情報保護學會論文誌
第 22 卷 第 4 號, 2012. 8

반복문 오류 주입을 이용한 개선된 Triple DES 라운드 축소 공격*

최 두 식,† 오 두 환, 박 정 수, 하 재 철‡
호서대학교

An Improved Round Reduction Attack on Triple DES Using Fault Injection in Loop Statement*

Doo-Sik Choi,† Doo-Hwan Oh, Jeong-Soo Park, Jae-Cheol Ha‡
Hoseo University

요 약

블록 암호 알고리듬에 대한 라운드 축소 공격은 암호 디바이스에 일시적인 오류를 주입하여 암호 알고리듬이 정상 라운드를 수행하는 것이 아니라 특정 라운드까지만 수행하도록 하여 비밀 키를 추출하는 오류 주입 공격 방법이다. 본 논문에서는 Triple DES(Data Encryption Standard)에서 라운드를 반복하는 반복문을 수행하는 도중 오류를 주입하여 마스터 키를 추출할 수 있는 방법을 제시하고 이를 실험과 컴퓨터 시뮬레이션을 통해 검증하고자 한다. ATmega128 칩에 Triple DES 암호 알고리듬을 실제로 구현하고 레이저를 이용한 오류를 주입함으로써 제안한 공격이 오류 주입 대응책이 적용되지 않은 범용 마이크로프로세서 칩에 적용 가능함을 검증하였다. 기존 Triple DES에 대한 라운드 축소 공격은 총 9개의 정상-오류 암호문쌍이 필요하였지만 본 논문에서는 5개의 오류 암호문으로 모든 마스터 키를 찾아 낼 수 있었다.

ABSTRACT

The round reduction on block cipher is a fault injection attack in which an attacker inserts temporary errors in cryptographic devices and extracts a secret key by reducing the number of operational round. In this paper, we proposed an improved round reduction method to retrieve master keys by injecting a fault during operation of loop statement in the Triple DES. Using laser fault injection experiment, we also verified that the proposed attack could be applied to a pure microprocessor ATmega 128 chip in which the Triple DES algorithm was implemented. Compared with previous attack method which is required 9 faulty-correct cipher text pairs and some exhaustive searches, the proposed one could extract three 56-bit secret keys with just 5 faulty cipher texts.

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

I. 서 론

오류 주입 공격은 암호 알고리듬을 탑재하고 있는 암호 디바이스에 레이저 또는 전압 글리치 같은 물리적 공격 방법을 통해 일시적인 오류를 발생시킴으로써 비밀 키를 찾는 공격을 수행한다. 오류가 주입된 암호

접수일(2011년 12월 12일), 수정일(2012년 1월 30일), 게재확정일(2012년 1월 30일)
* 이 논문은 2011학년도 호서대학교의 재원으로 학술연구비 지원을 받아 수행한 연구임(2011-0273)
† 주저자, pori86@hanmail.net
‡ 교신저자, jcha@hoseo.edu

디바이스는 정상적인 암호문이 아닌 오류로 인해 발생된 오류 암호문을 출력하게 되고, 공격자는 이 오류 암호문과 정상 암호문을 분석하여 비밀 키를 추출하는 것이 가능하다. 이와 같은 오류 주입 공격은 1997년 Boneh 등이 RSA-CRT(Chinese Remainder Theorem)를 공격하는 방법으로 처음 제안하였으며[1], 이 후, Biham과 Shamir가 차분 오류 분석(Differential Fault Analysis, DFA) 공격을 제안하였다. 차분 오류 주입 공격은 DES나 AES와 같은 블록 암호 시스템에 오류를 주입하여 얻은 오류 암호문과 정상 암호문을 차분하여 비밀 키를 추출할 수 있는 공격 방법이다[2, 3, 4, 5].

DES[6]에 대한 차분 오류 분석 공격으로서 2004년 Hemme가 DES의 초기 라운드에 비트 단위의 오류를 주입하여 비밀 키를 얻을 수 있는 방법으로 제안한 바 있으며[7], 2008년에는 Baldwin 등에 의해 15 라운드에서의 오른쪽 블록에 오류를 주입하여 얻은 오류 암호문을 이용하여 비밀 키를 얻을 수 있는 방법도 제안되었다[8]. 이러한 오류 주입 공격은 암호 연산이 수행되는 중간 값에 대해 오류를 주입하는 데이터에 대한 오류 발생 기법을 이용하였다.

최근 Triple DES[9]에 대한 공격으로는 라운드 축소 공격을 이용하여 Triple DES에서 사용되는 3개의 모든 키를 찾아는 방법이 제안되었다[10]. 이 공격에서는 데이터에 대한 오류를 발생시키는 것이 아니라 Choukri-Tunstall이 제안했던 라운드 축소 오류 주입 방법[11]을 이용하고 있는데 AES 암호 알고리듬 공격에 이미 사용된 바도 있다[12]. 즉, Triple DES의 각 DES에서 마지막 라운드가 실행되지 않도록 반복문에 오류를 주입하고 비밀 키를 추출하는 방법이다. 기존에 제시된 이 공격 방법은 각 DES당 3번의 오류를 주입하여 총 9번의 오류 주입이 필요하며 2^{24}번의 전탐색 과정을 통해 3개의 유일한 56비트 마스터 키 추출이 가능하다.

본 논문에서는 논문 [10]에서와 같이 반복문에 오류를 주입하여 라운드를 축소할 수 있다는 동일한 가정하에 개선된 오류 주입 공격 기법을 제시한다. 즉, 이전 방법과 달리 Triple DES의 각 DES에서 마지막 라운드가 실행되지 않도록 오류를 주입하는 것이 아니라 3번째 DES(암호화), 2번째 DES(복호화)에서는 1라운드와 2라운드까지만 수행한 오류 암호문 두 개와, 1번째 DES(암호화)에서는 1라운드만 수행한 오류 암호문, 총 5개의 오류 주입과 $3*2^{24}$번의 전탐색 과정을 통해 3개의 유일한 마스터 키를 추출할 수 있는 공격 방법을 제시한다. 그리고 컴퓨터 시뮬레이션을 통해 제시한 공격 방법에 대해 비밀키를 추출할 수 있음을 검증하였으며, ATmega 128 칩에 Triple DES를 구현하고 레이저를 이용하여 오류를 주입하는 실험을 수행함으로써 제안한 공격 방법이 실제 환경에서 적용 가능하다는 것을 증명하였다.

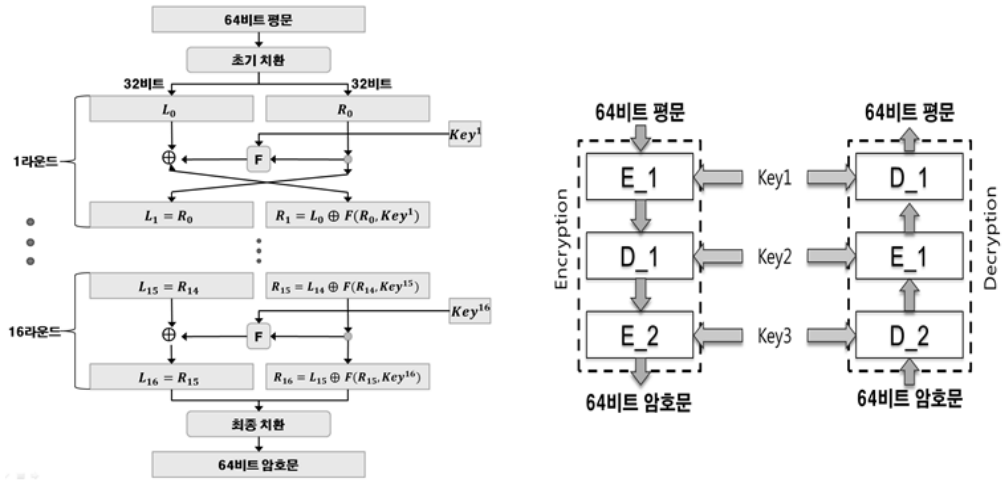
본 논문의 구성은 다음과 같다. 2장에서는 Triple DES와 기존의 Triple DES에 대한 라운드 축소 공격을 소개한다. 3장에서는 본 논문에서 제시하고자 하는 공격 방법을 소개하며, 4장에서는 제시한 공격 방법에 대한 오류 주입 실험 및 컴퓨터 시뮬레이션 결과를 보이고자 한다. 마지막으로 5장에서는 결론을 맺는다.

II. Triple DES에서의 오류 주입 공격

2.1 Triple DES

DES는 64비트의 키를 이용하여 64비트의 평문을 64비트의 암호문으로 암호화하는 대칭키 블록 암호 알고리듬이다. DES의 암호화에서 입력되는 평문은 초기 치환을 수행하고, Feistel 구조의 16라운드 연산을 수행한 후, 최종 치환을 수행함으로써 암호문으로 출력된다. 복호화의 경우 암호화와 같은 구조로 수행되며 암호화에서 사용되었던 키를 반대 순서로 사용함으로써 복호화가 가능하다. 각 라운드는 2개의 32비트 블록으로 나누어 수행되며 오른쪽 블록은 다음 라운드의 왼쪽 블록으로 이동되고 왼쪽 블록은 F함수를 수행한 오른쪽 블록과 XOR된 결과 값이 다음 라운드의 오른쪽 블록으로 이동된다. 그러나, 마지막 라운드를 마치고는 두 블록의 위치는 교환하지 않고 그대로 출력된다.

Triple DES는 DES의 안전성을 향상시키기 위한 방법으로 총 3번의 DES 연산을 통해 최종 암호문 값을 출력한다. Triple DES에서의 암호화는 총 3번의 DES를 이용하여 암호화, 복호화, 암호화 순서로 이루어지고, 복호화는 DES 복호화, 암호화, 복호화 순서로 암호화와 반대 연산을 수행함으로써 평문을 얻을 수 있다. 이때 사용되는 키는 각 DES마다 다른 키를 사용하여 총 3개의 키를 가지는 DES-EDE3 방식이 있으며, 첫 번째 암호화와 세 번째 암호화가 같은 키를 사용하여 총 2개의 키를 가지는 DES-EDE2 방식이 있다. DES 각 라운드 과정과 Triple DES의 구조는 [그림 1]과 같으며, 본 논문에서의 총 3개의 키



〔그림 1〕 DES의 라운드 과정과 Triple DES

를 가지는 DES-EDE3 방식을 중심으로 설명한다.

2.2 라운드 축소를 이용한 Triple DES 공격

최두식 등이 제안한 Triple DES에 대한 라운드 축소 공격은 공격자가 정상적으로 수행된 DES의 정상 암호문 C와 DES의 마지막 라운드를 실행시키지 못하도록 하는 오류를 주입하여 15라운드까지만 수행된 오류 암호문 C^*를 얻을 수 있다는 가정 하에 제안된 공격 방법이다[10]. 〔그림 2〕에서 보는 바와 같이 공격자가 C와 C^*를 얻으면 최종 치환을 역으로 계산한 C를 통해, 16라운드의 결과 값 L_{16}, R_{16}을 얻을 수 있고, C^*를 통해, 15라운드의 결과 값 L_{15}, R_{15}를 얻을 수 있다.

그리고 공격자는 L_{16}, R_{16}, L_{15}, R_{15}를 이용하여 16라운드 F함수의 입력 값(F_{in})과 출력 값(F_{out})을 얻을 수 있다. F_{in}의 경우에는 R_{15}가 F_{in}이기 때문에 별다른 연산없이 얻는 것이 가능하며, F_{out}의 경우에는 F함수 연산을 수행한 R_{15}의 결과 값이 F_{out}이 되고, F_{out}과 L_{15}를 XOR한 결과 값이 L_{16}이기 때문에 L_{15}와 L_{16}을 XOR하면 F_{out}을 얻을 수 있다.

$$F_{in} = R_{15} = R_{16}$$
$$F_{out} = L_{15} \oplus L_{16} \rightarrow F_{out} \oplus L_{15} = L_{16}$$

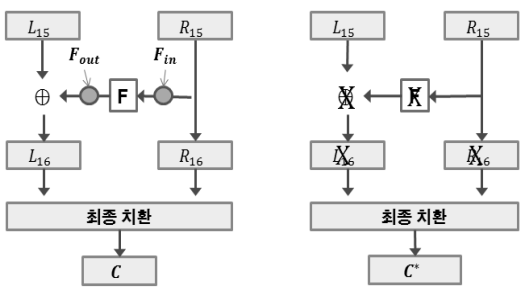
16라운드의 F_{in}과 F_{out}을 알고 있는 공격자는 F함수에서 사용되는 16라운드 키를 S-box 단위로 전탐색하여 추출할 수 있다. 16라운드 키를 전탐색하여 후보키를 추출하는 과정은 다음과 같다.

① F_{out}을 단순 치환으로 역계산한다. 즉, S-Box의 출력 값(S_{out})을 계산한다.

② 계산된 S_{out}을 다시 S-Box를 역으로 계산한다. 즉, S-Box의 입력 값(S_{in})을 계산한다. 이때, S-box는 총 8개가 존재하며, S_{out}의 경우 S-Box 하나당 4비트의 크기를 가지고 S_{in}의 경우 S-Box 하나당 6비트의 크기를 가진다. 따라서, 1개의 S_{out} 값은 4개의 S_{in} 값을 가지게 된다. 즉 $S_{in}^1 \sim S_{in}^8$까지 존재하며, 하나의 S_{in}은 4개의 후보 값을 가지게 된다.

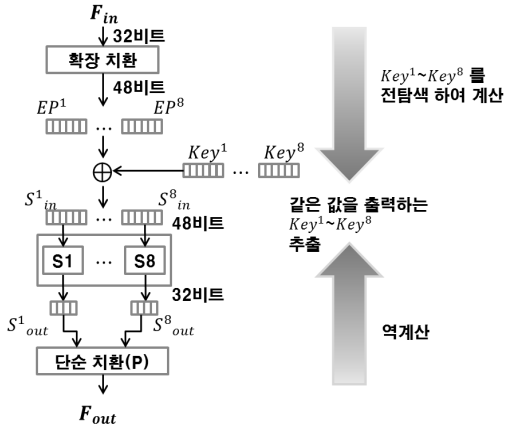
③ F_{in}을 확장 치환으로 계산한다. 즉, 확장 치환을 거친 48비트 출력 값(EP)을 계산한다.

④ Key를 전탐색하여 EP와 XOR 연산을 수행한다. 이때, Key와 EP는 $S_{in}^1 \sim S_{in}^8$까지와 마찬가지로 6비트씩 $Key^1 \sim Key^8$, $EP^1 \sim EP^8$ 단위로 연산을



〔그림 2〕 기존 라운드 축소 오류 주입

수행하며, $Key^1 \oplus EP^1$의 연산 결과 값이 S^1_{in}과 같은 값을 출력하는 Key^1을 찾으면 된다. S^1_{in}은 4개의 후보 값을 가지기 때문에 Key^1도 4개의 후보 값을 가지게 된다. 따라서, $Key^1 \sim Key^8$까지 각 4개의 후보 값을 가지게 된다.



〔그림 3〕 F함수에서의 Key 추출 과정

공격자는 위와 같은 방식으로 각 4개의 후보 값을 가지고 있는 $Key^1 \sim Key^8$을 추출하는 것이 가능하다. $Key^1 \sim Key^8$는 4개씩의 후보 값을 가지기 때문에 16라운드 키의 후보는 총 4^8개라고 할 수 있다. 공격자는 16라운드 키의 후보군을 줄이기 위해서 또 다른 정상, 오류 암호문 쌍을 이용하며, 3쌍의 정상, 오류 암호문을 이용하면 약 66%의 확률로 유일한 16라운드 키를 추출하는 것이 가능하다. 48비트의 유일한 16라운드 키를 추출하였다고 하더라도 DES의 56비트 마스터 키를 추출하기 위해서는 2^8개의 예측이 필요하다. 따라서, 유일한 16라운드 키를 추출하였다고 하더라도 2^8개의 후보 마스터 키가 발생되고, Triple DES의 경우 3개의 마스터 키를 추출하여야 하기 때문에 총 2^{24}개의 후보 마스터 키가 발생된다.

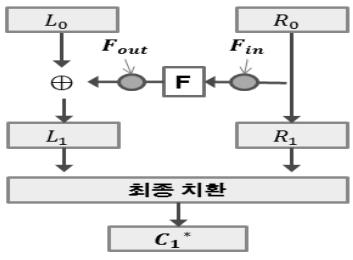
III. 제안하는 라운드 축소 오류 주입 공격

기존의 Triple DES의 마지막 라운드를 축소하는 공격 방법은 3개의 마스터 키를 추출하기 위해 약 9번의 오류 주입이 필요하며 2^{24}개의 후보 마스터 키가 발생된다. 이것도 최소 66%의 확률로 추출이 가능하기 때문에 더 많은 오류 주입 공격 회수가 필요하다. 본 논문에서는 DES의 초기 라운드만 실행시키도록 오류를 주입하여 마스터 키를 추출할 수 있는 개선된 공격 방법을 제안하고자 한다. 즉, 세 번째 DES(E_2)와 두 번째 DES(D_1)에서는 1라운드까지만 실행하는 오류, 2라운드까지만 실행하는 오류와 2^{24}의 계산 복잡도로 마스터 키를 추출하고, 첫 번째 DES(E_1)에서는 1라운드 실행한 오류와 2^{24}의 계산 복잡도로 마스터 키를 추출하는 방법을 제시한다. 따라서 본 논문에서 제안하는 공격 방법을 사용하면 Triple DES에서 사용하는 총 3개의 마스터 키를 추출하기 위해서 총 5번의 오류 주입과 $3*2^{24}$의 계산 복잡도가 필요하다.

3.1 DES에서의 라운드 축소 공격 방법

Triple DES에서의 공격 방법을 제안하기에 앞서 DES에 대한 기본적인 공격 개념을 설명하고자 한다. 기존의 오류 주입을 이용한 DES 공격의 개념은 한 라운드만 생략한 오류 암호문과 정상 암호문 쌍을 이용한 것이다. 그러나 제안 방식에서는 DES의 라운드 중 반복문 오류를 주입하여 한 라운드만 수행하도록 한 결과 값을 이용하여 비밀 키를 추출한다. 결국 공격자는 하나의 F함수에서 사용되는 라운드 키를 추출하기 위해서 F함수의 F_{in}과 F_{out}을 추출하여야 한다. 이를 위해 공격자는 반복문에 오류를 주입하여 1라운드만 수행하도록 오류를 주입하여 오류 암호문을 얻는다. 따라서 공격자는 〔그림 4〕와 같이 오류 암호문과 입력 평문만으로 F 함수의 입출력 F_{in}과 F_{out}을 추출하는 것이 가능하다. 즉, F_{in}의 경우 R_0이기 때문에 추출이 가능하고, F_{out}의 경우 R_1과 L_0을 XOR 연산하는 것으로 추출이 가능하다.

$$F_{in} = R_0$$
$$F_{out} = L_0 \oplus R_1$$



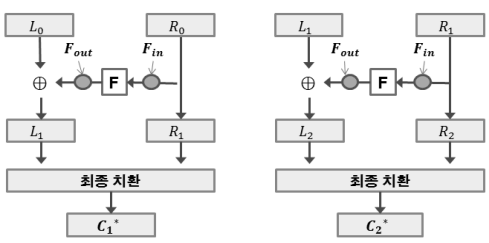
〔그림 4〕 1라운드 오류 주입

1라운드의 F_{in}과 F_{out}을 추출한 공격자는 2.2절에서 설명한 16라운드 키 추출 방법과 같은 방법을 이용하여 1라운드 키를 추출할 수 있으며, 추출된 1라운드 키는 $4^8(2^{16})$개의 후보군을 가지게 된다. 또한, 하나의 1라운드 키로부터 마스터 키를 추출하기 위해서는 2^8개의 후보군이 필요하기 때문에 총 2^{24}개의 후보 마스터 키를 추출할 수 있다. 마스터 키의 후보가 2^{24}개로 많은 후보키를 가지고 있다고 하더라도 평문으로부터 DES의 16라운드를 정상적으로 수행한 정상 암호문을 출력할 수 있는 키는 1개만 존재한다. 따라서, 공격자는 2^{24}개 후보키 중에서 정상 암호문을 출력하는 후보키를 전수 조사(exhaustive search)를 하면 유일한 마스터 키를 추출할 수 있다. 이와 같이 공격자가 오류 주입 공격을 통하여 DES의 1라운드만을 수행한 오류 암호문을 얻을 수 있다면, 1번의 오류 주입과 2^{24}번의 전탐색을 통하여 유일한 56비트 마스터 키 추출이 가능하다.

3.2 Triple DES에서의 라운드 축소 공격 방법

상기한 바와 같이 DES에서의 라운드 축소 공격은 공격자가 평문을 알 수 있기 때문에 1번의 오류 주입으로 1라운드의 F_{in}과 F_{out}을 추출하는 것이 가능하다. 하지만 Triple DES에서는 3개의 DES를 사용하며, 3개의 DES 중 E_2에 오류를 주입하여 E_2의 1라운드만 수행한 오류 암호문을 얻을 수 있더라도 E_2에 입력되는 중간 암호값을 알아낼 수 없기 때문에 1라운드의 F_{in}과 F_{out}을 추출할 수 없다.

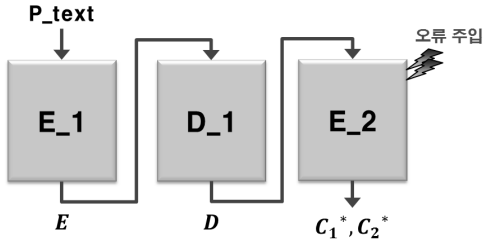
1번의 오류 주입만으로 1라운드의 F_{in}과 F_{out}을 얻을 수 없는 공격자는 F_{in}와 F_{out}을 추출하기 위하여 E_2의 1라운드만 수행하는 오류와 2라운드까지만 수행하도록 하는 반복문 오류 2개를 주입하여 1라운드 오류 암호문(C_1^*)과 2라운드 오류 암호문(C_2^*)을 얻는다. E_2의 1라운드만 수행한 오류 암호문과 2라운드만 수행한 오류 암호문을 얻은 공격자는 L_1, R_1, L_2, R_2를 추출할 수 있으며, 이를 이용하여 E_2의 2라운드의 F_{in}과 F_{out}을 추출할 수 있다. F_{in}과 F_{out}을 얻은 공격자는 3.1절과 마찬가지로 총 2^{24}개의 후보 마스터 키를 추출할 수 있다. 이러한 방법을 이용하여 E_1, D, E_2 단계에서 유일한 마스터 키를 찾는 방법을 차례로 설명하도록 한다.



〔그림 5〕 1라운드와 2라운드 오류 주입

■ 1단계 : E_2의 유일한 마스터 키 추출

공격자가 E_2의 후보 마스터 키를 추출하면 유일한 마스터 키를 추출하기 위하여 DES 연산을 통해 올바른 정상 암호문을 출력하는 후보 마스터 키를 찾는 것이 필요하다. 이를 위해 E_2의 입력 값(D)을 알아야 하지만, E_2의 입력 값을 알아낼 수 없기 때문에 1라운드 오류 암호문(C_1^*)과 2라운드 오류 암호문(C_2^*)을 이용한다. 공격자는 56비트 후보 마스터 키를 이용하여 DES의 모든 라운드 키를 생성한다. 그 후, C_1^*을 역 최종 치환한 것을 2라운드부터 마지막까지 암호화 연산을 수행한다. 이렇게 생성된 암호문이 정상적인 Triple DES 암호문과 같은 지를 확인함으로써 마스터 키를 추출한다. 따라서 2번의 반복문 오류 주입과 2^{24}번의 전탐색으로 E_2의 유일한 마스터 키 추출이 가능하다.



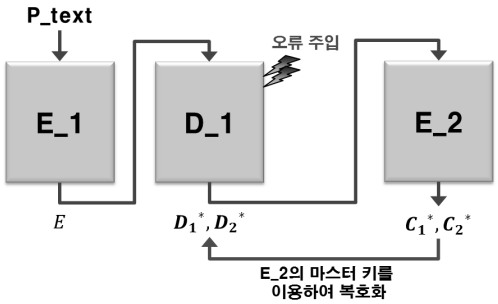
〔그림 6〕 E_2에 대한 1라운드, 2라운드 반복문에 대한 오류 주입

■ 2단계 : D_1의 유일한 마스터 키 추출

D_1의 마스터 키를 추출하기 위하여 D_1에 라운드 축소 오류를 주입하더라도 E_2는 정상적으로 수행되기 때문에 D_1의 출력 값을 알아내는 것이 필요하다. 이를 위해 추출된 E_2의 마스터 키를 이용하여 D_1에 오류를 주입한 1라운드 후의 오류 암호문, 2라운드 후의 오류 암호문, 정상 암호문에 대한 복호화를 수행함으로써 D_1에 대한 1라운드 오류 출력 값(D_1^*), 2라운드 오류 출력값(D_2^*), 정상 출력값(D)을

알아낸다.

공격자는 D_1^*과 D_2^*을 알고 있기 때문에 F_{in}과 F_{out}의 추출이 가능하고, 후보 라운드 키도 추출이 가능하다. 여기서 후보 라운드 키는 D_1이 복호화 알고리듬이기 때문에 15라운드 키의 후보를 뜻하며 키 스케줄 과정을 역으로 수행하여 2^{24}개의 후보 마스터 키 추출이 가능하다. 따라서 2번의 반복문에 대한 오류 주입과 2^{24}번의 전탐색으로 E_2에서의 마스터 키 추출 방법과 유사한 방법으로 D에 대한 유일한 마스터 키 추출도 가능하다.

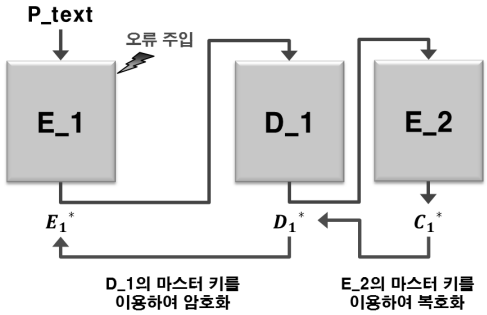


〔그림 7〕 D에 대한 1라운드, 2라운드 오류 주입

■ 3단계 : E_1의 유일한 마스터 키 추출

E_1의 경우 공격자가 평문을 알고 있기 때문에 E_2와 D_1과 같이 2번의 오류 주입을 통해 1라운드 후의 오류 암호문과 2라운드 후의 오류 암호문을 추출할 필요없이 1라운드 후의 오류 암호문과 평문만으로 1라운드 F_{in}과 F_{out}을 추출할 수 있다.

E_1에 오류를 주입한 공격자는 E_2의 마스터 키와 D_1의 마스터 키를 이용하여 1라운드 오류 암호문과 정상 암호문에 대한 복호화와 암호화를 차례로 수행하면 E_1에 대한 1라운드 후의 오류 출력값(E_1^*)과 정상 출력값(E)을 얻을 수 있다. 따라서 공격자는 3.1절과 같은 방법을 이용하여 1번의 반복문 오류 주입과 2^{24}번의 전탐색으로 E_1에 대한 마스터 키를 추출할 수 있다.



〔그림 8〕 E_1에 대한 1라운드 오류 주입

IV. 공격 방법 비교 분석 및 실험

4.1 Triple DES 에서의 오류 주입 공격 비교

지금까지 제안된 Triple DES에 대한 주요 오류 주입 공격의 결과를 비교 분석한 것이 〔표 1〕이다. Hemme의 방법〔7〕은 DES의 초기 라운드에 비트 오류를 주입하는 공격으로서 많은 횟수의 오류 주입 공격이 필요하여 실제 적용하기에는 쉽지 않다. 이후 Baldwin 등의 방법〔8〕에서는 15라운드의 오른쪽 암호문에 오류를 주입하는 방법으로서 6개 정도의 오류 암호문만 필요하지만 전수 조사를 해야 하는 계산 복잡도가 2^{30} 정도였다. 최두식 등은 각 DES 알고리듬의 마지막 라운드를 생략하는 반복문 오류 주입 공격을 시도하였다〔10〕. 그 결과 약 9개의 오류 암호문과 2^{24}의 전수 조사를 통해 66%정도의 확률로 마스터키를 찾아낼 수 있었다. 반면 본 논문에서는 1개의 정상 암호문과 5개의 반복문 오류 암호문만을 이용하면 $3*2^{24}$번의 전수조사를 통해 마스터 키를 추출하는 방법을 제안하였다. 따라서 지금까지 제시된 Triple DES의 오류 주입 공격 중 가장 적은 오류 암호문으로 마스터 키를 추출할 수 있었다.

〔표 1〕 Triple DES 오류 주입 공격 비교

오류 주입 공격	오류 주입	오류 암호문 수	전수조사 계산 복잡도
Hemme〔7〕	2, 3, 4라운드 S-box에 비트 오류	$6.9 * 10^5$	$2.76 * 10^6$
Baldwin 등〔8〕	15라운드 오른쪽 32비트 암호문 오류	6	2^{30}
최두식 등〔10〕	16 라운드를 생략하는 라운드 축소 오류	9개 이상	2^{24}
제안 공격	중간 라운드를 생략하는 라운드 축소 오류	5	$2^{24} * 3$

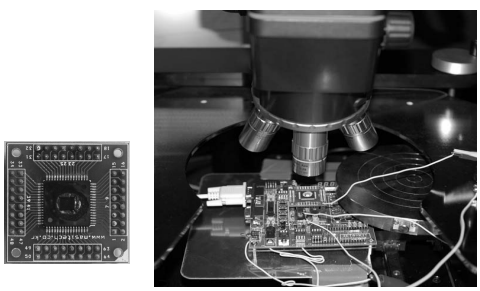
```
"D:₩2011₩연구₩논문 작성₩한국정보보호학회₩오류
* Input key1 :  1 23 45 67 89 ab cd ef
* Input key2 : cd ef 43 57 bb c1 4f  1
* Input key3 : 67 34 ed 86 ea 14 cd  8

* 56-bit key : left(28-bit), right(28-bit)
  left = f0ccaa0,  right = aaccf00
* 56-bit key : left(28-bit), right(28-bit)
  left = 336f121,  right = 5e4b538
* 56-bit key : left(28-bit), right(28-bit)
  left = 5c55172,  right = 196fd42

Plain text :a4 ce 18 1a 94 71 ef 8b
E_1 Output :47  f cc 28 83 46 68 3a
D  Output :36 85 b9 71 8c a5 18 f4
E_2 Output :76 ea 39 90 30 ec 7c ef

Round reduction in E_2
After 1st round :33 42 5c 3a ce 72 8e 70
After 2nd round :b9 2b  6 37 c7 99 c7 98
Press any key to continue
```

〔그림 9〕 시뮬레이션을 이용한 라운드 축소시 오류 암호문

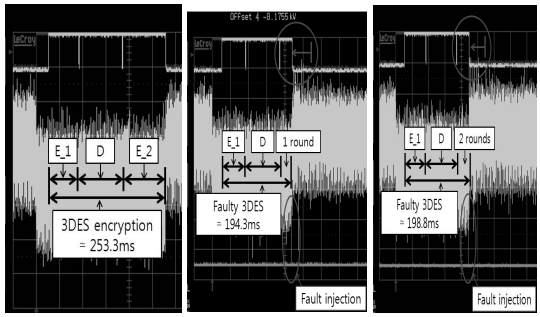
4.2 오류 주입 공격 실험

이 절에서는 Triple DES를 암호용 칩에 구현할 경우, 반복문 오류 주입이 가능한지를 검증하기 위해 ATmega128 칩에 Triple DES 암호 알고리듬을 구현하고 오류 주입 공격을 시도해 보았다. 실험의 정확성을 검증하기 위해 먼저 Triple DES를 컴퓨터 시뮬레이션을 통해 각 라운드의 반복문을 건너뛸 수 있는지 확인해 보았다. 〔그림 9〕는 Triple DES의 입력 키와 암호 후 출력 그리고 E_2 과정에서 반복문 오류 시 1라운드 후의 결과와 2라운드 후의 결과를 나타낸 것이다.

오류 주입 공격을 위해서는 ATmega128 칩의 표면을 디캡핑(decapping)하였으며 EzLaze 3 레이저 장비를 사용하였다. 〔그림 10〕은 디캡핑된 ATmega128 칩과 실험 장치를 나타낸 것이다〔13〕. 제안한 공격 방법에서는 먼저 Triple DES의 E_2에서 1라운드와 2라운드 수행 후 암호문을 출력하는지를 실험하였다. 〔그림 11〕의 (a)는 Triple DES의 수행 시 전력 파형을 오실로스코프로 관측한 것이다.



〔그림 10〕 오류 주입 실험 칩과 실험 장치



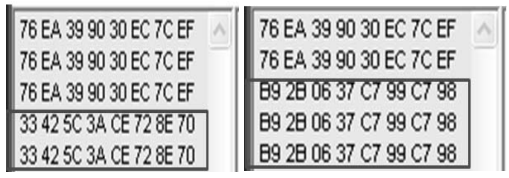
(a) (b) (c)

〔그림 11〕 반복문 오류 주입 시 출력 파형

그림에서 보는 바와 같이 약 253ms의 시간이 소요됨을 볼 수 있었다. 그리고 (b)는 E_2의 1라운드까지만 수행한 후의 출력파형인데 수행시간이 짧아졌음을 확인할 수 있었다. 또한 (c)는 E_2의 2라운드까지만 수행한 후의 출력파형인데 수행시간이 198.8ms임을 확인할 수 있었다.

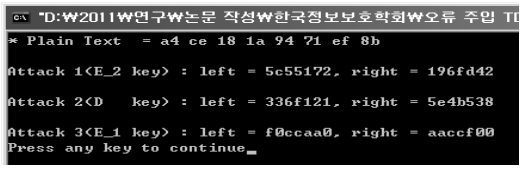
반복문 오류 주입 후의 출력 암호문을 나타낸 것이 〔그림 12〕이다. (a)는 E_2의 1라운드까지만 수행한 오류 암호문이며, (b)는 E_2의 2라운드까지만 수행한 오류 암호문이다. 이 결과를 컴퓨터로 시뮬레이션한 〔그림 9〕와 동일함을 볼 수 있다. 따라서 오류 주입 공격 실험이 실제로 가능함을 증명할 수 있다.

위에서와 같은 반복문 오류 주입을 통해 얻은 5개의 오류 암호문들을 이용하여 Triple DES의 3개의 마스터 키를 $3*2^{24}$번의 전탐색 공격으로 추출할 수 있음을 보이고자 한다. 시뮬레이션을 위하여 AMD 애슬론 6400 프로세서, 3G RAM의 사양을 갖춘 PC를 사용하였으며, 개발 툴로는 Visual Studio 2008을 사용하였다. 〔그림 13〕는 제안한 공격 기법을 이용하여 Triple DES에서 사용하는 3개의 마스터 키를 추출할 수 있다는 것을 보여주고 있다. DES 하나의 마스터 키를 추출하기 위해서는 2^{24}번의 DES 연산이 필요하기 때문에 약 10분 정도의 시간이 소요된다. 따



(a) (b)

〔그림 12〕 반복문 오류 주입 시 출력되는 오류 암호문



〔그림 13〕 Triple DES의 마스터 키 추출 공격

라서 3개의 마스터 키를 추출하기 위해서는 약 30분 정도의 시간이 소요되었다.

V. 결 론

본 논문에서는 반복문에 오류를 주입하여 라운드를 축소시킬 수 있는 오류 주입 공격을 이용하여 Triple DES에서 사용하는 3개의 마스터 키를 추출하는 방법을 제안하였다. 기존 라운드 축소 공격을 이용하여 Triple DES를 공격하는 방법이 존재하지만 총 9번의 오류 주입이 필요하고 2^{24}의 계산 복잡도가 필요하였다. 본 논문에서는 총 5번의 오류 주입과 $3*2^{24}$의 계산 복잡도로 마스터 키를 추출할 수 있는 오류 주입 공격 기법을 제안하였다. 또한 제안한 공격 기법을 컴퓨터 시뮬레이션 및 오류 주입 장치 실험을 통해 칩 보호에 대한 대응책이 없는 경우에는 내부의 비밀 키가 노출될 수 있음을 검증하였다. 결론적으로 반복문 라운드 축소를 이용한 오류 주입 공격은 Trple DES는 물론 표준 암호 알고리듬인 AES에도 적용할 수 있는 위험한 공격〔12〕이므로 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〕 C. Giraud, "DFA on AES," Advanced Encryption Standard-AES'04, LNCS 3373, pp. 27 - 41, 2005.

〔4〕 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.

〔5〕 W. Li, D. Gu, and J. Li, "Differential Fault Analysis on the ARIA Algorithm," Information Science. vol. 178, no. 19, pp. 3727-3737, 2008.

〔6〕 NIST, "Data Encryption Standard(DES)," NIST FIPS PUB 46-3, 1999.

〔7〕 L. Hemme, "A Differential Fault Analysis Against Early Rounds of (Triple)-DES," CHES'04, LNCS 3156, pp. 254-267, 2004.

〔8〕 B. Baldwin, E. Provici, M. Tunstall, and W. P. Marnane, "Fault Injection Platform for Block Ciphers," IIET Irish Signals and Systems Conference - ISSC 2008, pp. 10-15. Aug. 2008

〔9〕 NIST, "Recommendation for the Triple Data Encryption Algorithm(TDEA) Block Cipher," NIST FIPS PUB 800-67, 2008.

〔10〕 최두식, 오두환, 배기석, 문상재, 하재철, "오류 주입을 이용한 Triple DES에 대한 라운드 축소 공격," 한국정보보호학회 논문지, 21(2), pp. 91-100, 2011년 4월.

〔11〕 H. Choukri and M. Tunstall, "Round reduction using faults," FDTC'05, pp. 13-24. 2005.

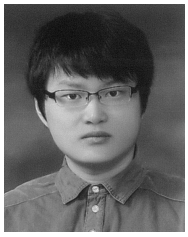
〔12〕 박제훈, 배기석, 오두환, 문상재, 하재철, "AES에 대한 반복문 오류주입 공격," 한국정보보호학회 논문지, 20(6), pp. 59-65, 2010년 12월.

〔13〕 Atmel사 홈페이지, http://www.atmel.com/atmel/acrobat/doc2467.pdf

〈著者紹介〉

최 두 식 (Doo-Sik Choi) 정회원
2010년 2월: 호서대학교 정보보호학과 졸업
2010년 3월~현재: 호서대학교 대학원 정보보호학과 석사 과정
2012년 6월~현재: ㈜ 소프트포럼 연구원
〈관심분야〉 네트워크 보안, 부채널 공격

오 두 환 (Doo-Hwan Oh) 정회원
2010년 2월: 호서대학교 정보보호학과 졸업
2010년 3월~현재: 호서대학교 대학원 정보보호학과 석사 과정
2012년 3월~현재: ㈜ 윈스테크넷 연구원
〈관심분야〉 네트워크 보안, ID-기반 암호화 시스템, 오류주입 공격



박 정 수 (Jeong-Soo Park) 정회원
2011년 2월: 호서대학교 컴퓨터공학과 졸업
2011년 3월~현재: 호서대학교 대학원 정보보호학과 석사 과정
〈관심분야〉 스마트 폰 보안, 부채널 공격, 시스템 보안

하 재 철 (Jae-Cheol Ha) 종신회원
1989년 2월: 경북대학교 전자공학과 졸업
1993년 8월: 경북대학교 전자공학과 석사
1998년 2월: 경북대학교 전자공학과 박사
1998년 3월~2007년 2월: 나사렛대학교 정보통신학과 부교수
2003년 1월~현재: 한국정보보호학회 이사
2009년 1월~현재: 한국산학기술학회 이사
2007년 3월~현재: 호서대학교 정보보호학과 부교수
〈관심분야〉 정보보호, 네트워크 보안, 부채널 공격