블록암호에 대한 상관관계 전력분석 공격

안효식* · 신경욱

*금오공과대학교

A Correlation Power Analysis Attack on Block Cipher

Hyo-Sik An* · Kyung-Wook Shin*

*Kumoh National Institute of Technology

E-mail : spyu12@kumoh.ac.kr

요 약

AES-128 블록 암호에 대해 상관관계 전력분석 공격을 통해 비밀키를 추출할 수 있는 보안공격 시스템의 프로토타입을 개발했다. Verilog HDL로 모델링된 AES-128 암호 코어의 RTL 시뮬레이션을 통해 switching activity 정보를 추출하고, 이를 PowerArtist 툴을 이용하여 순시 전력을 도출하였다. 추출된 순시 전력으로부터 출력 레지스터의 hamming Weight 모델링과 상관관계 분석을 통해 128 비트의 비밀키 중 일부를 획득하는 보안공격 시스템을 개발하였다.

키워드

Block Cipher, Side Channel Analysis, Correlation Power Analysis

Ⅰ. 서 론

인텔 시큐리티 맥아피 연구소(McAfee Labs)의 보고서에 의하면, IoT 디바이스의 확산 속도에 비해 보안기술 적용이 미비하여 IoT의 보안 취약성을 악용한 각종 범죄가 급격히 증가할 것으로 예상되고 있다[1]. 사용자 주변의 IoT 디바이스들이 사용자의 프라이버시나 개인 정보를 저장, 처리, 전송하는 경우에 외부 공격으로 정보가 노출되면 2차, 3차 피해로 확대될 수 있다. 특히, 헬스 케어나 산업시설 제어에 적용되는 IoT 디바이스가 외부 공격에 의해 침해되는 경우 단순한 경제적 피해를 넘어서 인명 피해가 유발될 수 있으므로, IoT에서 보안 기술은 필수적이다. 최근에는 제한된 성능과 자원을 갖는 IoT 환경에 적합한 암호 알고리듬이 많이 연구되고 있다.

정보보안 기술이 발전함에 따라 각종 보안공격 기술도 함께 발전하는 추세이므로 보안위협이 계속 증가하고 있다. 1998년 Kocher 등에 의해 암호 알고리듬이 구현된 하드웨어나 소프트웨어에서 암호연산이 수행되는 동안 누출되는 소비 전력, 전자파 등을 분석하여 비밀 정보가 노출될 수 있음이 입증되었으며[2], Kelsely는 이러한 공격 방식을 부채널 공격(side channel attack)이라 정의했다[3].

본 논문에서는 대표적인 블록암호 알고리듬인 AES에 대한 상관관계 전력분석 공격(correlation power analysis attack)을 설명한다. 상관관계 전력분석 공격을 위해 AES 암호 코어의 RTL 시뮬레이션을 통해 switching activity 정보를 추출하고, 이를 PowerArtist 툴을 이용하여 순시 전력을 도출하였다. 수집된 전력소모 파형과 출력 레지스터의 hamming weight 모델링으로 상관관계 전력분석 공격을 하여 암호화에 사용된 AES의 비밀키가 추출될 수 있음을 보였다.

Ⅱ. AES 알고리듬

AES는 non-Feistel 구조를 바탕으로 하는 128 비트 블록암호이며, 128/192/256 비트의 세 가지 키 길이를 지원하여 키 길이에 따라 10, 12, 14회의 라운드 연산으로 암호/복호를 수행한다[4]. 본 논문에서는 8 비트 데이터 패스로 구현된 AES 코어를 전력분석 공격의 대상으로 사용한다. 그림 1은 8 비트 데이터 패스로 구현된 라운드 블록이며, XOR1에 의해 라운드키 가산이 이루어지고, 마지막 라운드는 XOR2에서 라운드키 가산이 이루어져 암호문으로 출력된다.

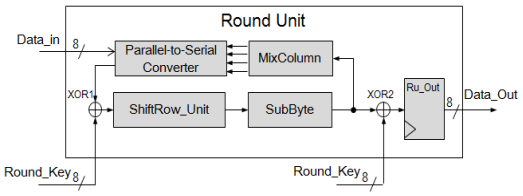


Fig. 1. AES round unit (8 bits data-path)

III. 부채널 공격

부채널 공격은 능동적 형태의 오류 분석 공격과 수동적 형태의 시차 분석 공격, 전자기파 공격, 전력분석 공격 등으로 구분된다. 암호 알고리듬이 하드웨어로 구현된 경우에 하드웨어의 전력 소모 부채널 정보를 완전히 제거할 수 없으므로, 전력분석 공격은 위협적인 공격법으로 인식되고 있다. 차분 전력분석 (differential power analysis; DPA) 공격은 공격자가 가정한 공격지점의 비트 값이 '0' 또는 '1' 인 경우에 따라 연산중에 발생한 전력소모 파형을 분류하고, 분류된 전력소모 평균의 차분을 구하여 비밀 정보를 알아내는 공격법이다. Brier 등에 의해 알려진 상관관계 전력분석 공격(correlation power analysis; CPA) 공격은 DPA 보다 향상된 기법으로서 비트 값이 0에서 1 또는 1에서 0으로 스위칭 될 때 전력소모가 발생한다는 사실에 근거한다. 비트 값의 스위칭 이전 상태와 스위칭 이후 상태의 hamming weight 값은 스위칭이 발생한 비트의 개수와 같으므로, 공격자는 암호 연산 중간값의 hamming weight를 모델링하여 실제 전력 소모량간의 상관관계 분석을 통해 비밀정보를 획득할 수 있다[7].

IV. 상관관계 전력분석 공격 방법 및 실험

기존의 상관관계 전력분석 공격에 대한 연구는 스마트카드와 같은 제한된 환경에서 구현된 암호 알고리듬의 S-Box나 키 가산 XOR 연산에 대해 공격이 이루어졌다[5-6]. 상관관계 전력분석을 위해서는 전력소모 파형과 공격지점의 hamming weight 모델링이 필요하다. 스위칭이 발생할 때의 소비전력을 W, 스위칭된 비트들의 hamming weight 값을 HW, 1 비트의 hamming weight가 갖는 소비전력 크기를 a, 평문과 비밀키에 상관없이 일정한 값을 갖는 오프셋 성분과 잡음 성분의 합을 b라고 하면 총 소비전력은 식 (1)과 같이 표현된다.

$$W = aHW + b \tag{1}$$

스마트카드가 아닌 일반적인 하드웨어 구현 환경을 고려하는 경우, 각각의 비트들의 전력소모량이 다를 수 있으며, S-Box나 XOR 연산에서의 소비전력이 전체 소비전력에 미치는 비중이 매우 작다면 선형성을 제대로 판별할 수 없다.

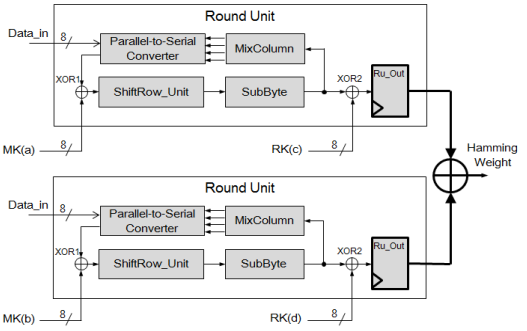


Fig. 2. Hamming Weight Modeling

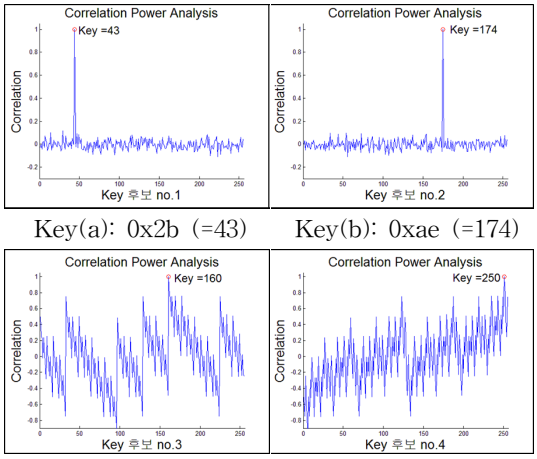
본 논문에서는 일반적인 환경을 고려하여 전체 소비전력에 미치는 비중이 가장 큰 그림 1의 라운드 블록의 출력 레지스터 Ru_Out에 대해 상관관계 전력분석 공격을 수행한다. II장에서 설명했듯이, 마지막 라운드 연산이 끝나면 레지스터 Ru_Out에 저장된 값이 암호문으로 출력된다. 그러나 마지막 라운드 이전의 라운드 연산과정에서도 Ru_Out 레지스터에 dummy 데이터가 저장되므로 그림 2와 같이 초기 라운드에 Ru_Out 레지스터에 저장되는 값에 hamming weight 모델링을 적용한다. 차분 전력분석 공격은 다음의 과정으로 이루어진다.

1) N개의 평문 P에 대한 소비전력 W를 측정
2) 2^n개의 모든 비밀키와 평문 P와의 암호 연산 공격지점의 Hamming weight 값 HW를 계산 (n : 비밀 키의 길이)
3) 식 (2)에 의해 피어슨 상관계수 r를 계산

$$r = \frac{\sum (HW - \overline{HW})(W - \overline{W})}{\sqrt{\sum (HW - \overline{HW})^2}\sqrt{\sum (W - \overline{W})^2}} \tag{2}$$

식(2)에서 $\overline{HW}$와 $\overline{W}$는 각각 HW와 W의 평균값을 나타낸다. 상관계수는 $-1 \le r \le 1$의 값을 가지며 -1과 1에 가까울수록 각각 음, 양의 상관관계를 가지며 0에 가까울수록 상관관계가 없다. 식(1)에 의해 소비전력 W와 hamming weight 값 HW는 양의 선형 관계를 가지므로 올바른 키로 HW값을 모델링 했다면 상관계수 r의 값은 1에 가깝게 나오게 된다.

본 실험에서는 1,000개의 128 비트 평문 블록을 사용한 RTL 시뮬레이션을 통해 switching activity를 구하고, PowerArtist 툴로 전력소모 파형을 구하였다. hamming weight 모델링에 사용된 네 개의 8 비트 비밀키 후보 가운데 두 개의 8 비트 마스터키 $MK(a)$, $MK(b)$와 두 개의 8 비트 라운드키 $RK(c)$, $RK(d)$를 획득하는 예에 대해 실험을 수행하였다. 사용된 128 비트의 마스터



Key(a): 0x2b (=43) Key(b): 0xae (=174)

Key(c): 0xa0 (=160) Key(d): 0xfa (=250)

Fig. 3. Correlation Coefficient of Key

키는 0x2b7e_1516_28ae_d2a6_abf7_1588_09cf_4f2c 이며, 키확장을 통해 생성된 첫 번째 라운드키는 0xa0fa_6417_8854_b6b1_23a3_a339_2a6c_ec15이다. 초기 라운드의 첫 번째 클록에서 CPA 공격으로 획득할 수 있는 정보는 마스터키의 일부인 0x2bxx_xxxx_xxae_xxxx_xxxx_xxxx_xxxx_xxxx와 첫 번째 라운드키의 일부인 0xa0fa_xxxx_xxxx_xxxx_xxxx_xxxx_xxxx_xxxx이다. 이와 같은 방법으로 비밀키를 획득하기 위해 2^{32}개의 키 조합에 대해 전수검사를 실시해야 한다. 본 논문의 실험에서는 32 비트 중, 24 비트의 키를 실제 사용된 값으로 고정시킨 상태에서 비밀키의 나머지 8 비트에 대한 획득 가능 여부를 확인하여 고정시키는 키를 줄여가면서 16, 24, 32 비트의 비밀키를 획득하는 방식으로 진행하였다. $MK(a)$, $MK(b)$의 경우에는 라운드키 가산 후, 추가 연산과정을 거치기 때문에 올바른 키 값에 대해서만 소비전력과의 선형성을 가지게 되며, 상관계수 값이 1에 가깝게 나타난다. $RK(c)$, $RK(d)$의 경우에는 $HW(ae \oplus fa) = HW(X \oplus Y)$를 만족하는 잘못된 키 값 (X, Y)에 대해서도 선형성을 가지므로, 다소 높은 상관계수를 보인다.

V. 결론 및 향후 연구 계획

본 논문에서는 8 비트 데이터 패스로 구현된 AES-128의 출력 레지스터에 대해 상관관계 전력분석 공격을 수행하는 방법을 연구하였으며, 일부 조건하에서 올바른 비밀키가 획득됐음을 확인하였다. 비밀키 획득을 위해 32 비트 전수검사가 필요하므로, 비밀키 획득 시간이 다소 소요되지만 스마트카드가 아닌 일반적인 상황에서도 전력분석 공격이 가능함을 보였다. 향후 국내에서 개발된 경량 블록암호 LEA에 대해서 전력분석 공격을 연구할 계획이다.

참고문헌

[1] http://www.mcafee.com/sg/resources/reports/rp-quarterly-threat-q3-2014.pdf

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” in CRYTO’99, pp. 388-397, 1999.

[3] Kelsey, B. Schneier, D. Wagner, and C. Hall, “Side Channel Cryptanalysis of Product Cipher,” Proceedings of ESORICS’98, pp. 97-110, 1998.

[4] National Institute of Standard and Technology (NIST), Advanced Encryption Standard (AES), FIPS-197, 2001.

[5] K.H. Boey, P. Hodgers, Y. Lu, M. O’Neill and R. Woods, “Security of AES Sbox designs to power analysis,” 17th IEEE International Conference on Electronics, Circuits and Systems (ICECS), pp. 1232-1235, 2010.

[6] Y. Han, X. Zou, Z. Liu and Y. Chen, “Improved Differential Power Analysis Attacks on AES Hardware Implementation,” International Conference on Wireless Communications, Networking and Mobile Computing, pp. 2230-2233, 2007.

[7] E. Brier, C. Clavier, and F. Oliver, “Correlation Power Analysis with a Leakage Model”, in CHES 2004, pp. 16-29, 2004.