Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.6, Dec. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.6.1247

이종(異種) 오류원 기반의 현실적인 다중 오류 주입 시스템*

이 종 혁,[1†] 한 동 국[2‡]
[1,2]국민대학교 (대학원생, 교수)

Realistic Multiple Fault Injection System Based on Heterogeneous Fault Sources*

JongHyeok Lee,[1†] Dong-Guk Han[2‡]
[1,2]Kookmin University (Graduate student, Professor)

요 약

스마트홈 시대가 도래하면서 실생활의 다양한 곳에 기밀성을 제공하거나 인증을 수행하는 장비들이 존재하게 되었다. 이에 따라 암호화 장비 및 인증 장비에 물리적인 공격으로부터의 안전성이 요구되고 있다. 특히 외부에서 인위적으로 오류를 주입하여 비밀 키를 복구하거나 인증 과정을 우회하는 오류 주입 공격은 매우 위협적인 공격 방법의 하나다. 오류 주입 공격에 사용되는 오류원은 레이저, 전자파, 전압 글리치, 클락 글리치 등이 있다. 오류 주입 공격은 오류가 주입되는 횟수에 따라 단일 오류 주입 공격과 다중 오류 주입 공격으로 분류된다. 기존의 다중 오류 주입 시스템은 일반적으로 단일 오류원을 사용하였다. 단일 오류원을 여러 차례 주입하도록 구성된 시스템은 물리적인 지연 시간이 존재한다는 점과 추가적인 장비가 필요하다는 단점이 존재한다. 본 논문에서는 이종(異種) 오류원을 사용하는 다중 오류 주입 시스템을 제안한다. 그리고 제안하는 시스템의 효용성을 보이기 위해 Riscure사의 Piñata 보드를 대상으로 다중 오류 주입 공격을 수행한 결과를 보인다.

ABSTRACT

With the advent of the smart home era, equipment that provides confidentiality or performs authentication exists in various places in real life. Accordingly security against physical attacks is required for encryption equipment and authentication equipment. In particular, fault injection attack that artificially inject a fault from the outside to recover a secret key or bypass an authentication process is one of the very threatening attack methods. Fault sources used in fault injection attacks include lasers, electromagnetic, voltage glitches, and clock glitches. Fault injection attacks are classified into single fault injection attacks and multiple fault injection attacks according to the number of faults injected. Existing multiple fault injection systems generally use a single fault source. The system configured to inject a single source of fault multiple times has disadvantages that there is a physical delay time and additional equipment is required. In this paper, we propose a multiple fault injection system using heterogeneous fault sources. In addition, to show the effectiveness of the proposed system, the results of a multiple fault injection attack against Riscure's Piñata board are shown.

Keywords: Fault Injection Attack, Multiple Fault, Heterogeneous Fault Sources

Received(10. 06. 2020), Modified(11. 12. 2020), Accepted(11. 12. 2020)

* 이 논문은 2020년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2017-0-00520,SCR-Friendly 대칭키 암호 및 응용모드 개발)

† 주저자, n_seeu@kookmin.ac.kr

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

I. 서 론

부채널 분석(Side-Channel Analysis, SCA)은 암호화 동작을 수행하는 중 장비에서 발생하는 부가적인 정보(소비 전력, 방출 전자파, 연산 시간 등)를 이용하여 비밀 정보를 도출해내는 공격 방법이다. 수학적으로 안전하게 설계된 암호 알고리즘을 실제 장비에 구현할 때 부채널 분석을 고려하여 구현하지 않는다면 결과적으로 수학적인 안전도보다 현저히 낮은 물리적 안전도를 제공하는 데 그치게 된다. 스마트홈의 보편화로 다양한 IoT(Inter of Things) 기기들이 보급되었다. 이들은 개인 정보를 다룸에 따라 기밀성을 제공해야 하고 인증을 수행해야 하는 등의 요구가 발생하였다. 그리고 IoT 기기들에 대한 접근이 누구나 가능함에 따라 물리적인 공격에 대한 안전성이 필수적으로 요구되고 있다. 특히 부채널 분석은 다양한 물리적인 공격 중에 가장 위협적인 공격 방법의 하나로 고려되고 있다.

부채널 분석은 공격자 가정에 따라 비침입 공격(non-invasive attacks), 준침입 공격(semi-invasive attacks), 침입 공격(invasive attacks)으로 나뉜다.

오류 주입 공격(Fault Injection Attacks, FIA)은 대표적인 준침입 공격 방법으로 대상 마이크로컨트롤러(microcontroller)에 외부에서 인위적인 오류를 주입하여 도출된 결과 값을 이용하여 비밀 정보를 복구한다.

오류 주입 공격에 관한 연구는 대칭키 암호 알고리즘이나 공개키 암호 알고리즘을 대상으로 비밀 키를 도출하는 것을 목적으로 하고 있지만[1,2], 최근에는 인증 시스템에 대한 우회를 목적[3,4]으로 하는 등 다양한 영역으로 적용 범위를 넓혀가고 있다. 또한, 스마트폰 등의 상용 장비를 대상으로 하는 오류 주입 공격 결과가 보고됨[3]에 따라 암호화 장비 및 인증 장비에 대한 오류 주입 공격이 매우 위협적인 공격으로 고려되고 있다.

이에 따라 오류 주입 공격에 대한 안전성 검증을 수행하기 위한 시스템 개발도 활발히 이루어졌다. 초기에는 다양한 오류원을 이용하는 단일 오류 주입 시스템 개발이 주로 진행되었지만, 최근에는 레이저(laser)를 오류원으로 사용하는 다중 오류 주입 시스템이 제시되었다[5,6]. 하지만 동일한 오류원을 사용하는 경우 물리적인 지연 시간으로 인해 연속적인 오류 주입이 불가능하고, 레이저를 오류원으로 다중 오류 주입 시스템은 추가적인 레이저 발생 장비가 요구된다는 단점이 존재한다. 현재까지 다양한 오류원을 혼합하여 사용하는 다중 오류 주입 시스템은 아직 제시된 바 없다.

본 논문에서는 이종(異種) 오류원을 사용하는 다중 오류 주입 시스템을 제안한다. 본 시스템은 기존 단일 오류 주입 시스템에 비해 추가적으로 요구되는 장비가 없다는 장점과 오류원 마다의 특성들을 혼합하여 활용할 수 있다는 장점이 존재한다. 제안하는 시스템에 대한 효용성을 보이기 위해 Riscure사의 Piñata 보드[7]를 대상으로 다중 오류 주입 실험을 수행하였다. 본 논문에서는 전자파 오류원과 전압 글리치(glitch) 오류원을 사용하는 다중 오류 주입 시스템을 예로 들어 설명한다.

본 논문의 구성은 다음과 같다. 2장에서는 오류 주입 공격을 소개하고 3장에서는 기존에 제시된 다중 오류 주입 시스템과 제안하는 다중 오류 주입 시스템을 비교하여 설명한다. 그리고 4장에서 제안하는 다중 오류 주입 시스템의 실험 결과를 보인다. 마지막으로 5장에서 결론을 짓는다.

II. 오류 주입 공격

오류 주입 공격은 대상 장비에 외부에서 인위적으로 오류를 주입하여 비밀 정보를 획득하거나 원하는 결과를 끌어내는 준침입 공격 방법의 하나다. 오류가 주입된 암호문과 정상적인 암호문과의 차분을 이용하는 차분 오류 분석(Differential Fault Analysis, DFA) 방법[1,2]과 오류가 실질적으로 영향을 미치는 파라미터를 이용하는 오류 민감도 분석(Fault Sensitivity Analysis, FSA) 방법[8] 등을 이용해 비밀 정보를 찾을 수 있다.

오류 주입 공격에 사용되는 대표적인 오류원은 레이저, 전자파, 전압 글리치, 클락(clock) 글리치이다. 레이저를 이용한 오류 주입 공격은 대상 마이크로컨트롤러를 디캡슐레이션(decapsulation)하여 반도체에 직접 레이저를 접촉해야 한다는 단점이 존재한다. 전압 글리치와 클락 글리치는 대상 마이크로컨트롤러에 외부에서 전압 또는 클락을 인가하기 위해 인위적인 조작을 가해야 한다는 단점이 있다. 반면에 전자파 오류는 디캡슐레이션과 인위적인 조작이 없어 물리적인 단점이 존재하지는 않지만, 대상 마이크로컨르롤러 근방에 전자파 프로브(probe)를 위치해야 한다는 한계점이 존재한다.

레이저 오류 주입은 반도체가 빛에 민감하다는 특성을 이용해 반도체에 직접적으로 레이저를 가하여 비트를 반전시킨다. 전자파 오류 주입은 대상 마이크로컨트롤러 인근에서 강한 자기장을 발생시켜 마이크로컨트롤러 내부에 와전류를 생성시킨다. 이로 인해 오류가 발생한다. 전압 글리치는 GND(ground) 신호를 일시적으로 상승시키거나 하강시켜 오류를 유발한다. 클락 글리치는 일정한 주기의 클락 신호에 비정상적인 클락을 발생시켜 연산의 흐름을 방해시켜 오류를 유도한다.

오류 주입 공격은 주로 대칭키 암호 알고리즘과 공개키 암호 알고리즘의 비밀 키를 도출하는 방법에 관해 연구[1,2]가 진행되었지만, 최근에는 보안 부팅(booting) 시스템을 우회[3]하거나 인증 시스템을 우회[4]하는 등 시스템 우회를 목적으로 하는 연구 또한 진행되고 있다.

III. 다중 오류 주입 시스템

3.1 기존 다중 오류 주입 시스템

CC(Common Criteria) 인증, EMV(Europay Master Visa) 인증과 CMVP(Cryptographic Module Validation Program) 인증 등에서 오류 주입 공격을 포함하는 부채널 분석에 대한 안전성을 요구함에 따라 단일 및 다중 오류 주입 시스템의 개발이 활발히 이루어졌다.

Riscure사, ALPhANOV사와 NewAE사는 대표적인 오류 주입 시스템 제작 업체들이다. 이들은 레이저, 전자파, 전압 글리치와 클락 글리치 등의 다양한 오류원을 사용하는 오류 주입 시스템을 제작하고 이를 이용하여 보다 용이하게 안전성 검증 절차를 수행하게 한다.

Fig. 1은 Riscure사의 이중 레이저 주입 시스템[5]이고 Fig. 2는 ALPhANOV사의 이중 레이저 주입 시스템[6]이다. 두 제조사 모두 레이저 소스(source)를 2개 사용하여 레이저를 이중으로 주입할 수 있도록 시스템을 구성하였다.

동일한 오류원을 사용하여 다중 오류 주입 시스템을 구성하는 경우 물리적인 지연 시간으로 인해 다른 위치에 연속적으로 오류를 주입하는 것이 불가능하다. 또한, 2장에서 설명한 바와 같이 오류원 마다 다른 특성들이 존재하는데, 다양한 특성들을 함께 활용할 수 없다는 한계점이 존재한다.

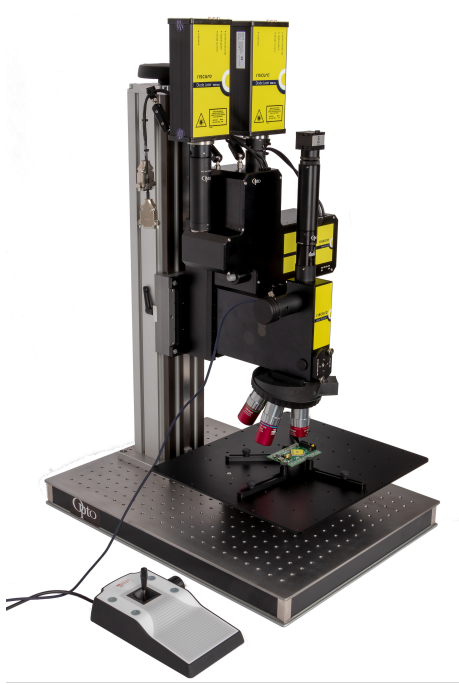


Fig. 1. Riscure's dobule laser injection system

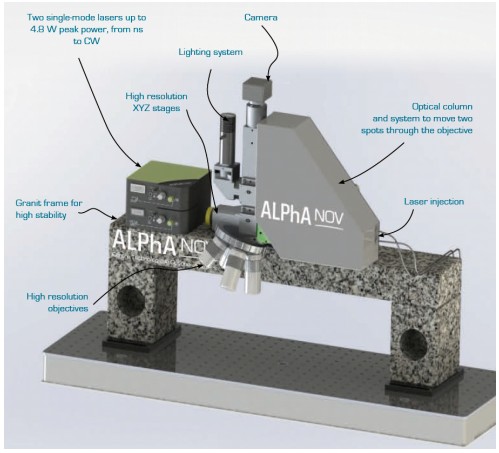


Fig. 2. ALPhANOV's dobule laser injection system

3.2 제안하는 다중 오류 주입 시스템

본 절에서는 Riscure사의 오류 주입 장비들을 활용하여 서로 다른 오류원을 혼합해 사용하는 다중 오류 주입 시스템을 제안한다.

Riscure사의 Spider[9]는 분석 대상 임베디드(embedded) 장비로의 다양한 인터페이스를 제공하

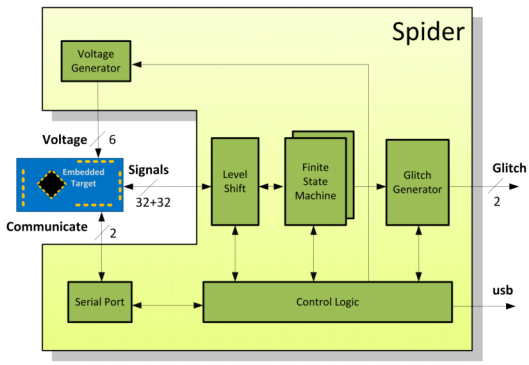


Fig. 3. System overview of the Spider

여 오류 주입 공격을 자동화하는 데에 사용된다. 또한, 글리치 및 전압을 생성하는 기능을 제공하며 이를 이용하여 전자파 오류 주입 장비를 제어하거나 전압 글리치 주입 공격을 수행한다. 이처럼 오류 주입 시스템을 구성하는데 필수적인 역할을 하는 Spider의 내부 구조는 Fig. 3과 같다. Spider는 대상 장비에 전원을 공급하고 시리얼 포트(serial port)로 통신을 수행함과 동시에 글리치를 생성한다. 생성한 글리치는 오류 주입에 사용된다. 주목할만한 점은 Spider 내의 유한 상태 기계(Finite State Machine, FSM)가 2개라는 점이다. 각 FSM은 임베디드 장비와 통신하며 글리치를 생성한다. Spider는 글리치 포트 또한 2개를 제공한다. 2개의 FSM과 글리치 포트를 이용해 서로 다른 오류원을 생성하여 다중 오류 주입 시스템을 구성할 수 있다.

Fig. 4는 전자파 오류원과 전압 글리치 오류원을 사용하는 다중 오류 주입 시스템의 모식도이다. Riscure사의 EM-FI Transient Probe[10]를 이용하여 전자파 오류를 주입하고 Spider를 이용하여 전자파 오류 주입 장비를 제어함과 동시에 전압 글리치 오류를 주입한다. Fig. 3은 Spider의 전압 생성기를 이용해 대상 임베디드 장비에 전원을 인가하는 구성을 보여주지만, 제안하는 다중 오류 주입 시스템에서는 전압 글리치 오류 주입을 수행하기 위해 글리치 생성기를 이용해 전원을 공급한다. 만약 전자파 오류원과 클락 글리치 오류원을 사용하는 다중 오류 주입 시스템을 구성하고자 할 때는 대상 임베디드 장비에 전압 생성기를 이용해 전원을 인가하고 글리치 생성기를 이용하여 외부 클락을 공급해주도록 시스템을 구성하면 된다.

오류 주입 실험 시 대상 임베디드 장비에서 트리

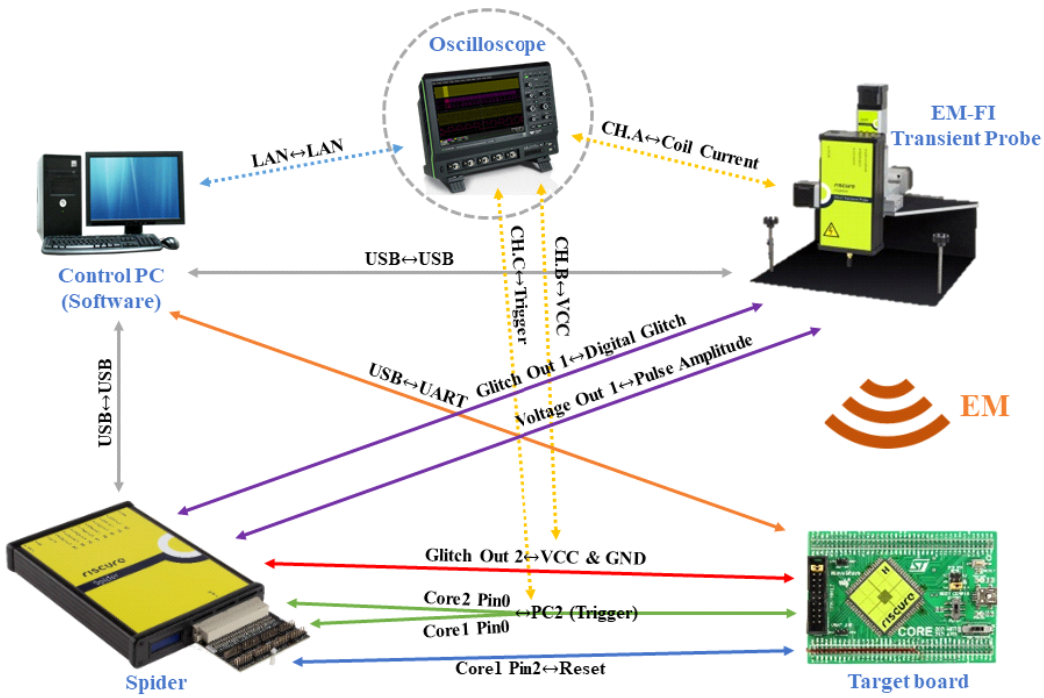


Fig. 4. Double fault injection system using heterogeneous fault sources

거(trigger)를 생성하는데 Fig. 4는 전자파 오류 주입과 전압 글리치 오류 주입이 동일 트리거를 사용하도록 구성하였기 때문에 2개의 FSM에 동일한 트리거를 연결하였다. 서로 다른 트리거를 사용하도록 구성하고자 한다면, 각각의 FSM에 각각의 트리거를 연결하도록 구성하면 된다.

Fig. 4의 오실로스코프(oscilloscope)는 트리거 신호와 대상 임베디드 장비에 인가되는 전압을 관찰하기 위해 Spider로부터의 VCC 선과 트리거 선에 연결하였다. 그리고 전자파 오류 주입 장비에서 발생되는 전자파를 관찰하기 위해 EM-FI Transient Probe에서 제공하는 Coil Current 포트에 연결하였다. 이종 오류 주입 시스템 구성에서 오실로스코프는 필수적인 장비가 아니다. 사용자가 원하는 시점에 오류가 제대로 주입되는지를 확인하기 위한 장비이다.

위와 같이 구성한 이종 오류원을 사용하는 다중 오류 주입 시스템은 서로 다른 오류원을 사용하기 때문에 물리적인 지연 시간이 발생하지 않으며 서로 다른 오류원의 특성을 모두 이용할 수 있는 장점이 있다. 기존 레이저 오류원을 사용하는 다중 오류 주입 시스템은 레이저 소스를 생성하는 모듈이 추가적으로 요구되어 비용적인 부담이 증가한다. 하지만 제안하는 시스템은 기존 단일 오류 주입 시스템의 장비 구성 외에 추가적으로 요구되는 장비가 존재하지 않아 추가 비용이 발생하지 않는 점 또한 장점이다.

IV. 실험 결과

본 장에서는 Riscure사의 Piñata 보드[8]를 대상으로 이종 오류원을 사용하는 다중 오류 주입 시스템의 실험 결과를 소개한다.

Piñata 보드는 ARM Cortex-M4F 코어(core)[11]를 사용하며 168MHz의 동작 주파수에서 작동한다. 1Mbyte의 내부 플래시(flash) 메모리와 196Kbyte의 내부 SRAM을 제공한다. 진난수 발생기(True Random Number Generator, TRNG)가 존재하며, 제공하는 암호 알고리즘들은 소프트웨어 DES, 하드웨어 DES, 소프트웨어 AES-128, 하드웨어 AES-128, 32 비트 T-tables을 이용하는 소프트웨어 AES-128, 하드웨어 TDES, CRT(Chinese Remainder Theorem)을 이용하는 소프트웨어 1024 비트 RSA 복호화이다.

본 장에서 소개하는 실험 결과는 두 종류이다. 첫 번째로 오실로스코프를 이용하여 전자파 오류원과 전압 글리치 오류원이 Piñata 보드에 영향을 미치는지 확인한다. 그 후 직접 구현한 ARIA-128 암호 알고리즘[12]을 대상으로 다중 오류 주입 기반의 차분 오류 분석 방법에 대한 실험 결과를 보인다.

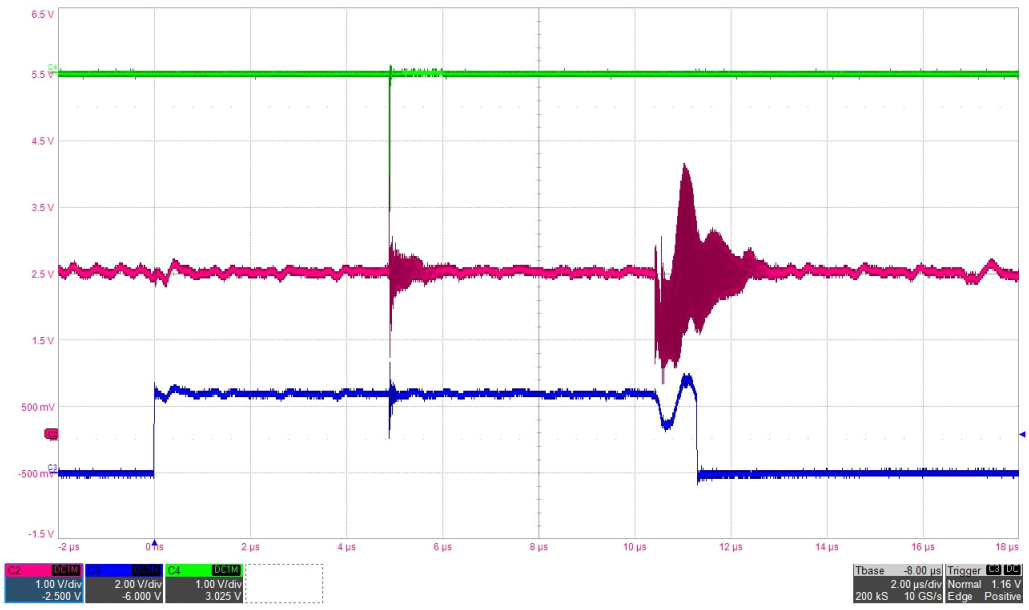


Fig. 5. Experiment result of double fault injection system using heterogeneous fault sources

4.1 오실로스코프를 통한 검증

Fig. 5는 오실로스코프로 트리거, 공급 전압, 전자파 오류 주입 장비에 인가되는 글리치를 관찰한 결과이다. 초록색 신호(C4)는 전자파 오류 주입 장비에 인가되는 글리치 신호이고 자주색 신호(C2)는 Piñata 보드에 인가되는 전압 신호이다. 그리고 파란색 신호(C3)는 Piñata 보드에서 생성되는 트리거 신호이다. 트리거로부터 약 5μs 이후 전자파 오류를 주입하도록 설정하였고 10.5μs 이후 전압 글리치 오류를 주입하였다. 전자파 오류를 주입한 시점과 전압 글리치 오류를 주입한 시점에서 트리거와 전압 신호가 흔들림을 관찰할 수 있다.

이로써 전자파 오류원과 전압 글리치 오류원을 사용하는 다중 오류 주입 시스템이 대상 마이크로컨트롤러에 영향을 끼침을 확인하였다.

4.2 ARIA-128 대상 다중 오류 주입 기반 차분 오류 분석

Park 등은 단일 오류 주입 모델로 ARIA-128 암호 알고리즘에 오류를 주입한 경우, 8개의 오류가 주입된 암호문들을 이용해 비밀 키를 복구하는 방법을 제안하였다[13]. 이후 박한별 등은 이를 활용하여 다중 오류 주입 환경에서 4개의 오류가 주입된 암호문들을 이용해 비밀 키를 복구할 수 있음을 밝혔다[14].

Fig. 6은 한국인터넷진흥원(Korea Internet & Security Agency, KISA)에서 제공하는 ARIA-128 오픈 소스(open source)[15]의 확산 계층 구현 코드이다. T 변수를 사용하여 4개의 바이트 계산에 공통으로 사용되는 연산들을 먼저 처리한 후 4개 바이트의 계산을 추가로 수행하도록 구성되어 있다. 따라서 T 변수의 계산 과정에 오류를 주입하면 확산 계층의 출력 네 바이트에 영향을 끼칠 수 있다.

이중 오류 주입을 T 변수의 계산 과정 두 번에 수행하면 최종적으로 확산 계층 출력 여덟 바이트에 영향을 끼치게 된다. 이를 11라운드 확산 계층에 적용하면 Fig. 7과 같다. 첫 번째와 세 번째 T 변수에 오류가 주입된 경우 12라운드 S-box 계층 입력 값은 다음과 같이 계산된다.

```
// Diffusion Layer
void DL(const Byte *i, Byte *o)
{
  Byte T;

  T = i[3] ^ i[4] ^ i[9] ^ i[14];
  o[0] = i[6] ^ i[8] ^ i[13] ^ T;
  o[5] = i[1] ^ i[10] ^ i[15] ^ T;
  o[11] = i[2] ^ i[7] ^ i[12] ^ T;
  o[14] = i[0] ^ i[5] ^ i[11] ^ T;
  T = i[2] ^ i[5] ^ i[8] ^ i[15];
  o[1] = i[7] ^ i[9] ^ i[12] ^ T;
  o[4] = i[0] ^ i[11] ^ i[14] ^ T;
  o[10] = i[3] ^ i[6] ^ i[13] ^ T;
  o[15] = i[1] ^ i[4] ^ i[10] ^ T;
  T = i[1] ^ i[6] ^ i[11] ^ i[12];
  o[2] = i[4] ^ i[10] ^ i[15] ^ T;
  o[7] = i[3] ^ i[8] ^ i[13] ^ T;
  o[9] = i[0] ^ i[5] ^ i[14] ^ T;
  o[12] = i[2] ^ i[7] ^ i[9] ^ T;
  T = i[0] ^ i[7] ^ i[10] ^ i[13];
  o[3] = i[5] ^ i[11] ^ i[14] ^ T;
  o[6] = i[2] ^ i[9] ^ i[12] ^ T;
  o[8] = i[1] ^ i[4] ^ i[15] ^ T;
  o[13] = i[3] ^ i[6] ^ i[8] ^ T;
}
```

Fig. 6. Diffusion layer code of ARIA-128 provided by KISA

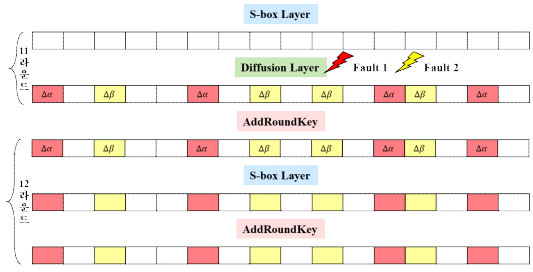


Fig. 7. Double fault injection based differential fault analysis on ARIA-128

$$\Delta_0 = SL^{-1}(C_0 \oplus ck_{13,0}) \oplus SL^{-1}(C_0^* \oplus ck_{13,0})$$
$$\Delta_5 = SL^{-1}(C_5 \oplus ck_{13,5}) \oplus SL^{-1}(C_5^* \oplus ck_{13,5})$$
$$\Delta_{11} = SL^{-1}(C_{11} \oplus ck_{13,11}) \oplus SL^{-1}(C_{11}^* \oplus ck_{13,11})$$
$$\Delta_{14} = SL^{-1}(C_{14} \oplus ck_{13,14}) \oplus SL^{-1}(C_{14}^* \oplus ck_{13,14})$$
$$\Delta_2 = SL^{-1}(C_2 \oplus ck_{13,2}) \oplus SL^{-1}(C_2^* \oplus ck_{13,2})$$
$$\Delta_7 = SL^{-1}(C_7 \oplus ck_{13,7}) \oplus SL^{-1}(C_7^* \oplus ck_{13,7})$$
$$\Delta_9 = SL^{-1}(C_9 \oplus ck_{13,9}) \oplus SL^{-1}(C_9^* \oplus ck_{13,9})$$
$$\Delta_{12} = SL^{-1}($$

위 식에서 SL은 S-box 계층을 의미하며 C_i는 암호문의 i번째 바이트, C_i^*는 오류가 주입된 암호문의 i번째 바이트를 의미한다. 그리고 $ck_{13,i}$는 13라운드 키의 i번째 바이트를 의미한다. 네 바이트에 동

Table 1. Experiment results of double fault injection based differential fault analysis on ARIA-128

Type	Data
①	9F 72 FC 42 93 71 C6 A7 ED 76 95 C1 9F 93 93 1A
	9F 72 FC 42 A5 71 C6 A7 ED 76 0D C1 9F 93 93 1A
②	46 CC 4D 74 B8 CE 2E EB 68 EB 84 40 64 6A 8D 52
	46 CC 35 42 B8 CE C6 DD ED 0F 84 40 5F 93 8D 52

일한 오류가 주입되었으므로 $\Delta_0 = \Delta_5 = \Delta_{11} = \Delta_{14} = \Delta\alpha$이고 $\Delta_2 = \Delta_7 = \Delta_9 = \Delta_{12} = \Delta\beta$이다. 이에 대한 만족성 여부를 통해 키 후보를 축소할 수 있다. 이 방법을 이용하면 기존 방법보다 필요한 오류가 주입된 암호문을 절반으로 줄일 수 있다.

Table 1은 다중 오류 주입 결과를 보여준다. 전자파 오류 주입 강도를 75%로 고정하였고 주입 시 트리거로부터의 지연 시간은 11라운드 전체에 랜덤하게 주입하도록 설정하였다. 전압 글리치 주입으로는 평시 전압을 2.5V로 설정하고 1.0V로 낮추도록 주입한다. 전압 글리치 주입 시점 또한 11라운드 전체에 랜덤하게 주입하도록 하였으며 글리치 길이는 6ns부터 200ns까지의 범위에서 랜덤하게 선택하도록 했다. Type ①은 첫 번째와 두 번째 T 변수에 오류가 주입된 결과이고 Type ②는 세 번째와 네 번째 T 변수에 오류가 주입된 결과이다. 이를 통해 ARIA-128의 13라운드 키를 기존 단일 오류 주입 대비 필요한 오류 주입 암호문 수가 50% 감소한 상태에서 복구할 수 있었다.

V. 결 론

기존 다중 오류 주입 시스템은 동일 오류원을 사용하여 여러 차례 오류를 주입하는 방식으로 구성되었다. 이를 위해 추가적인 장비들이 요구되었고 오류원 마다의 특성들을 활용할 수 없었다. 따라서 본 논문에서는 이종 오류원을 이용한 다중 오류 주입 시스템을 제안한다. 본 시스템은 기존 단일 오류 주입 장비들을 활용하여 구성되어 추가적인 장비가 요구되지 않는다. 제안하는 시스템을 사용하여 실제 마이크로컨트롤러에 다중 오류가 영향을 끼침을 보여주었으며 ARIA-128 암호 알고리즘을 대상으로 다중 오류 주입 기반의 차분 오류 분석 방법을 통해 비밀 키 획득이 가능함을 보였다.

다양한 오류원들은 다소 다른 오류 주입 모델을 띄기 때문에 이종 오류원을 사용하는 시스템으로 새로운 오류 모델을 구성할 수 있을 것으로 기대된다.

References

[1] C. Giraud, "Dfa on aes," International Conference on Advanced Encryption Standard, pp. 27-41, 2004.

[2] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," Annual international cryptology conference, pp. 513-525, 1997.

[3] A. Vasselle, H. Thiebeauld, Q. Maouhoub, A. Morisset, and S. Ermeneux, "Laser-induced fault injection on smartphone bypassing the secure boot," IEEE Transactions on Computers, 2018.

[4] J. Lee, Y.-J. Cho, and D.-G. Han, "Authentication Bypass Attacks By Electromagnetic Fault Injection," Conference on Information Security and Cryptography 2018 Summer, pp. 535-540, 2018.

[5] Riscure, "Twin Scan LS2 Upgrade," 2020. https://getquote.riscure.com/en/quote/2101118/twin-scan-ls2-upgrade.htm

[6] ALPhANOV, "Double laser fault injection microscope - D-LMS," 2020. https://www.alphanov.com/en/products-services/double-laser-fault-injection

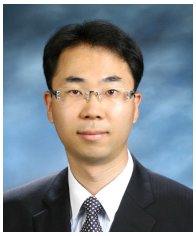
[7] Riscure, "Pinata H (Hardware crypto)," 2020. https://getquote.riscure.com/en/quote/2101126/pinata-h-hardware-crypto.htm

[8] Y. Li, K. Sakiyama, S. Gomisawa, T. Fukunaga, J. Takahashi, and K. Ohta, "Fault sensitivity analysis,"

International Workshop on Cryptographic Hardware and Embedded Systems, pp. 320-334, 2010.
〔9〕 Riscure, "Spider," 2020. https://getquote.riscure.com/en/quote/2101116/spider.htm
〔10〕 Riscure, "EM-FI Transient Probe," 2020. https://getquote.riscure.com/en/quote/2101068/em-fi-transient-probe.htm
〔11〕 Arm, "ARM Cortex-M4." 2020. https://developer.arm.com/ip-products/processors/cortex-m/cortex-m4
〔12〕 D. Kwon, J. Kim, S. Park, S. H. Sung, Y. Sohn, J. H. Song, Y. Yeom, E.-J. Yoon, S. Lee, J. Lee, and others, "New block cipher: ARIA," International Conference on Information Security and Cryptology. pp. 432-445, 2003.
〔13〕 J. Park, and J. Ha, "Improved differential fault analysis on block cipher ARIA," International Workshop on Information Security Applications, pp. 82-95, 2012.
〔14〕 H. Park, J. Lee, and D.-G. Han, "New Differential Fault Analysis Method using Multiple Fault Injection," Conference on Electromagnetic Engineering And Science 2020 Summer, 8(1), pp. 600, 2020.
〔15〕 Korea Internet & Security Agency, "Block cipher ARIA," 2019. https://seed.kisa.or.kr/kisa/Board/19/detailView.do

〈저자소개〉

이 종 혁 (JongHyeok Lee) 학생회원
2017년 2월: 국민대학교 수학과 학사
2017년 3월~현재: 국민대학교 금융정보보안학과 석박사통합과정
〈관심분야〉 부채널 분석 및 대응법 설계, 대칭키 암호 알고리즘, 스마트 카드 보안, 오류 주입 공격



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