KIPS Tr. Comp. and Comm. Sys.
Vol.4, No.3 pp.105~108 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2015.4.3.105

Differential Fault Analysis on Symmetric SPN Block Cipher with Bitslice Involution S-box

HyungChul Kang† · Changhoon Lee††

ABSTRACT

In this paper, we propose a differential fault analysis on symmetric SPN block cipher with bitslice involution S-box in 2011. The target block cipher was designed using AES block cipher and has advantage about restricted hardware and software environment using the same structure in encryption and decryption. Therefore, the target block cipher must be secure for the side-channel attacks. However, to recover the 128-bit secret key of the targer block cipher, this attack requires only one random byte fault and an exhausted search of 2^8. This is the first known cryptanalytic result on the target block cipher.

Keywords : Block Cipher, Differential Fault Analysis, Symmetric SPN Block Cipher, AES

비트 슬라이스 대합 S-박스에 의한 대칭 SPN 블록 암호에 대한 차분 오류 공격

강 형 철† · 이 창 훈††

요 약

본 논문에서는 2011년에 제안된 비트 슬라이스 대합 S-박스에 의한 대칭 SPN 블록 암호에 대한 차분 오류 공격을 제안한다. 이 블록 암호는 AES를 기반으로 설계되었으며, 암호화와 복호화를 동일하게 구성하여 제한적 하드웨어 및 소프트웨어 환경에서 장점을 가지도록 설계되었으므로, 이 블록 암호는 부채널 분석에 대한 안전성을 가져야 한다. 그러나 본 논문에서 제안하는 공격 방법은 1개의 랜덤 바이트 오류 주입과 2^8번의 전수 조사를 통해 본 블록 암호의 128-비트 비밀키를 복구한다. 이 분석 결과는 본 블록 암호에 대한 첫 번째 결과이다.

키워드 : 블록 암호, 차분 오류 공격, 대칭 SPN 블록 암호, AES

1. 서 론

차분 오류 공격(Differential Fault Analysis, DFA)은 1997년에 Biham과 Shamir가 DES에 대한 공격을 통해 처음 소개한 부채널 분석 기법 중 하나이다[1]. DFA는 차분 공격(Differential Cryptanalysis)[2]과 부채널 공격 기법인 오류 주입 공격(Fault Injection Attack)[3]을 결합한 것이다. 처음 소개된 DES에 대한 공격뿐만 아니라 다양한 블록 암호 알고리즘에 적용되었으며[4-7], 특히 AES 기반 블록 암호 알고리즘에 대한 공격이 활발하게 소개되었다[8-13].

2011년에 한국전자통신학회논문지에 소개된 비트 슬라이스 대합 S-박스에 의한 대칭 SPN 블록 암호(이하 대칭 SPN 블록 암호)는 AES[14]에 기반을 둔 128-비트 블록 암호로서, 128/192/256-비트 비밀키를 사용하며, 키 사이즈에 따라 각각 10/12/14 라운드이다[15]. 대칭 SPN 블록 암호는 비트 슬라이스 대합 S-박스를 이용하여 암호화 과정과 복호화 과정이 동일하게 설계되어 AES에 비해 제한적 하드웨어 및 소프트웨어 환경인 스마트카드와 RFID 환경에서 효율적이라는 장점이 있다.

DFA가 하드웨어 환경에서 적용 가능한 부채널 분석 기법 중 하나이고, 대칭 SPN 블록 암호가 하드웨어 환경에서 장점을 가지도록 설계되었으므로 반드시 DFA에 대한 안전성 분석이 수행되어야 한다.

본 논문에서는 비트 슬라이스 대합 S-박스에 의한 대칭 SPN 블록 암호에 대한 차분 오류 공격을 제안한다. 본 논문에서는 [8]에서 소개된 공격 아이디어를 이용하여 본 블록 암호를 분석하였다. 먼저, 8 라운드에 1개의 랜덤 바이트 오

※ 이 논문은 서울과학기술대학교 교내 학술연구비 지원에 의하여 연구되었음.
† 준 회 원 : 고려대학교 정보보호대학원 석·박사통합과정
†† 종신회원: 서울과학기술대학교 컴퓨터공학과 교수
Manuscript Received : January 7, 2015
Accepted : February 6, 2015
* Corresponding Author : chlee@seoultech.ac.kr

류를 주입하여 방정식을 구성한다. 이 방정식을 풀어서 2^{32}개의 라운드 키 후보를 찾는다. 찾은 라운드 키 후보를 키 스케줄과 9 라운드 차분 패턴을 이용하여 라운드 키 후보를 2^8개로 줄인다. 마지막으로 라운드 키 후보 2^8개를 전수조사하여 128-비트 비밀키를 복구한다. 이 공격 결과는 대칭 SPN 블록 암호에 대한 첫 번째 안전성 분석 결과이다.

본 논문은 다음과 같이 구성된다. 먼저, 2절에서 대칭 SPN 블록 암호를 간략히 소개한다. 다음으로 3절에서는 [8]에서 제안된 공격 방법을 소개하고, 이를 이용하여 4절에서는 대칭 SPN 블록 암호에 대한 차분 오류 공격을 제안한다. 마지막으로 5절에서 결론을 맺는다.

2. 대칭 SPN 블록 암호

비트 슬라이스 대합 S-박스에 의한 대칭 SPN 블록 암호는 AES에 기반을 두고 설계된 128-비트 블록 암호이다. 대칭 SPN 블록 암호는 128/192/256-비트 비밀키를 사용하며 키 사이즈에 따라 각각 10/12/14 라운드로 구성된다(Fig. 1 참고).

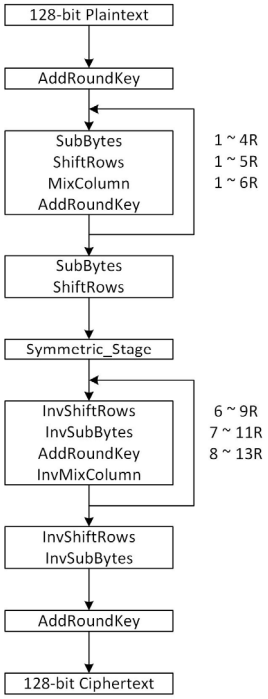

Fig. 1. Full Structure of Symmetric SPN Block Cipher

대칭 SPN 블록 암호는 Fig. 1과 같이 1～4/5/6 라운드(각각 128/192/256-비트 비밀키)는 정함수를 사용한다. 마지막 6/7/8～9/11/13 라운드(각각 128/192/256-비트 비밀키)는 역함수를 사용한다. 그리고 정함수와 역함수를 대칭으로 연결해주기 위한 대칭단(Symmetirc_Stage)이 존재하여 암호화와 복호화가 동일하다.

정함수의 각 라운드는 비선형 바이트 치환 함수(SubBytes), 바이트 교환 함수(ShiftRows), 선형 변환 함수(MixColumn), 키 덧셈 함수(AddRoundKey)의 네 가지 내부 함수로 구성된다. 역함수의 각 라운드는 네 가지 내부 함수의 역함수로 구성된다.

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

Fig. 2. 16-bytes State

각 내부 함수는 Fig. 2와 같이 4×4 정방 행렬인 스테이트(state) 단위로 수행된다. 본 논문에서는 특정 스테이트 S의 i번째 바이트를 $S[i](0 \le i \le 15)$로 표기한다.

대칭 SPN 블록 암호의 내부 함수는 다음과 같다.

- SubBytes : 8-비트 AES S-박스를 이용한 비선형 바이트 치환 함수이다.
- ShiftRows : 스테이트 각각의 행에 대한 바이트별 순환 이동 함수로 아래와 같다.
  - $S[0,4,8,12] \rightarrow S[0,4,8,12]$
  - $S[1,5,9,13] \rightarrow S[5,9,13,1]$
  - $S[2,6,10,14] \rightarrow S[10,14,2,6]$
  - $S[3,7,11,15] \rightarrow S[15,3,7,11]$
- MixColumn : 스테이트 각각의 열을 변환하는 4×4 행렬로 $GF(2^8)$ 상에서 연산된다(Equation (1) 참고).

$$\begin{bmatrix} S'[i] \\ S'[i+1] \\ S'[i+2] \\ S'[i+3] \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} S[i] \\ S[i+1] \\ S[i+2] \\ S[i+3] \end{bmatrix} \quad (1)$$

- AddRoundKey : 비밀키로부터 키 스케줄에 의해 생성된 라운드 키와 스테이트의 바이트별 XOR 연산이다.
- InvShiftRows : ShiftRows 함수의 역함수이다.
  - $S[0,4,8,12] \rightarrow S[0,4,8,12]$
  - $S[1,5,9,13] \rightarrow S[13,1,5,9]$
  - $S[2,6,10,14] \rightarrow S[10,14,2,6]$
  - $S[3,7,11,15] \rightarrow S[7,11,15,3]$
- InvSubBytes: SubBytes 함수의 역함수이다.
- InvMixColumn : MixColumn의 역함수이다(Equation (2) 참고).

$$\begin{bmatrix} S'[i] \\ S'[i+1] \\ S'[i+2] \\ S'[i+3] \end{bmatrix} = \begin{bmatrix} E & B & D & 9 \\ 9 & E & B & D \\ D & 9 & E & B \\ B & D & 9 & E \end{bmatrix} \cdot \begin{bmatrix} S[i] \\ S[i+1] \\ S[i+2] \\ S[i+3] \end{bmatrix} \quad (2)$$

- Symmetric_Stage : 정함수와 역함수를 대칭으로 연결해주기 위한 대칭단으로 4-비트 S-박스를 32번 적용하

는 함수이다. 여기서 사용되는 4-비트 S-박스는 Table 1과 같다.

Table 1. S-box of Symmetric_Stage(hexadecimal)

x	0	1	2	3	4	5	6	7
S(x)	b	5	f	3	c	1	8	7
x	8	9	a	b	c	d	e	f
S(x)	6	e	a	0	4	d	9	2

3. AES-128에 대한 DFA

본 장에서는 [8]에서 제안된 AES에 대한 DFA를 간략히 소개한다. 이 공격의 오류 주입 가정은 랜덤 바이트 오류 주입 모델에 기반을 둔다. 하지만 2009년 FDTC에서 Fukunaga 등은 AES의 특정 라운드에서 원하는 위치에 정확히 오류를 주입하는 것이 가능하다고 소개하였다[16]. 따라서 8 라운드의 입력 스테이트 중 첫 번째 바이트($S_8[0]$)에 오류가 주입된 경우만을 소개한다.

본 논문에서는 다음과 같은 표기법을 사용한다.

- $C[i]$: 오류가 주입되지 않은 암호문의 i번째 바이트
- $C^*[i]$: 오류가 주입되어 얻은 암호문의 i번째 바이트
- RK_r : r 라운드의 라운드 키
- $RK_r[i]$: r 라운드의 라운드 키의 i번째 바이트 $(0 \le i \le 15)$
- f : 오류가 주입되어 발생한 차분
- f^*, F_j, A_l : 주입된 오류가 S-박스를 통과하여 변경된 차분$(0 \le j \le 3,\ 0 \le l \le 15)$

$S_8[0]$에 주입된 오류에 의해 발생한 차분 f에 의한 차분 확산 경로는 Fig. 3과 같다. 이를 이용하여 128-비트 비밀키를 복구하기 위해서는 다음과 같은 단계를 수행한다..

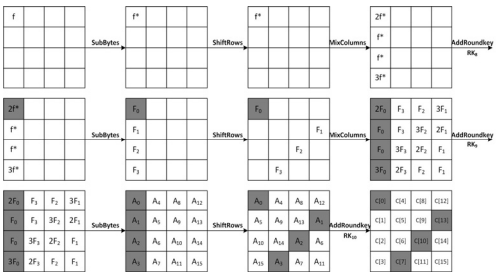

Fig. 3. Differential Characteristic of DFA on AES

먼저, 10 라운드의 32-비트 라운드 키 $RK_{10}[0,7,10,13]$을 추측한 후, 다음의 Equation (3)을 이용하여 $RK_{10}[0,7,10,13]$의 수를 2^{32}개에서 $2^8(=2^{32} \cdot 2^{-24})$개로 줄인다.

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

위의 과정을 다른 바이트에 해당되는 RK_{10}에 반복 적용하여 $2^{32}(=2^{8 \cdot 4})$개의 후보를 얻는다. 다음으로 AES-128의 키 스케줄 특성을 이용하여 RK_{10}의 후보에서 RK_9를 계산한다. 계산한 RK_9를 이용하여 (RK_9, RK_{10}) 후보에 대한 9 라운드 입력 스테이트 $S_9[0,1,2,3]$의 차분을 계산한다. 차분 패턴 $(2f^*, f^*, f^*, 3f^*)$를 체크함으로써 (RK_9, RK_{10}) 후보를 2^{32}개에서 $2^8(=2^{32} \cdot 2^{-24})$개로 줄일 수 있다.

마지막으로 각각의 2^8개 후보에 대해 키 스케줄을 이용하여 비밀키를 계산한 후, 올바른 비밀키인지 확인한다. 이와 같은 단계를 이용하면 1개의 랜덤 바이트 오류와 2^8번의 전수조사를 이용하여 128-비트 비밀키를 복구할 수 있다.

4. 대칭 SPN 블록 암호에 대한 DFA

본 절에서는 대칭 SPN 블록 암호에 대한 차분 오류 공격을 제안한다. 본 공격은 3절에서 소개한 공격을 이용하며 [16]의 결과에 따라 동일한 오류 주입 가정을 이용한다. 본 공격을 소개하기 위해 3절에서 소개한 표기법을 그대로 사용한다.

$S_8[0]$에 주입된 오류에 의해 발생한 차분 f에 의한 차분 확산 경로는 Fig. 4와 같다. 이를 이용하여 128-비트 비밀키를 복구하기 위해서는 다음과 같은 단계를 수행한다.

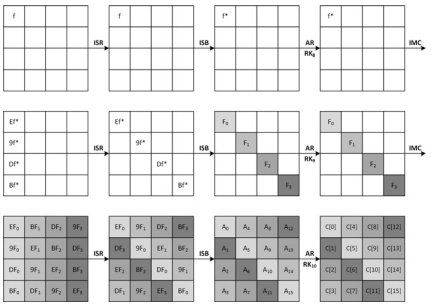

Fig. 4. DFA on Symmetric SPN Block Cipher

(1) [오류가 발생하지 않은 데이터 수집] 평문 P에 대한 암호문 C를 얻는다.

(2) [오류가 발생한 데이터 수집] 알고리즘 동작 중에 8 라운드의 입력값 $S_8[0]$에 오류 f를 주입하여 암호문 C^*를 얻는다.

(3) [$RK_{10}[0,5,10,15]$ 후보 계산] $RK_{10}[0,5,10,15]$를 추측한 후, 각각의 (C, C^*)에 대해 10 라운드에서 ISB 함수의 입력값을 계산한다. 그리고 Equation (4)와 같은 방정식을 이용하여 $RK_{10}[0,5,10,15]$의 수를 2^{32}개에서 $2^8(=2^{32} \cdot 2^{-24})$개로 줄인다.

$$\begin{aligned} EF_0 &= S(C[0] \oplus RK_{10}[0]) \oplus S(C^*[0] \oplus RK_{10}[0]) \\ 9F_0 &= S(C[5] \oplus RK_{10}[5]) \oplus S(C^*[5] \oplus RK_{10}[5]) \\ DF_0 &= S(C[10] \oplus RK_{10}[10]) \oplus S(C^*[10] \oplus RK_{10}[10]) \\ BF_0 &= S(C[15] \oplus RK_{10}[15]) \oplus S(C^*[15] \oplus RK_{10}[15]) \end{aligned} \tag{4}$$

(4) [차분 $F_{1,2,3}$과 연관 있는 바이트에 해당되는 RK_{10} 후보 계산] 나머지 96비트 라운드 키 RK_{10}에도 (3)단계와 비

슷한 방정식을 반복 적용하여 $2^{32}(=2^{8\cdot 4})$개의 후보를 얻는다.

(5) [RK_{10} 후보 필터링] 키 스케줄을 이용하여 각각의 RK_{10} 후보에 대응되는 RK_9를 계산한다. 계산된 각각의 (RK_9, RK_{10}) 후보를 이용하여 9 라운드 ISB 입력 스테이트 $S_9[0,5,10,15]$의 차분을 계산한다. 차분 패턴 $(Ef^*, 9f^*, Df^*, Bf^*)$를 체크함으로써 (RK_9, RK_{10}) 후보를 $2^8(=2^{32}\cdot 2^{-24})$개로 줄일 수 있다.

(6) [128 비트 비밀키 복구] 키 스케줄을 이용하여 각각의 2^8개 후보에 대한 비밀키를 계산한 후, 암호화를 통해 올바른 비밀키인지 확인한다.

틀린 비밀키 개수의 기댓값은 2^{-120}개로, 본 논문에서 제안하는 공격의 성공률은 매우 높다. 그러므로 본 논문에서 제안하는 방법으로 1개의 랜덤 바이트 오류 주입과 2^8번의 전수조사를 통해 대칭 SPN 블록 암호의 128-비트 비밀키를 찾을 수 있다.

5. 결 론

본 논문에서는 차분 오류 공격을 이용하여 비트 슬라이스 대합 S-박스에 의한 대칭 SPN 블록 암호에 대한 첫 번째 안전성 분석 결과를 제안하였다. 본 논문에서 제안하는 공격은 1개의 랜덤 바이트 오류 주입과 2^8번의 전수조사를 통해 본 블록 암호의 128-비트 비밀키를 복구할 수 있다. AES 구조와의 유사성 때문에 대칭 SPN 블록 암호에도 AES에 적용되었던 공격이 비슷하게 적용될 수 있을 것이라고 생각된다. 향후 차분 오류 공격 외에 다른 분석 방법을 본 블록 암호에 추가로 적용해볼 것이다.

References

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

[2] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystem," *Journal of Cryptology*, Vol.4, No.1, pp.3-72, 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*, Vol.16, No.1, pp.70-75, Feb., 2012.

[6] K. Jeong, "Differential Fault Analysis on Block Cipher Piccolo-80," *JKONI*, Vol.16, No.3, pp.510-517, Jun., 2012.

[7] K. Jeong, C. Lee, "Differential Fault Analysis on Lightweight Block Cipher LBlock," *JKONI*, Vol.16, No.5, pp.871-878, Oct., 2012.

[8] P. Dusart, G. Letourneux, and O. Vivolo, "Differential fault analysis on A.E.S," ACNS 2003, LNCS 2849, pp.293-306, Springer-Verlag, 2003.

[9] A. Moradi, M. T. Manzuri Shalmani, and M. Salmasizadeh, "A generalized method of differential fault attack against AES cryptosystem," CHES 2006, LNCS 4249, pp.91-100, Springer-Verlag, 2006.

[10] C. H. Kim, J.-J. Quisquater, "New differential fault analysis on aes key schedule: Two faults are enough," CARDIS 2008, LNCS 5189, pp.48-60, Springer-Verlag, 2008.

[11] C. Giraud, A. Thillard, "Piret and Quisquater's DFA on AES revisited," Cryptology ePrint Archive, Report 2010/440, 2010. http://eprint.iacr.org/

[12] 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.

[13] C. H. Kim, "Differential Fault Analysis against AES-192 and AES-256 with Minimal Faults," FDTC 2010, IEEE, pp.3-9, 2010.

[14] FIPS PUB 197, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," U.S. Department of Commerce, 2001.

[15] G. Cho, H. Song, "Symmetric SPN block cipher with Bit Slice involution S-box," *Journal of KIICE*, Vol.6, No.2, pp.171-179, Apr., 2011.

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

강 형 철

e-mail : kanghc@korea.ac.kr

2010년 고려대학교 산업시스템정보공학과 (학사)

현 재 고려대학교 정보보호대학원 석·박사통합과정

관심분야 : 블록 암호와 해시 함수 설계 및 분석, 인증 암호화 설계

이 창 훈

e-mail : chlee@seoultech.ac.kr

2001년 한양대학교 수학과(학사)

2003년 고려대학교(공학석사)

2008년 고려대학교(공학박사)

2009년~2011년 한신대학교 컴퓨터공학부 전임강사

2011년~2012년 한신대학교 컴퓨터공학부 조교수

현 재 서울과학기술대학교 컴퓨터공학과 조교수/한국디지털포렌식학회논문지 편집위원장

관심분야 : 정보보호, 암호학, 디지털포렌식, 융합보안