情報保護學會論文誌
第15券 第3號, 2005. 6

6 라운드 AES에 대한 향상된 불능 차분 공격*

김 종 성,[1†] 홍 석 희,[1] 이 상 진,[1] 은 희 천[2‡]
[1]고려대학교 정보보호기술연구센터(CIST), [2]고려대학교 자연과학대학 정보수학과

Improved Impossible Differential Attacks on 6-round AES*

Jongsung Kim,[1†] Seokhie Hong,[1] Sangjin Lee,[1] Hichun Eun[2‡]
[1]CIST, Korea University, [2]Information Mathematics, Korea University

요 약

미 연방 표준 블록 암호 AES에 대한 불능 차분 공격은 $2^{91.5}$개의 선택 평문과 2^{122}번의 암호화 과정을 요구하는 6 라운드 공격이 제시되었다[4]. 본 논문에서는 AES에 대한 여러 가지 4 라운드 불능 차분 특성을 소개하고, 이를 이용하여 6 라운드 AES에 대한 향상된 불능 차분 공격을 제시한다. 향상된 6 라운드 불능 차분 공격은 $2^{83.4}$개의 선택 평문과 $2^{105.4}$번의 암호화 과정으로 첫 번째와 마지막 라운드 키의 11 바이트를 찾는다.

ABSTRACT

Impossible differential attacks on AES have been proposed up to 6-round which requires $2^{91.5}$ chosen plaintexts and 2^{122} 6-round AES encryptions. In this paper, we introduce various 4-round impossible differentials and using them, we propose improved impossible differential attacks on 6-round AES. The current attacks require $2^{83.4}$ chosen plaintexts and $2^{105.4}$ 6-round AES encryptions to retrieve 11 bytes of the first and the last round keys.

Keywords : *Block Ciphers, AES, Impossible Differentials, Impossible Differential Attack*

Ⅰ. 서 론

미연방 표준 블록 암호 AES는 입출력 크기가 128 비트인 블록 암호로 128, 192 또는 256 비트의 키를 사용하며, 각각의 키 길이에 따라 10, 12 또는 14 라운드를 사용한다. 한 라운드는 SPN 구조로 비선형층으로는 ByteSub 함수를, 선형층으로 ShiftRow, MixColumn,AddRoundKey 함수를 사용하며, 첫 번째 라운드 전에 AddRoundKey 함수를 적용하고, 마지막 라운드에서 MixColumn 함수를 생략한다. 본 논문에서는 128 비트 키를 사용하는 AES의 안전성 분석에 초점을 맞춘다 (이하 128 비트 키를 사용하는 AES를 AES-128로 표기한다).

현재까지 알려진 AES-128에 대한 공격으로는 포화 공격[5], 불능 차분 공격[3,4]과 부분 합 공격[6]이 있다. AES-128에 대한 포화 공격과 부분 합 공격을 이용한 6, 7 라운드 공격이, 불능 차분 공격을 이용한 5, 6 라운드 공격이 제시되었다. 자세한 공격 복잡도는 표 1에 나타나 있다. AES-128에 대한

접수일 : 2005년 3월 7일 ; 채택일 : 2005년 6월 7일
* 본 연구는 고려대학교 특별연구비에 의하여 수행 되었습니다.
† 주저자 : joshep@cist.korea.ac.kr
‡ 교신저자 : hceun@korea.ac.kr

이들 공격은 4 바이트로 구성된 각 열에 대한 Mix-Column 함수의 최대 확산 성질을 이용하였다. 즉, 0이 아닌 입력 바이트 수가 $n(0<n\leq 4)$일 때 Mix-Column 함수를 거친 후의 0이 아닌 출력 바이트 수가 최소 5-n이라는 사실을 이용하였다.

본 논문에서는 AES-128에 대한 새로운 여러 불능 차분 특성을 소개하고, 이를 이용한 6 라운드 불능 차분 공격을 소개한다. 본 논문에서 소개하는 6 라운드 AES-128에 대한 불능 차분 공격 또한 MixColumn 함수에 대한 위의 성질을 이용한다. 본 논문의 AES-128에 대한 불능 차분 공격은 포화 공격, 부분 합 공격보다 효율적이지는 못하지만, 기존 6 라운드 불능 차분 공격에서 요구하는 공격 복잡도를 현저히 낮출 수 있다. 이는 AES-128의 6 라운드에 대한 불능 차분 공격에 대한 안전성이 기존의 예상보다 낮음을 의미한다. AES-128의 기존 분석 결과와 본 논문의 결과를 요약하면 표 1과 같다. 표 1에서 데이터 복잡도는 필요한 선택 평문 수를 시간 복잡도는 AES-128의 공격 라운드에 대한 암호화 과정을 단위로 한다.

표 1. AES-128에 대한 공격 결과

공격 방법	라운드 수	데이터 복잡도	시간 복잡도
포화[5]	6	2^{32}	2^{72}
부분합[6]	6	$6\cdot 2^{32}$	2^{44}
부분합[6]	7	$2^{128}-2^{119}$	2^{120}
불능 차분[3]	5	$2^{29.5}$	2^{31}
불능 차분[4]	6	$2^{91.5}$	2^{122}
불능 차분(본 논문)	6	$2^{83.4}$	$2^{105.4}$

Ⅱ. AES-128 알고리즘의 소개

AES-128은 입출력 크기가 128 비트인 블록 암호로 128 비트 키를 사용하며, 10 라운드로 구성되었다. AES-128의 암호화 과정 상의 128 비트 상태 값은 그림 1와 같이 16개 바이트로 이루어진 4X4 행렬로 나타낼 수 있다. AES-128의 한 라운드는 ByteSub(BS), ShiftRow(SR), MixColumn(MC), AddRoundKey(ARK) 함수를 차례대로 사용하며, 첫 번째 라운드 전에 ARK 함수를 적용하고, 마지막 라운드에서 MC 함수를 생략한다. 각 함수는 다음과 같이 동작한다.

- BS 함수는 각각의 바이트에 동일한 비선형 S-박스를 적용한다.
- SR 함수는 행 0,1,2,3을 왼쪽으로 각각 0,1,2,3 바이트 순환 이동 시킨다.
- MC 함수는 선형 변환으로 4 바이트로 구성된 각 열을 변환시키는 4X4 행렬로 $GF(2^8)$ 위에서 연산한다.
- ARK 함수는 키와 상태값의 비트별 합(exor) 연산을 수행한다.

본 논문에서 다루는 불능 차분 공격은 AES-128의 키 스케줄 동작 과정과는 무관하게 적용되므로, AES-128에 대한 키 스케줄의 설명은 생략한다.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

그림 1. AES-128의 16 바이트 상태 값

Ⅲ. AES-128에 대한 불능 차분 특성

본 절에서는 AES-128에 대한 여러 가지 4 라운드 불능 차분 특성을 살펴본다. 본 절에서 다루는 불능 차분 특성은 마지막 라운드의 MC 함수와 ARK 함수를 생략한 4 라운드 불능 차분 특성을 의미한다.

앞서 언급한 것과 같이 MC 함수는 다음과 같은 성질을 갖고 있다. 0이 아닌 입력 바이트 수가 $n(0<n\leq 4)$일 때 MC 함수를 거친 후의 0이 아닌 출력 바이트 수가 최소 5-n이 된다. 이 사실을 이용하여 2 라운드 AES-128에 대한 다음의 세 가지 차분 특성을 얻을 수 있다.

- 만약 주어진 입력쌍이 한 바이트만 다르면, 2 라운드 암호화 후의 출력쌍은 16개 모든 바이트가 서로 다르다.
- 만약 주어진 입력쌍이 두 바이트만 다르면, 2 라운드 암호화 후의 출력쌍은 최소 12개의 바이트가 서로 다르다.
- 만약 주어진 입력쌍이 세 바이트만 다르면, 2 라운드 암호화 후의 출력쌍은 최소 8개의 바이

트가 서로 다르다.

첫 번째 라운드의 MC 함수와 ARK 함수를 생략한 2 라운드 복호화 과정에 대해서도 위와 비슷한 결과를 얻을 수 있다. (1,8,11,14) 바이트를 A1 워드, (2,5,12,15) 바이트를 A2 워드, (3,6,9,16) 바이트를 A3 워드, (4,7,10,13) 바이트 를 A4 워드라 표기하자.

- 만약 주어진 입력쌍 A1, A2, A3, A4 중 적어도 하나의 워드가 같다면, 2 라운드 복호화 후의 출력 쌍은 최대 12개의 바이트가 서로 다르다.
- 만약 주어진 입력쌍 A1, A2, A3, A4 중 적어도 두개의 워드가 같다면, 2 라운드 복호화 후의 출력 쌍은 최대 8개의 바이트가 서로 다르다.
- 만약 주어진 입력쌍 A1, A2, A3, A4 중 적어도 세 개의 워드가 같다면, 2 라운드 복호화 후의 출력쌍은 최대 4개의 바이트가 서로 다르다.

위의 6가지 2 라운드 차분 특성을 이용하여, 4 라운드 AES-128 불능 차분 특성을 다음과 같이 유도할 수 있다.

성질 1. 만약 주어진 입력쌍이 하나의 바이트를 제외한 나머지 15개 바이트가 모두 같다면, 4 라운드 암호화 후의 출력 쌍은 A1, A2, A3, A4 중 적어도 한 개의 워드가 다르다[3].

성질 2. 만약 주어진 입력쌍이 두개의 바이트를 제외한 나머지 14개 바이트가 모두 같다면, 4 라운드 암호화 후의 출력 쌍은 A1, A2, A3, A4 중 적어도 두 개의 워드가 다르다.

성질 3. 만약 주어진 입력쌍이 세 개의 바이트를 제외한 나머지 13개 바이트가 모두 같다면, 4 라운드 암호화 후의 출력 쌍은 A1, A2, A3, A4 중 적어도 세 개의 워드가 다르다.

Ⅳ. AES-128에 대한 불능 차분 공격

본 절에서는 Ⅲ 절의 성질 1에 제시된 불능 차분 특성을 이용하여 AES-128에 대한 기존의 6 라운드 불능 차분 공격을 향상시킨다. 본 절에서 소개하는 AES-128에 대한 불능 차분 공격은 4 라운드의 불능 차분 특성을 이용하여 시작과 끝에 각각 한 라운드를 더하여 6 라운드를 공격한다. 이 공격은 마지막 라운드의 MC 함수를 생략한 6 라운드 AES-128에 대한 공격이며, 다음의 순서를 따른다 (그림 2 참고).

1. 하나의 structure를 (1,6,11,16)의 네 개의 바이트를 제외한 모든 바이트가 고정된 값을 갖는 평문들의 집합으로 정의하자. 그러면 하나의 structure는 2^{32}개의 평문과 $2^{32}\cdot(2^{32}-1)\cdot(1/2)\approx 2^{63}$개의 평문 쌍으로 이루어져 있다.
2. 고정된 값을 변화시켜 $2^{51.4}$개의 structure를 구성하자. $2^{51.4}$개의 structure는 $2^{83.4}$개의 평문과 $2^{114.4}$개의 평문 쌍으로 이루어져 있다. 그리고 각 structure의 평문을 암호화하여 각 structure의 암호문 쌍이 (3,4,6,7,9,10, 13,15,16)의 9개 바이트에서 0 차분을 갖는 평문 쌍을 고르자. 이와 같은 평문 쌍의 개수에 대한 기대치는 $2^{114.4}\cdot 2^{-72}=2^{42.4}$이다. (본 알고리즘은 제시된 structure의 개수보다 적은 양으로 수행할 수 있지만, 본 알고리즘의 성공 확률을 충분히 높이기 위해 $2^{51.4}$개의 structure를 사용한다.)
3. (1,2,5,8,11,12,14)의 위치에 해당하는 마지막 라운드 키 K_6의 7개 바이트를 추측하자.
4. 단계 2를 통과한 각 평문 쌍에 대응하는 암호문 쌍 (C, C*)에 대하여, C_5 ($=BS^{-1}\circ SR^{-1}(C\oplus K_6)$)와 $C_5^*=BS^{-1}\circ SR^{-1}(C^*\oplus K_6)$)의 첫 번째 열과 두 번째 열의 값을 계산한다. 단 C_5, C_5^*의 14번째 바이트 값은 계산하지 않는다. (그림 2 참조) $C_5\oplus C_5^*$의 첫 번째 열과 두 번째 열의 MC^{-1}값을 계산하고, 계산된 값이 (1,14), (2,5), (6,9), 또는 (10, 13) 위치에서 차분이 0이 되는 평문쌍을 고르자. (주의: C_5와 C_5^*의 값이 아닌 차분을 고려하므로 K_5^{-1}에 대한 계산은 무시할 수 있다). 각 평문 쌍에 대하여 이렇게 될 확률이 $p=2^{-16}\cdot 4=2^{-14}$이므로, 이 단계를 통과할 평문 쌍의 개수에 대한 기대치는 $2^{42.4}\cdot 2^{-14}=2^{28.4}$이다.
5. 단계 4를 통과한 평문 쌍 (P, P*)과 (1,6,11 ,16) 위치에 해당되는 첫 라운드 키 K_0 의 4 바이트 키 후보에 대하여 첫 번째 열 위치에서 $MC\circ SR(BS(P\oplus K_0)\oplus BS(P^*\oplus K_0))$를 계산하고, 이들 중 오직 하나의 바이트를 제외한 모든 바이트에서 0 차분을 가지는 쌍을 고르자. MC는 일대일 대응 함수이기 때문에 위

의 경우가 일어날 확률은 약 $q=2^{-24}\cdot 4=2^{-22}$ 이다.

6. 단계 5를 통과하는 평문 쌍이 존재한다면, 추측한 (K_6, K_0)의 부분키를 올바른 키 후보에서 제거하자. 만약 추측한 K_0에 대해 단계 5를 통과하는 평문 쌍이 존재하지 않는다면, 단계 3에서 추측한 K_6과 함께 올바른 키로 출력하고, 그렇지 않다면 단계 3으로 돌아가자.

성질 1에 의하여 단계 4와 단계 5를 만족하는 차분 특성은 나타날 수 없으므로, 단계 4와 단계5를 통과하는 모든 키는 잘못된 키이다. 단계 4를 통과한 $2^{28.4}$개의 평문 쌍에 대해 단계 5를 통과할 키의 평균 개수는 $2^{32}\cdot(1-2^{-22})^{2^{28.4}}\approx 2^{32}\cdot e^{-2^{6.4}}\approx 2^{-89.8}$ 이다. 따라서 추측한 K_6의 7개 바이트 각각에 대해서 약 $2^{-89.8}$개의 K_0 키 후보가 남으므로, 단계 3-5을 반복 적용한다면, (K_6, K_0)의 남아 있는 키의 개수에 대한 기대값은 $2^{-89.8}\cdot 2^{56}=2^{-33.8}$이 된다. 그리고 옳은 키는 단계 3-5를 통과하지 못하므로 출력되는 키 쌍은 높은 확률로 올바른 키 쌍이 될 것이다.

본 알고리즘의 시간 복잡도를 살펴보면 단계 4에서는 $2\cdot 2^{42.4}\cdot 2^{56}\cdot(1/6)\cdot(2/4)\cdot(1/2)=2^{94.8}$의 6 라운드 AES-128 암호화 과정이 필요하며, 단계 5에서는

$$2^{56}\cdot 2\cdot(1/6)\cdot(1/4)\cdot 2^{32}\cdot(1+(1-2^{-22})+(1-2^{-22})^2+\cdots+(1-2^{-22})^{2^{28.4}})\approx 2^{105.4}$$

의 6 라운드 AES-128 암호화 과정을 요구한다. 여기서, 1/6는 6 라운드 중 한 라운드의 암호화 과정을 2/4와 1/4은 네개 열 중에서 두개 열, 한개 열의 암호화 과정을 각각 나타낸 것이며, 1/2는 공격 알고리즘이 출력하기까지의 평균 확률을 의미한다. 따라서, 본 공격 알고리즘은 $2^{83.4}$개의 선택 평문과 $2^{105.4}$번의 6 라운드 AES-128 암호화 과정을 요구한다.

3 장에서 제시한 성질 2, 3의 4 라운드 불능 차분 특성을 이용하여도, 6 라운드 AES-128을 공격할 수 있다. 하지만, 성질 1의 4 라운드 불능 차분을 이용하는 것이 성질 2, 3의 불능 차분을 이용하는 것보다 더 효율적으로 적용되므로, 성질 2, 3을 이용한 6 라운드 AES-128 공격 과정에 대한 설명은 생략한다.

V. 결 론

본 논문에서는 기존에 제시된 4 라운드 AES-128에 대한 불능 차분 특성을 확장하였으며, 4 라운드 불능 차분 특성을 이용하는 기존의 6 라운드 AES-128에 대한 불능 차분 공격 보다 더 효율적인 공격 알고리즘을 제시하였다. 본 논문의 결과에 의하면, 6 라운드 AES-128은 불능 차분 공격에 의해 $2^{83.4}$개의 선택 평문과 $2^{105.4}$번의 6 라운드 AES-128 암호화 과정으로 공격될 수 있다. 이는 AES-128의 6 라운드에 대한 불능 차분 공격에 대한 안전성이 기존의 예상보다 낮음을 의미한다.

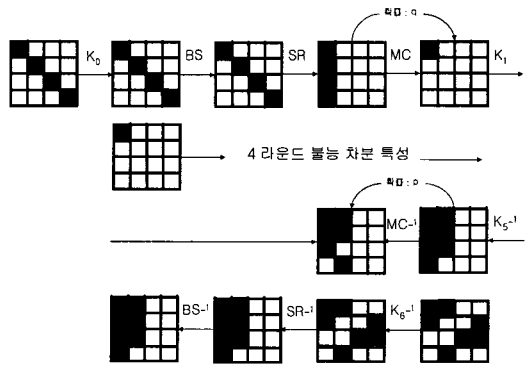


그림 2. AES-128에 대한 6 라운드 불능 차분 공격

참 고 문 헌

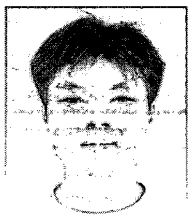
[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like Cryptosystems," *Advances in Cryptology - CRYPTO'90*, LNCS 537, pp. 2-21, Springer-Verlag, 1990.

[2] E. Biham, A. Biryukov and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," *Advances in Cryptology - EUROCRYPT'99*, LNCS 1592, pp. 12-23, Springer-Verlag, 1999.

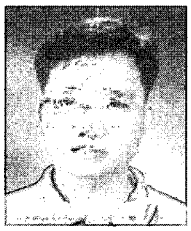
[3] E. Biham, and N. Keller, "Cryptanalysis of Reduced Variants of Rijndael," http://csrc.nist.gov/encryption/aes/

round2/conf3/aes3paper.html
[4] J.H. Cheon, M.J. Kim, K. Kim, J.Y. Lee, and S.W. Kang, "Improved Impossible Differential Cryptanalysis of Rijndael and Crypton," *ICISC 2001*, LNCS, Springer-Verlag, 2001.
[5] J. Daemen, and V. Rijmen, "AES Proposal : Rijndael," http://csrc.nist.gov/encryption/aes/rijndael/ http://csrc.nist.gov/encryption/aes/round2/conf3/aes3paper.html
[6] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved Cryptanalysis of Rijndael," *FSE 2000*, LNCS 1978, pp. 213-230, Springer-Verlag, 2001.

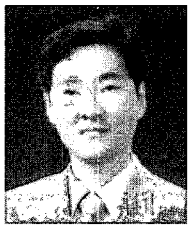
〈著者紹介〉



김 종 성 (Jong-Sung Kim)
2000년 8월: 고려대학교 수학과 학사
2002년 8월: 고려대학교 수학과 석사
2002년 8월~현재: 고려대학교 정보보호대학원 박사 과정
〈관심분야〉 블록 암호, 스트림 암호, 해쉬 함수 및 운영 모드의 분석과 설계



홍 석 희 (Seok-Hie Hong)
1995년 2월: 고려대학교 수학과 학사
1997년 2월: 고려대학교 수학과 석사
2001년 2월: 고려대학교 수학과 박사
2001년 3월~2004년 2월: 고려대학교 정보보호기술연구센터 선임 연구원
2004년 4월~2005년 2월: 벨기에 COSIC 박사후 연구원
2005년 3월~현재: 고려대 정보보호대학원 조교수
〈관심분야〉 블록 암호, 스트림 암호, 해쉬 함수, 공개키 암호



이 상 진 (Sang-Jin Lee)
1987년 2월: 고려대학교 수학과 학사
1989년 2월: 고려대학교 수학과 석사
1994년 8월: 고려대학교 수학과 박사
1989년 2월~1999년 2월: 한국전자통신연구소 선임 연구원
1999년 3월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 8월~현재: 고려대학교 정보보호대학원 부교수
〈관심분야〉 블록 암호 및 스트림 암호의 분석과 설계, 포렌식, 정보은닉이론

은 희 천 (Hi-Chun Eun)
1969년 2월: 고려대학교 수학과 학사
1974년 2월: 고려대학교 수학과 석사
1982년 2월: 고려대학교 수학과 박사
1982년 3월~현재: 고려대학교 자연과학대학 정보수학과 교수