능동형 RFID에 대한 차분 전력 주파수 분석 공격†

박제훈*, 한동호*, 하재철**, 이훈재***, 문상재* 최용제****, 김호원****

*경북대학교 전자공학과

**나사렛대학교 정보통신학과

***동서대학교 인터넷공학부

****한국전자통신연구원

Differential Power Frequency Analysis on Active RFID

JeaHoon Park*, DongHo Han*, JaeCheol Ha**, HoonJae Lee***, SangJae Moon*

*Dept. of Electronics, Kyungpook National Univ.

**Dept. of Information and Communication, Korea Nazarene Univ.

***School of Internet Engineering, Dongseo Univ.

****Electronics and Telecommunications Research Institute, Korea.

요 약

부채널 정보를 이용한 공격이 제안된 이후, 스마트카드와 RFID와 같은 저 전력 정보보호 장치 내부의 암호 프로세서에서 소비되는 전력을 분석하여 암호 연산에 사용된 비밀 정보를 알아내는 공격 방법은 가장 위협적인 물리적 공격 방법으로 알려져 있다. 하지만 측정된 소비 전력 신호를 시간 영역에서 분석하는 기존의 분석 기법들은 암호 연산 시점이 시간 축 상에서 동일하여야 된다는 단점을 가지고 있다. 제안하는 주파수 분석 공격 방법은 공격이 적용되는 장치에서 측정된 시간 영역에서 정렬되지 않는 신호를 Fourier 변환을 하여 주파수 영역에서 분석함으로써 기존 전력 분석 공격이 시간 영역에서 정렬된 소비 전력 신호를 필요로 하는 문제점을 해결하였다. UC Berkeley에서 제작된 능동형 RFID 모듈에 국내 표준인 ARIA 알고리즘을 응용프로그램으로 탑재하여 기존 전력 분석 공격과 제안하는 주파수 분석 공격을 적용하여 결과를 분석 하였다.

I. 서론

지금까지의 많은 암호시스템은 이론적으로 안전하다고 알려진 이산대수 문제나 소인수분해 문제에 기반을 하여 개발되었다. 그러나 이론적인 안전도와는 별개로 암호 알고리듬을 실제로 구현 시에 부가적으로 비밀 값에 대한 누출이 있다. 특히 스마트카드와 같은 장치의 경우에는 다양한 종류의 비밀 키와 관련된 정보들이 누출되고 있다. 이와 같이 정보보호 장치들에서 연산 수행 시 누출되는 정보를 이용한 공격을 부채널 공격이라고 한다 [1]. 부채널 공격에는 오류 분석 주입 공격[2,3], 시간 공격, 전력 분석 공격[4-6]이 대표적이다. 전력 분석 공격에는 단순히 측정된 전력 신호를 관찰함으로써 비밀 키의 정보를 알아내는 단순 전력 분석(Simple Power Analysis, SPA)과 측정된 전력 신호에 통계학적인 방법과 에러 정정 기법을 적용하여 비밀 키의 정보를 알아내는 차분 전력 분석(Differential Power Analysis, DPA)이 있다.

본 논문 에서는 UC Berkeley에서 제작된 능동형 RFID 모듈에 국내 표준 ARIA 알고리즘

† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업의 연구결과로 수행되었음.

을 응용프로그램으로 탑재하여 ARIA 알고리즘의 치환함수에서 사용되는 $S-box$ 연산에 기존의 전력 분석 공격을 적용한 후, 문제점을 분석하였다. 또한 기존의 전력 분석 공격은 암호 연산이 이루어지는 시점이 항상 같아야 한다는 단점을 보완하여 시간 영역의 정렬되지 않은 소비 전력 신호를 이용해서도 전력 분석 공격을 적용할 수 있는 전력 주파수 분석 공격 방법을 제안한다.

2장에서는 ARIA 알고리즘, 전력 분석 공격, 전력 주파수 분석 공격과 공격 대상에 대해서 설명하고, 3장에서는 제안하는 DPFA 공격 방법을 설명한 후 실험 과정을 설명하고 4장에서 결론을 맺고 있다.

II. Related Works

2.1 ARIA 블록 암호 알고리즘

2004년 국가보안기술연구소(NSRI), 국가정보원, 학계 등은 128 비트 메시지를 사용하고 128, 192, 256 비트로 가변되는 키를 사용하는 블록 암호화 알고리듬 ARIA를 제안하였다 [7]. ARIA는 암호화 과정과 복호화 과정이 동일한 Involution SPN 구조의 블록 암호 알고리듬으로써 하드웨어적인 구현에 적합하며, 미국·유럽 등의 새로운 표준 제정 시 고려된 여러 가지 안전성 및 효율성 기준에 부합되도록 설계되었다. 다음의 그림 2.1은 1 라운드 ARIA의 암호 과정을 대략적으로 나타내고 있다.

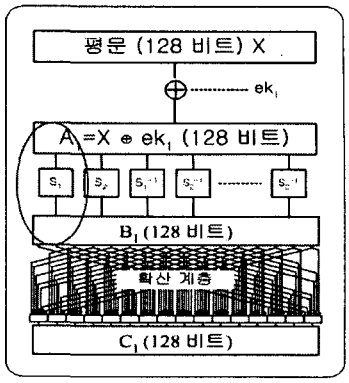

그림 2.1. ARIA 1 라운드 암호화 과정

2.3 능동형 RFID

일반적으로 RFID는 크게 능동형과 수동형으로 구분할 수 있다. 수동형 RFID는 자체 전원을 가지지 않고 리더기의 송신 전파를 이용하여 동작하여 CPU의 연산능력이나 통신 거리 등에 많은 제약을 가지고 있다. 하지만 능동형 RFID는 자체 전원을 내장하여 수동형 RFID의 많은 제약점을 보완하고 있다. 본 논문에서 대상으로 하고 있는 능동형 RFID는 UC Berkeley에서 개발한 Telos 모듈이고 CPU는 TI사의 MSP430 칩을 사용 한다 [8]. 그림 2.2는 공격 대상을 나타내고 있다.

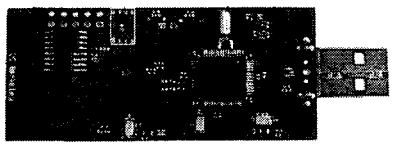

그림 2.2. 공격 대상 능동형 RFID

공격 대상 능동형 RFID는 센싱이 가능하고, radio 통신과 안테나로 동작 가능하다. TinyOS로 동작하고 프로그램 가능하며, 8 MHz의 bus 속도를 가지고 2 KB RAM과 60 KB의 프로그램 가능한 메모리 공간을 가진다.

2.2 전력 분석 공격

정보보호 장치들에서 연산 수행 시 누출되는 정보를 이용한 공격을 부채널 공격이라고 한다. 부채널 공격에는 오류 분석 공격, 시간 공격, 전력 분석 공격이 대표적이다. 전력 분석 공격은 1999년 Kocher에 의해 제안된 공격 방법으로써 정보보호 장치 내에서 비밀 키와 관련한 연산이 수행될 때에 정보보호 장치가 소비하는 전력 신호를 측정하고 관찰해서 비밀 키의 정보를 알아내는 단순 전력 분석 (Simple Power Analysis, SPA)과 측정된 전력 신호에 통계학적인 방법과 에러 정정 기법을 적용하여 비밀 키의 정보를 알아내는 차분 전력 분석 (Differential Power Analysis, DPA)이 있다 [4-6]. DPA 공격은 크게 세 가지로 나뉘어 진다.

- Single-Exponent Multiple-Data (SEMD) Attack
  : 비밀 키를 알고 있는 정보보호 장치를 가지고 있을 때 적용 가능.
- Multiple-Exponent Single-Data (MESD) Attack
  : 비밀 키를 변경 가능한 정보보호 장치를 가지고 있을 때 적용 가능.
- Zero-Exponent Multiple-Data (ZEMD) Attack
  : Off-line으로 중간 값의 계산이 가능할 때 적용 가능.

2.4 Differential Power Frequency Analysis

C. C. Tiu와 C. H. Gebotys는 암호 연산중에 측정되는 소비 전력 신호를 주파수 영역에서 분석하는 방법을 제안하였다 [9,10]. 측정된 소비 전력 신호의 Power Spectral Density를 계산하여 전력 분석 공격에 사용하였고, 올바른 키가 추측되었을 때의 소비 전력 파형을 구별하기 위해서 차분 전력 파형의 표준 편차를 사용하였다. 다음의 그림 2.3은 DPFA(Differential Power Frequency Analysis)공격 알고리즘을 설명하고 있다.

◎ **DPFA**(T)
1. $P \leftarrow PowerSpectralDensity(T)$
2. for each $K, K \in \{0, ..., 255\}$
3. $\{P^0, P^1\} \leftarrow partitionTraces(P)$
4. $STD\_R \leftarrow STD\_DOM(P^0, P^1)$
5. $Diff \leftarrow Mean(P^0) - Mean(P^1)$
6. $sumPeak(key) \leftarrow 0$
7. for each $f, f \in \left\{0, ..., \frac{m}{2} - 1\right\}$
8. if($abs(Diff(f) > 2 * STD\_R(f))$
   $sumPeak(K)$
   $\leftarrow sumPeak(K) + (abs(Diff(f)) - 2 * STD\_R(f))$
9. return $sumPeak$

그림 2.3. DPFA 알고리즘

그림 2.3의 출력 값인 sumPeak는 표준 편차의 값을 벗어나는 값이 얼마나 많이 존재하느냐를 판단한다. 올바른 키를 추측하였을 경우에는 소비 전력 파형이 해밍웨이트에 따라 잘 분류가 되어 일반적인 소비 전력 파형의 차분 값보다 표준 편차 값을 많이 벗어나게 된다.

III. 능동형 RFID에 대한 DPFA

3.1 능동형 RFID에 대한 DPA 공격의 문제점

매번 다른 메시지를 입력하는 ZEMD 형태의 공격 방법은 TinyOS의 응용프로그램으로 구현된 ARIA 알고리즘에 적용하기가 쉽지 않기 때문에, 본 논문에서는 기존의 ZEMD 형태의 공격 방법과는 조금 다른 내부 연산단위에 기반하는 DPA 공격을 능동형 RFID에 적용하였다 [11]. 적용된 전력 분석 공격 방법은 다음과 같다.

① 입력 평문(X)의 최상위 8 비트를 변화시켜가면서 256가지의 가능한 입력을 만든다. 가능한 입력을 $X_1, X_2, ... X_{256}$로 둔다.

② $X_1, X_2, ... X_{256}$를 입력으로 ARIA 알고리즘을 수행하여 소비 전력을 측정한다. 측정된 소비 전력 파형을 $P_1, P_2, ..., P_{256}$로

둔다.

③ 측정된 소비 전력 파형을 각각 차분한다.

$$P_1 - P_2, P_1 - P_3, \ldots, P_{255} - P_{256}$$

④ 차분 파형에서 피크의 크기를 비교하여 가장 큰 피크 값을 가지는 전력 소비 파형의 쌍을 찾는다.

⑤ 차분 파형에서 가장 큰 피크 값을 가지는 입력 메시지 쌍과 $S-box$ 입·출력 관계를 분석하여 비밀키 8 비트를 알아낸다.

다음의 그림 3.1은 다른 입력 메시지에 대한 ARIA 알고리즘의 평균 소비 전력 파형을 비교하고 있다.

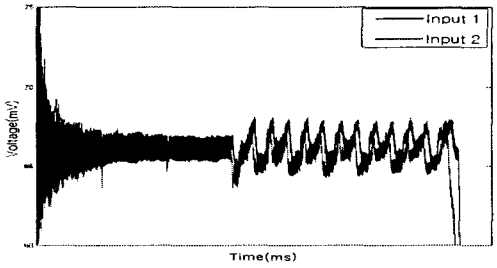

그림 3.1. ARIA 평균 전력 소비 파형 (1~12라운드)

그림 3.1과 같이 각각의 입력 메시지에 대해 측정되어 평균된 소비 전력 파형이 시간 축 상에서 정렬되지 않고 있고, 알고리즘 수행 시간 또한 다르다는 것을 알 수 있다. 따라서 기존의 전력 분석 공격 방법은 적용이 되지 않는다는 것을 알 수 있다.

3.2 능동형 RFID에 대한 DPFA

제안하는 전력 분석 공격 방법은 기존의 전력 분석 공격이 가지고 있는 문제점을 보완하고 TinyOS의 응용프로그램으로 구현된 ARIA 알고리즘에 효과적으로 적용하기 위해서 주파수 분석 방법과 내부 연산 단위에 기반을 둔 전력 분석 공격 방법을 사용하였다.

◎ Proposed_DPFA(T)
1. $P \leftarrow PowerSpectralDensity(T_i)$
2. for each M_1, M_2 ($M_1, M_2 \in \{0, \ldots, 255\}$)
3. $STD\_R \leftarrow STD\_DOM(P^1, P^2)$
4. $Diff \leftarrow Mean(P^1) - Mean(P^2)$
5. $sumPeak(M_1, M_2) \leftarrow 0$
6. for each f ($f \in \left\{0, \ldots, \frac{m}{2} - 1\right\}$)
7. if($abs(Diff(f) > 2*STD\_R(f))$
$sumPeak(M_1, M_2)$
$\leftarrow sumPeak(M_1, M_2) + (abs(Diff(f)) - 2*STD\_R(f))$
8. return $sumPeak$

그림 3.2. 제안하는 DPFA 알고리즘

그림 3.2에서 M_i는 T_i를 생성할 때 입력되는 8 비트 메시지이며 가능한 입력 메시지의 256가지로 만들 수 있는 모든 가능한 메시지의 쌍에 대해서 실험을 반복하여서 sumPeak 값이 가장 클 때 입력한 메시지의 쌍으로 비밀키를 추측할 수 있다. 그림 3.3은 Telos 모듈에서 연산되는 ARIA 알고리즘의 전력 소비 파형의 일부분을 오실로스코프에서 측정한 그림이다.

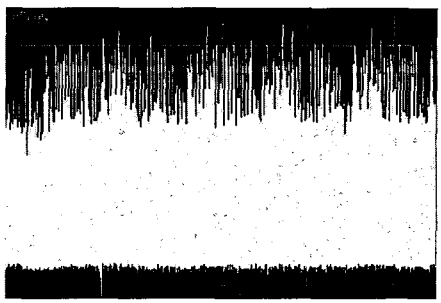

그림 3.3. ARIA 전력 소비 파형 (1~4라운드)

그림 3.4는 1500개의 ARIA 전력 소비 파형을 평균한 그림이다.

그림 3.5와 그림 3.6은 시간 영역의 소비 전

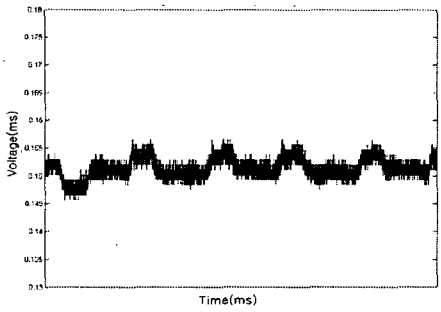

그림 3.4. ARIA 평균 전력 소비 파형 (1~4라운드)

력 파형을 주파수 영역으로 변환한 결과를 보여주고 있다.

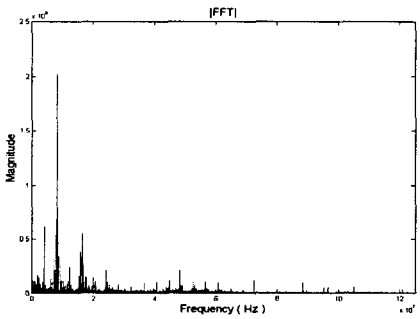

그림 3.5. 그림 3.3의 |FFT| 결과

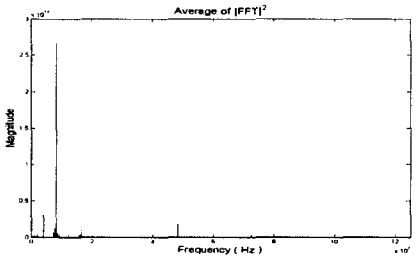

그림 3.6. 그림 3.5의 PSD 평균

그림 3.7은 ARIA 1라운드 $S-box\,S_1$에 DPFA을 적용하여 PSD 평균 파형의 차분결과와 ±2*STD 영역을 나타내고 있다.

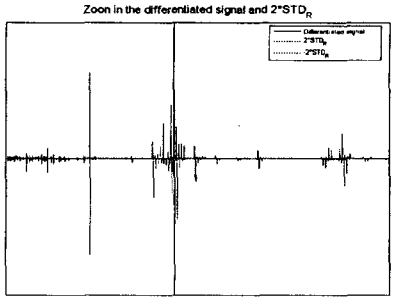

그림 3.7. PSD 차분 파형과 ±2*STD 파형

그림 3.8은 서로 다른 해밍웨이트 차이가 나는 입력 메시지 쌍을 입력 하였을 때의 sumPeak 값을 나타내고 있다.

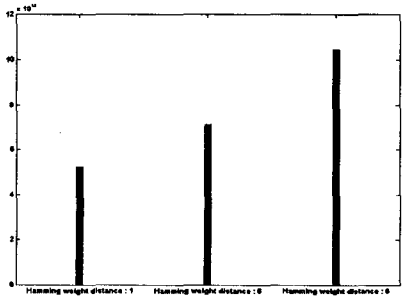

그림 3.8. 해밍웨이트 차이에 따른 *sumPeak* 결과

그림 3.8의 제안하는 DPFA 적용결과에서와 같이 sumPeak의 값이 해밍웨이트 차이에 비례한다는 것을 알 수 있으므로, 가장 큰 sumPeak 값을 가지는 입력 메시지 쌍은 $S_1 S-box$ 출력의 해밍웨이트 차이가 8이라는 사실을 이용하여 비밀키를 알아낼 수 있다. 공격자는 입력 메시지의 쌍을 알고, ARIA $S_1 S-box$의 출력에서 해밍웨이트 차이가 8이 되는 $S_1 S-box$의 입력 쌍을 알 수 있기 때문에 AddRoundKey 함수의 성질을 이용하여 비밀키를 알아낼 수 있다. 예를 들어 0xA9와 0x86을 입력 메시지 쌍으로 하였을 때 차분 파형에서 가장 큰 피크 파형을 관찰하였다면, ARIA 1라운드의 연산 절차는 그림 3.9와 같이 나타낼 수 있다.

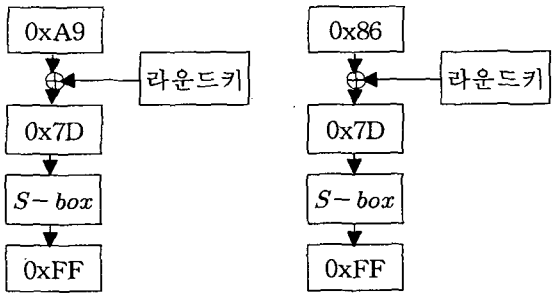

그림 3.9. 비밀키 유추 과정

그림 3.9에서와 같이 0xA9나 0x86을 입력하였을 때 $S-box$ 출력 값으로 0xFF를 출력하는 0x7D가 입력 메시지와 라운드 키의 XOR 연산 결과 값이 되므로 라운드 키는 0xD4 또는 0xFB가 된다.

IV. 결론

전력 분석 공격 방법은 암호 알고리즘의 이론적인 안전도와는 상관없는 매우 위협적인 공격 방법으로 알려져 있다. 하지만 암호 알고리즘 연산중의 세부적인 암호 연산들 모두가 항상 동일한 시간에서 동일한 시간동안 수행되어야 한다는 제약점을 가지고 있다. 하지만 기존의 스마트카드와 같이 별도의 암호프로세서에서 연산되는 경우와는 다르게 공격 대상으로 하고 있는 능동형 RFID의 경우에는 암호 알고리즘이 tinyOS의 응용프로그램으로 동작되어 OS 자체의 여러 가지 원인에 의한 인터럽트의 영향으로 암호 알고리즘 내부의 세부 암호 연산들이 항상 동일한 시점에서 연산되지 않으며, 또한 동일한 시간 동안 수행되지 않음을 관찰할 수 있었다. 따라서 측정된 소비 전력 파형이 시간 축 상에서 정렬되지 않기 때문에 기존의 전력 분석 공격 방법을 적용하기 어렵다.

본 논문에서는 내부 연산단위에 기반을 두는 DPA 알고리즘을 이용한 주파수 분석 공격 방법을 제안 하였고, 능동형 RFID에 국내 표준 알고리즘인 ARIA 블록 알고리즘을 구현한 후, 직접 공격을 적용하여 라운드 키를 알아낼 수 있었다.

[참고문헌]

[1] J. Keley, B. Schneier, D. Wagner, and C. Hall, "Side channel cryptanalysis of product cipher," in Proceedings of ESORICS '98, pp. 97-110, Springer-Verlag, Sep.1998.

[2] Bellcore Press Release, "New threat model breaks crypto codes," Sep. 1996 or D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," In Advances in Cryptology-EUROCRYPT '97, LNCS 1233, pp. 37-51, Springer-Verlag, 1997.

[3] S. M. Yen, S. J. Kim, S. G. Lim, and S. J. Moon, "A countermeasure against one physical cryptanalysis May Benefit Another Attack," In Proc. of the ICISC 2001, Korea. Dec. 2001

[4] P. Kocher, J. Jaffe, and B. Jun, "Introduction to differential power analysis and related attacks," http://www.cryptography.com/dpa/technical, 1998.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Advances in Cryptology-CRYPTO'99, pp. 388-397, Springer-Verlag, 1999.

[6] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power analysis attacks on modular exponentiation in Smart cards," in Proc. of CHES 1999, pp. 144-157, Springer-Verlag, 1999.

[7] 국가보안기술연구소 (NSRI), "민관겸용 블록 알고리즘 ARIA, http://www.nsri.re.kr

[8] Motoeiv Corporation, http://www.moteiv.com/

[9] Chin Chi Tiu, "A New Frequency-Based Side Channel Attack for Embedded Systems", thesis of Master deg.,

University of Waterloo, 2005.

[10] C.H. gebotys, Simon Ho, C.C. Tiu, "EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA," LNCS3659 - CHES2005, pp250-264, 2005.

[11] JeaHoon Park, "A New Frequency-Based Side Channel Attack for Embedded Systems", thesis of Master deg., Kyungpook National University, 2005.