JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

기반 기술

J. Adv. Navig. Technol. 19(1): 48-52, Feb. 2015

SSB 암호 알고리즘에 대한 차분 오류 공격

Differential Fault Attack on SSB Cipher

강 형 철[1] · 이 창 훈[2*]
[1]고려대학교 정보보호대학원
[2]서울과학기술대학교 컴퓨터공학과

HyungChul Kang[1] · Changhoon Lee[2*]

[1]Graduate School of Information Security, Korea University, Seoul 136-713, Korea

[2]Department of Computer Science and Engineering, Seoul National University of Science and Technology, Seoul 139-743, Korea

[요 약]

본 논문에서는 2011년에 제안된 암호와 복호가 동일한 블록 암호 SSB에 대한 차분 오류 공격을 제안한다. 이 알고리즘은 국제 표준 블록암호를 기반으로 설계된 블록 암호로써 하드웨어 구현에서 장점을 갖게 설계되었다. 차분 오류 공격은 부채널 공격 기법 중 하나로 오류 주입 공격과 차분 공격을 결합한 것이다. SSB는 하드웨어 환경에 적합한 알고리즘이므로 차분 오류 공격에 대해 안전성을 가져야 한다. 그러나 본 논문에서 제안하는 차분 오류 공격을 이용하면, 1 개의 랜덤 바이트 오류를 주입과 2^8 의 전수조사를 통해 SSB의 128 비트 비밀키를 복구할 수 있다. 이 결과는 암호와 복호가 동일한 블록 암호 SSB의 안전성을 분석한 첫 번째 결과이다.

[Abstract]

In this paper, we propose a differential fault analysis on SSB having same structure in encryption and decryption proposed in 2011. The target algorithm was designed using advanced encryption standard and has advantage about hardware implementations. The differential fault analysis is one of side channel attacks, combination of the fault injection attacks with the differential cryptanalysis. Because SSB is suitable for hardware, it must be secure for the differential fault analysis. However, using proposed differential fault attack in this paper, we can recover the 128 bit secret key of SSB through only one random byte fault injection and an exhausted search of 2^8. This is the first cryptanalytic result on SSB having same structure in encryption and decryption.

Key word : Block cipher, Differential fault analysis, SSB, Same structure in encryption and decryption.

http://dx.doi.org/10.12673/jant.2015.19.1.48

Received 8 December 2014; **Revised** 26 January 2015
Accepted (Publication) 23 February 2015 (28 February 2015)

***Corresponding Author; Changhoon Lee**

Tel: +82-2-970-6712
E-mail: chlee@seoultech.ac.kr

Ⅰ. 서 론

1997년 Biham과 Shamir가 최초로 제안한 차분 오류 공격 (DFA; differential fault attack)은 부채널 공격 기법 중 하나이다 [1]. 이 공격은 오류 주입 공격 (fault injection attack)[2]과 차분 공격 (differential cryptanalysis)[3]를 결합한 것으로 DES (data encryption standard)[1] 뿐만 아니라 AES (advanced encryption standard)[4]-[8], SEED[9], LED[10], Piccolo[11], LBlock[12] 등 다양한 블록 암호 알고리즘을 분석하는데 적용되었다. 이는 DFA가 블록 암호 알고리즘의 안전성을 분석하는데 고려되어져야할 중요한 공격 방법이라는 것을 의미한다.

2011년에 제안된 암호와 복호가 동일한 블록 암호 SSB (symmetric SPN block cipher)[13]는 AES[14]에 기반을 둔 128 비트 블록 암호 알고리즘이며 128/192/256 비트 비밀키를 사용한다. S-박스와 S^{-1}-박스, 두 종류를 사용하고 복호화 키를 생성할 때 선형 변환 함수를 사용하여 암호와 복호를 동일하게 구성하였다. 암호와 복호가 동일하므로 블록 암호 SSB는 하드웨어 구현에서 AES에 비해 면적이 절반으로 감소한다는 장점이 있다.

DFA가 하드웨어 환경에서 적용 가능한 공격이며 블록 암호 SSB가 제한적 하드웨어 환경에서 장점을 가지게 설계되었으므로 이 블록 암호의 DFA에 대한 안전성 분석은 반드시 고려되어야한다.

본 논문에서는 2011년 한국해양정보통신학회논문지에서 제안된 암호와 복호가 동일한 블록 암호 SSB에 대한 차분 오류 공격을 제안한다. 본 논문에서 제안하는 공격 방법은 [8]에서 제안된 공격 아이디어를 이용하였다. [8]에서는 128 비트 비밀키를 사용하는 AES에 대한 DFA가 제안되었다. 먼저, AES의 8 라운드에 1 개의 랜덤 바이트 오류를 주입하여 9 라운드에서 발생하는 차분 특성을 분석한다. 그리고 10 라운드 키를 추측하여 9 라운드에서 발생하는 차분 특성과 비교하여 라운드 키 후보를 찾는다. 찾은 라운드 키 후보와 키스케쥴을 특성을 이용하여 128 비트 비밀키를 복구한다. 본 논문에서는 블록 암호 SSB에 [8]에서 제안하는 공격 방법을 적용한다. 8 라운드에 1 개의 랜덤 바이트 오류를 주입하여 2^8 개의 10 라운드 키 후보를 찾는다. 그리고 2^8의 전수조사를 통해 128 비트 비밀키를 복구한다. 이 공격 결과는 암호와 복호가 동일한 블록 암호 SSB에 대한 첫 번째 안전성 분석 결과이다.

본 논문은 다음과 같이 구성된다. 먼저, 2장에서 블록 암호 SSB를 간략히 소개하고, 3장에서는 차분 오류 공격을 소개한다. 4장에서는 [8]에서 제안된 공격 방법을 이용하여 블록 암호 SSB에 대한 차분 오류 공격을 제안한다. 마지막으로 5장에서 결론을 맺는다.

Ⅱ. 암호와 복호가 동일한 블록 암호 SSB

암호와 복호가 동일한 블록 암호 SSB(이하 SSB)는 128 비트 블록 암호이며 블록 암호 AES에 기반을 두어 설계되었다. SSB

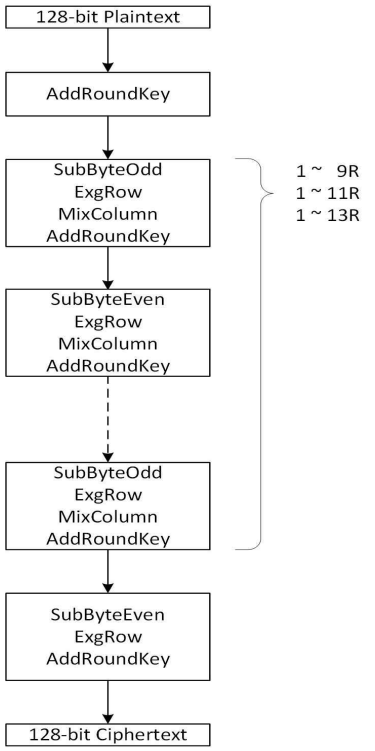

그림 1. 블록 암호 SSB의 전체 구조
Fig. 1. Full structure of block cipher SSB.

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]

그림 2. 16 바이트 상태
Fig. 2. 16 bytes state.

는 128/192/256 비트 비밀키를 사용하며, 그림 1과 같이 비밀키의 사이즈에 따라 각각 10/12/14 라운드로 구성한다. 홀수 라운드와 짝수 라운드에서 서로 다른 SubByte 함수를 적용하여 암호와 복호가 동일하게 구성하였다.

각 라운드는 키 덧셈 함수 (AddRoundKey), 비선형 바이트 치환 함수 (SubByteOdd, SubByteEven), 바이트 교환 함수 (ExgRow) 및 선형 변환 함수 (MixColumn)의 네 가지 내부 함수로 구성한다. 내부 함수는 그림 2와 같이 16 개의 바이트로 구성된 4×4 정방 행렬인 스테이트(state) 단위로 수행한다. 본 논문에서는 특정 스테이트 S의 i 번째 바이트 값을 $S[i]$로 표기하며 특정 라운드(r)의 스테이트 S 의 i 번째 바이트 값을 $S_r[i]$ 로 표기하기로 한다($i=0,1,\cdots,15$).

SSB의 내부 함수는 다음과 같은 함수들이 사용된다.

o AddRoundKey(AR): 키스케쥴에 의해 비밀키로부터 생성된 라운드 키와 스테이트의 바이트 별 XOR 연산으로 이루

어진다.

o SubByteOdd(SBO): 홀수 라운드에서 8 비트 S-박스를 이용한 비선형 바이트 치환 함수이다. S-박스와 S^{-1}-박스를 번갈아가며 사용한다.

o SubByteEven(SBE): 짝수 라운드에서 8 비트 S-박스를 이용한 비선형 바이트 치환 함수이다. S^{-1}-박스와 S-박스를 번갈아가며 사용한다.

o ExgRow(ER): 스테이트 각각의 행에 대한 바이트 별 순환 이동 변환으로 아래와 같다.

- $S[0,4,8,12] \rightarrow S[0,4,8,12]$
- $S[1,5,9,13] \rightarrow S[5,1,13,9]$
- $S[2,6,10,14] \rightarrow S[14,10,6,2]$
- $S[3,7,11,15] \rightarrow S[11,15,3,7]$

o MixColumn(MC): 스테이트 각각의 열을 변환 시키는 4×4 행렬로 $GF(2^8)$ 상에서 연산된다(식 (1) 참고).

$$\begin{bmatrix} S'[i] \\ S'[i+1] \\ S'[i+2] \\ S'[i+3] \end{bmatrix} = \begin{bmatrix} 0x1b & 0x1c & 0x14 & 0x12 \\ 0x1c & 0x1b & 0x12 & 0x14 \\ 0x14 & 0x12 & 0x1b & 0x1c \\ 0x12 & 0x14 & 0x1c & 0x1b \end{bmatrix} \cdot \begin{bmatrix} S[i] \\ S[i+1] \\ S[i+2] \\ S[i+3] \end{bmatrix} \quad (1)$$

Ⅲ. 차분 오류 공격

본 장에서는 AES에 수행되었던 다양한 공격 중 하나인 차분 오류 공격에 대해 간략히 소개한다. 차분 오류 공격은 부채널 공격 기법 중 하나로, 차분 공격과 오류 주입 공격을 하나로 합친 기법이다. 즉, 특정 위치에 오류를 주입하고, 이 주입된 오류로 인해 발생한 차이를 이용하여 비밀키를 복구하는 공격이다.

지금까지 AES에 대한 다양한 차분 오류 공격이 제안되었다[4]-[8]. 이 중에서 [8]에서 제안된 공격 방법이 오류 하나만을 사용하여 AES 128 비트 비밀키를 복구하므로 가장 강력하다고 말할 수 있다. 이 공격의 오류 주입 가정은 랜덤 바이트 오류 주입 모델에 기반을 둔다.

[8]에서 제안하는 AES에 대한 차분 오류 공격은 그림 3과 같이 8 라운드에 오류를 주입한다. 먼저 평문에 대한 올바른 암호문을 얻는다. 그리고 다시 동일한 평문에 대해 암호화를 동작 시키고 동작 중, 8 라운드에 오류를 주입한다. 이때, 랜덤 바이트 오류 주입 모델에 의하여 16 바이트 중 임의의 한 바이트에 임의의 오류가 주입되고 잘못된 암호문(Ciphertext*)을 얻는다. 이렇게 얻어진 올바른 암호문과 잘못된 암호문을 이용하여 차분 공격을 수행할 수 있다. 즉, 마지막 라운드 키를 추측하여 9 라운드에서 발생하는 차분 특성과 비교하여 라운드 키를 복구하는 것이다.

[8]에서 제안하는 차분 오류 공격을 수행하기 위해서는 공격자가 원하는 차분 특성을 얻어야 한다. 원하는 차분 특성을 얻기 위해서는 원하는 위치에 정확히 오류가 주입되어야 하므로 수번의 오류 주입을 수행해야한다.

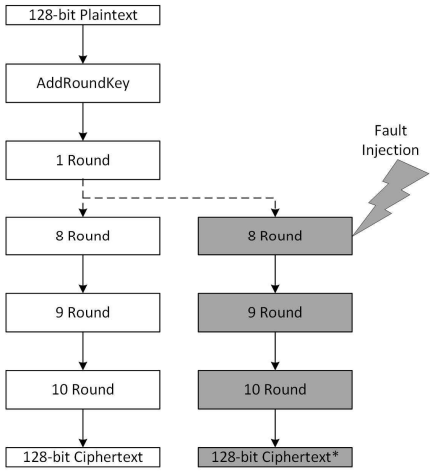

그림 3. AES에 대한 차분 오류 공격 시나리오
Fig. 3. Scenario of DFA on AES.

하지만 2009년 FDTC에서 Fukunaga 등은 AES의 특정 라운드에서 원하는 위치에 정확히 오류를 주입하는 것이 가능하다고 소개하였다[15]. 따라서 공격자는 AES의 동작 중에 8 라운드의 원하는 위치에 정확히 오류를 주입할 수 있다. 이와 같은 방법을 이용하면 공격자는 1 개의 랜덤 바이트 오류 주입으로 128 비트 비밀키를 복구할 수 있다.

Ⅳ. SSB에 대한 차분 오류 공격

본 장에서는 암호와 복호가 동일한 블록 암호 SSB에 대한 차분 오류 공격을 제안한다. 본 공격은 3장에서 소개한 공격을 이용하며 [15]의 결과에 따라 동일한 오류 주입 가정을 이용한다. 본 논문에서는 다음과 같은 표기법을 사용한다[16].

o $C[i]$: 오류가 주입되지 않은 암호문의 i 번째 바이트
o $C^*[i]$: 오류가 주입되어 얻은 암호문의 i 번째 바이트
o RK_r: r 라운드의 라운드 키
o $RK_r[i]$: r 라운드의 라운드 키의 i 번째 바이트($0 \le i \le 10$)
o f: 오류가 주입되어 발생한 차분
o f^*, F_j, A_l: 주입된 오류가 S-박스를 통과하여 변경된 차분 ($0 \le j \le 3, 0 \le l \le 15$)

본 공격에서는 8 라운드의 $S_8[0]$에 각각 랜덤 바이트 오류 f를 주입하여 128 비트 비밀키를 복구한다. $S_8[0]$에 주입된 오류에 의한 차분 f에 의한 차분 확산 경로는 그림 4와 같다. 이를 이용하여 128 비트 비밀키를 복구하기 위해서는 다음과 같은 단계를 수행한다.

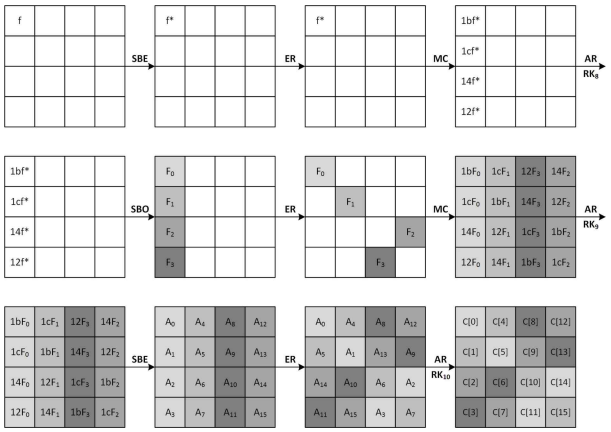

그림 4. SSB에 대한 DFA의 차분 특성
Fig. 4. Differential characteristic of DFA on SSB.

(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) [$RK_{10}[0,5,11,14]$ 후보 계산] $RK_{10}[0,5,11,14]$를 추측한 후, 각각의 (C, C^*)에 대해 10 라운드에서 SBE 함수의 입력값을 계산한다. 그리고 다음과 같은 방정식을 이용하여 $RK_{10}[0,5,11,14]$의 수를 2^{32} 개에서 $2^8 (= 2^{32} \cdot 2^{-24})$ 개로 줄인다.

$$
\begin{aligned}
1bF_0 &= S^{-1}(C[0] \oplus RK_{10}[0]) \oplus S^{-1}(C^*[0] \oplus RK_{10}[0]) \\
1cF_0 &= S(C[5] \oplus RK_{10}[5]) \oplus S(C^*[5] \oplus RK_{10}[5]) \\
14F_0 &= S^{-1}(C[14] \oplus RK_{10}[14]) \oplus S^{-1}(C^*[14] \oplus RK_{10}[14]) \\
12F_0 &= S(C[11] \oplus RK_{10}[11]) \oplus S(C^*[11] \oplus RK_{10}[11])
\end{aligned} \tag{3}
$$

(4) [나머지 바이트에 해당되는 RK_{10} 후보 계산] 나머지 96 비트 $RK_{10}[1,4,10,15]$, $RK_{10}[3,6,8,13]$, $RK_{10}[2,7,9,12]$에도 단계 (3)을 반복 적용하여 총 $2^{32} (= 2^{8 \cdot 4})$ 개의 후보를 얻는다.

(5) [RK_{10} 후보 필터링] 각각의 RK_{10} 후보에 대응되는 RK_9를 계산한다. 각각의 (RK_9, RK_{10}) 후보를 이용하여 9 라운드 입력 스테이트 $S_9[0,1,2,3]$의 차분을 계산한다. 차분 패턴$(1bf^*, 1cf^*, 14f^*, 12f^*)$를 체크함으로써 (RK_9, RK_{10}) 후보를 $2^8 (= 2^{32} \cdot 2^{-24})$ 개로 줄일 수 있다.

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

틀린 비밀키가 단계 (6)을 통과할 확률은 2^{-128}이다. 따라서 단계 (6)을 통과하는 틀린 비밀키 후보 개수의 기댓값은 $2^{-120} (= 2^8 \cdot 2^{-128})$ 개다. 이는 본 논문에서 제안하는 공격을 통해 찾은 비밀키는 옳은 비밀키일 확률이 매우 높다는 것을 의미한다. 그러므로 본 논문에서 제안하는 공격은 1개의 랜덤 바이트 오류를 주입하고 2^8의 전수조사를 하면 높은 확률로 암호와 복호가 동일한 블록 암호 SSB의 128 비트 비밀키를 복구할 수 있다.

Ⅴ. 결 론

본 논문에서는 차분 오류 공격 알고리즘을 제안하고, 암호와 복호가 동일한 블록 암호 SSB의 안전성을 분석하였다. 본 논문에서 제안하는 공격은 1개의 랜덤 바이트 오류 주입과 2^8의 전수조사를 통해 SSB의 128 비트 비밀키를 복구할 수 있다. SSB는 AES의 구조와 매우 유사하기 때문에 AES에 적용되었던 공격이 동일하게 적용될 수 있었다. 향후 DFA 외에 AES에 치명적인 결과를 보인 분석 방법을 SSB에 추가로 적용할 것이다.

감사의 글

이 연구는 서울과학기술대학교 교내 학술연구비 지원으로 수행되었습니다.(2014-0381)

참고 문헌

[1] E. Biham and A. Shamir, “Differential fault analysis of secret key cryptosystems,” in *Proceeding of Crypto `97*, Santa Barbara: CA, pp. 513-525, 1997.

[2] D. Boneh, R. DeMillo and R. Lipton, “On the importance of checking cryptographic protocols for faults,” in *Proceeding of Eurocrypt `97*, Konstanz: Germany, pp. 37-51, 1997.

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

[4] P. Dusart, G. Letourneux, and O. Vivolo, “Differential fault analysis on A.E.S,” Cryptology ePrint Archive, Report 2003/010, 2003, Available: http://eprint.iacr.org/.

[5] A. Moradi, M. T. Manzuri Shalmani, and M. Salmasizadeh, “A generalized method of differential fault attack against AES cryptosystem,” in *Proceeding of the 8th Workshop on Cryptographic Hardware and Embedded Systems*, Yokohama: Japan, pp. 91-100, 2006.

[6] C. H. Kim and J.-J. Quisquater, “New differential fault analysis on aes key schedule: two faults are enough,” in *Proceeding of the 8th Conference on Smart Card Research and Advanced Applications*, London: UK, pp. 48-60, 2008.

[7] C. Giraud and A. Thillard, “Piret and quisquater’s DFA on AES revisited”, Cryptology ePrint Archive, Report 2010/440, 2010, [Internet]. Available: http://eprint.iacr.org/.

[8] M. Tunstall, D. Mukhopadhyay and S. Ali, “Differential fault analysis of the advanced encryption standard using a single fault,” in *Proceeding of the 5th International Conference on Information Security Theory and Practice*, Heraklion, Crete: Greece, pp. 224-233, 2011.

[9] K. Jeong, Y. Lee, J. Sung and S. Hong, “Differential fault analysis on block cipher SEED”, *Mathematical and Computer Modelling*, Vol. 55, Issues 1-2, pp. 26-34, Jan. 2012.

[10] K. Jeong, “Security analysis of block cipher LED-64 suitable for wireless sensor network environments,” *Journal of the Korea Navigation Institute*, Vol. 16, No. 1, pp. 70-75, Feb. 2012.

[11] K. Jeong, “Differential fault analysis on block cipher Piccolo-80,” *Journal of the Korea Navigation Institute*, Vol. 16, No. 3, pp. 510-517, June 2012.

[12] K. Jeong and C. Lee, “Differential fault analysis on lightweight block cipher LBlock,” *Journal of the Korea Navigation Institute*, Vol. 16, No. 5, pp. 871-878, Oct. 2012.

[13] G. Kim, “SPN block cipher SSB having same structure in encryption and decryption,” *Journal of the Korea Institute of Maritime Information and Communication Sciences*, Vol. 15, No. 4, pp. 860-868, Apr. 2011.

[14] NIST: Announcing the advanced encryption standard (AES), Nationtal Institute of Standards and Technology, Washington D.C., Federal Information Processing Standards Publication 197, 2001.

[15] T. Fukunaga and J. Takahashi, “Practical fault attack on a cryptographic LSI with ISO/IEC 18033-3 block ciphers,” in *Proceeding of the 6th Workshop on Fault Diagnosis and Tolerance in Cryptography*, Lausanne: Switzerland, pp. 84-92, 2009.

[16] C. Lee, “Differential fault analysis on symmetry structured SPN block cipher,” *Journal of Advanced Navigation Technology*, Vol. 17, No. 5, pp. 568-573, Oct. 2013.

강 형 철 (HyungChul Kang)
2010년 2월 : 고려대학교 산업시스템정보공학과 (공학사)
2010년 3월 ~ 현재 : 고려대학교 정보보호대학원 석박사통합과정
※ 관심분야 : 블록 암호와 해쉬 함수 설계 및 분석, 인증 암호화 설계

이 창 훈 (Changhoon Lee)
2001년 2월 : 한양대학교 수학과 (이학사)
2008년 2월 : 고려대학교 정보보호대학원 (공학박사)
2011년 3월 ~ 2012년 2월 : 한신대학교 컴퓨터공학부 조교수
2012년 3월 ~ 현재 : 서울과학기술대학교 컴퓨터공학과 조교수
※ 관심분야 : 정보보호, 암호학, 디지털포렌식, 융합보안
2003년 2월 : 고려대학교 정보보호대학원 (공학석사)
2009년 3월 ~ 2011년 2월 : 한신대학교 컴퓨터공학부 전임강사