http://dx.doi.org/10.7840/kics.2014.39B.5.317

블록 암호 연산 모드 RBF(Random Block Feedback)의 알려진/선택 평문 공격에 대한 안전성 비교 분석

김 윤 정◆°, 이 강*

Safety Comparison Analysis Against Known/Chosen Plaintext Attack of RBF (Random Block Feedback) Mode to Other Block Cipher Modes of Operation

Yoonjeong Kim◆°, Kang Yi*

요 약

데이타 보안과 무결성은 유무선 통신 환경에서 데이터 전송 시에 중요한 요소이다. 대량의 데이터는 전송 전에, 통상 암호 연산 모드를 이용한 블록 암호 알고리즘에 의하여 암호화된다. ECB, CBC 등의 기존 연산 모드 외에 블록 암호 연산 모드로 RBF 모드가 제안된 바 있다. 본 논문에서는, 알려진 평문 공격 (known plaintext attack) 및 선택 평문 공격 (chosen plaintext attack)에 대한, RBF 모드의 안전성을 기존 모드들과 비교 분석한 내용을 소개한다. 분석 결과, 기존의 연산 모드들이 알려진/선택 평문 공격에 취약한데 반하여, RBF 모드는 이들 공격에 안전함을 알 수 있었다.

Key Words : RBF (Random Block Feedback), Block cipher, Modes of operation, ECB (Electronic CodeBook), CBC(Cipher Block Chaining)

ABSTRACT

Data security and integrity is a critical issue in data transmission over wired/wireless links. A large amount of data is encrypted before transmission, by block cipher using mode of operation. RBF mode is a block cipher mode of operation which uses random characteristics. In this paper, we analyze the safety against known plaintext attack and chosen plaintext attack of RBF mode compared to the traditional modes. According to the analysis, RBF mode is known to be secure while the traditional modes are not secure against them.

Ⅰ. 서 론

블록 암호 연산 모드는 대량의 데이터를 블록 암호 알고리즘을 이용하여 암호 후 전송할 때, 블록 암호가 기본적으로 처리하는 단위 크기로 데이터를 나누어서 암호화하고 전송할 수 있는 기법을 제공한다. 대표적인 블록 암호 연산 모드에는 ECB(Electronic Code Book), CBC(Cipher Block Chaining) 등과 CTR 등이 있다[1-4]. 블록 암호 연산 모드의 중요성을 인지하고 새로운 연산 모드를 제안하고 이에 대한 안전성 분

※ 본 연구는 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (No. NRF-2010-0025596)
◆° First Author and Corresponding Author : Dept. of Information Security, Seoul Women's University, yjkim@swu.ac.kr, 정회원
* 한동대학교 전산전자공학부, yk@handong.edu
논문번호 : KICS2014-04-116, Received April 7, 2014; Revised April 23, 2014; Accepted April 23, 2014

석 등을 수행한 연구들도 있다[5-7]. 2000년에 블록 암호 DES(Data Encryption Standard)에 대한, 안전성이 강화되고 효율적인 RBF (Random Block Feedback) 모드가 제안된 바 있는데[8,9], 최근에는 이를 AES (Advanced Encryption Standard)에 적용하는 방안이 발표된 바 있다[10,11].

한편, 암호 시스템을 공격하는 기법 중 대표적인 공격으로, 알려진 평문 공격 (known plaintext attack)과 선택 평문 공격 (chosen plaintext attack)이 있다[12,13]. 알려진 평문 공격은, 알려진 평문과 이에 대한 암호문을 이용하여, 암호 알고리즘의 키를 찾는 공격이다. 선택 평문 공격은, 임의로 선택한 평문과 이에 대한 암호문을 이용하여, 암호 알고리즘의 키를 찾는 공격이다.

본 논문에서는, RBF 모드의 알려진 평문 공격과 선택 평문 공격에 대한 안전성을 기존의 블록 암호 연산 모드들과 비교 분석한 내용을 소개한다. 분석결과, 기존의 블록 암호 연산 모드들이 알려진/선택 평문 공격에 취약한데 반하여, RBF 모드는 이들 공격에 안전함을 알 수 있었다.

본 논문의 구성은 다음과 같다. 먼저 II 장에서는 연구 배경으로서, 기존의 블록 암호 연산 모드들과 RBF 모드의 수행 방식과, 알려진/선택 평문 공격에 대하여 기술한다. 다음으로 III 장에서는 연산 모드 별 알려진/선택 평문 공격에 대한 안전성 분석 결과를 제시한다. IV 장에서 이들을 종합한 결과와 본 논문의 연구와 타 연구와의 비교를 기술하며, V 장에서 결론을 기술한다.

Ⅱ. 연구 배경

2.1 블록 암호 연산 모드들

2.1.1 ECB

ECB (Electronic Codebook Mode)는 그림 1과 같이 주어진 평문을 블록 암호 연산단위로 나누어 $P_1, P_2, ..., P_n$을 구성하고, 이들 P_i $(i=1,...,n)$에 대하여 독립적으로 암호 연산을 수행한다. 암호화 결과는 $C_1, C_2, ..., C_n$이다. 이들은 식 (1)과 같이 표현된다.

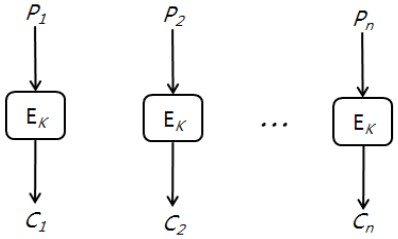

그림 1. ECB 모드
Fig. 1. ECB mode

$$C_i = E_K(P_i), \quad 1 \le i \le n \tag{1}$$

2.1.2 CBC

CBC 모드는 그림 2와 같이, 이전 암호문 블록과 평문을 xor한 결과에 암호화를 진행한다. 첫 번째 블록은 초기벡터 IV와 xor된 후 암호화된다. 이들은 식 (2)와 같이 표현된다.

$$\begin{aligned} C_1 &= E_k(P_1 \oplus IV) \\ C_i &= E_k(P_i \oplus C_{i-1}), \ 2 \le i \le n \end{aligned} \tag{2}$$

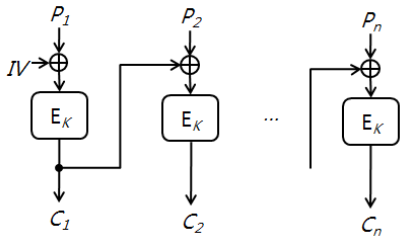

그림 2. CBC 모드
Fig. 2. CBC mode

2.1.3 CTR

CTR 모드는 그림 3과 같이, $Counter_i$ 값을 암호화한 값과, 평문 P_i를 xor하여 암호문 C_i를 생성한다. 이들은 식 (3)과 같이 표현된다.

$$\begin{aligned} T_i &= E_K(Counter_i), \ 1 \le i \le n \\ C_i &= P_i \oplus T_i, \qquad 1 \le i \le n \end{aligned} \tag{3}$$

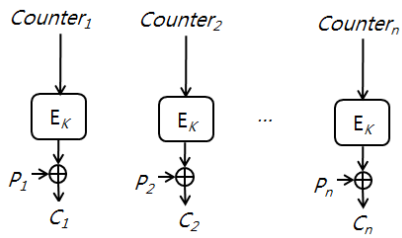

그림 3. CTR 모드
Fig. 3. CTR mode

2.1.4 RBF

RBF 모드는 그림 4와 같이, 이전 블록의 암호화시에 알려지지 않은 동적 키 udk_i를 생성하고, 평문 P_i와

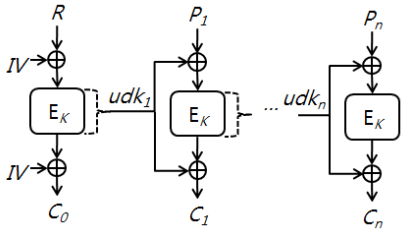

그림 4. RBF 모드
Fig. 4. RBF mode

이 udk_i를 xor한 결과를 암호화하고, 이 암호화 결과와 udk_i를 다시 xor하여 암호문 C_i를 생성한다. 첫 번째 블록 P_1을 위한 udk_1은 난수블록 R을 암호화하는 과정에서 구해지며, 난수블록 R을 위한 udk_0는 초기 벡터 IV로 주어진다. 이들은 식 (4)와 같이 표현된다.

$$C_i = E_K(P_i \oplus udk_i) \oplus udk_i, \quad 1 \le i \le n$$
$$\text{단, } C_0 = E_K(R \oplus IV) \oplus IV \tag{4}$$

RBF 모드는 난수에 기반하고 있는 특성으로, 다른 모드들에 비하여 안전한 특성을 갖는다. 그러나, ECB 모드나 CTR 모드가 갖는 장점인 병렬처리가 가능한 점과 오류가 전파되지 않는 특성은 갖지 않는다.

2.2 공격 방법

암호 알고리즘을 공격하는 기법 중 대표적인 것으로, 알려진 평문 공격과 선택 평문 공격을 들 수 있다[12-15].

2.2.1 알려진 평문 공격 (known plaintext attack)

알려진 평문과 이에 대한 암호문을 이용하여, 암호 알고리즘의 키를 찾는 공격이다.

예를 들어, 이전 버전의 zip 형식에서 사용하던, PKZIP 스트림 암호는 알려진 평문 공격에 취약하다고 알려져 있다[14].

2.2.2 선택 평문 공격 (chosen plaintext attack)

임의로 선택한 평문과 이에 대한 암호문을 이용하여, 암호 알고리즘의 키를 찾는 공격이다. 예를 들어, 7-라운드 128-비트 AES의 경우, $2^{112.2}$개의 선택된 평문을 이용하여 차분 공격 (differential cryptanalysis)를 수행할 수 있음이 알려져 있다[15].

Ⅲ. 연산 모드별 알려진/선택 평문 공격에 대한 안전성 분석

암호화 하고자 하는 평문을 $P_1, P_2, ..., P_n$이라 하고 암호화 결과 얻어지는 암호문을 $C_1, C_2, ..., C_n$ 이라 하자. 이 때, 암호 시스템 E_K의 입력을 입력 평문 $I_1, I_2, ..., I_n$으로, 암호 시스템 E_K의 출력을 출력 암호문 $O_1, O_2, ..., O_n$이라 하자. 기본 블록 암호의 경우, 입력 평문 I_i는 평문 P_i로부터 얻어지며, 출력 암호문 O_i는 암호문 C_i로부터 얻어진다. 이 관계가 그림 5에 나타나 있다.

본 장에서는 블록 암호 연산 모드들에서 대하여, 알려진 평문 공격과 선택 평문 공격의 가능성을 분석한다. 특히, 차분 공격을 예로 들어, RBF 모드가 다른 모드들과 비교하여 안전함을 보인다.

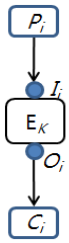

그림 5. 블록 암호
Fig. 5. block cipher

3.1 ECB 모드 안전성 분석

그림 6은 ECB 모드의 알려진/선택 평문 공격시 암호 시스템에 사용되는 입력 평문과 출력 암호문이 안이 채워진 작은 동그라미인 I_i와 O_i로 표시되어 있다.

그림 6에서 암호 시스템 E_K의 입력 평문 I_i는 P_i로, 출력 암호문 O_i는 C_i로 주어짐을 알 수 있다. 따라서, 공격자가 평문 P_i와 암호문 C_i를 획득한 후 알려진/선택 평문 공격을 하는 경우 공격이 진행된다,

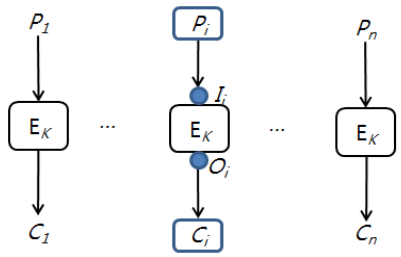

그림 6. ECB 모드의 알려진/선택 평문 공격
Fig. 6. known/chosen plaintext attack of ECB mode

여기서, $I_i = P_i$이고, $O_i = C_i$이다.

즉, ECB 모드를 이용하는 7-round 128 비트 AES의 경우, 공격자는 $2^{112.2}$개의 평문 P_i와 대응 암호문 C_i 쌍을 획득하여 차분 공격을 할 수 있다.

3.2 CBC 모드 안전성 분석

그림 7에는 CBC 모드의 알려진/선택 평문 공격시 암호 시스템에 사용되는 입력 평문과 출력 암호문이 안이 채워진 작은 동그라미인 I_i와 O_i로 표시되어 있다.

그림 7에서 암호 시스템 E_K의 입력 평문 I_i는 $P_i \oplus C_{i-1}$로, 암호 알고리즘의 출력 암호문 O_i는 C_i로 얻을 수 있음을 알 수 있다. 따라서, 공격자가 평문 P_i와 암호문 C_{i-1}, C_i를 획득한 후 알려진/선택 평문 공격을 하는 경우 공격이 진행된다. 여기서, $I_i = P_i \oplus C_{i-1}$이고, $O_i = C_i$이다.

즉, CBC 모드를 이용하는 7-round 128 비트 AES의 경우, 공격자는 $2^{112.2}$개의 평문 P_i와 대응 암호문 C_i 쌍을 획득하여 차분 공격을 할 수 있다.

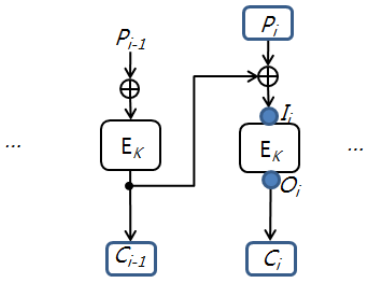

그림 7. CBC 모드의 알려진/선택 평문 공격
Fig. 7. known/chosen plaintext attack of CBC mode

3.3 CTR 모드 안전성 분석

그림 8에는 CTR 모드의 알려진/선택 평문 공격시의 암호 시스템에 사용되는 입력 평문과 출력 암호문이 안이 채워진 작은 동그라미인 I_i와 O_i로 표시되어 있다.

그림 8에서 암호 시스템 E_K의 입력 평문 I_i는 $Counter_i$로, 출력 암호문 O_i는 $P_i \oplus C_i$로 주어짐을 알 수 있다. 따라서, 공격자가 카운터 값 $Counter_i$와 평문 P_i, 암호문 C_i를 획득한 후 알려진/선택 평문 공격을 하는 경우 공격이 진행된다. 여기서, $I_i = Counter_i$이고, $O_i = P_i \oplus C_i$이다. $Counter_i$는 초기값과 증가함수가 알려진 경우 값을 계산할 수 있다.

즉, CTR 모드를 이용하는 7-round 128 비트 AES의 경우, $Counter_i$를 미리 알 수 있다면 공격자는 $2^{112.2}$개의 평문 P_i와 대응 암호문 C_i 쌍을 획득하여 차분 공격을 할 수 있다.

3.4 RBF 모드 안전성 분석

그림 9에는 RBF 모드의 알려진/선택 평문 공격시 암호 시스템에 사용되는 평문과 암호문이 안이 채워진 작은 동그라미인 I_i와 O_i로 표시되어 있다.

그림 9에서 암호 시스템 E_K의 입력 평문 I_i는 $P_i \oplus udk_i$로, 출력 암호문 O_i는 $C_i \oplus udk_i$로 주어짐을 알 수 있다. 여기서, udk_i는 그림 4의 RBF 모드 동작에 보여지는 것처럼, 블록의 암호화 과정에서 얻어지며 계속적으로 이전 블록들의 영향을 받아 최종적으로 초기 난수 R에 기반한다.

RBF 모드를 이용하는 7-round 128 비트 AES를 공격자가 공격한다고 할 때[15], 공격자는 $2^{112.2}$개의 블록을 한 번에 암호화하여 대응 암호문을 구할 수도 있고, 입력 평문을 한 개 블록씩 나누어 이들 한 개 블록의 암호화를 $2^{112.2}$ 번 수행할 수도 있다. 전자의 경우에는, 평문 P_i, 암호문 C_i를 획득한다 하더라도 난수에 기반한 udk_i를 알 수 없게 된다. 즉, 각 블록마다 다른 udk_i 값이 P_i와 C_i 값을 변경시켜, 입력 평문 I_i와 출력 암호문 O_i를 알 수 없게 한다. 후자의 경우는, 매 암호화시마다 난수 R의 값이 동일해야 한다. 128

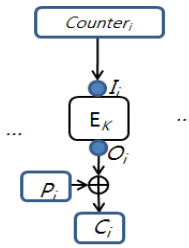

그림 8. CTR 모드의 알려진/선택 평문 공격
Fig. 8. known/chosen plaintext attack of CTR mode

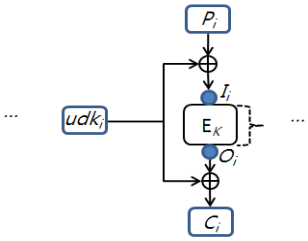

그림 9. RBF 모드의 알려진/선택 평문 공격
Fig. 9. known/chosen plaintext attack of RBF mode

비트의 난수가 $2^{112.2}$ 번 같을 확률은 $(1/2^{128})^{2^{112.2}-1}$ 이다.

Ⅳ. 안전성 분석 총괄과 토의

표 1에는 ECB, CBC, CTR, RBF 모드의 알려진/선택 평문 공격에 대한 안전성 분석 결과가 나타나 있다.

표 2에는 ECB, CBC, CTR, RBF 모드의 7-라운드 128-비트 AES 공격에 대한 안전성 분석 결과가 나타나 있다.

기존 연구들과 본 논문의 연구 결과와의 차이점은 다음과 같다. 김해중 등의 연구는[5] 간단한 컨트롤만으로도 파이프라인 된 암호 모듈로의 입출력값을 연산하고 선택할 수 있는 암호 모듈의 입출력 모듈을 설계한 것으로, 본 논문에서 공격에 대한 안전성을 분석한 것과는 차이가 있다. 양상근 등의 연구는[6] 카운터를 사용한 블록 암호 연산 모드를 제안하고 이의 구현 및 수행 성능을 다른 모드과 비교한 것으로, 본 논문에서 주로 한 연산 모드 간 안전성 비교 분석과는 차이가 있다. Huang 등의 연구는[7], 새로운 연산 모드 KSPC와 ODC 모드를 제안하고, 이 연산모드들의 선택 평문 공격에 대한 안전도를 논한 것으로, 본 논문에서 알려진/선택평문 공격에 대한 안전성 분석을 RBF 모드와 기존 모드들에 대하여 수행한 것과는 차이가 있다.

표 1. 연산 모드의 알려진/선택 평문 공격에 대한 안전성
Table 1. Safety of modes of operation against known/ chosen plaintext attack

Encryption Mode	Safety against known/ chosen plaintext attack
ECB	weak
CBC	weak
CTR	weak
RBF	strong

표 2. 7-라운드 128-비트 AES에 대한 연산 모드의 차분 공격에 대한 안전성
Table 2. Safety of modes of operation for 7-round 128-bit AES, against differential cryptanalysis

Encryption Mode	differential cryptanalysis of 7-round 128-bit AES
ECB	needs $2^{112.2}$ plaintext/ciphertext pairs
CBC	needs $2^{112.2}$ plaintext/ciphertext pairs
CTR	needs counter values and $2^{112.2}$ plaintext/ciphertext pairs
RBF	could be succeeded with probability $(1/2)^{128 \cdot (2^{1122}-1)}$, when $2^{112.2}$ plaintext/ciphertext pairs are given

Ⅴ. 결 론

본 논문에서는 블록 암호 연산 모드 ECB, CBC, CTR, RBF 모드들에 대한 알려진/선택 평문 공격 가능성을 분석하였다. 분석 결과, RBF 모드는 난수에 기반하고 있는 특성으로, 다른 모드들에 비하여 알려진/선택 평문 공격에 더 강한 안전도를 가짐을 알 수 있었다. 대량의 데이터를 블록 암호를 이용하여 전송하는 경우 RBF 모드를 이용하게 되면, 알려진/선택 평문 공격에 강한 특성을 유지하며 전송할 수 있고, 따라서 안전한 통신 시스템 구축에 기여하게 된다.

References

[1] Data Encryption Standard, FIPS (Federal Information Processing Standards Publication) 46-3, National Institute of Standard & Technology (NIST), 1999.

[2] Announcing the Advanced Encryption Standard (AES), FIPS (Federal Information Processing Standards Publication) 197, National Institute of Standard & Technology (NIST), 2001.

[3] Morris Dworkin (Editor), Recommendation for Block Cipher Modes of Operation – Methods and Techniques, Special Publication 800-38A, National Institute of Standard & Technology (NIST), 2001.

[4] P. J. Lee, “ISO/IEC JTC1/SC27 International Standard 8372 - Information Processing - Modes of operation for a 64-bit block cipher algorithm,” *J. Korea Inst. Inf. Security & Cryptology*, vol. 4, no. 1, Mar. 1994.

[5] H. J. Kim and Y. J. Jeong, “Design of I/O module for pipelining crypto processors,” in *Proc. KICS*, pp. 1926-1929, Korea, Jul. 2002.

[6] S. K. Yang, G. H. Kim, C. S. Park, and G. Y. Cho, “Study for block cipher operating Mode using counter,” in *Proc. KIICE*, Daejoen, Korea, Oct. 2008.

[7] Y. Huang, F. Leu, J. Liu, J. Yang, C. Yu, C. Chu, and C. Yang, “Building a block cipher mode of operation with feedback keys,” in

Proc. IEEE ISIE, Taipei, Taiwan, May 2013.

[8] Y. Kim, An efficient mode of operation for block ciphers and a remote audit system using the mode, Ph.D Dissertation, Seoul National University, 2000.

[9] Y. Kim and Y. Cho, "The random block feedback mode for block ciphers," *IEICE Trans. Fundamentals*, vol. E00-A, no. 6, Jun. 2000.

[10] Y. Kim, J. Yoon, J.-H. Joo, and K. Yi, "Robust lightweight fingerprint encryption using random block feedback," *IET Electronics Lett.*, vol 50, Issue 4, Feb. 2014.

[11] Y. Kim, J. Yoon, and K. Yi, "Random block feedback mode for AES: A more secure mode of operation with small overhead," submitted, 2014.

[12] D. Stinson, *Cryptography: Theory and Practice*, Florida: CRC Press, 2006.

[13] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Crytography*, Florida: CRC Press, 1996.

[14] E. Biham and P. C. Kocher, "A known plaintext attack on the PKZIP stream cipher," *Fast Software Encryption, Lecture Notes in Comput. Sci.*, vol. 1008, pp. 144-153, 1995.

[15] J. Lu, O. Dunkelman, N. Keller, and J. Kim, "New impossible differential attacks on AES," *INDOCRYPT 2008, LNCS*, vol. 5365, pp. 279-293, 2008.

김 윤 정 (Yoonjeong Kim)

1991년 2월 : 서울대학교 컴퓨터공학과 학사

1993년 2월 : 서울대학교 컴퓨터공학과 석사

2000년 8월 : 서울대학교 전기·컴퓨터공학부 박사

2000년 7월~2001년 5월 : (주) 엔써커뮤니티 제품개발연구소 차장

2001년 5월~2002년 2월 : (주) 데이타게이트 인터내셔널 보안기술연구소 차장

2009년 1월~2010년 1월 : Baylor 대학교 (TX, USA) 방문연구원

2002년~현재 : 서울여자대학교 정보보호학과 부교수

<관심분야> 암호학, 시스템 보안, 암호 응용

이 강 (Kang Yi)

1990년 2월 : 서울대학교 컴퓨터공학과 학사

1992년 2월 : 서울대학교 컴퓨터공학과 석사

1997년 8월 : 서울대학교 컴퓨터공학과 박사

1998년 3월~1999년 2월 : 인제대학교 정보통신공학과 전임강사

2005년 8월~2006년 7월 : University of California, Irvine 방문교수

2012년 8월~2013년 7월 : (재)스마트IT융합연구단 초빙교수

1999년 3월~현재 : 한동대학교 전산전자공학부 교수

<관심분야> Embedded Computing, Energy-Aware Multimedia System Design, Multimedia Encryption.