Interlacing과 Decomposition을 적용한 블록 암호에 대한 분석*

*강진건 **최준근 ***정기태 ****이창훈 *****홍석희

고려대학교 정보경영공학전문대학원

*kjk@cist.korea.ac.kr

Cryptanalysis on a Block Cipher Involving Interlacing and Decomposition

*Jinkeon Kang **Joongeun Choi ***Kitae Jung

****Changhoon Lee *****Seokhie Hong

Graduate School of Information Management and Security, Korea University

요 약

Kumar 등은 interlacing과 decomposition을 적용한 112-비트 블록 암호를 제안하였다.[1] 본 논문에서는 이 블록 암호에 대한 첫 번째 분석 결과를 소개한다. 이 블록 암호를 구성하는 연산들은 모두 선형성만을 가지고 있다. 따라서 112개의 독립인 평문/암호문 쌍이 주어졌을 경우, 비밀키를 복구하지 않더라도 임의의 암호문을 복호화할 수 있다. 본 논문의 분석 결과를 통하여 이 블록 암호는 매우 취약함을 알 수 있다.

1. 서론

Kumar 등은 interlacing과 decomposition을 적용한 112-비트 블록 암호를 제안하였다.[1] 이 블록 암호는 196-비트 비밀키를 사용하고 가변적인 라운드 수를 가지며 한 라운드는 평문과 비밀키 행렬의 곱셈과 interlacing 과정으로 구성된다. 그리고 매 라운드마다 비밀키가 그대로 사용된다. 본 논문에서는 편의상 이 블록 암호를 InDe라 표기하기로 한다.

본 논문에서는 InDe에 대한 첫 번째 분석 결과를 제시한다. InDe를 구성하는 연산들은 모두 선형성만을 가지고 있다. 일반적으로 블록 암호를 구성할 때, 비선형성과 선형성을 적절히 사용하여 설계된다. 하지만 알고리즘을 구성하는 연산들이 모두 선형성만을 가지고 있을 경우, 평문과 암호문에 대한 선형식을 구성할 수 있다. 따라서 비밀키를 복구하지 않더라도 임의의 암호문을 복호화할 수 있다. InDe의 경우, 112개의 독립인 평문/암호문 쌍이 주어졌을 경우, 비밀키와 상관없이 임의의 암호문을 복호화할 수 있다. 본 논문의 분석 결과를 통하여 InDe는 매우 취약함을 알 수 있다.

본 논문의 구성은 다음과 같다. 2절에서는 InDe를 소개하고 3절에서는 이 블록 암호의 분석 결과를 제시한다. 마지막 4절에서는 결론을 맺는다.

2. InDe 블록 암호

본 절에서는 먼저 InDe 블록 암호에 사용되는 interlacing과 decomposition 과정을 소개하고 InDe 블록 암호를 소개한다.

* 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-(C1090-0801-0025))

가. Interlacing과 Decomposition

7×4 행렬 $X_i(1 \le i \le 4)$를 다음과 같이 정의한다.

$$X_i = [x_{ijk}](1 \le i \le 4, 1 \le j \le 7, 1 \le k \le 4).$$

$$X_1 = \begin{bmatrix} x_{111}\,x_{112}\,x_{113}\,x_{114} \\ x_{121}\,x_{122}\,x_{123}\,x_{124} \\ x_{131}\,x_{132}\,x_{133}\,x_{134} \\ x_{141}\,x_{142}\,x_{143}\,x_{144} \\ x_{151}\,x_{152}\,x_{153}\,x_{154} \\ x_{161}\,x_{162}\,x_{163}\,x_{164} \\ x_{171}\,x_{172}\,x_{173}\,x_{174} \end{bmatrix}, X_2 = \begin{bmatrix} x_{211}\,x_{212}\,x_{213}\,x_{214} \\ x_{221}\,x_{222}\,x_{223}\,x_{224} \\ x_{231}\,x_{232}\,x_{233}\,x_{234} \\ x_{241}\,x_{242}\,x_{243}\,x_{244} \\ x_{251}\,x_{252}\,x_{253}\,x_{254} \\ x_{261}\,x_{262}\,x_{263}\,x_{264} \\ x_{271}\,x_{272}\,x_{273}\,x_{274} \end{bmatrix},$$

$$X_3 = \begin{bmatrix} x_{311}\,x_{312}\,x_{313}\,x_{314} \\ x_{321}\,x_{322}\,x_{323}\,x_{324} \\ x_{331}\,x_{332}\,x_{333}\,x_{334} \\ x_{341}\,x_{342}\,x_{343}\,x_{344} \\ x_{351}\,x_{352}\,x_{353}\,x_{354} \\ x_{361}\,x_{362}\,x_{363}\,x_{364} \\ x_{371}\,x_{372}\,x_{373}\,x_{374} \end{bmatrix}, X_4 = \begin{bmatrix} x_{411}\,x_{412}\,x_{413}\,x_{414} \\ x_{421}\,x_{422}\,x_{423}\,x_{424} \\ x_{431}\,x_{432}\,x_{433}\,x_{434} \\ x_{441}\,x_{442}\,x_{443}\,x_{444} \\ x_{451}\,x_{452}\,x_{453}\,x_{454} \\ x_{461}\,x_{462}\,x_{463}\,x_{464} \\ x_{471}\,x_{472}\,x_{473}\,x_{474} \end{bmatrix}.$$

Interlacing은 각각의 X_i을 입력 받아 다음과 같은 과정을 수행하여 $< X_i >$를 출력한다.

① X_4에서 7 번째 행의 마지막 열인 x_{474}를 새로운 첫 번째 행렬 $< X_1 >$의 첫 번째 행의 첫 번째 열로 옮긴다.

② x_{464}는 새로운 두 번째 행렬 $< X_2 >$의 첫 번째 행의 첫 번째 열로 옮긴다.

③ 단계 ①과 단계 ②와 같은 방식으로 행렬 X_i의 모든 항들을 다음

과 같이 $< X_i >$에 대입한다.

$$< X_1 > = \begin{bmatrix} x_{474}\,x_{434}\,x_{463}\,x_{423} \\ x_{452}\,x_{412}\,x_{441}\,x_{374} \\ x_{334}\,x_{363}\,x_{323}\,x_{352} \\ x_{312}\,x_{341}\,x_{274}\,x_{234} \\ x_{263}\,x_{223}\,x_{252}\,x_{212} \\ x_{241}\,x_{174}\,x_{134}\,x_{163} \\ x_{123}\,x_{152}\,x_{112}\,x_{141} \end{bmatrix}, < X_2 > = \begin{bmatrix} x_{464}\,x_{424}\,x_{453}\,x_{413} \\ x_{442}\,x_{471}\,x_{431}\,x_{364} \\ x_{324}\,x_{353}\,x_{313}\,x_{342} \\ x_{371}\,x_{331}\,x_{264}\,x_{224} \\ x_{253}\,x_{213}\,x_{242}\,x_{271} \\ x_{231}\,x_{164}\,x_{124}\,x_{153} \\ x_{113}\,x_{142}\,x_{171}\,x_{131} \end{bmatrix},$$

$$< X_3 > = \begin{bmatrix} x_{454}\,x_{414}\,x_{443}\,x_{472} \\ x_{432}\,x_{461}\,x_{421}\,x_{354} \\ x_{314}\,x_{343}\,x_{372}\,x_{332} \\ x_{361}\,x_{321}\,x_{254}\,x_{214} \\ x_{243}\,x_{272}\,x_{232}\,x_{261} \\ x_{221}\,x_{154}\,x_{114}\,x_{143} \\ x_{172}\,x_{132}\,x_{161}\,x_{121} \end{bmatrix}, < X_4 > = \begin{bmatrix} x_{444}\,x_{473}\,x_{433}\,x_{462} \\ x_{422}\,x_{451}\,x_{411}\,x_{344} \\ x_{373}\,x_{333}\,x_{362}\,x_{322} \\ x_{351}\,x_{311}\,x_{244}\,x_{273} \\ x_{233}\,x_{262}\,x_{222}\,x_{251} \\ x_{211}\,x_{144}\,x_{173}\,x_{133} \\ x_{162}\,x_{122}\,x_{151}\,x_{111} \end{bmatrix}.$$

Decomposition 과정은 interlacing의 역과정이며, 각각의 행렬 X_i를 입력받아 $> X_i <$를 출력한다 $(1 \le i \le 4)$.

나. InDe 블록 암호

InDe는 196-비트 비밀키를 사용하고 112-비트 입출력 크기를 갖는 r-라운드 블록 암호이다. 112-비트 평문 P는 16개의 문자로 구성되고 각 문자는 7-비트 아스키 코드로 표현된다. 따라서 P는 4개의 7×4 행렬 $P_i(1 \le i \le 4)$로 구성되고 한 문자는 행렬의 열에 해당된다. 196-비트 비밀키 K는 28개의 숫자로 구성되고 각 숫자는 7-비트 아스키 코드로 표현되며 0부터 127사이의 수이다. 따라서 K는 4개의 7×7 행렬 $K_i(1 \le i \le 4)$로 구성되고 한 숫자는 행렬의 행에 해당된다.

InDe는 112-비트 평문 P로부터 112-비트 암호문 C를 생성하기 위해 다음과 같은 라운드 함수를 r번 반복하여 수행한다.

① $GF(2)$ 상에서 각각의 행렬 K_i와 P_i를 곱하여 7×4 행렬 Q_i를 생성한다 $(1 \le i \le 4)$.

$$Q_i = K_i P_i (1 \le i \le 4).$$

② Q_i를 interlacing 과정에 적용하여 $< Q_i >$를 생성하고 이를 P_i에 대입한다 $(1 \le i \le 4)$.

$$P_i = < Q_i > \quad (1 \le i \le 4).$$

라운드 함수를 r번 반복 수행한 후 생성된 4개의 7×4 행렬 C_i는 다음과 같다: $C_i = P_i (1 \le i \le 4)$. 각각의 C_i들을 다음과 같이 연결하여 112-비트 암호문 $C=(c_1,c_2,\cdots,c_{112})$를 얻는다.

$$(c_1,c_2,\cdots,c_{112}) = (c_{111},c_{121},\cdots,c_{171},c_{112},\cdots,c_{174},c_{211},c_{221},\cdots,c_{474})$$

3. InDe 블록 암호에 대한 분석

본 절에서는 InDe 블록 암호에 대한 분석 결과를 소개한다. InDe를 구성하는 연산들은 모두 선형성만을 가지고 있고 평문 P는 비밀키 K로만 갱신된다. 따라서 서로 다른 두 개의 평문 $P=(p_1,p_2,\cdots,p_{112})$와 $P^*=(p_1^*,p_2^*,\cdots,p_{112}^*)$에 대한 암호문 $C=(c_1,c_2,\cdots,c_{112})$와 $C^*=(c_1^*,c_2^*,\cdots,c_{112}^*)$는 식 (1)과 같이 표현된다. 여기서 112×112 행렬 M은 비밀키 곱셈 과정과 interlacing 과정을 합성한 함수를 의미한다.

$$\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_{112} \end{pmatrix} = M \cdot \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_{112} \end{pmatrix}, \quad \begin{pmatrix} c_1^* \\ c_2^* \\ \vdots \\ c_{112}^* \end{pmatrix} = M \cdot \begin{pmatrix} p_1^* \\ p_2^* \\ \vdots \\ p_{112}^* \end{pmatrix}. \tag{1}$$

식 (1)을 이용하여 $C \oplus C^*$는 식 (2)와 같이 표현된다.

$$\begin{pmatrix} c_1 \oplus c_1^* \\ c_2 \oplus c_2^* \\ \vdots \\ c_{112} \oplus c_{112}^* \end{pmatrix} = M \cdot \begin{pmatrix} p_1 \oplus p_1^* \\ p_2 \oplus p_2^* \\ \vdots \\ p_{112} \oplus p_{112}^* \end{pmatrix}. \tag{2}$$

식 (2)는 서로 다른 암호문 C와 C^*를 XOR한 값과 평문 $P \oplus P^*$를 암호화한 값이 동일함을 의미한다. 즉,

$$\mathrm{InDe}(P) \oplus \mathrm{InDe}(P^*) = \mathrm{InDe}(P \oplus P^*).$$

실제 구현 결과를 통하여 이를 확인할 수 있다. InDe 블록 암호가 16라운드로 구성되었다고 가정할 때, 2개의 평문 P="All the enemies "와 P^*="are killed, no w"에 대한 암호문은 각각 다음과 같다.

$$\begin{aligned} \mathrm{InDe}(P) = {} & 10000111100110000000001100010 \\ & 00100011010000010100111100011 \\ & 00101111000001011011001011100 \\ & 00001010001101101110110011111, \\ \mathrm{InDe}(P^*) = {} & 10010101100000001101001110000 \\ & 11101011100000101010011001010 \\ & 00111001110011111001011010010 \\ & 10100010110010111001010000110. \end{aligned}$$

평문 $P \oplus P^*$에 대한 암호문은 다음과 같다. 이 암호문은 2개의 평문에 대한 암호문을 XOR한 값과 같음을 알 수 있다.

$$\begin{aligned} \mathrm{InDe}(P \oplus P^*) = {} & 00010010000110011010000010010 \\ & 11001000110001111110100101001 \\ & 00010110110010101001111111110 \\ & 10101000111111010111100010001, \\ \mathrm{InDe}(P) \oplus \mathrm{InDe}(P^*) = {} & 00010010000110011010000010010 \\ & 11001000110001111110100101001 \\ & 00010110110010101001111111110 \\ & 10101000111111010111100010001. \end{aligned}$$

따라서 독립인 112개의 평문/암호문 쌍 (P^i, C^i) $(i=1,\cdots,112)$이 주어진다면 임의의 암호문에 대한 평문을 얻을 수 있다. 즉, 공격자에게 임의의 암호문 C가 주어지면, 공격자는 자신이 가지고 있는 독립인 112개의 암호문들을 적절히 XOR하여 결과값이 C와 같게 하는 인덱스들의 집합 I를 찾을 수 있다.

$$C = \bigoplus_{i \in I} C^i.$$

집합 I에 해당하는 P^i들을 XOR 조합하면 공격자가 원하는 평문 P를 구할 수 있다.

$$P = \bigoplus_{i \in I} P^i.$$

4. 결론

본 논문에서는 [1]에서 제안된 InDe 블록 암호의 첫 번째 분석 결과를 제시하였다. InDe를 구성하는 연산들은 모두 선형성만을 가지고 있고 평문은 비밀키만을 이용하여 갱신된다. 따라서 112개의 독립인 평문/암호문 쌍이 주어졌을 경우, 비밀키를 복구하지 않더라도 임의의 암호문을 복호화할 수 있다. 본 논문의 분석 결과를 통하여 이 블록 암호는 매우 취약함을 알 수 있다.

참고문헌

[1] S. Kumar, V. Sastry and A. Babu, "A Block Cipher Involving Interlacing and Decomposition", Information Technology Journal, Vol. 6, No. 3, pp. 396-404, 2007.