가역 셀룰러 오토마타 기반 블록 암호에 대한 취약점 분석(1)

*류한성 **이제상 ***이창훈 ****성재철 *****홍석희
고려대학교, ****서울시립대학교
*ybr251@cist.korea.ac.kr

Distinguish Attack of block ciphers based on Reversible Cellular Automata

*Ryu, Han-Seong **Lee, Je-Sang ***Lee, Chang-Hoon ****Sung, Jae-Chul *****Hong, Seok-Hie
Korea University, ****University of Seoul

요약

셀룰러 오토마타(CA:cellular automata)의 특징 중에서 확산(Diffusion)과 국소적인 상호 작용(Local Interaction)은 암호시스템을 설계하는데 적합하여 암호 알고리즘, 의사난수 생성기를 비롯한 암호시스템의 설계 논리로 활용되고 있다. 본 논문에서는 2004년에 제안된 가역 셀룰러 오토마타 기반 블록 암호(BCRCA)에 대한 취약점 분석을 소개한다[1]. BCRCA는 224 비트의 안전성을 가져야 하지만, 균일한 키를 이용할 경우 통계적 취약점을 이용하여 191.8 비트의 안전성을 갖는다.

1. 서론

셀룰러 오토마타(CA: cellular automata)는 스스로 조직화하고 재생산할 수 있는 모델로서, 국소적 상호작용을 통하여 동시에 상태가 갱신되는 셀들로 구성된 유한상태머신이다. 이것은 Neumann에 의해 처음 소개되었으며[2], Wolfram에 의해 처음으로 암호학에 응용되었다[3]. 셀룰러 오토마타의 특징 중에서 확산(Diffusion)과 국소적인 상호 작용(Local Interaction)은 암호시스템을 설계하는데 적합하여 LFSR의 대안으로 제시되었으며, 부울 방정식의 해법, 의사난수 생성기, 암호 알고리즘 설계 등과 같은 다양한 응용분야에서 사용되고 있다. 셀룰러 오토마타는 AND, OR, NOT, XOR와 같은 단순한 연산을 이용하여 상태를 갱신한다.

암호알고리즘이 안전하기 위해서는 키를 모르는 상태에서도 평문과 암호문의 어떠한 연관관계도 유출할 수 없어야 하며 키와 암호문 사이의 연관 관계 또한 찾을 수 없어야 한다. 그러나 알고리즘에 의해 암호문이 생성되기 때문에 평문과 암호문, 키와 암호문 사이에는 특별한 연관 관계가 존재한다. 따라서 키 전수 조사보다 적은 계산량으로는 미지의 암호문으로부터 키나 평문의 어떠한 정보도 이끌어 낼 수 없을 때 주어진 암호알고리즘은 안전하다라고 한다. 암호 알고리즘의 출력문인 암호문에 대한 난수성 검정은 그 암호 알고리즘의 안전성을 증명할 수 있는 필요조건이고, 그렇기 위하여 0과 1이 균일하게 나타나야 한다. 0과 1이 균일하지 않으면 편차(bias)가 발생하기 때문에 암호알고리즘이 안전하지 않다.

본 논문에서는 2004년에 제안된 가역 셀룰러 오토마타 기반 블록 암호에 대한 안전성 분석을 소개하고, 논문 전개상의 편의성을 위하여 BCRCA라 표기한다[1]. BCRCA는 224 비트의 안전성을 가져야 하지만, 균일한 키를 이용할 경우 통계적 취약점을 이용하여 191.8 비트의 안전성을 갖는 것을 보였다.

본 논문의 구성은 다음과 같다. 2 장에서는 CA에 대한 기본적인 내용을 소개하고, 3 장에서는 BCRCA 알고리즘을 간략히 소개한다. 4 장에서는 BCRCA의 취약점을 분석하고, 마지막으로 5 장은 본 논문의 결론이다.

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

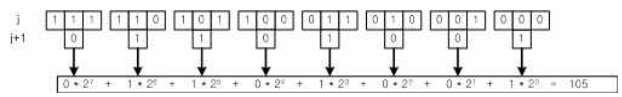
2. 셀룰러 오토마타(CA)

가. 1차원 CA

CA는 셀의 크기, 초기 구성(configuration) , 이웃, 법칙과 경계 조건으로 정의된다. 크기는 셀의 개수이고, 모든 셀은 아래의 식과 같이 특정한 법칙 R에 의하여 다음 단계로 갱신된다. s_i^j는 단계 j에서 i번째 셀의 값이고, r은 이웃의 반지름(radius)이다.

$$s_i^{j+1} = R(s_{i-r}^j, \cdots, s_{i-1}^j, s_i^j, s_{i+1}^j, \cdots, s_{i+r}^j)$$

반지름이 1인 법칙에 대한 예제는 [그림 1]과 같다. 여기에서 105는 CA의 갱신2진수를 10진수로 표현한 것이다.



[그림 1] 법칙 105

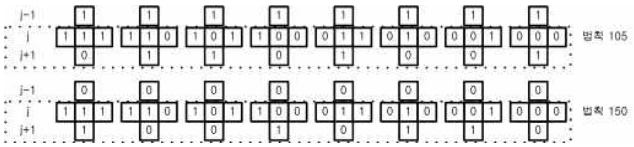
유한 CA는 일반적으로 순환 경계 조건을 이용한다. 본 논문에서는 초기 구성을 C_0라 정의하고, 동일한 법칙에 의하여 갱신한다. CA에서 모든 셀이 같은 법칙을 사용하면 uniform CA라고 하고, 그렇지

않으면, non-uniform CA라고 한다. BCRCA는 이웃의 반지름이 2와 3인 1차원 uniform CA를 사용한다.

나. 가역 CA

가역 CA는 모든 구성(configuration)이 유일한 이전 상태값과 이후 상태값을 갖는 CA를 말한다. 가역 CA는 일반적인 1차원 CA와 다르게 법칙을 단계 j-1, j에 적용하여 갱신한다. 가역 CA의 법칙은 [그림 2]와 같이 2개의 보수 법칙으로 구성한다. 여기에서 단계 j-1에서 셀의 값이 1이면 법칙 105를 이용하고, 0이면 법칙 150을 이용한다.

$$s_i^{j+1} = R(s_{i-r}^j, \cdots, s_{i-1}^j, s_i^j, s_i^{j-1}, s_{i+1}^j, \cdots, s_{i+r}^j)$$



[그림 2] 가역 법칙 105/150

3. BCRCA

본 장에서는 BCRCA에 대한 알고리즘과 키 생성 방법에 대하여 간략히 소개한다.

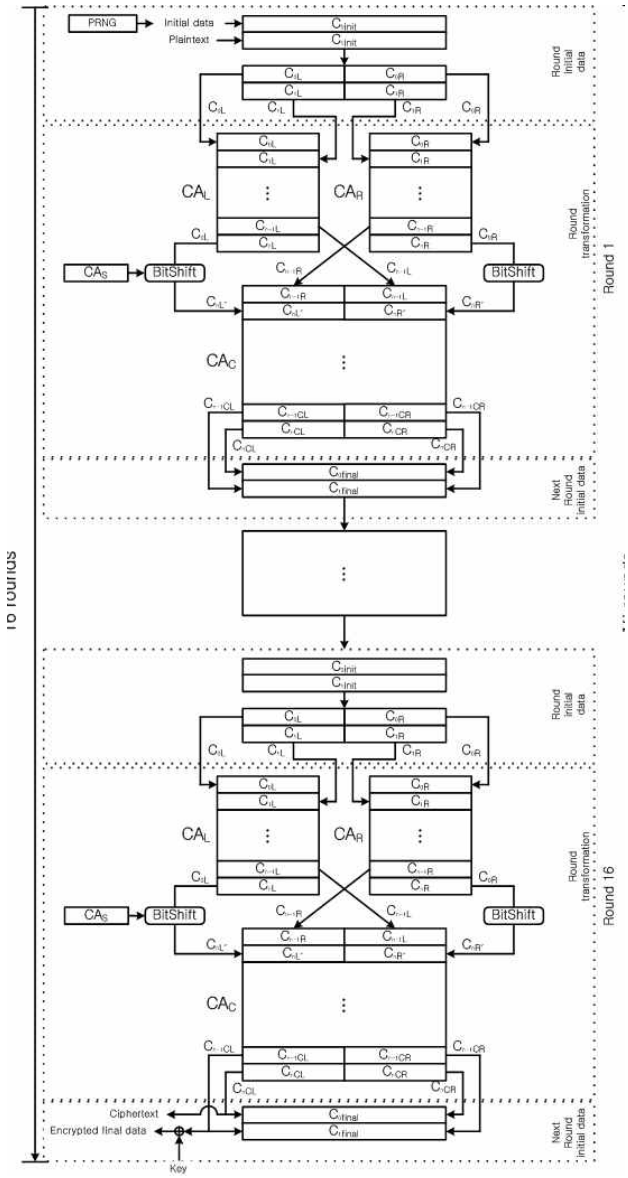
가. BCRCA 알고리즘

BCRCA 알고리즘은 [그림 3]과 같다. 평문과 암호문은 64 비트 블록이고, 키는 224 비트이다. BCRCA는 16 라운드로 구성하고, 각 라운드는 CA_L, CA_R, CA_C, CA_S로 구성되어 있으며, 자세한 내용은 뒤에서 언급한다.

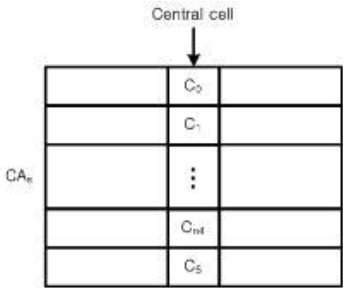
나. 1 라운드 알고리즘

각 라운드는 2개의 64 비트값(C_{0init}와 C_{1init})을 갖는 초기 데이터로 시작한다. 첫 라운드에서 C_{0init}는 의사난수생성기로부터 얻은 초기 데이터이고, C_{1init}는 평문이다. 2~16 라운드에서 C_{0init}와 C_{1init}는 이전 라운드에서 얻은 결과를 이용한다. 각각 64 비트는 32 비트로 나누어 C_{0L}, C_{0R}, C_{1L}, C_{1R}로 나타낸다. CA_L의 초기 구성은 C_{0L}과 C_{1L}로 설정하고, CA_R의 초기 구성은 C_{0R}과 C_{1R}로 설정하며, CA_L과 CA_R은 n_1번 반복한다. C_{nL}과 C_{nR}은 BitShift 변환에서 n_s만큼 왼쪽 순환 이동하고,. 각 라운드에서 CA_S는 [그림 4]와 같이 n_s를 생성한다. C_{n-1L}과 C_{n-1R}은 스왑하고, $C_{nL}{}'$과 $C_{nR}{}'$와 함께 CA_c의 초기 구성으로 설정한다. 마지막으로 CA_c는 n_2번 반복한다. 반복된 마지막 2개의 열은 다음 라운드의 초기 데이터가 된다. 마지막 라운드에서 C_{0final}은 암호문이 되고, C_{1final}은 다음 블록의 암호화 과정을 위한 초기 데이터가 된다. 첫 번째와 마지막 평문 블록을 암호화 할 때에는 특별한 경우가 발생한다. 첫 번째 경우에서 초기 데이터 C_{0init}는 임의로 생성된 64 비트이고, 두 번째 경우에서 XOR 연산은 C_{1fianl}와 키의 첫 번째 64 비트를 적용하며, 식은 아래와 같다.

$$C_{1fianl}{}' = key \oplus C_{1fianl}$$



[그림 3] BCRCA 알고리즘



[그림 4] n_s의 생성

다. 키 생성

모든 CA_L, CA_R, CA_C, CA_S는 가역 법칙을 따르며 [표 1]과 같이 각각 키 길이는 32, 32, 128, 32 비트이기 때문에 총 224 비트이다. 여기서 키는 의사난수생성기를 이용하여 랜덤하게 생성해야만 한다. CA_C의 마지막 구성은 CA_C에 해당되는 키의 첫 번째 64 비트(비트 0~63)를 이용하여 XOR 연산을 하고, CA_S의 마지막 구성은 CA_C에 해당되는 키의 비트 64~95를 이용하여 암호화한다.

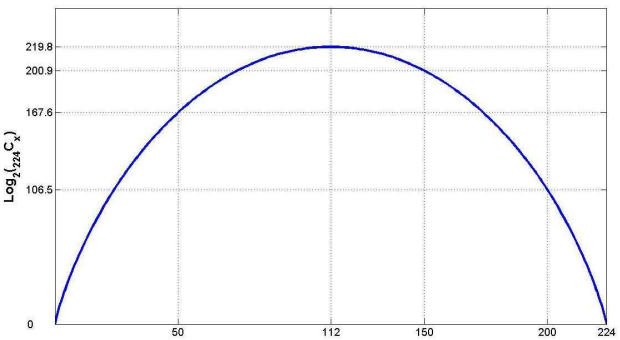
	CA_L	CA_R	CA_C	CA_S
셀 크기	32	32	64	16
가역 법칙의 반지름	2	2	2	3
키 길이	32	32	128	32

[표 1] BCRCA에 이용된 CA

4. 취약점 분석

암호알고리즘이 안전하기 위해서는 키를 모르는 상태에서도 평문과 암호문의 어떠한 연관관계도 유출할 수 없어야 하며 키와 암호문 사이의 연관 관계 또한 찾을 수 없어야 한다. 그러나 알고리즘에 의해 암호문이 생성되기 때문에 평문과 암호문, 키와 암호문 사이에는 특별한 연관 관계가 존재한다. 따라서 키 전수 조사보다 적은 계산량으로는 미지의 암호문으로부터 키나 평문의 어떠한 정보도 이끌어 낼 수 없을 때 주어진 암호알고리즘은 안전하다라고 한다. 암호 알고리즘의 출력문인 암호문에 대한 난수성 검정은 그 암호 알고리즘의 안전성을 증명할 수 있는 필요조건이고, 그렇기 위하여 0과 1이 균일하게 나타나야 한다. 0과 1이 균일하지 않으면 편차(bias)가 발생하기 때문에 암호알고리즘이 안전하지 않다. 이를 이용하여 BCRCA은 [경우1]과 [경우 2]와 같이 안전성을 분석을 한다.

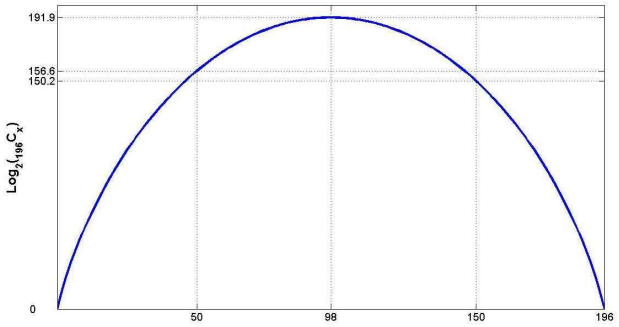
[경우 1] BCRCA의 키 길이는 224 비트이지만, 실제 키 길이는 219. 8 비트의 안전성을 갖는다. 암호알고리즘이 안전하기 위하여 키는 균일 성질을 만족해야 하기 때문에, 0과 1이 각각 112개여야 한다. 즉, $\log_2\binom{224}{112} = 219.8$ 비트의 안전성을 갖는다.



[그림 5] [경우 1]에 대한 안전성 분석

[경우 2] 일반적으로, 키는 키보드를 이용하여 입력한다. 문자를 입력시 ASCII CODE는 1 바이트로 하나의 문자를 정의하지만, 최상위 비트는 0으로 고정되어 있다. 즉, 224 비트는 28 바이트이므로, BCRCA는 196 비트의 안전성을 갖는다. [경우 1]과 같이 암호알고리즘이 안전하기 위하여 키는 균일 성질을 만족해야 하기 때문에, 0과 1이 각각 98개여야 한다. 즉, $\log_2\binom{196}{98} = 191.9$ 비트의 안전성을 갖는다.

본 논문에서 분석하는 BCRCA는 224 비트의 안전성을 가져야 하지만, [경우 1]과 [경우 2]와 같은 취약점을 이용하여 191.9 비트의 안전성을 갖는다.



[그림 6] [경우 2]에 대한 안전성 분석

5. 결론

본 논문에서는 [1]에서 제안된 가역 셀룰러 오토마타 기반 블록 암호 BCRCA에 대한 취약점 분석을 소개하였다. 본 논문의 결과는 통계 분석을 이용하여 제안 논문에서 제시한 안전성을 만족하지 못한다.

참 고 문 헌

[1] M. Seredynski, P. Bouvry, “Block Cipher based on Reversible Cellular Automata”, Proc. of CEC, pp. 2138-2143, 2004

[2] J. V. Neumann. The Theory of Self-Reproducing Automata. A. W. Burks (ed), Univ. of Illinois Press, Urbana and London, 1966.

[3] S. Wolfram "Cryptography with Cellular Automata", Advances in Cryptology - CRYPTO 85, LNCS Vol.218, pp.429-432, 1985.