논문 2012-49CI-3-9

하드웨어 DES에 적용한 다중라운드 CPA 분석

(Multi-Round CPA on Hardware DES Implementation)

김 민 구*, 한 동 국**, 이 옥 연***

(Min-Ku Kim, Dong-Guk Han, and Okyeon Yi)

요 약

최근 Nakatsu는 전력파형의 정보가 충분하지 못한 환경에서 분석 성능을 향상 시키는 하드웨어 AES(Advanced Encryption Standard)에 대한 다중 라운드 CPA (Correlation Power Analysis, CPA) 분석기법을 제안하였다. 본 논문에서는 하드웨어로 구현된 DES(Data Encryption Algorithm)에 1라운드와 2라운드를 분석하여 마스터키를 찾아내는 다중 라운드 CPA 분석 방법을 제안한다. 제안된 다중 라운드 CPA 분석 기법은 DPA Contest에서 제공한 하드웨어 DES 암호 알고리즘의 전력파형을 사용하여 시뮬레이션을 하였다. 그 결과 300개의 전력파형의 정보만으로도 마스터키의 모든 정보를 찾을 수 있었다. 또한 단일라운드 CPA 분석 기법보다 다중라운드 CPA 기법이 더 효과적으로 마스터키를 분석하는 것을 검증하였다.

Abstract

Recently at SCIS2011, Nakatsu et. al. proposed multi-round Correlation Power Analysis(CPA) on Hardware Advanced Encryption Standard(AES) to improve the performance of CPA with limited number of traces. In this paper, we propose, Multi-Round CPA to retrieve master key using CPA of 1round and 2round on Hardware DES. From the simulation result for the proposed attack method, we could extract 56-bit master key using the 300 power traces of Hardware DES in DPA contes. And it was proved that we can search more master key using multi-round CPA than using single round CPA in limited environments.

Keywords : Side channel Attack, DES, CPA, 다중라운드 CPA, DPA contest v1

Ⅰ. 서 론

비밀정보의 보안을 위해 보안 알고리즘이 탑재된 디바이스의 사용이 증가하고 있다. 디바이스에 탑재된 보안 알고리즘은 통계적, 대수적 분석에 있어서 암호학적으로 안전함이 입증되어 있는 표준 알고리즘을 사용한다. 하지만, 입증된 안전성과는 무관하게, 보안 알고리즘이 디바이스에서 구현되어 사용되는 과정에서 물리적으로 전력소모량이나 전자기파, 동작시간 등의 부채널 정보가 발생하게 된다. 공격자는 발생된 부채널 정보를 관찰하여, 암호 알고리즘에 사용되는 비밀정보를 찾아낼 수 있다. 이러한 방법을 부채널 분석(Side Channel Analysis, SCA)이라고 한다[1].

입력 값과 출력 값만 가지고 수학적인 분석을 시도하는 전통적인 암호분석법과는 달리 부채널 분석은 연산 중간에 발생하는 부채널 정보를 이용하여 디바이스에서 사용되는 암호 알고리즘의 비밀키를 찾아 낼 수 있다.

Kocher등은 알고리즘의 구동 시간을 분석하여 비밀키의 값을 찾아내는 방법인 Timing Attack을 소개하였다[1]. 이후 소비전력 정보를 사용하여 부채널 분석을 하는 전력분석 기법이 소개되었다. 전력분석 기법은 디바이스에서 연산이 진행될 때 직접 소비되는 전력 신호의 특성을 파악하여 비밀키에 대한 정보를 알아내는

* 학생회원, ** 정회원-교신저자, *** 정회원,
국민대학교 수학과
(Department of Mathematics, Kookmin University)
※ 본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다. (UD060048AD)
접수일자: 2012년1월30일, 수정완료일: 2012년4월26일

Kocher등이 소개한 단순전력분석(Simple Power Analysis, SPA) 기법과 고정된 비밀키에 대해 많은 수의 동일한 알고리즘을 동작하여 수집된 전력 소모량 측정치들 사이에 상관관계를 통계적으로 분석하여 키 값을 유도해 내는 Goubin와 Patarin이 소개한 기법인 차분전력분석(Differential Power Analysis, DPA)기법 그리고 Brier등이 소개한 상관전력 분석(Correlation Power Analysis, CPA) 기법이 있다[2~4].

CPA기법은 특정 위치의 수행 결과 값의 상관관계를 구하여 비밀키를 추정하는 방법으로서 전통적인 DPA 기법보다 더욱 비밀키를 효과적으로 찾을 수 있는 기법으로 알려져 있으며, 공격을 더욱더 효율적으로 수행하기 위해, 비밀키와 유사한 계산이 되어 분석성능을 저하시키는 Ghost key의 패턴에 대한 연구 등이 다양하게 진행되고 있다[5~6]. 또 다양한 디바이스에서 생성되는 부채널 정보는 각기 다른 특징을 가지고 있으므로, 디바이스의 특징에 대한 연구도 진행되고 있다[7].

DPA와 CPA기법은 분석 특성상 많은 양의 부채널 정보가 필요하게 된다. 하지만 충분한량의 부채널 정보가 주어지지 않았을 때는 부채널 분석의 효과를 기대하기 어렵다.

최근 충분하지 못한 부채널 정보를 가지고 효과적인 분석인 다중라운드 부채널 공격에 대한 연구가 Suzuki와 Saeki에 의해 제안되었다. Suzuki와 Saeki에 의해 제안된 Dual round attack 방법은 평문과 암호문을 사용하여 첫 번째와 마지막 라운드에 대한 부채널 분석을 진행한다.

최근에는 Nakatsu등에 의해 발표된 하드웨어에서 구현된 AES에 대한 다중라운드 부채널 분석방법이 제안되었다[8]. Nakatsu등에 의해 제안된 방법은 공격자가 AES 암호 알고리즘의 암호문을 사용하여, 10라운드에 단일 부채널 분석을 하고, 분석된 비밀키 정보를 사용하여 9라운드에 부채널 분석을 적용하는 방법이다. 이 방법은 충분하지 못한 부채널 정보로 단일라운드 부채널 분석이 되지 않는 상황에서 다중라운드 부채널 분석을 하여 비밀키를 찾아 낼 수 있다.

본 논문에서는 Nakatsu등이 제안한 AES에 대한 다중라운드 부채널 분석 방법을 활용하여 하드웨어에서 구현된 DES에 다중라운드 CPA 분석을 적용하고자 한다[9]. 하드웨어 DES의 부채널 정보는 DPA contest에서 제공한 소비전력정보를 사용하였다. DES는 알고리즘의 특성상 평문 혹은 암호문 정보만을 가지고 1,2 라운드 또는 15, 16 라운드에 다중라운드 CPA 분석이 적용 가능하다[10].

1, 2 라운드에 다중라운드 CPA 분석을 적용한 결과 단일 라운드 CPA 분석 시 전력파형을 300개, 400개 그리고 500개를 사용 하여 56비트의 마스터키 중 각각 36비트, 42비트, 그리고 48비트를 찾았을 수 있었던 것에 비해 전력파형 300개만을 사용하여 56비트의 마스터키를 모두 찾아 낼 수 있었다.

본 논문은 다음과 같이 구성하였다. Ⅱ장에서는 관련연구로 DES와 CPA에 대한 설명 하며, Ⅲ장에서는 제안하는 다중라운드 CPA 분석 방법에 대하여 설명한다. Ⅳ장에서는 제안한 다중라운드 CPA 분석 방법의 실험결과에 대해 기술하고 Ⅴ장에서는 결론에 대해 기술한다.

Ⅱ. 관련 연구

1. DES

가. DES 암호화 과정

DES[9]는 패리티(parity) 체크 비트 8비트를 포함하는 64비트의 키를 이용하여 64비트의 평문을 64비트의 암호문으로 암호화하는 대칭키 블록 암호 알고리즘이다. 그림 1 은 DES의 구성을 나타낸 것이다. DES는 초기 치환과 최종 치환 그리고 16라운드의 Feistal 구조로 구성되어 있다. 64비트의 입력된 평문은 초기 치환을 거쳐 두 개의 32비트로 나누어지고 이를 각각 L 과 R 로 표기 하였다. 각 라운드마다 f 함수가 있어 R 을 입력으

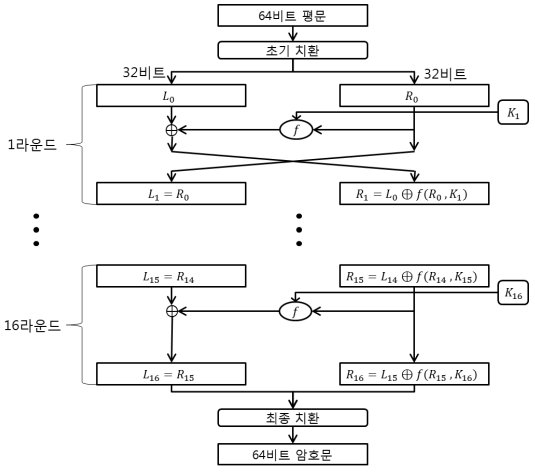

그림 1. DES 구성
Fig. 1. Structure of DES.

로 한 결과를 L과 XOR연산을 하여 그 결과를 다음라운드의 R로 설정하고, R을 그대로 다음라운드의 L로 설정한다. DES는 이와 같은 라운드를 모두 16번 수행하고 최종 라운드에서는 L과 R을 바꿔 설정한다. 마지막으로 최종치환 과정을 거쳐 DES의 암호화 과정이 끝난다.

나. DES의 키 생성 과정

DES는 16개의 라운드에서 48비트의 라운드 키가 사용된다. 16개의 라운드 키들은 64비트의 마스터키로부터 생성된다. 그림 2에서 볼 수 있듯이 키 생성과정은 64비트의 마스터키가 패리티 체크 과정을 거쳐 56비트로 축소되며 이는 각각 28비트 크기로 나누어진다. 이를 각각 C와 D로 표기 하였다. C와 D는 각각 라운드마다 로테이션을 거치고 축약 치환을 통해 48비트 라운드 키를 생성하게 된다. 이와 같은 과정을 반복하여 16개의 라운드 키가 생성된다.

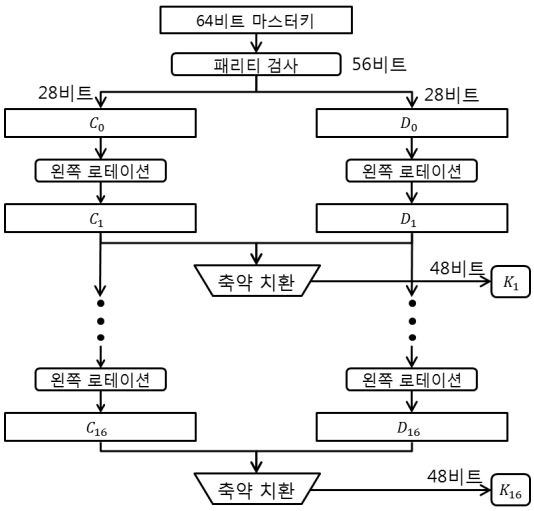

그림 2. DES 키 생성
Fig. 2. Key generation of DES.

2. CPA

Brier[5]등에 의해 발전된 CPA 분석 기법은 전력분석 공격방법의 하나로 강력한 분석 방법 중 하나이다. CPA 분석 기법은 암호 알고리즘에 다양한 데이터를 입력한 중간 결과 값을 전력소모 모델에 따라 변환한 후, 알고리즘이 수행 되면서 관찰할 수 있는 전력 소모량과의 상관계수를 계산하여 비밀정보를 알아내는 분석 공격이다. 이를 통하여, 전력 소모 파형에서 어느 시점이 해당 연산이 계산되는지 알 수 있으며, 해당 연산에서 사용되는 비밀 값도 알 수 있다. 전력소모 모델은 알고리즘이 구현되고 실행된 환경에 따라 결정된다. 일반적으로 전력 소비 모델은 전력을 소비하는 장비들의 특성에 따라서 해밍 웨이트 모델과 해밍 디스턴스 모델로 나눌 수 있는데 해밍 웨이트 모델은 이진데이터의 1의 개수에 따라 전력을 소비 하며, 해밍 디스턴스 모델은 이진데이터에서 비트 별로 비트의 값이 변화된 개수에 따라 전력을 소비한다.

가. DES의 단일라운드 CPA

DES의 F함수는 그림 3과 같이 구성된다. 공격자는 평문정보를 이용하여 1라운드에 대한 CPA 분석을 하거나 암호문 정보를 이용하여 16라운드에 대한 CPA 분석을 할 수 있다. DES가 구현된 환경에 따라 전력소모 모델이 달라진다. DPA contest[10]에서 제공한 하드웨어에서 구현된 DES의 소비전력정보는 해밍 디스턴스 모델을 따르며 라운드의 입력값과 출력값의 디스턴스 값으로 전력이 소비된다. 입력데이터와 출력데이터의 디스턴스 값은 두 값의 XOR연산으로 계산할 수 있다.

해밍 디스턴스 모델을 따르는 DES의 CPA 분석은 DES의 구조상 S-Box를 고려하여 분석이 된다. S-Box 입력에 사용되는 라운드 키를 추측하게 되는데 S-Box 구조상 6비트씩 8번 반복된다. 추측된 키에 대한 상관계수 값은 추측키와 XOR 연산이 되는 6비트의 중간값과 연관되는 대한 4비트의 라운드 입력값과 4비

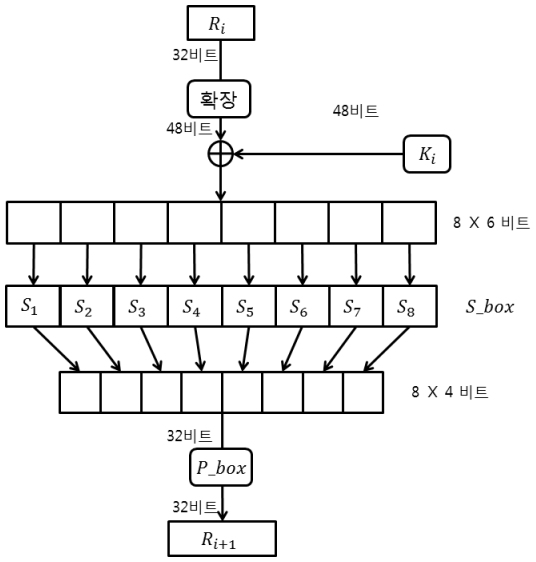

그림 3. F 함수구성
Fig. 3. Structure of F function.

트의 라운드 출력값의 디스턴스값으로 계산된다. 공격자가 암호문을 가지고 있는 경우에도 위와 같은 방법을 16라운드에 적용하면 CPA 분석이 가능하다.

DES에 대한 CPA 분석 기법은 통계적인 분석방법이므로 전력소모 파형의 개수에 의존되며, 파형의 개수가 적을수록 분석 결과의 신뢰성이 낮아진다. 또한 DES와 같은 경우 1라운드 혹은 16라운드의 키만을 분석 하였다고 하더라도 마스터키를 분석하는 것은 불가능 하며, 별도의 정보가 필요하다.

본 논문에서는 적은수의 전력소모 파형만을 가지고도 기존의 단일라운드 CPA 분석 기법보다 효과적으로 마스터키를 분석할 수 있는 다중라운드 CPA 방법을 제안한다.

Ⅲ. DES에 대한 다중라운드 CPA 제안

1. 다중라운드 CPA

본 논문에서 제안하는 DES의 다중라운드 CPA 분석 방법에 대하여 설명한다. 다중라운드 CPA 분석 방법은 연이은 두 개의 라운드에 적용 가능하며, 1번째 라운드에 대해 기존의 단일라운드 CPA 분석 방법을 적용한 뒤 2번째 라운드에 대한 CPA 분석 시에는 이전 라운드에서 추측된 라운드 키를 이용하여 추측키를 생성한 다음 분석을 진행한다.

다중라운드 CPA 분석 방법은 하나의 라운드에 먼저 단일라운드 CPA 분석 방법을 적용하여 분석된 라운드의 부분키를 상관도가 높은 순서로 정렬한다. 이때, 정렬된 라운드의 부분키에서 상관계수가 가장 높은 2개의 추측 부분키가 가지는 상관계수 값의 비율이 일정수치의 Threshold를 넘으면 가장 큰 상관계수 값을 갖는 추측키는 올바른 부분키로 확정하고 threshold를 넘지 않는 추측키 들은 정렬된 순서에 따라 다음라운드에 사용된다.

정렬된 라운드 부분키 정보들을 가지고 다음 라운드에 적용할 CPA 분석에 대한 추측키를 생성한다. 또한 정렬된 라운드 키들의 정보를 사용하여 다음 라운드에서 분석 대상이 되는 중간값을 생성하는 데도 사용이 된다. 이전 라운드에서 올바른 키가 추측이 되지 않았다면, 다음라운드의 평문값과 라운드 키가 올바르게 생성되지 않는다.

생성된 평문값과 라운드 키를 가지고 다음라운드에 단일라운드 CPA 분석 방법을 적용하여 생성된 라운드 키들에 대한 상관관계 값을 계산하여 라운드 키를 추측한다.

2. DES의 다중라운드 CPA

DES의 다중라운드 CPA 분석 기법은 1, 2라운드 혹은 16, 15라운드에 적용할 수 있으며, 공격자가 평문 혹은 암호문 정보를 가지고 있느냐에 따라서 선택되어진다.

DES의 다중라운드 CPA 분석은 1라운드에 단일라운드 CPA 분석을 적용하여, Threshold를 넘는 부분키 들을 확정 하며, Threshold를 넘지 않는 키들은 상관계수가 높은 순으로 정렬하여 2라운드 단일라운드 CPA 분석에 사용한다.

이전 라운드에서 추측된 키들을 차례로 사용하여 2라운드 CPA 분석에 사용될 부분키를 생성하고, 2라운드에 단일라운드 CPA 분석 기법에서 사용될 입력 정보도 생성한다. 이렇게 생성된 2라운드 입력 정보와 부분키를 사용하여 2라운드에 CPA 분석을 적용한다.

가. 2라운드 추측 키 계산

DES의 16개의 라운드 키들은 그림 2에서 보는 것과 같이 하나의 마스터키로부터 생성되며, 왼쪽 로테이션과 축약치환만을 거쳐 생성되므로 라운드 키들 사이에는 연관성이 있다. 그림 4는 6비트의 2라운드 부분키와 1라운드의 라운드 키 사이의 연관성을 보여준다. 처음 6비트의 부분키 중 4비트는 1라운드 라운드 키의 9, 10, 15, 24비트와 동일한 값이며, G로 표시된 나머지 2비트는 1라운드 키를 생성할 때 축약치환에서 제외된 마스터키의 일부 값이다.

표 1은 2라운드의 라운드 키 48비트를 6비트의 부분키로 표현 하였을 때의 연관성이 있는 6비트단위의 1라운드 부분키와 축약치환에서 제외된 마스터키의 비트수를 표시하였다. 부분키 셀에 있는 숫자는 S박스 순서에 따라 연산되어지는 6비트의 부분키를 의미한다. 2라운드의 2번째 6비트 부분키는 1라운드의 1, 3, 4번째 S

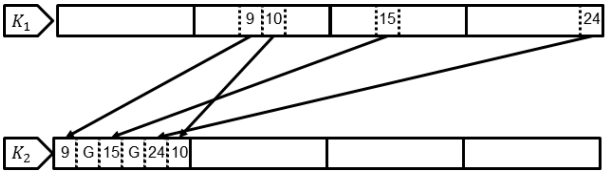

그림 4. DES 1, 2 라운드 키의 연관성
Fig. 4. Relation of round key.

표 1. 2라운드 키의 연관성
Table 1. Relation of 2nd round key.

2라운드 부분키	2라운드 키와 연관 있는 1라운드 부분키	제외된 비트
1	2, 3, 4	2
2	1, 3, 4	1
3	1, 4	1
4	1, 2, 3	0
5	6, 7, 8	1
6	5, 7, 8	0
7	6, 8	2
8	5, 6	1

박스 입력값과 XOR연산이 되는 6비트의 부분키 정보와 관련이 있으며, 1라운드 키를 생성할 때 축약치환에 의해 제외된 1비트와 관련이 있다.

2라운드의 부분키 들은 1라운드 CPA 분석 결과 정렬된 1라운드 부분키 정보들을 사용하여 계산할 수 있으며, 1라운드 부분키와 연관성이 없는 비트는 추측을 통하여 계산할 수 있다.

나. 2라운드 평문정보 생성

2라운드에 단일라운드 CPA 분석을 하기 위해서는 2라운드 입력정보를 알아야 한다. 이 정보는 1라운드 출력 정보와 동일하며, 1라운드에 적용한 단일라운드 CPA 분석 결과 얻을 수 있는 1라운드 부분키 정보를 사용하여 계산 가능하다.

2라운드 입력값은 DES의 평문정보와 추측된 1라운드 키를 사용하여 계산할 수 있다. 이때 추측된 1라운드 키가 사용이 되므로, 올바른 키가 추측되어야 올바른 2라운드 입력값이 계산되어진다. 따라서 올바른 2라운드 입력값을 계산하기 위해서는 2라운드 키 계산과 동일한 방법으로 추측된 1라운드 부분키 들을 상관계수 순서에 따라서 사용하여 계산한다.

물론 평문정보 생성에 사용되는 1라운드 부분키로 2라운드 부분키를 생성해야 한다. 이렇게 생성된 2라운드 입력값과 라운드 키로 단일라운드 CPA 분석을 하여 2라운드 키를 분석한다.

Ⅳ. 실 험

본 논문에서는 그림 5에서 볼 수 있는 DPA contest

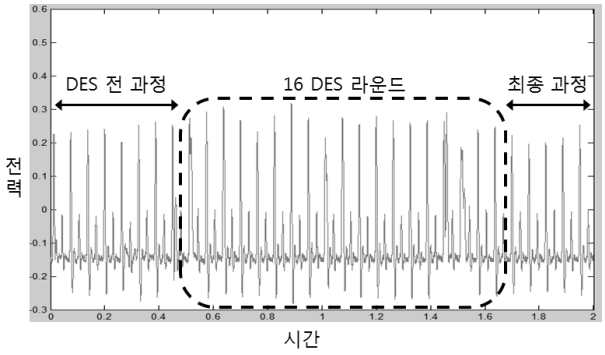

그림 5. DPA contest v1 DES H/W 전력파형
Fig. 5. DES H/W Power waveform of DPA contest v1.

에서 공개된 하드웨어 DES의 전력 파형을 사용하여 다중라운드 CPA 분석을 실시하였다[10]. DPA contest에서 공개된 하드웨어 DES의 전력 파형은 DES의 16개의 라운드에 대한 정보와 초기치환과 최종치환 등의 정보를 가지고 있으며, 이 정보는 DES에 사용되는 평문과 암호문을 사용하여 1라운드 와 16라운드에 CPA 분석을 적용하여 알아 낼 수 있다.

실험은 단일라운드 CPA 분석과 다중라운드 CPA 분석을 각각 적용하여 64비트의 마스터키 정보 중에 패리티를 검사하는 8비트를 제외한 56비트를 찾는 것을 목적으로 분석을 진행하였다.

1. 단일라운드 CPA 분석

DES파형에 단일라운드 CPA 분석을 DES 1라운드를 대상으로 실시하였다. CPA 분석 결과 300개의 파형정보를 사용했을 때는 36비트, 400개의 파형정보를 사용했을 때는 42비트 그리고 500개의 파형정보를 사용했을 때는 48비트의 라운드키의 정보를 찾을 수 있었다. 하지만 56비트 마스터키 정보를 모두 찾을 수는 없었다. 1라운드 단일라운드 CPA 분석 결과로 찾아진 1라운드 키를 이용하여 2라운드 입력값을 생성하여 2라운드에 단일라운드 CPA 분석을 실시하였다. 올바른 2라운드 입력값을 생성하기 위해 1라운드의 키가 모두 분석된 결과만을 사용 하였다. 500개의 파형정보를 사용했을 때 24비트의 라운드키의 정보를 찾을 수 있었다. 1000개의 파형정보를 사용했을 때는 36비트의 라운드키 정보를 찾을 수 있었다.

2. 다중라운드 CPA 분석

DES파형에 다중라운드 CPA 분석을 DES 1, 2 라운드를 대상으로 실시하였다. CPA 분석 결과 300개의 파

형정보를 사용했을 때 56비트 마스터키의 정보를 모두 찾을 수 있었다.

3. 비교

표 2는 단일라운드 CPA 분석과 제안한 다중라운드 CPA 분석에 대한 결과를 나타낸다. 1, 2 라운드 CPA 분석 셀에 표시되는 정보는 파형 수에 따른 라운드키 48비트 중에 분석 후에 알 수 있는 비트의 수를 나타냈으며, 다중라운드 CPA 분석 셀은 마스터키 56비트 중에 분석 후에 알 수 있는 비트의 수를 나타냈다.

1, 2 라운드에 단일 CPA 분석을 적용하였을 때 1000개의 파형을 사용하여 1라운드의 키는 찾을 수 있었으나 2 라운드키의 모든 부분키를 찾지 못하여 마스터키의 모든 정보를 찾지 못하였다. 하지만 제안한 다중라운드 CPA 분석으로는 300개의 파형정보만을 사용하여 마스터키의 모든 정보를 찾을 수 있었다.

단일라운드 CPA 분석과 다중라운드 CPA 분석 기법은 1라운드에 대한 CPA 분석의 키 추측 횟수는 동일하지만, 2라운드에 대한 CPA 분석의 키 추측 횟수에 차이가 발생된다. 단일라운드 CPA 분석에서는 6비트의 키의 추측을 8번하여 분석을 하지만, 다중라운드 CPA 분석은 6비트의 키를 분석에 사용할 때 기존 1라운드에서 분석된 키 정보를 이용하므로 몇 개의 키들을 후보로 정하느냐에 따라서 단일라운드 CPA 분석 보다 더 많은 키 추측을 해야 한다. 하지만 Threshold값을 사용하여 일부 부분키 들을 찾을 수 있고, 키 후보를 줄일 수 있어 진행한 실험에서는 단일라운드 CPA 분석의 키 추측과 거의 동일한 횟수로 키 추측을 하였다.

단일라운드 CPA 기법은 2라운드에 CPA를 적용하기 위해서 1라운드의 올바른 키를 찾아야 하므로 실제 1라운드키 들이 올바른 키인지 확인할 수 있는 추가적인 실험이나 정보가 필요한 단점이 발생한다.

표 2. CPA 분석 결과
Table 2. Results of CPA.

파형수 (개)	1라운드 CPA 분석 (비트/비트)	2라운드 CPA 분석 (비트/비트)	다중라운드 CPA 분석 (비트/비트)
300	36/48	-	56/56
400	42/48	-	-
500	48/48	24/48	-
1000	48/48	36/48	-

V. 결 론

본 논문에서는 하드웨어 DES에 적용한 다중라운드 CPA 분석 기법을 제안하였다. 제안된 다중라운드 CPA 분석 기법은 1라운드 CPA 분석 기법에 비하여 더 적은 파형수로 마스터키의 정보를 더 많이 알아 낼 수 있음을 실험을 통해 볼 수 있었으며, 1, 2라운드에 차례로 적용한 단일라운드 CPA 분석 기법에서는 찾을 수 없는 마스터키의 정보를 제안한 다중라운드 CPA 분석 기법을 적용하여 찾을 수 있는 것을 실험을 통해 볼 수 있었다.

제안한 다중라운드 CPA 분석 기법은 부수적인 정보 없이 평문 정보만을 이용하여 마스터키를 모두 찾을 수 있었으며, DES의 특성상 16, 15 라운드에 같은 방법이 가능하다.

본 논문에서 제안한 다중라운드 CPA 분석 기법은 다른 암호 알고리즘 등에도 적용 할 수 있을 것으로 사료된다. 하지만 다중라운드 CPA 분석 기법을 적용할 때 필요한 Threshold값을 정하는 방법과 키 후보들을 어떤 방법으로 선정하여 2라운드에 대한 CPA 분석을 실시 할지 등에 대한 연구가 필요할 것으로 예상이 된다. 따라서 다중라운드 분석의 실제적이며 향상된 결과를 얻기 위한 더 많은 연구가 필요하다.

참 고 문 헌

[1] P. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”, CRYPTO ’96, LNCS 1109, Springer, pp.104-113, 1996.

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis”, CRYPTO 1999, LNCS 1666, Springer, pp. 388-397, 2003.

[3] L. Goubin and J. Patarin, “DES and Differential Power Analysis - The Duplication Method”, Cryptographic Hardware and Embedded Systems 1999, LNCS 1717, Springer, pp. 158-172, 1999.

[4] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model”, Cryptographic Hardware and Embedded Systems 2004. LNCS 3156, Springer, pp. 16-29, 2004.

[5] 박종연, 최지선, 한동국, 이옥연, “RSA에 대한 향상된 등간격 선택 평문 전력 분석 방법”, 대한전자공학회 2010년 하계종합학술대회, 1877-1880쪽, 한국, 제주도, 2010년 6월.

[6] 박종연, 한동국, 이옥연, 최두호, “RSA-CRT의 향상된 등간격 선택 평문 전력 분석”, 전자공학회논문지, 제48권 CI편, 제2호 117-126쪽, 2011년 3월.
[7] 강준기, 최두호, 강유성, 김주환, 김태성, 오경희, 최용제, “SCARF: Side-Channel Analysis Resistance Framework”, 대한전자공학회 2010년 하계종합학술대회, 1887-1889쪽, 한국, 제주도, 2010년 6월.
[8] D. Nakatsu, K. Ohta, and K. Sakiyama, “AES-128 に對する複數ラウンドCPA”, Symposium on Cryptography and Information Security 2011, 2011.
[9] NBS, “Data Encryption Standard”, FIPS Pub, 46, U.S, National Bureau of Standards, Washington DC, 1997.
[10] DPA contest wepsite, “http://www.dpacontest.org/index.php”, 2008.

저 자 소 개

김 민 구(학생회원)
2011년 국민대학교 수학과 학사 졸업.
2011년~현재 국민대학교 수학과 석사과정
<주관심분야 : 부채널 분석, Secure multiparty computation, 스마트그리드 보안>

이 옥 연(정회원)
1988년 고려대학교 수학과 학사 졸업
1990년 고려대학교 수학과 석사 졸업
1996년 8월 University of Kentucky 이학박사
1999년 7월~2001년 8월 한국전자통신연구원 선임연구원
2000년 3월~2001년 8월 한국전자통신연구원 팀장
2001년 9월~현재 국민대학교 수학과 교수
<주관심분야 : 스마트 그리드 보안, 무선보안, 4G 보안, 스마트워크 보안>

한 동 국(정회원)-교신저자
1999년 고려대학교 수학과 학사 졸업
2002년 고려대학교 수학과 석사 졸업
2005년 고려대학교 정보보호 대학원 박사
2004년 4월~2005년 4월 일본 Kyushu Univ. 방문연구원
2005년 4월~2006년 4월 일본 Future Univ. -Hakodate, Post Doc.
2006년 6월~2009년 2월 한국전자통신연구원 정보보호연구본부 선임연구원
2009년 3월~현재 국민대학교 수학과 조교수
<주관심분야 : 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석, RFID/USN 정보보호 기술>