아날로그 수신기를 이용한 SPA 성능 향상 연구

장승규, 한동국, 이옥연
국민대학교 수학과
e-mail : {jangskyu, christa, oyyi}@kookmin.ac.kr

A Study on SPA Performance Enhancement using the Analog Receiver

Seung-Kyu Jang, Dong-Guk Han, Okyeon Yi
Dept. of Mathematics, Kookmin University

요 약

단순전력분석(Simple Power Analysis, SPA)은 적은 수의 평문으로 암호 알고리즘에 대한 패턴 뿐만 아니라 비밀키의 정보를 찾는 전력 분석(Power Analysis)의 방법 중 하나이다. SPA의 장점은 차분전력분석(Differential Power Analysis, DPA) 또는 상관전력분석(Correlation Power Analysis, CPA)보다 적은 계산량으로 비밀키 분석을 할 수 있고, DPA 또는 CPA 분석을 하기 위해 필요한 분석위치 탐지에 효율적으로 활용이 되어 진다는 것이다. 하지만 최근 SPA 분석 성능을 저하시키기 위해 클락 노이즈, 전력 노이즈, 딜레이 노이즈 등 다양한 방법들이 제안되어지고 있다. 본 논문에서는 다양한 노이즈가 있는 환경에서 아날로그 수신기를 활용하여 특정 주파수 영역을 필터링한 후 노이즈를 제거하는 방법을 소개한다. 실험을 통해, 아날로그 수신기를 사용하였을 경우에 사용하지 않았을 경우보다 뚜렷한 대칭키 암호의 라운드 함수가 구분되어지며, 라운드 내 함수 구분도 가능함을 보인다. 이는 DPA 또는 CPA를 이용하여 분석을 수행하고자 할 때 분석 위치를 결정하데 아주 유용하게 활용되어지며, 분석 성능향상에도 기여할 것으로 기대되어진다.

1. 서론

부채널 분석(Side-Channel Analysis, SCA)[1]은 암호 알고리즘이 구현 장비(Embedded Device)내에서 구현되어질 때 발생하는 부가적인 물리적 특성들을 이용하여 알고리즘 내의 비밀 정보를 찾아내는 방법이다. 부가적인 물리적 정보에는 전력, 전자파 등이 있으며, 이러한 정보를 수집하여 분석에 이용하게 된다. 부채널 분석에는 단순전력분석(Simple Power Analysis, SPA), 차분전력분석(Differential Power Analysis, DPA), 상관전력분석(Correlation Power Analysis, CPA) 등의 방법으로 세분화 되어있다[2,3].

부채널 분석 공격 방법 중 SPA 공격은 DPA 및 CPA에 비해 적은 수의 전력신호와 적은 시간으로 비밀키를 분석 할 수 있는 공격법이다. 또한 SPA는 DPA 또는 CPA의 분석을 하기 위한 분석 위치 탐지에 효율적이기 때문에 필수적으로 활용되어진다. SPA의 공격 방법이 처음 제안되었을 때, DES에 대해서 분석이 되었으며, DES의 16개의 라운드 함수가 구분되어지고, 키 생성부분이 구분됨을 보였다.

하지만 최근 SPA 분석 성능을 저하시키기 위해 하드웨어적으로 클락 노이즈를 발생시키기도 하며, 소프트웨어적으로 구현상의 딜레이 노이즈를 주기도 한다. 또한 암호 알고리즘이 구현되어질 때, 구현 장비에서 발생하는 전력 노이즈 성분들이 암호 알고리즘의 전력신호에 영향을 미쳐 SPA 분석 성능을 떨어뜨리기도 한다. SPA 분석 성능이 저하됨에 따라 분석 위치의 선정에 있어서 어려움이 발생하고, DPA 및 CPA의 분석 성능에 있어서도 영향을 미치게 된다.

따라서 다양한 노이즈 성분을 제거하여 SPA의 성능을 향상시키기 위해 필터(Filter)을 이용하거나 Fourier Transform[4] 등과 같은 다양한 소프트웨어적인 노이즈 제거 기술들이 많이 개발되고 있다.

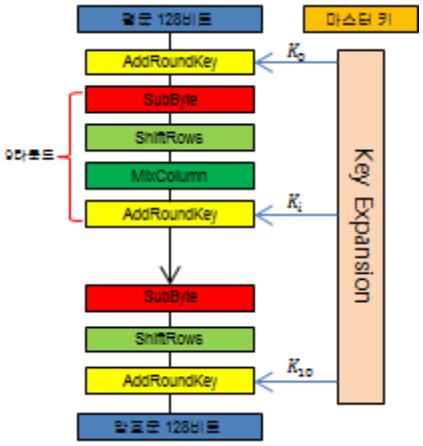
본 논문에서는 아날로그 수신기[5]를 활용하여 특정 주파수 영역을 필터링하여 노이즈를 감소시켜 SPA의 성능을 향상시키는 방법을 소개한다. 2장에서는 본 논문의 실험에서 사용된 암호 알고리즘과 SPA 공격법에 대하여 설명하며, 3장에서는 실험을 통하여 아날로그 수신기의 사용 여부에 따른 SPA 공격 결과를 설명하며, 마지막으로 4장에서는 본 논문의 결론을 짓는다.

2. 배경지식

2.1 AES Algorithm

AES는 128bit의 데이터 블록을 128, 192, 256bit의 다양한 길이의 암호화 키를 이용하여 암호화 하는 국제 표준 대칭키 알고리즘이다. 암호화 키의 길이에 따라 10, 12, 14라운드를 수행하며, (그림 1)은 키 길이가 128bit인 10개

의 라운드를 가진 AES의 암호화 과정을 그림으로 나타내었다. 마지막 라운드를 제외한 1~9라운드는 총 4개의 함수로 이루어져 있으며, 그 함수는 SubBytes(SB), ShiftRows(SR), MixColumns(MC), AddRoundKey(AR)이다. SubBytes는 각 바이트를 S-box를 이용하여 치환하는 함수이며 ShiftRows는 행 단위로 왼쪽 순환 시프트하는 함수를 나타낸다. MixColumns은 행렬곱 연산을 수행하며, 마지막으로 AddRoundKey는 KeyExpansion으로부터 생성된 라운드키(K_i)와 각 바이트들간의 XOR 연산을 하는 함수이다. 마지막 라운드에서는 MixColumns을 제외한 SubBytes, ShiftRows, AddRoundKey의 3단계로 이루어져 있다.



(그림 1) AES 암호화 과정

2.2 SPA

SPA는 암호 알고리즘에서 사용되는 전력 소비 패턴을 관찰하여 암호 알고리즘에 사용되는 비밀키의 정보를 직접 분석하는 방법이다. 하드웨어에서 암호 알고리즘이 구현될 때 프로세서의 명령에 따라 각기 다른 전력을 갖는다는 사실을 외부에서 관측할 수 있으며, 이로부터 비밀키 또는 순간 작동중인 명령에 대한 정보를 추론하는 공격 방법이다.

SPA를 하기 위해서는 공격자가 암호 알고리즘에 대하여 자세히 알고 있어야 한다. 암호 알고리즘을 수행시켜 얻은 전력 신호로부터 어느 부분에서 어떠한 연산이 수행되는지, 또 어떤 명령어들이 사용되는지 판단할 수 있어야만 해당 암호 알고리즘에 대한 SPA 공격을 수행할 수 있다.

암호 알고리즘은 대칭키 암호와 공개키 암호로 나뉘는데, 대칭키 암호에는 AES, ARIA, SEED, DES 등이 있으며, 공개키 암호에는 RSA, ECC, Elgamal 등이 있다. 대칭키 암호와 공개키 암호에서의 SPA 공격 의미는 조금 다르다. 대칭키 암호의 SPA는 라운드를 구분하며, 반복문의 수를 파악하는데 쓰인다면, 공개키 암호에서 SPA는 암호 알고리즘에서 쓰인 비밀키의 정보를 직접 찾을 수 있으며, 알고리즘의 상세 구현법에 대해서도 추측할 수 있다.

3. SPA 실험 및 성능 비교

3.1 실험 환경

본 논문에서 실험에 사용한 구현 장비는 ARM 보드를 사용하였다. ARM 보드는 S3C2410(ARM920T)의 CPU를 가지며, 1M boot Flash, 8M NAND Flash, 64M SRAM의 스펙을 갖는다. ARM 보든 270MHz의 내부 클럭으로 동작을 한다. 암호 알고리즘으로는 2장에서 설명한 AES 알고리즘을 소프트웨어로 구현하여 ARM 보드에 포팅하여 실험을 진행하였다.

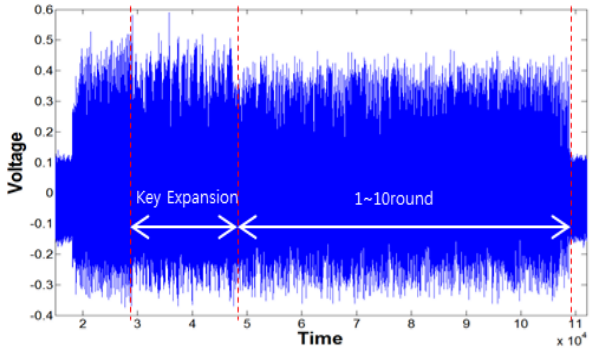
(그림 2) 일반적인 SPA 분석 환경

(그림 2)는 일반적인 SPA 분석 환경이다. 제어 컴퓨터로부터 데이터가 MCU(Micro Controller Unit) 보드 즉, 실험에 사용한 ARM 보드로 입력이 된다. 입력 된 신호는 ARM 보드 내에서 암호화 과정을 수행한 후 GND (Ground)로 이동되며, Trigger 신호를 사용하여 오실로스코프의 화면에 암호화 전력신호가 뿌려진다. 이때 전력신호를 사용하여 SPA 공격을 시도한다.

3.2 일반적인 SPA

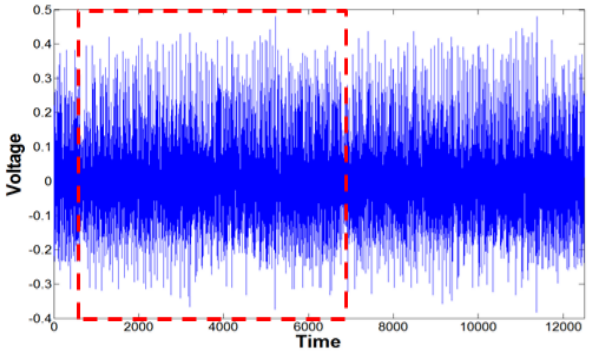
SPA 공격 방법은 적은 수의 평문에 대한 적은 수의 전력 신호만을 가지고 암호 알고리즘의 비밀키를 찾는 방법이며, 암호 알고리즘을 분석하기 위해 분석 위치를 결정하기 위한 방법이다.

다음 (그림 3)은 AES 암호화 연산이 수행될 때 소비되는 전력신호를 나타낸다.



(그림 3) AES 전력신호

(그림 3)는 AES의 전력신호이다. (그림 3)에서 보는 것과 같이 키 생성하는 부분인 KeyExpansion과 실제 암호화 연산이 이루어지는 Round부분이 서로 다른 전력 소비를 가져와 패턴이 다른 것을 확인할 수 있다. 하지만 KeyExpansion과 Round의 구분은 이루어지지만, 10개의 라운드 구분이 전혀 보이지 않는다.

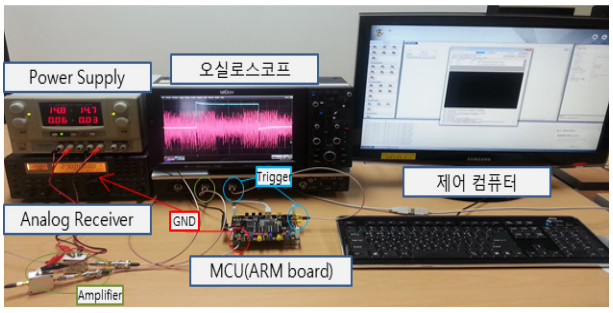


(그림 4) AES 1Round 전력신호

(그림 4)은 AES의 (그림 3)의 10개 Round 부분 중 1-2Round에 해당되는 부분을 확대한 그림이다. (그림 4)에서 빨간 점선 박스로 되어 있는 부분이 AES의 1Round에 해당되는 부분이다. AES의 1Round에는 SubBytes, ShiftRows, MixColumns 그리고 AddRoundKey 등 4개의 함수로 이루어져 있으나, 위 (그림 4)에서는 각 함수의 구분이 되지 않는다. CPA 및 DPA의 공격을 할 경우 보통 AES의 1Round S-box 출력 부분을 공격 지점으로 선택하지만, (그림 4)과 같이 SubBytes의 구분이 되지 않으면, 분석을 함에 있어서 시간 및 메모리의 비용이 늘어날 수 있다.

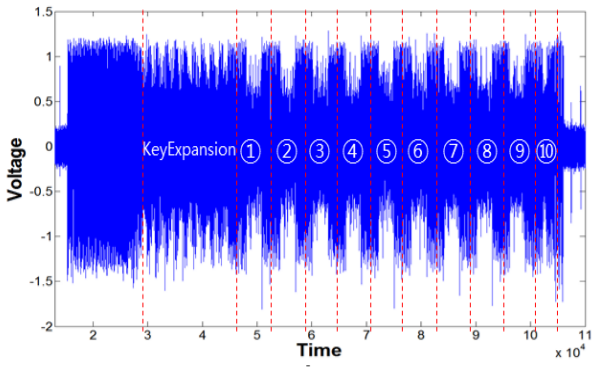
3.3 아날로그 수신기를 사용한 SPA

일반적인 SPA 공격법으로는 정확한 분석 지점을 설정하기 어려운 경우가 있다. 구현 장비로부터 암호 알고리즘이 수행되어질 때 알고리즘의 소비 전력만이 수집되지 않는다. 보드의 칩(Chip)에서 나오는 노이즈가 섞여 깨끗한 신호가 보이지 않을 수 있다.



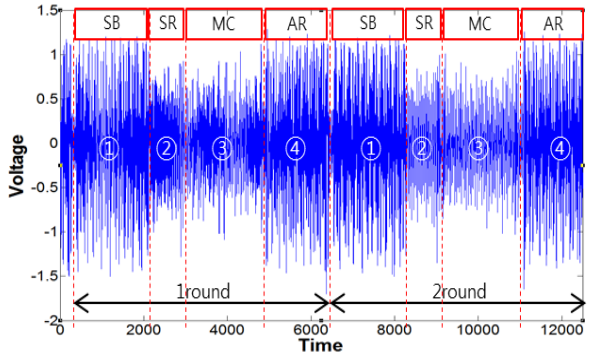
(그림 5) 아날로그 수신기를 사용한 AES 전력신호

본 절에서는 이러한 문제를 해결하기 위해 아날로그 수신기를 사용하였다. 아날로그 수신기는 ICOM 사(社)의 IC-R8500으로 100kHz ~ 1999MHz의 주파수 영역의 범위(Coverage)를 갖는다. 아날로그 수신기는 30MHz 이하의 저주파수 영역대와 30MHz 이상의 고주파수 영역대로 나뉜다. (그림 5)는 아날로그 수신기를 사용하여 SPA 분석 환경을 나타낸다. 제어 컴퓨터로부터 데이터가 ARM 보드로 입력이 되고 ARM보드에서 암호화 연산이 이루어진 후 GND 신호로 출력이 된다. 이때 출력된 전력 신호가 아날로그 수신기로 입력되어 특정 주파수 영역으로 필터링 된다. 필터링 된 신호는 Amplifier를 거쳐 신호가 증폭되며, 이 신호는 오실로스코프로 입력되어 디스플레이(Display)된다. 다음의 그림들은 (그림 5)의 환경에 의해 SPA 분석한 결과들이다.



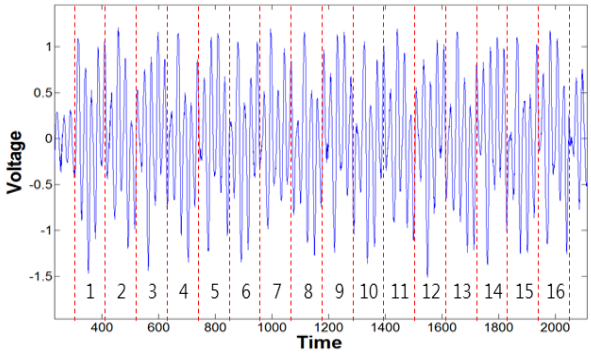
(그림 6) 아날로그 수신기를 사용한 AES 전력신호

(그림 6)는 IC-R8500의 아날로그 수신기를 사용하여 ARM 보드로부터 AES의 전력 신호를 수집한 신호를 나타낸다. 아날로그 수신기를 사용하지 않은 (그림 6)와는 다르게 KeyExpansion과 Round 사이의 구분이 뚜렷하며, KeyExpansion의 신호 내에서도 10개의 라운드 키가 생성되는 신호를 구분해 낼 수 있다. 또한 AES의 10개의 라운드 구분이 정확히 이루어진 깨끗한 전력 신호를 얻을 수 있었다.



(그림 7) 아날로그 수신기를 사용한 AES 1Round & 2Round 전력신호

(그림 7)는 (그림 6)의 1Round와 2Round의 부분을 확대하였다. (그림 4)에서는 라운드 안의 함수 구분이 전혀 보이지 않았었다. 반면 아날로그 수신기를 사용한 (그림 7)에서는 SubBytes(SB), ShiftRows(SR), MixColumn (MC) 그리고 AddRoundKey(AR) 등 4개의 함수 구분이 뚜렷이 구분되었다.



(그림 8) 아날로그 수신기를 사용한 AES SubBytes

(그림 8)은 AES SubBytes 부분만 확대하였다. AES의 구현상 8bit 단위로 연산이 이루어지며, 따라서 SubBytes의 입력비트가 128bit이므로 총 16개의 Sbox 연산이 이루어져야 한다. 아날로그 수신기를 사용하였을 경우, 16개의 Sbox 연산이 구분되어짐을 확인할 수 있다.

3.4 실험 결과

아날로그 수신기를 사용하였을 경우와 사용하지 않았을 경우 두 가지 경우에 대하여 실험을 하였다. 아날로그 수신기는 특정 주파수 영역의 신호를 필터링하여 노이즈의 감소에 큰 효과를 가져왔다. 아날로그 수신기를 사용하지 않았을 경우 라운드의 구분조차 되지 않았다. 반면 아날로그 수신기를 사용하자, 라운드 함수의 구분은 물론 라운드 내의 함수까지 구분 가능하였으며, SubBytes 함수의 16개의 반복문(loop)까지 구분이 가능하였다. 이로써 아날로그 수신기를 사용하여 SPA 분석의 성능을 향상시킬 수 있었다.

4. 결론

본 논문에서는 아날로그 수신기를 사용하여 신호의 노이즈 제거하는 방법을 소개하며, 실험으로써 전력신호의 노이즈가 감소됨을 보였다. 노이즈가 많은 전력신호에 대해서 SPA 분석이 잘 되지 않았다. 하지만 아날로그 수신기를 사용하였을 경우 암호의 라운드 함수가 구분되며, 라운드 내의 함수 구분도 가능함을 보였다. 더욱이 SubBytes의 16개 반복 구조 또한 확인할 수 있었다.

SPA는 DPA 및 CPA의 분석에 있어서 정확한 분석 위치의 선정에 큰 기여를 한다. 따라서 아날로그 수신기를 사용하여 SPA의 분석 성능이 향상되고, 정확한 분석 위치를 선정하여 DPA 및 CPA의 분석에도 성능의 향상에도 기여할 것으로 기대되어진다.

Acknowledgements

본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다. (UD060048AD)

참고문헌

[1] P.Kocher, J.Jaffe, and B. Jun, “Introduction to differential power analysis and related attacks” 1998, White Paper, Cryptography Research, http://www.cryptography.com/dpa/technical, 1998.

[2] P.Kocher, J.Jaffe, and B Jun, “Differential power analysis”, Advances In Cryptology - CRYPTO’ 99, LNCS 1666 Springer-Verlag, pp388-397, Santa Barbara, USA, August, 1999.

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

[4] O.Schimmel, P.Duplys, EBohl, J.Hayek, and W.Rosenstiel, “Correlation power analysis in frequency domain” COSADE 2010 - First International Workshop on Constructive Side-Channel Analysis and Secure Design, 2010.

[5] ICOMAMERICA website, http://www.icomamerica.com/en/