Practical Fault Model," Master Thesis, Kookmin University, pp.5-7, Oct. 2021.

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

[11] rambus, "DPA Workstation Analysis Platform," https://www.rambus.com/security/dpa-countermeasures/dpa-workstation-platform/, Aug. 2022.

[12] brightsight, "brightsight sideways," https://www.brightsight.com/test-tools, Aug. 2022.

[13] Kim, J., Oh, K., Choi, D., and Kim, H., "SCARF: profile-based side channel analysis resistant framework," Proceedings of the International Conference on Security and Management (SAM), p. 1, Jul. 2012.

[14] riscure, "riscure security tools," https://www.riscure.com/security-tools, Aug. 2022.

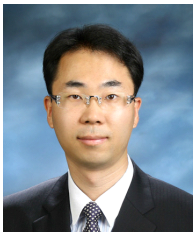
[15] Aljuffri, A., Zwalua, M., Reinbrecht, C. R. W., Hamdioui, S., and Taouil, M., "Applying thermal side-channel attacks on asymmetric cryptography," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol 29, no.11, pp. 1930-1942, Sep. 2021.

[16] Kuo, P. S., and Liu, C. Y., "Cutting-edge technologies for failure analysis and their applications in industry," Proceedings of the 2015 IEEE 22nd International Symposium on the Physical and Failure Analysis of Integrated Circuits, pp. 52-55, June. 2015.

〈저자소개〉

문 혜 원 (HyeWon Mun) 학생회원
2021년 2월: 국민대학교 정보보안암호수학과 졸업
2021년 3월~현재: 국민대학교 금융정보보안학과 석사과정
〈관심분야〉 정보보호, 암호 분석, 부채널 분석, 딥러닝, 오류 주입 공격

지 재 덕 (Jae-deok Ji) 종신회원
1996년 2월: 고려대학교 금속공학과 졸업
1998년 2월: 고려대학교 금속공학과 석사
2012년 8월: 고려대학교 정보보호학과 박사
〈관심분야〉 정보보호, 부채널, 임베디드 보안



한 동 국 (Dong-Guk Han) 종신회원
1999년 2월: 고려대학교 수학과 학사
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
〈관심분야〉 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석 및 대응법 설계, IoT 정보보호 기술