AES에 대한 차분전력분석공격과 대응책

김성진, 이동욱, 이동익
광주과학기술원 정보통신공학과
전화 : 062-970-2248 / Fax : 062-970-2204

Differential Power Analysis for AES and Countermeasure

Sung-Jin Kim, Dong-Wook Lee, Dong-Ik Lee
Dept. of Information & communication, Kwang-Ju Institute of Science & Technology
Email : {jiny8985, dwlee, dilee}@kjist.ac.kr

Abstract

Paul Kocher has developed new attacks based on the electric consumption of cryptographic device such as smartcard that performs cryptographic computation. Among those attacks, the Differential Power Analysis(DPA) is one of the most impressive and most difficult to avoid. By analysing the power dissipation of encryption in a device, the secret information inside can be deduced. This paper presents that Advanced Encryption Standard(AES) is highly vulnerable to DPA and readily leaks away all secret keys through the experimental results for DPA. After all, it is required an implementation of the AES algorithm that is not vulnerable to DPA. We also propose countermeasures that employ asynchronous circuit.

Ⅰ. 서론

현재 보편적으로 널리 사용되고 있는 Data Encryption Standard(DES)는 짧은 키 길이 문제로 안전성에 위협이 되고 있는 상황이다. 따라서 National Institute of Standard and Technology(NIST)에서 DES를 대신할 새로운 대칭형 암호 표준인 Advanced Encryption Standard(AES)로 Rijndael 알고리듬을 선정하였다[1]. Rijndael은 Field Programmable Gate Array(FPGA) 구현, 스마트카드 구현, Application Specific Integrated Circuit(ASIC) 구현에서 성능과 효율성 측면에서 하드웨어 구현에 가장 적합한 대칭 키 암호 알고리듬으로 평가받았다. 따라서 차후 DES 보다 안전한 AES 알고리듬이 스마트카드용 암호 알고리듬으로 대체될 것으로 예측된다.

스마트카드는 마이크로 프로세서와 메모리를 통한 데이터 연산 처리 기능과 데이터 저장 기능을 바탕으로 전자상거래, 이동 통신, 금융 결재, 교통, 의료 등 다양한 응용분야에 사용되고 있다. 이와 같이 스마트카드의 응용 분야가 급격히 확대되어 감에 따라 고도의 보안성과 안전성이 필요하다.

1998년 스마트카드의 안전성을 위협하는 공격방법인 전력분석공격(Power Analysis Attack)이 Paul Kocher에 의해 처음 소개되었다[2]. 전력분석공격은 스마트카드의 암호 알고리듬에 사용하는 비밀키를 얻기 위해 물리적인 측정을 이용하는 방법으로 DES를 비롯한 다양한 암호화 알고리듬에 공격 가능한 것으로 보고되고 있다. 전력분석공격에는 스마트카드에서 수행되는 암호 연산의 전력소비패턴을 직접적으로 분석하는 Simple Power Analysis(SPA)와 데이터와 전력 소비 패턴간의 상호 연관성을 이용하여 키 값을 유출하는 통계적인 분석 방법인 Differential Power Analysis(DPA)로 나누어진다. 이러한 전력분석공격 방법을 이용하여 암호 알고리듬이 장착된 스마트카드와

보안 시스템에 대한 공격이 이루어지고 있으며 대부분의 암호 알고리듬은 DPA에 취약한 것으로 알려진다[3].

본 논문에서는 AES로 채택된 Rijndael 암호 알고리듬에 대해서 DPA에 취약한 암호 연산에 대한 DPA 공격을 수행한 실험 결과를 나타내고, DPA에 대한 대응책으로써 비동기 이중선로방식(Dual-rail)의 Delay Insensitive Min-term Synthesis(DIMS) 회로 설계 기법을 제안한다.

Ⅱ. Rijndael 알고리듬

NIST에서 DES를 대체할 후속 대칭키 암호 알고리듬으로 2000년 5개의 후보 알고리듬 중 최종적으로 Rijndale이 선정되었다[1]. DES를 비롯한 대부분의 대칭키 암호 알고리듬들은 Feistel 구조의 라운드 변환을 기반으로 하는데 비해, Rijndael 암호 알고리듬은 non-Feistel 구조를 바탕으로 하고 있으며, 3개의 독립된 역변환 가능한 라운드 변환으로 구성된다. 또한, Rijndael은 128, 192, 256 비트의 가변 길이를 지원하며, 블록 길이와 키 길이에 따라 라운드 수가 다른 특징을 가진다.

암호화 과정은 초기 라운드, 반복 라운드, 최종 라운드로 구성된다. 초기 라운드는 AddroundKey 단계를 수행하고 반복 라운드는 ByteSub, ShiftRow, MixColumn, AddRoundKey 단계를 라운드 수만큼 반복하는 과정이다. 최종 라운드는 Mixcolumn이 제외된 상태에서 수행이 이루어진다. 그림 1은 Rijndael 암호화 과정을 보여준다.

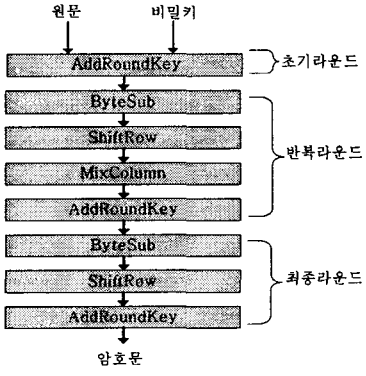

그림 1. Rijndael 암호화 과정

Rijndael 암호 알고리듬은 Bytesub, ShiftRow, MixColumn, AddRoundKey의 4 가지 라운드 변환을 수행한다. ByteSub는 State의 각 바이트 단위로 비선형 바이트 치환동작을 수행한다. 여기서 State는 암·복호 변형 과정의 중간 결과를 나타낸다. ShiftRow는 State의 행들을 고정된 오프셋만큼 왼쪽으로 이동시키는 변환 동작이다. MixColumn은 State의 각 열들은 $GF(2^8)$의 다항식으로 $b(x) = c(x) \otimes a(x)$ 형태의 다항식 곱셈으로 처리한다. c(x)는 $'03'x^3 + '01'x^2 + '01'x + '02'$ 형태의 고정된 계수 값을 갖는다. AddRoudKey는 라운드 키와 State값을 xor 연산하는 변환 동작을 수행한다.

Ⅲ. 전력분석공격

전통적인 암호분석가들은 수학적인 방법을 사용하여 암호알고리듬 자체의 취약성을 찾아내는 공격들을 수행하였다. 그러나 최근의 실제 많은 응용분야에서 암호 알고리듬은 소프트웨어나 하드웨어로 구현되어지며, 이 과정에서 암호 알고리듬 개발 시에는 간주되지 못하였던 부분들에 의하여 공격취약성을 가질 수 있다. Kelsely는 이런 방식의 정보의 유출을 부채널(side-channel)이라 정의하고 부채널을 이용한 공격방법을 부채널 공격이라 언급했다[4]. 부채널 공격은 시간공격(timing attack), 결함 주입공격(fault insertion attack), 전자기 누출공격(electromagnetic emission attack), 그리고 전력분석공격(power analysis attack) 등으로 나눌 수 있다[5][6][7].

3.1 Simple Power Analysis(SPA)

SPA는 전력소비패턴을 직접 분석하는 공격방법으로 전력소비패턴은 암호화 과정에서 처리되는 값들에 의존해서 나타난다. 따라서 SPA를 통해 암호 알고리듬의 암호 연산에 대한 수행 순서를 알 수 있고 이를 통해 비밀키와 원문에 대한 정보를 유출시킨다. SPA는 조건부 분기명령에 의해 비밀키를 예측할 수 있다. 따라서 조건부 분기명령을 사용하지 않고 비밀키에 의존하지 않는 명령 수행 순서를 가진다면 SPA를 쉽게 막을 수 있다.

3.2 Differential Power Analysis(DPA)

SPA보다 향상된 공격방법인 DPA는 데이터 값과 전력소비패턴과의 상호연관성을 이용하는 통계적인 방법이다. 입력 데이터 값 "0"과 "1"이 다른 전력 소비패턴을 가진다는 것에 기초하여 "0"과 "1"의 전력소비패턴의 차이를 통해서 비밀키를 유출하는 것이다.

DPA는 암호 알고리듬의 암호 연산의 취약성을 이용하는 것으로 공격자는 암호 알고리듬이 어떤 암호연산을 사용하는지 알아야한다. 즉, 알고리듬에서 사용

되는 암호 연산의 전력소비패턴이 데이터 값과 상호연관성을 가지는지를 분석함으로써 DPA를 수행할 수 있다.

3.3 Rijndael 암호 연산

Rijndael은 테이블 참조(table lookup), bitwise xor, 고정 좌측 순환(fixed shift)과 다항식 곱셈(polynomial multiplication) 연산으로 구성된다. DPA에 대한 각각의 특성은 다음과 같다[8].

(1) 테이블 참조 연산 : 입력 n을 가지고 출력 m을 발생시키는 동작으로 주소 값에 따른 데이터의 hamming weight를 통해 DPA에 취약할 수 있다.

(2) 고정 좌측 순환 연산 : 비트간의 고정된 자리바꿈과 순환 연산은 입력 데이터 값과 전력소비패턴간의 상호연관성이 존재하지 않는다.

(3) bitwise xor 연산 : xor 회로에서의 전력소비패턴의 차이는 데이터 값에 의존하기 때문에 전력소비패턴과 데이터 값은 상호연관성이 존재하여 DPA에 취약할 수 있다.

(4) 다항식 곱셈 연산 : 조건부 bitwise xor와 shift를 사용하여 구현했을 때, 시간공격(timing attack)에 취약할 수 있다. 따라서 테이블 참조, xor, 순환연산을 조합하여 시간공격을 막을 수 있다.

결과적으로 Rijndael은 bitwise xor 연산과 s-box 테이블을 사용하는 테이블 참조 연산이 DPA에 취약할 수 있다. 본 논문에서는 bitwise xor 연산에 따른 DPA 공격을 수행한다.

Ⅳ. DPA 공격방법

Rijndael 알고리듬의 초기 라운드와 마지막 라운드의 AddRoundKey 변환 과정에서 실제 DPA 공격이 가능하며, 비밀키와 임의의 원문이 연산될 때 소비되는 전력을 이용하여 비밀키를 알아낼 수 있다. 본 실험에서는 초기 라운드의 AddRoundKey 변환 과정에 DPA 공격을 수행한다[8].

(1 단계) N 비트의 비밀키를 $K(k_0, k_1, \cdots, k_{N-2}, k_{N-1})$라 정의하고 K의 j번째 비트를 공격한다고 가정한다.

(2 단계) 임의의 N비트 평문 $M_i(m_0, m_1, \cdots, m_{N-2}, m_{N-1})$을 선택하여 연산을 수행한 수 전력소비신호 $S_i[j]$를 구한다.

(3 단계) 각각의 평문에 대한 ℓ번째 비트의 값 "0"과 "1"에 대해 평문에 해당하는 전력소비신호를 분류한다.

S0 = [$S_i[j]$ | 평문 ℓ번째 비트의 값 : "0"]

S1 = [$S_i[j]$ | 평문 ℓ번째 비트의 값 : "1"]

(4 단계) 양분한 전력소비신호 데이터를 각각 평균하여 평균에 대한 차분신호 D[j]를 구한다.

$$D[j] = \frac{1}{|S_0|}\sum_{S_i[j]\in S_0} S_i[j] - \frac{1}{|S_1|}\sum_{S_i[j]\in S_1} S_i[j]$$
$$= S_0^*[j] - S_1^*[j]$$

(5 단계) 비밀키 K의 ℓ번째 비트의 값 k_ℓ을 결정한다.

If D[j] = "Positive", k_ℓ = "1"

If D[j] = "Negative", k_ℓ = "0"

Ⅴ. 실험 결과

본 실험에서는 Rijndael의 AddRoundKey 연산에 대해 DPA 공격에 대한 전력소비 시뮬레이션을 수행하였다. Rijndael은 Verilog HDL(Hardware Description Language)를 이용하여 설계되었으며, Synopsys 툴을 사용하여 합성하였고, POWERMILL™ 툴을 사용하여 전력소비신호 데이터를 얻었다. 128 비트 전체 비밀키를 얻기 위해서는 많은 수의 원문 샘플이 필요하다. 그 이유는 샘플 수의 증가가 "0"과 "1"에 대한 전류 파형을 명확하게 만들기 때문이다. 본 실험에서는 5,000개의 원문 샘플을 사용하였고, 임의의 원문과 전력소비신호를 분류할 분류함수를 통해 전력소비결과를 추출하였다.

그림 2는 1비트에 대한 DPA 전력소비 결과를 보여준다. 음의 전류 값을 갖는 이 결과는 비밀키 값이 "0"이라는 것을 나타내고 그림 3은 양의 전류 값을 나타내므로 비밀키 값은 "1"이 된다. 그림 4는 비밀키 최상위 4비트에 대한 실험 결과를 나타낸다. 이를 통해 128 비트 전체 비밀키 값을 획득하였다.

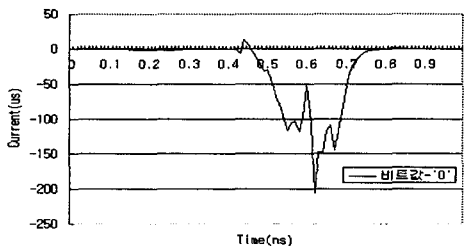

그림 2. 1비트에 대한 DPA 실험결과

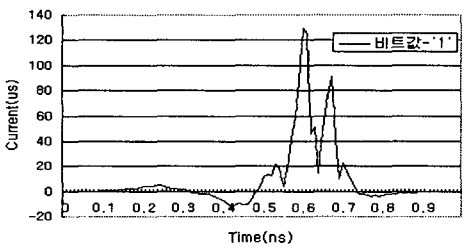

그림 3. 1비트에 대한 DPA 실험결과

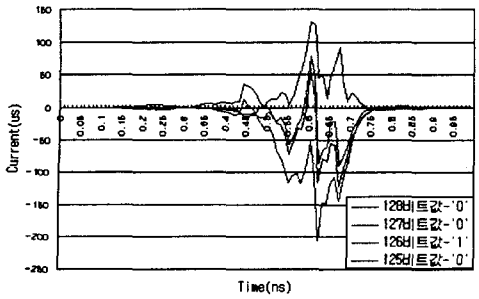

그림 4. 4비트에 대한 DPA 실험결과

VI. 대응책

DPA는 "0"과 "1"에 대한 전력소비패턴이 다르다는 것에 기초하여 정보를 유출시키므로 이를 막기 위해서는 전력소비를 균등하게 하는 하드웨어 구현이 필요하다. 이를 위해 비동기 이중선로방식(Dual-rail)의 Delay Insensitive Min-term Synthesis(DIMS) 회로 설계 기법을 제안한다[9].

비동기 이중선로방식은 데이터 한 비트를 두 개의 선로를 이용하여 나타내는 코딩방법으로 데이터 값에 데이터 유효성 정보까지 포함한다. 따라서, 유효한 데이터 "0"과 "1"이 전송되는 경우 두개의 경로는 모두 같은 개수의 "0"과 "1"을 가지게된다. 즉, 데이터 값 "1"은 "10", "0"은 "01"로 인코딩 된다. 이러한 코딩방법은 암호화 연산 수행 시에 데이터 비트 값에 따른 전력소비의 차이를 발생시키지 않는 특징을 가진다.

DIMS는 회로에 있는 c-element가 모든 입력 변수의 최소항을 생성하는 것으로 회로의 입력 값 "0"과 "1"의 전력 소모의 차이를 최소화 또는 제거하여 전력소비패턴과 연산되는 데이터 값들 사이의 상호연관성을 최소화 또는 제거시킨다. 이러한 비동기 이중선로방식의 DIMS 회로 설계 기법은 DPA 공격에 안전한 보안회로로써 대칭키 암호 알고리듬인 AES 뿐만 아니라 비대칭키 암호 알고리듬에도 사용될 수 있다.

VII. 결론

본 논문은 Rijndael 알고리듬에 대한 DPA 공격 방법과 전력소비 시뮬레이션 실험 결과를 보여주며, 비밀키 획득을 통해 DPA에 대한 Rijndael의 취약성을 나타내었다. DPA는 Rijndael 뿐만 아니라 대부분의 암호 알고리즘에 대해 공격 가능한 강력한 방법으로 고도의 보안을 요구하는 스마트카드에 사용되기 위해서는 DPA 공격에 강한 하드웨어로 설계되어져야 한다. 본 논문에서 제안한 비동기 이중선로방식의 DIMS 회로 설계 기법은 데이터 값과 전력소비패턴간의 상호연관성을 제거하여 DPA 공격에 안전할 수 있다.

VII. Acknowledgement

본 연구보고서는 정보통신부 정보통신연구진흥원에서 지원하고 있는 정보통신기초연구지원사업의 연구결과입니다.

VIII. 참고문헌

[1] Joan Daemen and Vincent Rijmen, "AES Proposal : Rijndael", NIST Document Version 2, March, 1999, http://www.nist.gov/aes.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", CRYTO'99, pp. 388-397, 1999.

[3] John Daemen, Vincent Rijnmen, "Resistance Against Implementation Attack, A comparative Study of the AES Proposals", Second AES Conference, 1999.

[4] Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Cipher", in Proceedings of ESORICS'98, pp. 97-110, 1998.

[5] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," CRYPTO'96, pp.104-113, 1996.

[6] E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems", CRYPTO'97, pp. 513-525, 1997.

[7] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic Analysis: Concrete Results", CHES'2001, pp. 255-265, 2001.

[8] Thomas Messernges, "Securing the AES Finalists Against Power Analysis Attacks", Proceedings of Fast Software Encryption Workshop, 2000.

[9] Jens SparsØ and Steve Furber, editors. "Principles of asynchronous circuit design", Kluwer Academic Publishers, 2001.