情報保護學會論文誌
第 21 卷 第 2 號, 2011. 4

오류 주입을 이용한 Triple DES에 대한 라운드 축소 공격*

최 두 식,[1†] 오 두 환,[1] 배 기 석,[2] 문 상 재,[2] 하 재 철[1‡]
[1]호서대학교, [2]경북대학교

A Round Reduction Attack on Triple DES Using Fault Injection*

Doo-sik Choi,[1†] Doo-hwan Oh,[1] Ki-soek Bae,[2] Sang-jae Moon,[2] Jae-cheol Ha[1‡]
[1]Hoseo University, [2]Kyungpook National University

요 약

Triple DES(Data Encryption Standard)는 DES의 안전성을 향상시키기 위하여 2번의 DES 암호화와 1번의 DES 복호화를 수행하는 국제 표준 암호 알고리즘이다. 본 논문에서는 Triple DES에서 수행되는 각각의 DES 알고리즘 중 마지막 라운드를 실행시키지 않도록 오류를 주입함으로써 비밀 키를 찾아내는 차분 오류 분석(Differential Fault Analysis, DFA)공격을 제안한다. 제안한 공격 방법을 이용하여 시뮬레이션 결과, 9개 정도의 정상-오류 암호문 쌍을 얻을 수 있으면 2^{24}번의 비밀 키 전탐색을 통해 3개의 비밀 키를 모두 찾을 수 있었다. 또한, ATmega128 칩에 Triple DES 암호 알고리즘을 실제로 구현하고 레이저를 이용한 오류를 주입함으로써 제안 공격이 오류 주입 대응책이 적용되지 않은 범용 마이크로프로세서 칩에 적용 가능함을 검증하였다.

ABSTRACT

The Triple Data Encryption Algorithm (Triple DES) is an international standard of block cipher, which composed of two encryption processes and one decryption process of DES to increase security level. In this paper, we proposed a Differential Fault Analysis (DFA) attack to retrieve secret keys using reduction of last round execution for each DES process in the Triple DES by fault injections. From the simulation result for the proposed attack method, we could extract three 56-bit secret keys using exhaustive search attack for 2^{24} candidate keys which are refined from about 9 faulty-correct cipher text pairs. Using laser fault injection experiment, we also verified that the proposed DFA attack could be applied to a pure microprocessor ATmega 128 chip in which the Triple DES algorithm was implemented

Keywords: Triple-DES, Differential Fault Analysis Attack, Round Reduction.

I. 서 론

암호용 칩에 대한 물리적 공격 방법 중 오류 주입(Fault Analysis, FA) 공격은 암호용 디바이스가 암호 연산을 실행하는 도중에 오류를 주입하고 이를 통해 추출한 오류 암호문을 이용하여 비밀 키를 찾아내는 공격 방법이다. 오류 주입 공격 기법은 1997년 Boneh 등이 RSA-CRT(Chinese Remainder Theorem) 서명 알고리즘의 동작 과정에서 오류를 주입하여 비밀 정보를 추출할 수 있는 공격 방법으로 처음 소개하였고[1], 같은 해 Biham과 Shamir에 의해 블록 암호에 오류를 주입하여 얻은 오류 암호문과 정

접수일(2010년 12월 30일), 수정일(2010년 3월 11일), 게재확정일(2011년 3월 24일)
* 이 논문은 2010년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행된 연구임. (2010-0079)
† 주저자, pori86@hanmail.net
‡ 교신저자, jcha@hoseo.edu

상 암호문을 차분하여 비밀 키를 얻을 수 있는 공격 방법인 차분 오류 분석(Differential Fault Analysis, DFA) 공격이 소개되었다[2]. 이후에도 DFA 공격에 대한 많은 연구가 진행되어 DES, AES, ARIA 등의 블록 암호 알고리즘에 대한 공격 방법이 제안되었다[3~7].

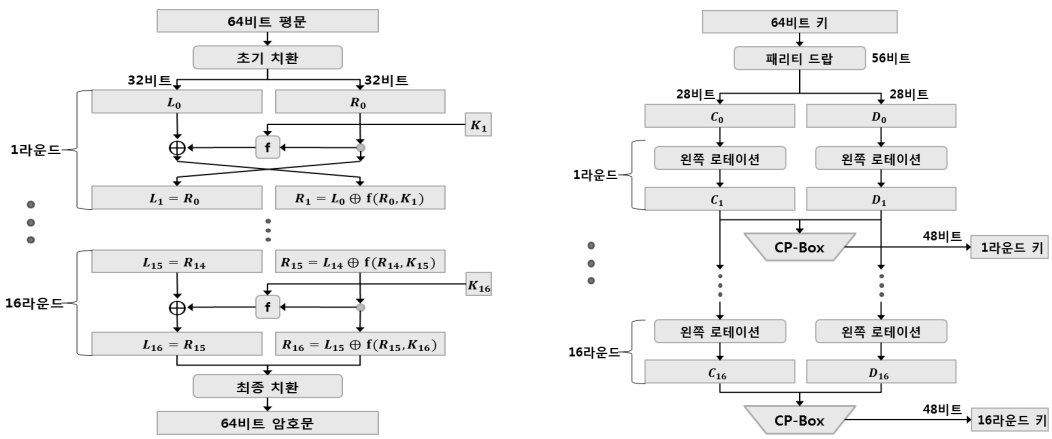
2004년에 Hemme는 DES[8]에서의 초기 라운드에 비트 단위의 오류를 주입하여 비밀 키를 얻을 수 있는 방법[9]을 제안하였고, 2006년에 Moratelli 등에 의해 마지막 라운드에서의 오른쪽 블록에 비트 단위의 오류를 주입하여 얻은 오류 암호문과, 정상 경우의 오른쪽 블록을 이용하여 비밀 키를 얻을 수 있는 방법도 제안되었다[10]. 최근에는 "for"문과 같은 반복문에 오류를 주입하여 AES의 비밀 키를 찾아내는 공격이 시도되었고 이를 실험적으로 증명한 바 있다[11, 14]. 문헌 [11, 14]와 같이 라운드가 반복되는 연산에 오류를 주입하여 암호 알고리즘의 일부 라운드를 수행하지 않도록 하는 공격을 라운드 축소(round reduction) 공격이라 부르기로 한다.

본 논문에서는 Triple DES[12]에 대해 라운드 축소 공격 개념을 적용하여 비밀 키를 공격하는 방법을 제안하고자 한다. 암호용 칩 개발자가 DES 알고리듬의 라운드를 반복 동작하도록 구현하였을 경우를 가정하고 마지막 라운드가 실행되지 못하도록 반복문에 오류를 주입하는 방법을 이용하였다. 즉, 마지막 라운드 축소 오류를 통해 얻은 오류 암호문과 정상 암호문과의 차분으로 비밀 키를 얻을 수 있는 방법을 처음으로 제안하였다. 제안한 공격 방법을 이용하면 9번의 오류 주입과 2^{24}번의 비밀 키 전탐색의 과정을 거쳐 3개의 비밀 키를 약 66%의 확률로 얻을 수 있다는 것을 시뮬레이션을 통하여 검증하였다. 또한, 반복적인 라운드 함수를 암호용 칩에 구현할 경우, 실제로 오류 주입 공격이 가능한지를 검증하기 위해 ATmega128 칩에 Triple DES 암호 알고리즘을 구현하고 레이저 오류 주입 장비를 사용하여 공격을 시도하였다. 그 결과, 오류 주입 방어 대책이 없는 암호 칩에 레이저 오류 주입 장치와 같은 정밀한 오류 주입 기술을 이용하면 비밀 키가 노출되는 위험성을 확인하였다.

II. DES 및 Triple DES에 대한 오류 주입 공격

2.1 DES 및 차분 오류 공격

DES는 64비트의 키를 이용하여 64비트의 평문을 64비트의 암호문으로 암호화하는 대칭키 블록 암호 알고리즘이다[12]. [그림 1]은 DES의 전체 구성도 및 키 생성 과정을 나타낸 것이다. DES는 초기 치환과 최종 치환 그리고 16개의 Feistel 라운드 함수로 구성되어 있다. 64비트의 입력된 평문은 초기 치환을 거쳐 두 개의 32비트로 나누어지고 이를 각각 L과 R로 표기한다. 각 라운드마다 R을 입력으로 하는 f함수의 출력과 L을 XOR한 결과 값을 다음 라운드의 R로 설정하고, R은 그대로 다음 라운드의 L로 설정한다. DES는 이와 같은 라운드를 모두 16번 수행하고 최종 치환 과정을 거치게 된다. 각 라운드에는 48비트의 라운드 키가 사용되며 이 키들은 64비트의 비밀 키로부터 생성된다. 라운드 키 생성과정을 보면, 패리티 비트 생략 과정을 거쳐 처음 64비트 키가 56비트로 축소되며 이는 각각 28비트 크기로 나누어진다. 또한 각 라운드마다 로테이션을 거친 56비트는 CP-Box(Com-



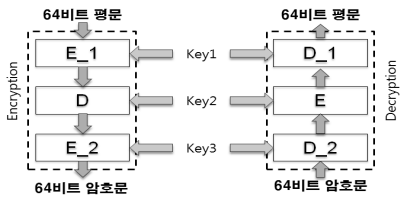
[그림 1] DES 구조 및 키 생성 과정

pression Permutation)를 통해 48비트 라운드 키를 생성하게 된다.

DES에 대한 오류 주입 공격으로는 Hemme가 제안한 DES의 각 라운드에 비트 단위의 오류를 주입하여 비밀 키를 얻는 방법이 있다[9]. 그러나 이 방식은 비트 단위의 정교한 오류 주입을 가정한 이론적 공격 방법이었고, 오류 암호문과 정상 암호문 쌍이 약 187개 정도까지 요구되는 비효율적인 공격 방법이다. 또한, 2006년에는 Moratelli 등에 의해 마지막 라운드에서의 오른쪽 블록에 비트 단위의 오류를 주입하여 얻은 오류 암호문과 정상 암호문의 오른쪽 블록을 이용하여 비밀 키를 얻을 수 있는 방법도 제안되었다[10]. 이 방법은 약 35개의 비트 오류 암호문과 정상 암호문 쌍이 필요하므로 실질적으로는 매우 정교한 오류 주입을 가정한 방법이다. 결론적으로 현재까지 DES에 대한 오류 주입 공격은 비트 단위의 중간 값 오류로만 가능하다고 시뮬레이션한 결과 정도만 있고 실험적으로 성공한 사례는 아직 없다.

2.2 Triple DES

DES는 64비트의 키를 가지고 있지만 라운드 키를 생성할 경우에는 실제로 56비트 키만 사용하고 나머지 8비트의 키를 사용하지 않으므로 2^{56}의 복잡도를 가진다. 따라서 DES의 안전성을 향상시키기 위한 방법으로 Triple DES가 제안되었다. 일반적으로 Triple DES는 [그림 2]에서 보는 것과 같이 3개의 키로 이루어져 있으며 2번의 암호화와 1번의 복호화 과정을 수행하여 64비트 평문으로부터 64비트 암호문을 얻을 수 있다. 또한, 2번의 복호화와 1번의 암호화 과정을 수행함으로써 64비트 암호문으로부터 64비트 평문을 얻는다. 이러한 Triple DES 구조를 DES-EDE3라 부르며 비밀 키는 총 56×3=168비트이다. 이에 반해 첫번째 암호 키와 세번째 암호 키를 동일하게 사용하는 DES-EDE2라 부르는 Triple DES 암호 알고리즘도 있다. 따라서 DES-EDE2 암호 알고리즘의 비밀 키는 총 56×2=112비트이다. 본 논문에서는 Triple DES 중 키를 3개 사용하여 암호 강도가 보다 높은 DES-EDE3 구조를 중심으로 설명하고자 한다. 지금까지 Triple DES에 대한 오류 주입 공격이 성공한 사례는 보고된 바가 없어 현재까지는 물리적으로 안전한 암호 알고리즘으로 인식되어 사용되고 있다.



[그림 2] DES-EDE3 방식의 Triple DES

III. Triple DES에 대한 차분 오류 공격 제안

본 논문에서 제안하는 Triple DES에 대한 공격은 각 암호화 과정에서 for문과 같은 반복문을 수행하여 16라운드를 수행한다는 것에 기반하였다. 즉, 공격자가 알고리즘이 수행될 때 15라운드까지 수행이 이루어진 후 for문에 오류를 주입하여 마지막 16라운드를 수행하지 못하도록 라운드를 하나를 축소하는 공격 기법이다. 따라서 공격자는 각 DES 알고리즘의 마지막 16라운드가 수행되지 않은 Triple DES의 출력 값을 얻을 수 있다고 가정한다. 공격자는 이렇게 얻은 오류 암호문과 정상 암호문 쌍을 이용하여 비밀 키를 찾는 공격을 시도한다.

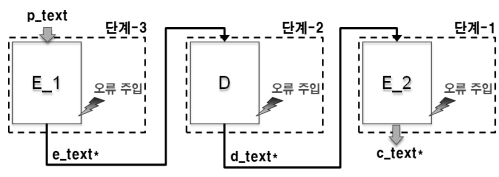
Triple DES는 3번의 DES 암·복호 알고리즘을 수행하며 3개의 키(실제로는 168 비트)로 이루어져 있다. 공격자는 3개의 모든 키를 추출하기 위해서 각 DES 알고리즘에 라운드 축소를 위한 오류를 주입한다. 본 논문에서는 Triple DES의 비밀 키를 추출하기 위해 [그림 3]과 같이 각 DES에 라운드 축소 오류를 주입하고 총 4단계로 나누어 공격한다.

단계 1 : 두번째 암호 과정 E_2에 오류 주입하는 공격으로 Key3의 후보 키 추출

단계 2 : 첫번째 복호 과정 D에 오류 주입하는 공격으로 Key2의 후보 키 추출

단계 3 : 첫번째 암호 과정 E_1에 오류 주입하는 공격으로 Key1의 후보 키 추출

단계 4 : Key1, Key2, Key3의 키 후보 중 전탐색을 통한 유일한 비밀 키 추출



[그림 3] Triple DES 공격 과정

■ 단계 1 : Key3의 후보 키 추출

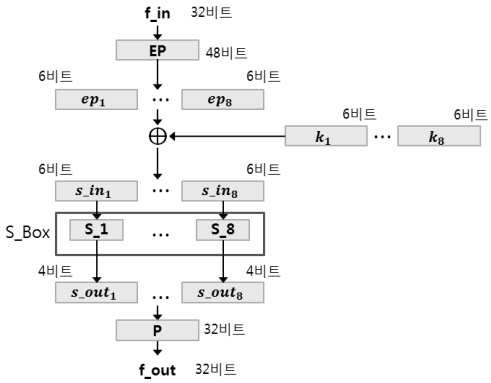
공격자는 먼저 특정한 평문을 입력으로 하는 Triple DES의 정상 암호문 c_text를 구한다. 그 후 두번째 암호화 과정에서 E_2의 15라운드까지 수행한 후 오류를 주입하여 마지막 16라운드는 수행하지 못하도록 함으로써 오류 암호문인 c_text*을 얻는다. 이 결과를 그림으로 도시한 것이 〔그림 4〕이다. 공격자는 출력으로부터 얻은 c_text와 c_text*에 대해 역최종 치환을 계산함으로써 32비트의 L과 R, 그리고 L*와 R*얻을 수 있다. 즉, c_text를 초기 치환함으로써 L과 R을 얻을 수 있고 c_text*를 초기 치환함으로써 L*와 R*를 얻을 수 있다. 여기서 L, R, L*, R*를 얻은 공격자는 다음 공식을 통해 마지막 라운드의 f함수 입력인 f_in과 출력인 f_out을 계산할 수 있다.

f_in = R

f_out = L ⊕ L*

공격자는 f_in과 f_out을 이용하여 마지막 16라운드 키를 추출할 수 있다. 즉, 공격자는 〔그림 5〕에서 보는 것과 같이 f_in에 대해 EP(Expansion Permutation)을 수행한 후, 하나의 S-Box 입력인 6비트의 부분 라운드 키 k_1를 예측하여 ep_1과 XOR한 결과 값인 s_in_1을 얻는다. 각각의 S-Box는 6비트 입력에 대해 4비트의 출력을 내는 구조로 되어 있으므로 하나의 P^{-1}(f_out)의 값을 가질 수 있는 S-Box의 입력은 4개가 존재한다. 즉, 한 개의 정상-오류 암호문 쌍을 이용하면 총 4개의 부분 키 k_1의 후보군을 얻을 수 있다.

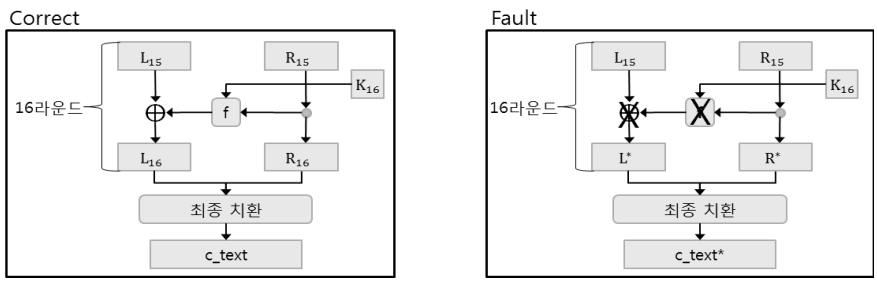
같은 방식으로 8개의 S-Box 별로 4개의 후보군을 가지는 k_2~k_8을 얻을 수 있다. 결국 16라운드 f함수의 입출력을 알고 있는 공격자는 k_1~k_8까지 4개씩의 후보 키를 찾을 수 있으므로 총 48개의 라운드 키 후보를 찾을 수 있다. 따라서 공격자는 16라운드 키의 후보를 줄이기 위해 이전에 사용하였던 평문과 다른



〔그림 5〕 6비트 단위 f 함수

평문을 사용하여 동일한 오류 주입 공격을 수행하고 새로운 키 후보군 k_1'를 추출한다. 그 후 이전의 키 후보군인 k_1 중에서 일치하는 키를 찾음으로써 키 후보를 줄일 수 있다. 이렇게 실험한 결과, 모두 3쌍의 정상-오류 암호문만 있으면 66%의 확률로 유일한 48비트 16라운드 키 k_1~k_8을 얻을 수 있었다. 마지막 16라운드 키를 추출하는데 필요한 오류-정상 암호문 쌍의 갯수에 대한 내용은 4장에서 추가로 설명한다.

이와 같은 방식으로 마지막 라운드 키를 찾은 공격자는 〔그림 1〕에서의 키 생성 과정을 역으로 계산하여 최종 비밀 키인 Key3을 얻을 수 있다. 하지만 유일한 마지막 라운드 키를 추출했다 하더라도 〔그림 1〕의 키 생성 과정에서 보는 것과 같이 48비트 라운드 키가 CP^{-1}(Inverse Compression Permutation)를 거치므로 56비트 최종 비밀 키를 찾기 위해서는 CP-Box에 존재하지 않는 8개의 비트를 예측해야 한다. 그러므로 16라운드 키를 계산한 공격자는 최종적으로 2^8 = 256개의 56비트 Key3 후보군을 찾게 된다. 이 단계에서 16라운드 키를 찾기 위해서는 한 개의 정상-오류 암호문 쌍을 대상으로 한 번의 f함수에 관한 연산량 정도이다.



〔그림 4〕 암호화 알고리즘 E_2에서의 16라운드 오류 주입

■ 단계 2 : Key2의 후보 키 추출

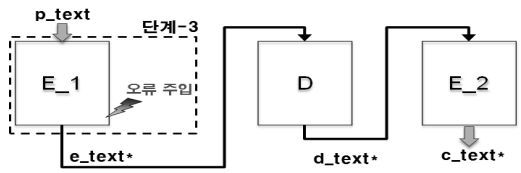
단계 1에서 암호화 알고리즘 E_2의 후보 키 256개를 찾았으므로 이제 복호화 알고리즘 D의 후보 키를 찾아야 한다. 복호화 알고리즘 D의 비밀 키를 찾기 위해 단계 1과 유사한 방법을 이용하여 〔그림 6〕에서 보는 것과 같이 D의 마지막 라운드는 실행되지 않도록 함으로써 공격자는 c_text*를 얻을 수 있다. 여기서 공격자는 D에서 사용된 비밀 키를 찾아야 하므로 D의 출력 값인 d_text와 d_text*를 얻어야 한다. d_text와 d_text*는 c_text와 c_text*를 단계 1에서 얻은 Key3의 후보 키 중 하나를 선택하여 복호화함으로써 얻을 수 있다. 결국, 공격자는 하나의 Key3 후보를 선택하여 d_text와 d_text*를 얻고, 〔그림 4〕와 같이 D의 출력인 L, R, L*, R*를 계산한다. 그리고 L, R, L*, R*를 이용하여 D에서의 f_in과 f_out을 얻을 수 있다.

따라서 공격자는 단계 1에서와 동일한 방법으로 D에서 사용된 마지막 라운드 키를 계산할 수 있다. 여기서 마지막 라운드 키는 D가 복호화 과정이므로 〔그림 1〕의 키 생성 과정에서 생성된 1라운드 키를 이용한다. 즉, 1라운드 키를 추출한 공격자는 CP^{-1}과 한 번의 오른쪽 로테이션을 통해 최종 비밀 키 Key2를 계산할 수 있다. 결국, 단계 2에서의 공격은 하나의 Key3의 후보 키에 대한 총 256개의 알고리듬 D에 사용된 비밀 키 Key2를 찾을 수 있다. 이 단계에서 16라운드 키를 찾기 위해서는 한 개의 정상-오류 암호문 쌍을 대상으로 총 2^9번의 DES 복호연산과 f함수를 연산하는 계산이 필요하다.

〔그림 6〕 복호화 알고리즘 D에 대한 오류 주입

■ 단계 3 : Key1의 후보 키 추출

공격자는 암호화 알고리즘 E_1에 사용된 비밀 키를 얻기 위하여 〔그림 7〕에서 보는 것과 같이 E_1의 마지막 라운드를 건너뛰는 오류를 주입한다. 그러므로 공격자는 E_1의 마지막 라운드를 수행하지 않은 c_text*를 얻을 수 있다. 여기서 공격자는 e_text와 e_text*를 얻기 위하여 c_text와 c_text*를 단계 1에서 얻은 Key3의 후보 키 중 하나를 선택하여 복호화하고, 다시 단계 2에서 얻은 Key2의 후보 키 중 하나를 선택하여 암호화를 수행한다. 이렇게 얻은 e_text와 e_text*를 이용하여 위에서 유사한 방법으로 암호화 알고리즘 E_1에서 사용된 마지막 16라운드 키를 추출할 수 있으며 최종적으로 256개의 Key1을 추출할 수 있다. 단계 3까지 수행한 공격자는 각각 256개씩의 Key1, Key2, Key3 후보를 얻을 수 있다. 이 단계에서 16라운드 키를 찾기 위해서는 한 개의 정상-오류 암호문 쌍을 대상으로 총 2^{17}번의 DES 복호-암호 연산과 f함수를 연산하는 계산이 필요하다.



〔그림 7〕 E_1에 대한 오류 주입

■ 단계 4 : 전탐색을 통한 유일한 비밀 키 추출

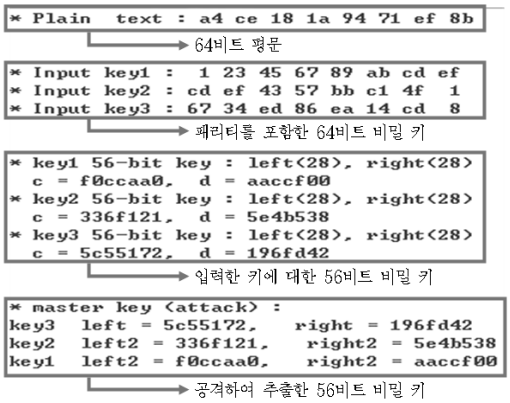
공격자는 단계 1, 단계 2, 단계 3을 수행하여 각각 2^8개씩의 Key1, Key2, Key3의 후보군을 얻을 수 있어 결국 2^{24}개의 후보 키를 찾을 수 있다. 공격자가 키의 후보군 중 유일한 하나의 키를 추출하기 위해서는 모든 후보 키 를 이용하여 Triple DES를 수행하고 올바른 출력 c_text를 출력하는 하나의 키를 찾음으로써 유일한 Key1, Key2, Key3을 추출한다.

IV. 시뮬레이션 및 실험

4.1 컴퓨터 시뮬레이션

본 논문에서 제안한 공격 기법을 컴퓨터로 시뮬레이션하여 그 가능성을 검증하였다. 시뮬레이션을 위해서는 AMD 애슬론 6400 프로세서, 3G RAM의 사양을 갖춘 PC와 Visual Studio 2008 개발 도구를 사용하였다. 〔그림 8〕은 제안한 공격 방법을 이용하여 시뮬레이션 한 결과로서, DES의 패리티 비트를 제외한 56비트 비밀 키를 찾아낼 수 있음을 보이고 있다. 그림에서 보는 바와 같이 컴퓨터로 라운드 축소 실험을 한 결과 정확히 168비트의 Triple DES의 최종 비밀 키를 찾아낼 수 있었다.

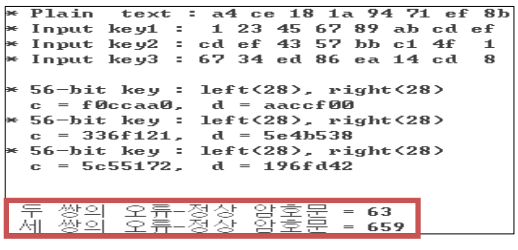
위에서 언급한 것과 같이 제안한 공격 방법은 먼저 알고리즘 E_2에서 사용한 Key3의 후보 키 256개를 추출하게 된다. 그런데 공격자가 Key3의 후보 키 256개를 추출하기 위해서는 E_2에 오류를 주입하여



〔그림 8〕 오류 주입 공격 시뮬레이션 결과

얻은 오류 암호문과 정상 암호문을 이용하여 유일한 16라운드 키를 추출하여야만 한다. 하지만 한 번의 오류 주입만으로 얻은 오류-정상 암호문 쌍으로는 유일한 16라운드 키를 찾을 수 없으며 총 4^8개의 라운드 키 후보를 찾을 수 있다.

그러므로 공격자는 여러 번의 오류 주입을 통해 16라운드 키의 후보군을 한 개까지 줄여야 한다. 본 논문에서는 몇 개정도의 오류-정상 암호문 쌍으로 16라운드 키를 찾을 수 있는지 시뮬레이션해 보았다. 시뮬레이션 결과, 총 1,000개의 DES 연산과정에서 하나의 오류-정상 암호문을 이용했을 경우에는 유일한 16라운드 키를 한 번도 찾을 수 없었다. 그러나 두 쌍의 오류-정상 암호문을 이용했을 경우에는 63번의 16라운드 키를 찾을 수 있었다. 또한, 세 쌍의 오류-정상 암호문을 이용했을 경우에는 659번에 걸쳐 정확한 16라운드 키를 찾을 수 있었다. 즉, 제안하는 공격에서 세 쌍의 오류-정상 암호문 쌍을 이용한다면 약 66%의 확률로 48비트의 16라운드 키를 찾아낼 수 있음을 확인하였다. 물론, 더 많은 오류-암호문 쌍을 이용하면 높은 확률로 16라운드 키를 찾을 수 있었지만 공격에는 세 쌍의 오류-정상 암호문으로도 충분하였다.

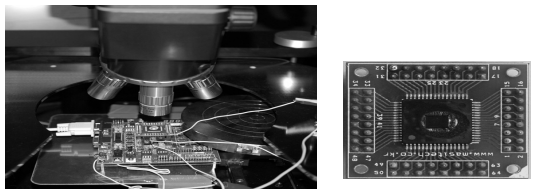


〔그림 9〕 유일한 16라운드 키 추출 가능성 테스트

4.2 하드웨어 오류 주입 실험

이 절에서는 반복적인 라운드 함수를 이용해 Triple DES를 암호용 칩에 구현할 경우, 오류 주입이 가능한지를 검증하기 위해 ATmega128 칩에 Triple DES 암호 알고리즘을 구현하고 오류 주입 공격을 시도해 보았다. 오류 주입을 위해서는 EzLaze 3 레이저 장비를 사용하였다. 물론, 파형 관측을 위해 고성능 오실로스코프 장비를 사용하였으며 오류가 주입되는 위치를 정확히 파악하고 레이저를 이용한 준침투형(semi-invasive) 공격을 위해 ATmega128 칩의 표면을 디캡핑(decapping)하였다. 〔그림 10〕은 레이저 오류 주입 공격 장치와 디캡핑된 ATmega128 칩을 나타낸 것이다[13]. 또한, 디캐핑한 칩에 공간적으로 정확한 오류 주입 위치를 잡기 위해 광학 현미경을 이용하였다. 유사한 물리적 구현 환경에서 라운드 축소를 이용한 오류 주입 공격 실험은 최근에 AES 암호 알고리즘에 적용되어 사용된 바 있다[11, 14].

표의 사용도 그림과 동일한 형식을 이용합니다. 표의 제목은 표의 상단(좌측)에 위치합니다. 표의 여백도 그림의 여백과 마찬가지로 다른 요소와 구분되기 위해 5mm의 여백을 주어야 합니다.



〔그림 10〕 디캐핑된 칩과 레이저 오류 주입 장치

실험을 위해 사용된 Triple DES의 비밀 키는 다음과 같다.

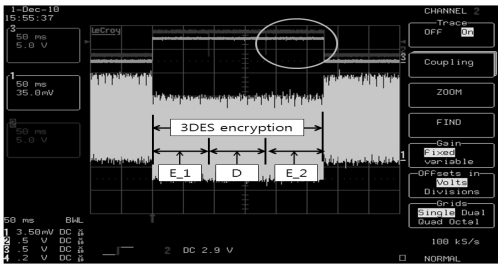
첫번째 암호 알고리즘 E_1의 키
- 0x 01 23 45 67 89 ab cd df

첫번째 복호 알고리즘 D의 키
- 0x cd ef 43 57 bb c1 4f 01

두번째 암호 알고리즘 E_2의 키
- 0x 67 34 ed 86 ea 14 cd 08

제안한 공격 방법에서는 Triple DES의 각 E_2, D, E_1의 16라운드를 수행하지 못하도록 오류를 주입하여야 한다. 그러므로 공격자는 오류를 주입할 시점을 결정하여야 하고 이는 Triple DES 동작에 대

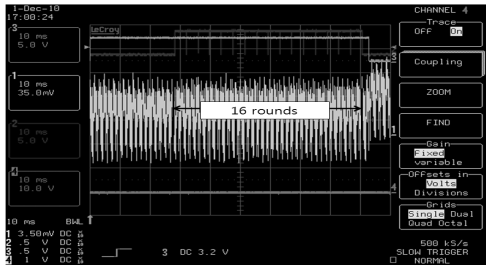
한 소비 전력 파형을 분석함으로써 오류 주입 시점을 결정할 수 있다. 〔그림 11〕은 ATmega128 칩에서 실제 Triple DES가 정상적으로 수행한 경우의 전력 파형을 보여주고 있다. 그림에서 맨 위의 빨간색 선은 Triple-DES 시작하기 위한 입력을 주는 시점과 그 결과를 출력하는 단계에서 발생하는 신호 파형을 검출함으로써 Triple-DES 구간을 나타낸 것이다. 또한, 파형의 굵은 노란색이 Triple-DES가 수행되는 동안의 칩의 전력 소비 파형을 나타낸 것인데 그림에서 보는 것과 같이 E_1, D, E_2가 실행되는 부분을 확인할 수 있다.



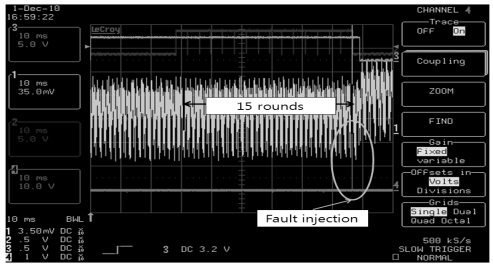
〔그림 11〕 정상적인 Triple DES 신호 전력

전력 파형을 통해 E_2가 실행되는 시점을 확인하였고 E_2에서 실행되는 16라운드를 확인하기 위해서 E_2 부분의 파형을 세밀하게 분석하였다. 〔그림 12-(a)〕는 E_2에 대한 확대 파형을 보여주고 있으며 1~16라운드까지 16개의 라운드로 구분되어 있으므로 각 라운드의 시점을 확인할 수 있었다. 〔그림 12-(b)〕는 16라운드에 직전에 오류를 주입함으로써 16라운드가 수행되지 않았음을 전력 파형을 통해 보여주고 있다. 〔그림 12-(b)〕에서 보는 것과 같이 16라운드가 수행되기 전에 오류를 주입하였으므로 정상적인 전력 파형보다 1라운드 일찍 종료되며 정상 전력 파형의 경우 16부분으로 나뉘지만 오류가 주입되었을 경우에는 15부분만 나누어지게 된다. 실제로 오류가 주입되어 마지막 라운드를 수행하지 않았는지의 여부는 오류에 의한 Triple DES의 출력 결과를 통해서 검증할 수 있다. 고성능의 오실로스코프와 광학 전자 현미경을 이용하여 공격 시점을 탐색하는 반복적인 실험을 통해 16라운드를 건너뛰는 오류 주입 공격이 가능함을 확인할 수 있었다.

〔그림 13〕은 〔그림 12-(a)〕와 같이 정상적으로 E_2의 암호화 과정을 수행함으로써 얻은 정상 암호문과 〔그림 12-(b)〕와 같이 오류를 주입하여 16라운드

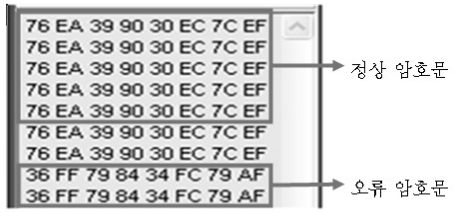


〔그림 12-(a)〕 정상적인 16라운드 전력 파형



〔그림 12-(b)〕 라운드가 축소된 전력 파형

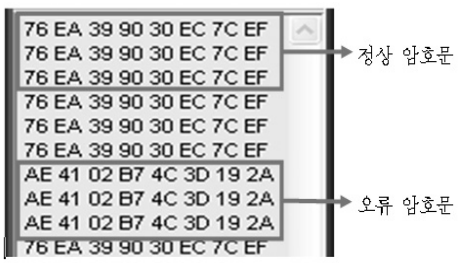
를 수행하지 못하도록 함으로써 얻은 오류 암호문을 순차적으로 보여주고 있다. 〔그림 13〕에서 보는 것과 같이 공격자가 정상 암호문과 오류 암호문을 얻을 수 있으므로 3장에서 제안한 공격 방법을 이용하여 E_2에서 사용된 비밀 키인 Key3의 후보 키 256개를 추출할 수 있다.



〔그림 13〕 알고리듬 E_2에 대한 정상-오류 암호문

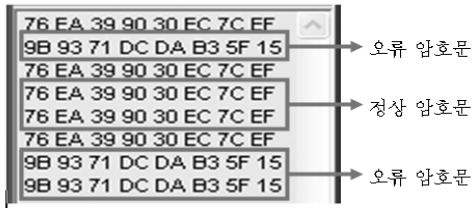
마지막 DES 암호의 비밀 키 Key3 후보를 추출한 후, 복호 알고리즘 D에서 사용된 Key2의 후보 키를 추출하기 위하여 알고리즘 D에 오류를 주입하여야 한다. D에 오류를 주입하는 것도 E_2와 동일한 방법을 통해 주입하며 오류가 성공적으로 주입되면, 〔그림 14〕와 같은 정상 암호문과 오류 암호문을 얻을 수 있다. 이 결과를 통해 이용하여 하나의 후보 키 Key3에 대해 복호 알고리듬 D에서 사용된 비밀 키인 Key2의

후보 키 256개씩을 추출할 수 있다.



〔그림 14〕 알고리즘 D에 대한 정상-오류 암호문

첫번째 암호 알고리즘 E_1도 위와 같은 방식으로 오류를 주입하여 정상 암호문과 오류 암호문을 얻을 수 있다. 〔그림 15〕는 정상 암호문과 오류 암호문이다. 이 결과를 통해 이용하여 하나의 후보 키 Key3와 Key2에 대해 암호 알고리즘 E_1에서 사용된 비밀 키인 Key1의 후보 키 256개씩을 추출할 수 있다.



〔그림 15〕 알고리즘 E_1에 대한 정상-오류 암호문

위에서 살펴본 것처럼 공격자는 ATmage 128 칩에서 동작하는 Triple DES의 전력 파형을 분석하여 오류 주입 시점을 확인할 수 있고 원하는 시점에 오류를 주입하는 것이 가능하다. 따라서 오류 주입 방어 대책이 없는 순수한 암호 칩에서 Triple DES를 구현한다면, 공격자는 레이저 오류 주입 장치와 같은 정밀한 오류 주입 기술을 이용하면 비밀 키가 찾을 수 있다. 이와 더불어 위에서 언급한 DES-EDE2 방식의 Triple DES에서는 비밀 키를 두개만 사용하므로 DES-EDE3 방식보다 더 쉽게 비밀 키를 찾아낼 수 있다. DES-EDE2 방식에서 첫 번째 암호 키와 세 번째 암호 키를 동일한 것을 사용하므로 3장에서 기술한 DES-EDE3 공격의 1단계와 2단계를 수행 후 바로 4단계를 수행하면 된다. 따라서 약 6번의 오류 주입과 216번의 후보 키 전수 조사를 사용하여 112비트의 비밀 키를 찾아낼 수 있다.

V. 결 론

본 논문에서는 오류를 주입하여 각 라운드 연산을 축소하는 방법으로 DES의 마지막 라운드를 실행시키지 못하도록 함으로써 얻은 오류 암호문과 정상 암호문으로 Triple DES의 비밀 키를 추출할 수 있는 공격 방법을 제안하였다. 제안한 공격 방법은 암·복호 알고리즘의 각 단계마다 3번의 오류를 주입함으로써 약 66%의 확률로 키 후보 추출이 가능하였다. 결국, Triple DES를 공격하는데 총 9번의 오류 주입과 2^{24}번의 후보 키 전수 조사를 사용하여 모든 비밀 키를 찾아낼 수 있었다. 그리고 제안 방식을 컴퓨터에서 시뮬레이션해 봄으로써 그 가능성을 검증하였으며, ATmega128 칩에 Triple DES를 직접 구현하여 실제 오류 주입 공격을 수행해 보았다. 결론적으로 라운드 축소를 이용한 오류 주입 공격은 표준 암호 알고리즘인 AES나 (Triple) DES와 같은 블록 암호 알고리즘에 사용될 수 있으므로 이에 대한 물리적 대응책 마련이 필요하다.

참고문헌

〔1〕 D. Boneh, R. DeMillo, and R. Lipton, "On the Importance of Checking Cryptographic Protocols for Faults," EUROCRYPTO'97, LNCS 1233, pp. 37-51, 1997.

〔2〕 E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," CRYPTO'97, LNCS 1294, pp. 513-525, 1997.

〔3〕 National Institute of Standards and Technology, "Advanced Encryption Standards," NIST FIPS PUB 197, 2001.

〔4〕 G. Piret and J. Quisquater, "A differential fault attack technique against SPN structures, with application to the AES and KHAZAD," CHES'03, LNCS 2779, pp. 77 - 88, 2003.

〔5〕 C. Giraud, "DFA on AES," Advanced Encryption Standard-AES'04, LNCS 3373, pp. 27 - 41, 2005.

〔6〕 C. Kim and J. Quisquater, "New Differential Fault Analysis on AES Key Schedule: Two Faults are enough,"

CARDIS'08, LNCS 5189, pp. 48-60, 2008.
〔7〕 W. Li, D. Gu, J. Li, "Differential Fault Analysis on the ARIA Algorithm," Information Science. Vol. 178, Issue. 19, pp. 3727-3737, 2008.
〔8〕 NIST, "Data Encryption Standard(DES)," NIST FIPS PUB 46-3, 1999.
〔9〕 L. Hemme, "A Differential Fault Analysis Against Early Rounds of (Triple)-DES," CHES'04, LNCS 3156, pp. 254-267, 2004.
〔10〕 C. R. Moratelli, E. Cota, M. S. Lubaszawski, "A Cryptography Core Tolerant to DFA Fault Attacks," SBCCI-2006, pp. 190-195, 2006.
〔11〕 H. Choukri and M. Tunstall, "Round reduction using faults," FDTC'05, pp. 13-24. 2005.
〔12〕 NIST, "Recommendation for the Triple Data Encryption Algorithm(TDEA) Block Cipher," NIST FIPS PUB 800-67, 2008.
〔13〕 Atmel사 홈페이지, http://www.atmel.com/atmel/acrobat/doc2467.pdf
〔14〕 박제훈, 배기석, 오두환, 문상재, 하재철, "AES에 대한 반복문 오류 주입 공격," 한국정보보호학회논문지, 20(6), pp. 59-65, 2010년 12월.

〈著者紹介〉

최 두 식(Doo-sik Choi) 학생회원
2010년 2월: 호서대학교 정보보호학과 졸업
2010년 3월~현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 신뢰 컴퓨팅, 네트워크 보안, 부채널 공격

오 두 환(Doo-hwan Oh) 학생회원
2010년 2월: 호서대학교 정보보호학과 졸업
2010년 3월~현재: 호서대학교 정보보호학과 석사과정
〈관심분야〉 부채널 공격, 네트워크 보안, 신뢰 컴퓨팅

배 기 석 (Ki-seok Bae) 학생회원
2006년 8월: 경북대학교 전자·전기공학부 졸업
2008년 8월: 경북대학교 전자공학과 석사
2009년 3월~현재: 경북대학교 전자공학과 박사과정
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안

문 상 재 (Sang-jae Moon) 종신회원
1972년 2월: 서울대학교 공업교육(전자전공)과 학사
1974년 2월: 서울대학교 전자공학과 석사
1984년 6월: 미국 UCLA 전기공학과 박사
1984년 7월~1985년 6월: UCLA Postdoctor 근무
1984년 7월~1985년 6월: 미국 OMNET 컨설턴트
1997년 9월~1998년 8월: 경북대학교 전자전기공학부 학부장
1974년 12월~현재: 경북대학교 IT대학 전자공학부 교수
2000년 8월~현재: 경북대학교 이동네트워크 정보보호기술 연구센터장
2002년 2월~현재: 한국정보보호학회 명예회장
〈관심분야〉 정보보호, 디지털 통신, 이동 네트워크

하 재 철 (Jae-cheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 학사
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2006년 7월~2006년 12월: QUT in Australia 연구 교수
2007년 3월~현재: 호서대학교 정보호호학과 부교수
2002년 3월~현재: 한국정보보호학회 이사
2009년 1월~현재: 한국산학기술학회 이사
〈관심분야〉 정보보호, 네트워크 보안, 스마트카드 보안