한국항행학회 논문지 제17권 제 5호 2013년 10월 (JKONI 17(5): 568-573, Oct. 2013)

대칭구조 SPN 블록 암호 알고리즘에 대한 차분 오류 공격

Differential Fault Analysis on Symmetry Structured SPN Block Cipher

이창훈*

Chang-Hoon Lee*

요 약

본 논문에서는 2008년에 제안된 대칭구조 SPN 블록 암호 알고리즘에 대한 차분 오류 공격을 제안한다. 이 알고리즘은 암호화 과정과 복호화 과정이 동일한 SPN 구조 블록 암호 알고리즘이다. 본 논문에서 소개하는 공격은, 1개의 랜덤 바이트 오류와 2^8의 전수조사를 이용하여, 타깃 알고리즘의 128-비트 비밀키를 복구한다. 본 논문의 공격 결과는 대칭구조 SPN 블록 암호 알고리즘에 대한 첫 번째 공격 결과이다.

Abstract

In this paper, we propose a differential fault analysis on symmetry structured SPN block cipher proposed in 2008. The target algorithm has the SPN structure and a symmetric structure in encryption and decryption process. To recover the 128-bit secret key of the target algorithm, this attack requires only one random byte fault and an exhaustive search of 2^8. This is the first known cryptanalytic result on the target algorithm.

Key words : Block cipher, Differential fault analysis, Symmetry structured SPN block cipher, Cryptanalysis

I. 서 론

차분 오류 공격(differential fault analysis, DFA)은 1997년 Biham과 Shamir에 의해 블록 암호 DES에 최초로 적용된 부채널 공격 기법 중 하나이다 [1]. 이 공격은 기존의 차분 공격(differential cryptanalysis) [2]을 오류 주입 공격(fault injection attack) [3]에 결합하여 DES 뿐만 아니라 AES, ARIA, SEED, LED, Piccolo, LBlock 등 대부분의 블록 암호 알고리즘에 적용되었다 [4]-[7]. 이는 DFA가 블록 암호 알고리즘의 안전성 분석에 매우 큰 영향을 주고 있음을 의미한다.

2008년에 제안된 대칭구조 SPN 블록 암호 알고리즘은 블록 암호 AES [8]에 기반을 둔 128-비트 블록 암호로서, 암호화 과정과 복호화 과정이 동일하도록 설계되었다 [9]. DFA가 하드웨어 환경에서 적용 가능한 공격이라는 점과 대칭구조 SPN 블록 암호 알고리즘이 제한적 하드웨어 및 소프트웨어 환경인 스마트카드와 전자칩이 내장된 태그와 같은 RFID 환경에서 안전하고 효율적으로 동작하도록 설계되었다는 점을 고려할 때, 이 블록 암호의 DFA에 대한 안전성 분석은 반드시 수행해야할 연구 분야이다.

따라서 본 논문에서는 2008년 멀티디미어학회 논문지에서 제안된 대칭구조 SPN 블록 암호 알고리즘에 대한 차분 오류 공격을 제안한다. 본 논문에서 제안하는 공격은 [10]에서 제안된 공격 아이디어에 기반을 둔다. [10]에서는 AES-128에 대한 DFA가 제안

* 서울과학기술대학교 컴퓨터공학과(Department of Computer Science and Engineering, Seoul National University of Science and Technology)
· 제1저자 (First Author) : 이창훈(Chang-Hoon Lee, Tel : +82-10-8650-3083, email : chlee@seoultech.ac.kr)
· 접수일자 : 2013년 8월 30일 · 심사(수정)일자 : 2013년 8월 30일 (수정일자 : 2013년 10월 21일) · 게재일자 : 2013년 10월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.5.568

되었다. 이 공격은 다음과 같은 세 개의 단계로 구성된다. 먼저, AES-128의 라운드 8에 1개의 랜덤 바이트 오류를 주입한 후 라운드 9에서 발생하는 차분 특성을 이용하여 12개의 선형 방정식을 구성한다. 그리고 라운드 10의 라운드 키를 추측한 후, 구성된 선형 방정식을 만족하는 후보 라운드 키를 계산한다. 이후 복구된 후보 라운드 키와 키스케줄 특성을 이용하여 128-비트 비밀키를 복구한다. 본 논문에서 소개하는 공격은 [10]에서 제안된 공격을 대칭구조 SPN 블록 암호 알고리즘에 적용한다. 즉, 라운드 9의 입력 레지스터 중 첫 번째 바이트 레지스터에 1개의 랜덤 바이트 오류를 주입하여 2^8개의 후보 비밀키를 계산한다. 그리고 2^8의 전수조사를 통하여 128-비트 비밀키를 복구한다. 본 논문에서 소개하는 공격 결과는 대칭구조 SPN 블록 암호 알고리즘에 대한 첫 번째 안전성 분석 결과이다.

본 논문은 다음과 같이 구성되어 있다. 먼저, 2장에서는 대칭구조 SPN 블록 암호 알고리즘을 간략히 소개하고, 3장에서 [10]에서 제안된 공격 과정을 소개한다. 4장에서는 대칭구조 SPN 블록 암호 알고리즘에 대한 DFA를 제안한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 대칭구조 SPN 블록 암호 알고리즘

128-비트 블록 암호인 대칭구조 SPN 블록 암호 알고리즘은 128-비트 비밀키를 사용하며, 128-비트 블록 암호 AES-128에 기반을 두어 설계되었다. 그림 1에서 알 수 있듯이, 라운드 1 ~ 라운드 5는 AES-128의 암호화 과정에서의 라운드 함수를 사용하고 라운드 6 ~ 라운드 10은 AES-128의 복호화 과정에서의 라운드 함수를 사용한다. 또한, 라운드 5와 라운드 6 사이에 Symmetry() 함수를 수행한다. 이런 대칭적인 구조로 인해, 이 암호 알고리즘의 암호화 과정과 복호화 과정은 동일하다.

128-비트 내부 상태값은 그림 2와 같이 16개 바이트로 구성된 4×4 행렬로 나타낸다. 본 논문에서는 특정 내부 상태값 S의 i번째 바이트 값을 $S[i]$로 표기하기로 한다 $(i=0,1,\cdots,15)$.

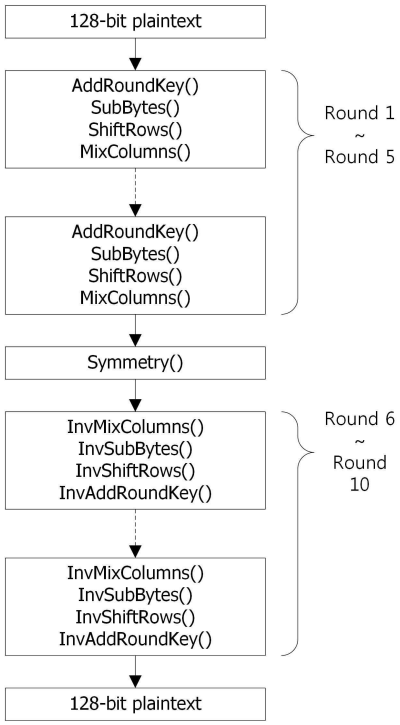


그림 1. 대칭구조 SPN 블록 암호 알고리즘
Fig. 1. Symmetry structured SPN block cipher algorithm.

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

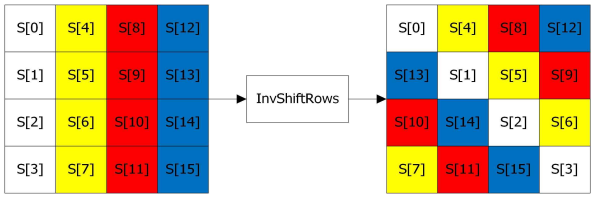
그림 2. 16-바이트 내부 상태값
Fig. 2. 16-byte inner state.

대칭적인 SPN 블록 암호 알고리즘의 라운드 함수에는 다음과 같은 함수들이 사용된다 [8].

- SubBytes(SB): 동일한 S-box를 각각의 내부 상태값 바이트에 적용시킨 비선형 대치 연산
- ShiftRows(SR): 내부 상태값의 각각의 행에 대한 바이트별 순환 이동 변환
- MixColumns(MC): 4 바이트로 구성된 각 열을 변환시키는 4×4 행렬로 $GF(2^8)$ 상에서 연산됨
- AddRoundKey(ARK): 키스케줄에 의해 비밀키로

부터 생성된 라운드 키와 내부 상태값의 비트별 XOR 연산으로 이루어짐

- InvSubBytes(ISB): SB의 역 연산
- InvShiftRows(ISR): SR의 역 연산



- InvMixColumns(IMC): MC의 역 연산

$$\begin{bmatrix} a' \\ b' \\ c' \\ d' \end{bmatrix} = \begin{bmatrix} 0E\ 0B\ 0D\ 09 \\ 09\ 0E\ 0B\ 0D \\ 0D\ 09\ 0E\ 0B \\ 0B\ 0D\ 09\ 0E \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}. \quad (1)$$

- InvAddRoundKey(IARK): ARK의 역 연산

Symmetry() 함수는 그림 3과 같이 동작한다. 128-비트 입력값을 64-비트 (A, B)로 나누고 각각의 A, B 블록은 32비트로 나누어 2-라운드 Feistel 구조를 갖는다. 그림에서 '$\cap$'과 '$\cup$'은 비트별 AND 연산과 OR 연산을 의미한다. 그리고 '$\lll i$'는 왼쪽으로 i-비트 순환 이동 연산을 의미한다.

대칭적인 SPN 블록 암호 알고리즘의 키스케줄은 AES-128의 키스케줄을 그대로 사용한다 [8].

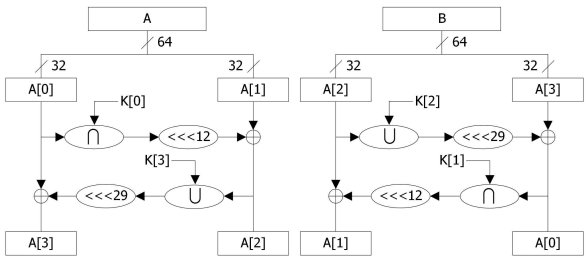


그림 3. Symmetry()
Fig. 3. Symmetry().

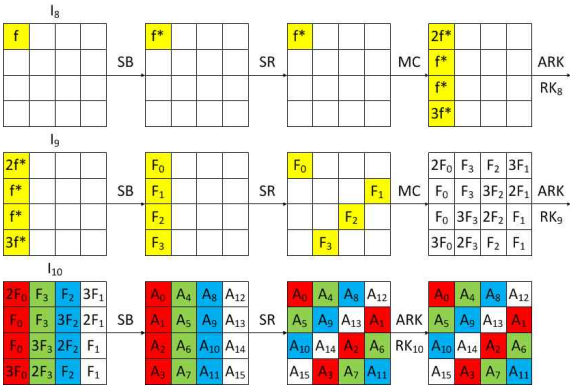


그림 4. AES-128에 대한 DFA
Fig. 4. DFA on AES-128.

Ⅲ. [10]에서 제안된 AES-128에 대한 DFA

본 장에서는 [10]에서 제안된 AES-128에 대한 DFA를 간략히 소개한다. 이 공격의 오류 주입 가정은 랜덤 바이트 오류 주입 모델에 기반을 둔다. 하지만, 최근 AES-128의 정확한 라운드에서 정확한 위치에 오류를 주입하는 것이 가능한 것으로 알려졌다 [11]. 따라서 본 장에서는 오류가 라운드 8의 입력 레지스터 중 첫 번째 바이트 레지스터 $I_8[0]$에 오류가 주입된 경우만을 소개한다.

오류 발생 여부에 따라 평문/암호문 쌍을 다음과 같이 표기한다.

- (P, C): 오류가 발생하지 않은 알고리즘을 이용하여 얻은 평문/암호문 쌍
- (P, C^*): 오류가 발생한 알고리즘을 이용하여 얻은 평문/암호문 쌍

오류 주입을 통해 발생한 차분이 f라고 할 때, 차분 확산 경로는 그림 4와 같다. 이를 이용하여 128-비트 비밀키를 복구하기 위해 다음과 같은 과정을 수행한다.

먼저, 라운드 10의 32-비트 라운드 키 $RK_{10}[0,7,10,13]$을 추측한 후, 다음과 같은 방정식 식을 이용하여 후보 $RK_{10}[0,7,10,13]$의 수를 $2^8 (= 2^{32} \cdot 2^{-24})$로 줄일 수 있다.

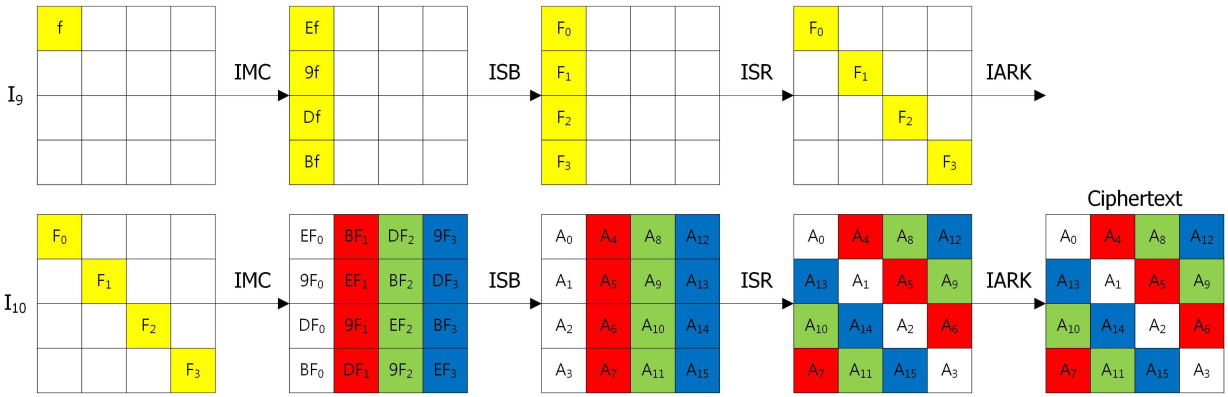


그림 5. 대칭적인 SPN 블록 암호 알고리즘에 대한 DFA
Fig. 5. DFA on symmetry structured SPN block cipher.

$$
\begin{aligned}
2F_0 &= S^{-1}(C[0]\oplus RK_{10}[0])\oplus S^{-1}(C^*[0]\oplus RK_{10}[0])\\
F_0 &= S^{-1}(C[13]\oplus RK_{10}[13])\oplus S^{-1}(C^*[13]\oplus RK_{10}[13])\\
F_0 &= S^{-1}(C[10]\oplus RK_{10}[10])\oplus S^{-1}(C^*[10]\oplus RK_{10}[10])\\
3F_0 &= S^{-1}(C[7]\oplus RK_{10}[7])\oplus S^{-1}(C^*[7]\oplus RK_{10}[7])
\end{aligned}
\tag{2}
$$

위의 과정을 $RK_{10}[1,4,11,14]$, $RK_{10}[2,5,8,15]$, $RK_{10}[3,6,9,12]$에 반복 적용하여 $2^{32}(=2^{8\cdot 4})$개의 후보 RK_{10}을 얻을 수 있다.

한편, RK_{10}을 이용하여 AES-128의 키스케줄을 통해 RK_9를 계산할 수 있음을 쉽게 알 수 있다. 따라서 각각의 후보 RK_{10}으로부터 RK_9를 계산할 수 있다. 각각의 후보 (RK_9, RK_{10})으로부터, 라운드 9의 32-비트 입력 차분 $\Delta I_9[0,1,2,3]$을 계산한다. 차분 패턴 $(2f^*, f^*, f^*, 3f^*)$를 체크함으로써, 후보 (RK_9, RK_{10})의 수를 $2^8(=2^{32}\cdot 2^{-24})$로 더 줄일 수 있다. 각각의 후보 (RK_9, RK_{10})로부터 1개의 128-비트 비밀키 K를 계산할 수 있다. 따라서 이 공격은 1개의 랜덤 바이트 오류와 2^8의 전수조사를 이용하여 128-비트 비밀키를 복구할 수 있다.

Ⅳ. 대칭적인 SPN 블록 암호 알고리즘에 대한 DFA

본 장에서는 대칭적인 SPN 블록 암호 알고리즘에 대한 차분 오류 공격을 제안한다. 본 공격은 3장에서 소개한 공격에 기반을 두며, 3장에서 언급한 바와 같이 [11]의 결과에 따라 정확한 라운드의 정확한 위치에 오류를 주입하는 것이 가능하다고 가정한다. 구체적으로, 라운드 9의 입력 레지스터 $I_9[0]$에 랜덤 바이트 오류를 주입하여 타깃 알고리즘의 128-비트 비밀키 K를 복구한다.

라운드 9의 $I_9[0]$에 오류가 주입되고, 이를 통해 발생한 차분값이 f일 때, 차분 확산 경로는 그림 5와 같다. 128-비트 비밀키 K를 복구하는 방법은 3장에서 소개한 방법과 유사하다. 본 장에서 제안하는 공격 과정은 다음과 같다.

(1) [오류가 발생하지 않은 데이터 수집] 오류가 발생하지 않은 알고리즘을 이용하여 평문 P에 대한 암호문 $C=(C[0],\cdots,C[15])$를 얻는다.
(2) [오류가 발생한 데이터 수집] 라운드 9의 입력 레지스터 중 첫 번째 바이트 레지스터 $I_9[0]$에 랜덤 바이트 오류 Δ를 주입한 후, 대응되는 암호문 C^*를 얻는다.
(3) [후보 $RK_{10}[0,5,10,15]$ 계산] 라운드 10의 32-비트 라운드 키 $RK_{10}[0,5,10,15]$을 추측한 후, 각각의 (C, C^*)에 대해 라운드 10에서 ISB 함수의 입력값을 계산한다. 그리고 다음과 같은 방정식을 이용하여 후보 $RK_{10}[0,5,10,15]$의 수를 2^{32}개에서 $2^8(=2^{32}\cdot 2^{-24})$로 줄인다.

$$EF_0 = ISB^{-1}(C[0] \oplus RK_{10}[0]) \oplus ISB^{-1}(C^*[0] \oplus RK_{10}[0])$$
$$9F_0 = ISB^{-1}(C[5] \oplus RK_{10}[5]) \oplus ISB^{-1}(C^*[5] \oplus RK_{10}[5])$$
$$DF_0 = ISB^{-1}(C[10] \oplus RK_{10}[10]) \oplus ISB^{-1}(C^*[10] \oplus RK_{10}[10])$$
$$BF_0 = ISB^{-1}(C[15] \oplus RK_{10}[15]) \oplus ISB^{-1}(C^*[15] \oplus RK_{10}[15]) \quad (3)$$

(4) [나머지 후보 RK_{10} 계산] 나머지 96-비트 $RK_{10}[3,4,9,14]$, $RK_{10}[2,7,8,13]$, $RK_{10}[1,6,11,12]$에도 단계 (3)을 반복 적용하여 총 $2^{32}(=2^{8\cdot 4})$개의 후보 RK_{10}을 얻는다.

(5) [후보 RK_{10} 필터링] 각각의 후보 RK_{10}에 대해, 대응되는 RK_9를 계산한다. 각각의 후보 (RK_9, RK_{10})으로부터, 라운드 9에서 ISB 함수의 입력 차분을 계산한다. 차분 패턴 $(Ef, 9f, Df, Bf)$를 체크함으로써, 후보 (RK_9, RK_{10})의 수를 $2^8(=2^{32}\cdot 2^{-24})$로 줄인다.

(6) [128-비트 비밀키 복구] 단계 (5)를 통과한 후보 (RK_9, RK_{10})에 대해 전수조사를 수행하여 대칭구조 SPN 블록 암호 알고리즘의 128-비트 비밀키 K를 복구한다.

틀린 후보 비밀키가 단계 (6)을 통과할 확률은 2^{-128}이다. 따라서 단계 (6)을 통과하는 틀린 후보 비밀키 개수의 기댓값은 $2^{-120}(=2^8\cdot 2^{-128})$이다. 이는 본 논문에서 제안하는 공격 알고리즘이 틀린 비밀키를 출력할 확률이 매우 낮음을 의미한다. 그러므로 본 논문에서 제안하는 공격은 1개의 랜덤 바이트 오류 주입과 2^8의 전수조사를 이용하여 대칭구조 SPN 블록 암호 알고리즘의 128-비트 비밀키를 복구할 수 있다.

V. 결 론

본 논문에서는 차분 오류 공격을 이용하여 대칭구조 SPN 블록 암호 알고리즘에 대한 첫 번째 안전성 분석 결과를 제안하였다. 본 논문에서 소개한 공격은 1개의 랜덤 바이트 오류 주입과 2^8의 전수조사를 이용하여 대칭구조 SPN 블록 암호 알고리즘의 128-비트 비밀키를 복구할 수 있다. 본 논문에서 소개한 공격 결과를 통해, 대칭구조 SPN 블록 암호 알고리즘의 구조가 AES-128의 구조와 유사하기 때문에 AES-128에 적용되었던 공격이 대칭구조 SPN 블록 암호 알고리즘에도 유사하게 적용될 수 있음을 알 수 있다.

감사의 글

본 연구는 서울과학기술대학교 교내학술연구 지원비로 수행되었습니다.

Reference

[1] E. Biham and A. Shamir, “Differential Fault Analysis of Secret Key Cryptosystems”, *Crypto 1997, LNCS 1294*, pp. 513-525, Springer-Verlag, 1997.

[2] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystem”, *Journal of Cryptology, Vol. 4, No. 1,* pp. 3-72m Springer-Verlag, 1991.

[3] D. Boneh, R. DeMillo and R. Lipton, “On the importance of checking cryptographic protocols for faults”, *Eurocrypt 1997, LNCS 1233,* pp. 37-51, Springer-Verlag, 1997.

[4] K. Jeong, Y. Lee, J. Sung and S. Hong, “Differential fault analysis on block cipher SEED”, *Mathematical and Computer Modelling,* Vol. 55, pp. 26-34, Elsevier, 2012.

[5] K. Jeong, “Security Analysis of Block Cipher LED-64 Suitable for Wireless Sensor Network Environments”, *JKONI 16(1): 70-75,* Feb. 2012.

[6] K. Jeong, “Differential Fault Analysis on Block Cipher Piccolo-80”, *JKONI 16(3): 510-517*, June 2012.

[7] K. Jeong and C. Lee, “Differential Fault Analysis on Lightweight Block Cipher LBlock”, *JKONI 16(5): 871-878,* Oct. 2012.

[8] FIPS PUB 197, “Announcing the ADVANCED ENCRYPTION STANDARD (AES)”, *U.S. Department of Commerce*, 2001.

[9] G. Kim, C. Park and G. Cho, “Symmetry structured SPN block cipher algorithm”, *Journal of Korea Multimedia Society, Vol. 11, No. 8*, pp. 1093-1100, Aug. 2008.

[10] M. Tunstall, D. Mukhopadhyay and S. Ali, “Differential Fault Analysis of the Advanced Encryption Standard Using a Single Fault”, *WISTP 2011, LNCS 6633,* pp. 224-233, Springer-Verlag, 2011.

[11] T. Fukunaga and J. Takahashi, “Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers”, *FDTC 2009,* pp. 84-92, IEEE, 2009.

이 창 훈 (Chang-Hoon Lee)

2001년 2월 : 한양대학교 수학과 (이학사)
2003년 2월 : 고려대학교 정보보호 대학원(공학석사)
2008년 2월 : 고려대학교 정보보호 대학원(공학박사)
2009년 3월 ~ 2012년 2월 : 한신대학교 컴퓨터공학부 조교수
2012년 3월 ~ 현재 : 서울과학기술대학교 컴퓨터공학과 조교수
관심분야 : 정보보호, 암호학, 디지털포렌식, 컴퓨터이론