로지스틱 맵을 활용한 Ping Pong 스트림 암호

김기환* · 이훈재*

*동서대학원 유비쿼터스 IT

**동서대학교 컴퓨터공학부

Ping Pong Stream cipher of Using Logistic Map

Ki-Hwan Kim* · Hoon-Jae Lee**

*Dept. of Ubiquitous IT Graduate School of Dongseo University

**Dept. of Computer Engineering, Dongseo University

E-mail : ghksdl90@naver.com, hjlee@dongseo.ac.kr

요 약

현대 컴퓨터 통신 및 저장 매체들은 대부분 암호화 기술을 지원하고 있다. 이 가운데 상당수의 Ping Pong 알고리즘은 LFSR 핵심구조로 난수를 발생하는 스트림 암호이다. LFSR은 주어진 크기의 최대 주기를 보장하는 구조를 가지고 있으나, 선형적인 구조를 가지고 있어 예측이 가능하다는 단점이 존재한다. 따라서 Ping Pong 알고리즘은 LFSR의 선형을 가변클럭과 함수를 통하여 비선형적인 구조로 만드는 특징을 가지고 있다. 본 논문에서는 LFSR의 선형적인 단점을 로지스틱 맵으로 치환하여 기존의 선형성을 개선해 보고자 한다.

ABSTRACT

Most modern computer communications and storage media support encryption technology. Many of the Ping Pong algorithms are stream ciphers that generate random numbers in the LFSR core structure. The LFSR has a structure that guarantees the maximum period of a given size, but it has a linear structure and can be predicted. Therefore, the Ping Pong algorithm has a feature of making the linearity of the LFSR into a nonlinear structure through variable clocks and functions. In this paper, we try to improve the existing linearity by replacing the linear disadvantages of LFSR with logistic maps.

키워드

Stream cipher, Ping Pong algorithm, LFSR, Logistic Map, randomness

Ⅰ. 서 론

컴퓨터는 정보화 사회에서 가장 중요한 요소에 해당하며 국가, 기업 및 개인의 정보를 저장하고 인터넷을 통해 빠르고 쉽게 전달할 수 있게 되었다. 이후 휴대성이 뛰어나고 다양한 기능을 제공하는 스마트폰을 계기로 일상생활 속에도 깊숙이 파고들어 왔다. 하지만 폭발적인 컴퓨터 사용에 비례하여 개인사진, 금융정보, 대화내용 등 타인에게 노출되지 말아야할 정보를 임의의 사람에게 전송될 일이 생겨나기 시작하였고 타인에게 노출을 막기 위하여 암호화가 도입되었다.

본 논문에서는 난수 발생기 구조를 가지는 카오스 시스템을 PingPong 알고리즘[1]과 로지스틱 맵[2]을 사용하는 것으로 비선형성 비트 스트림을 만들고자 한다.

II. 관련 연구

1.1.1. 스트림 암호

스트림 암호는 대칭 암호 알고리즘의 한 형태이며, 이는 블록 암호보다도 훨씬 빠르게 설계 될 수 있다. 블록 암호가 큰 블록의 데이터에 대하여 동작을 하는 반면에 스트림 암호는 비트 단위로 동작한다. 또한 키 스트림을 생성하고 암호화는 키 스트림과 해당 평문을 비트 단위로 배타적 논리합 연산에 의해 처리한다[3].

일반적으로 선형성은 취약점 회피와 LFSR에 계산된 수열 특성을 이용하기 위해 수열 발생기의 구성 요소로 LFSR을 사용하고, 비선형성은 조합함수, 필터링 함수 로 비선형 부울 함수를 사용하여 양쪽 모두 불규칙한 주기 LFSR을 사용한다[4].

1.1.2. 로지스틱 맵

카오스 이론은 자연계에 존재하는 일정한 규칙을 가진 불규칙해 보이는 현상을 연구하는 학문이다[3]. 카오스 이론을 이용하여 만든 카오스 시스템은 결정론적 시스템이라 할 수 있으며, 초기조건에 민감한 의존성을 가지고 있으며, 프랙탈 구조를 가지고 있다[5]. 카오스 맵에는 톱니맵, 텐트맵, 로지스틱 맵 이외에도 다양하게 존재한다.

로지스틱 맵(Logistic map)은 카오스 현상을 나타내는 비선형 차분방정식으로 2차 다항식으로 주어지는 이산 시간 동역학계[1]이다. 로지스틱 맵은 로지스틱 사상에 따르면, n+1번째 세대의 인구는 n번째 세대의 인구의 함수를 나타내며, 식(1)로 나타나며, $x_{n+1}=rx_n(1-x_n)$와 같은 성질을 보인다.

표 1. 로지스틱 맵의 r값에 따른 주기 변화

r값 범위	x결과
$0 \le x_n \le 1$	0
$1 \le r < 3$	$1-1/r$
$r=3$	$1-1/3$
$3 < r < 1+\sqrt{6}$	거의 모든 초기주기=2
$1+\sqrt{6} < r < 3.54409$	거의 모든 초기 조건 주기=4
$3.54409 < r < 3.56995$	거의 모든 초기 조건 주기=2^n
$3.56995 \le r < 4$	혼돈, 무한한 주기
$r=4$	혼돈, 해석적으로 풀 수 있음
$r > 4$	거의 모든 초기 조건 $\pm\infty$

1) 수학 또는 물리학의 한 분야로서 시간에 따른 움직임의 과정으로 정의된다.

[표 1]과 같이 개체 수가 매우 작다면 ($0 \le X_n \ll 1$), 개체 수는 매개 변수 r에 따라 기하급수적으로 증가하거나 ($r > 1$) 감소한다. 개체 수가 최댓값 x=1에 매우 가깝다면, 개체 수는 과밀도로 인하여 급격히 감소한다.

로지스틱 맵을 [그림 1]의 구조로 만들고 예측이 가능한 정수와 20비트이하의 소수값을 제외하기 위하여 부호, 정수, 소수0, 소수1 등 4개의 블록으로 나누어 소수1의 32비트만 사용하였다[7].

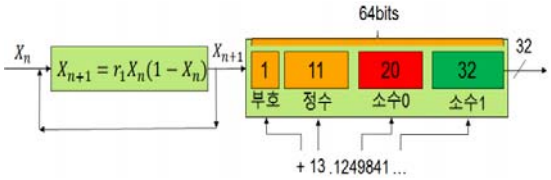

그림 1. 로지스틱 맵의 결과로 사용하는 영역을 분류

1.1.3. 난수 검증방식

스트림 암호의 난수 발생기는 통계적 테스트를 통해 무작위성을 판별한다. 하지만 모든 테스트가 수학적인 증명을 의미하지는 않으며, 단지 통계적 근거를 활용하여 초기값에 대한 결과를 사실로 보여주기 때문이다. 이를 증명하기 위하여 정규분포를 활용하며, 난수 검증 항목으로 빈도 검증, 계열검증, 포커 검증, 자기상관성 검증, 런 검증 등이 존재한다[8].

III. 난수성 검증 실험

로지스틱 맵은 64비트 레지스터에서 1라운드당 32비트 레지스터의 출력과 비교하여 LFSR은 1라운드당 1비트 레지스터의 출력을 가지고 있다. 따라서 기존의 Ping Pong 알고리즘의 1비트 입·출력 구조를 32비트 입·출력 구조로 변경해야할 필요성이 있다. [그림 2]의 Ping Pong 알고리즘은 총 128비트의 입력 레지스터와 상태를 저장하는 C_{j-1}와 D_{j-1}에서 각각 32비트로 구성되어 총 192비트의 레지스터에 32비트의 출력을 가진다.

본 논문에서 사용한 자기상관성 검증 기준값은 가우시안 분포에서 5%이내의 값을 허용한 수치이다. 2개의 로지스틱 맵을 활용한 Ping Pong 알고리즘은 3 회 실시하였다. 난수 검증에는 총 2,457,600비트를 사용하고 로지스틱 맵 초기값은 $Logistic\,Map_a$의 $x1=0.0002$, $Logistic\,Map_b$의 $x2=0.00003$ 만큼 증가시켜 서로 다른 초기값을 사용하였다. 실험 결과 [표 2]와 같이 총 3회의 서로 다른 초기값을 대입한 결과는 빈도 검증, 계열 검증, 일반적인 계열 검증, 포커 검증, 자기상관성 검증, 런 검증 등 5가지 검증 모두 하였다.

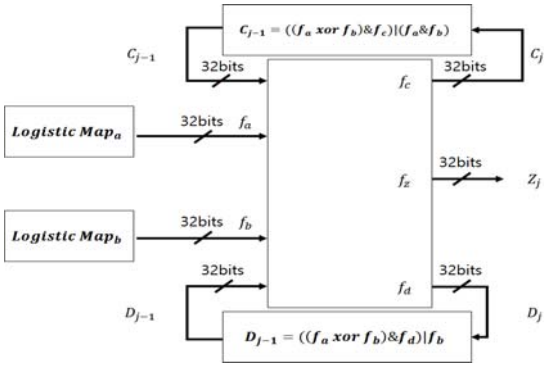

그림 2. 2개의 로지스틱 맵을 사용한 Ping Pong 알고리즘

표 2. 2개의 로지스틱 맵을 사용한 Ping Pong 알고리즘 난수 검증 결과

r1=3.999, r2=3.9999, 전체 실험 길이 : 2,457,600 비트, x1=0.7861 (0.0002씩 증가), x2=0.859167 (0.00003씩 증가)				
검증	허용값	실험 1	실험 2	실험 3
빈도	3.841	0.784	2.759	0.844
계열	5.991	0.845	3.073	2.352
일반적인 계열				
t=3 t=4 t=5	9.488 15.507 26.296	4.651 11.112 14.650	6.822 7.454 17.325	8.499 12.462 17.056
포커				
m=3 m=4 m=5	14.067 24.996 44.654	6.368 14.161 31.945	6.950 17.907 32.757	10.088 12.945 22.624
자기상관성	m ≤ 0.05	0.002753	0.002982	0.00311
런	p > 0.01	0.800961	0.576845	0.219434

1.1.4. 난수 검증방식

[그림 2]와 같은 구조가 난수 발생기로 사용이 가능함을 확인하였고 이를 토대로 비선형함수(F)의 구조에 의존적인지 확인하기 위하여 [그림 3]의 Ping Pong 알고리즘은 총 128비트의 입력 레지스터와 비선형함수(F) C_{j-1}와 D_{j-1}에서 각각 32비트로 구성되어 총 192비트의 레지스터에 32비트의 출력을 가진다. 난수 검증에는 총 2,457,600비트가 사용되었으며, 각각의 로지스틱 맵은 서로 다른 초기값을 사용하였다. 실험 결과 [표 3]과 같이 5가지의 실험 모두 만족하는 것을 확인할 수 있었다. 기존의 Ping Pong 알고리즘은 주기가 큰 것이 특징이며, 자기상관성이 작은 것이 단점인 것을 본 실험을 통하여 개선할 수 있음을 확인 할 수 있었다.

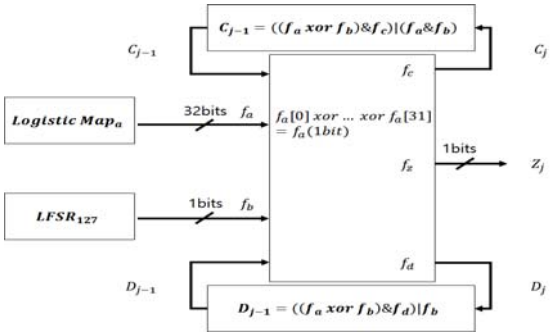

그림 3. 로지스틱 맵과 LFSR을 조합한 Ping Pong 알고리즘

표 3. 2개의 로지스틱 맵을 사용한 Ping Pong 알고리즘 난수 검증 결과

r1=3.999, 전체 실험 길이 : 2,457,600 비트, x1=0.7861 (0.0002씩 증가)				
검증	허용값	실험 1	실험 2	실험 3
빈도	3.841	1.774	7.239	0.002
계열	5.991	1.776	7.631	0.060
일반적인 계열				
t=3 t=4 t=5	9.488 15.507 26.296	5.598 7.743 21.641	8.297 12.451 31.346	3.523 6.825 17.299
포커				
m=3 m=4 m=5	14.067 24.996 44.654	10.601 7.680 30.088	11.413 14.723 58.692	2.923 13.642 33.627
자기상관성	m ≤ 0.05	0.0029	0.0036	0.0029
런	p > 0.01	0.9614	0.5341	0.8095

실험결과 [표 3]과 같은 결과를 확인하였다. 빈도 검증 측정값은 1.774로 기준값 3.841보다 작아 통과했고, 계열 검증도 1.776으로 5.991보다 작아 통과했고, 확장 계열 검증도 t=3,4,5일 때 각각 측정값이 5.598, 7.743, 21.641로 기준값 9.488, 15.507, 26.296보다 작아 통과하였다. 포커 검증도 m=3,4,5일 때 각각 측정값이 10.601, 7.680, 30.088로 기준값 14.067, 24.996, 44.654보다 작아 통과했고, 자기상관성 검증도 0.0029로 기준값 0.05보다 작아 통과하였고 마지막으로 런 검증도 0.9614로 0.01보다 큰 값으로 통과하였다.

로지스틱 맵과 LFSR Ping Pong 알고리즘의 초기값은 0.0002 증가시키고 LFSR은 동일한 값으로 실험을 진행하였다. 그 결과 실험 2 빈도 검증에서 '0'이 '1'보다 많이 확인되었으며, 기준값 3.841

을 초과하는 7.239를 기록했다. 계열 검증에서 '0'에서 '0'으로 변화된 수치가 상대적으로 높게 측정되어 기준값 5.991을 초과한 7.631을 기록하는 결과를 보였다. 또한 확장 계열 검증 및 포커 검증에서 모두 기준값을 초과하는 값을 나타내었다. 이는 초기값의 변화에 민감하게 반응하는 것으로 보이며, 외부의 공격에서 빈도 공격에 취약할 수 있는 부분으로도 해석된다. 하지만 이는 다양한 초기값에 따른 실험을 통해 평균적인 수치로 해석되어야 할 필요성이 존재한다.

실험 3은 실험 1과 같이 모든 난수 검증을 통과하였고 특히 상당히 낮은 수치로 통과하여 인상적인 모습을 보였다.

Ⅳ. 결론

본 논문에서는 스트림 암호인 Ping Pong의 선형 귀환 이동 레지스터를 카오스 맵에 해당하는 로지스틱 맵을 사용하여 실험해보았다. 서로 다른 계수를 가진 카오스 맵은 초기값에 민감한 특성을 나타내었다. 하지만 선형 귀환 이동 레지스터와 로지스틱 맵을 병행하여 사용할 경우 일부 실험에서 난수성에 문제가 있음을 발견 하였다. 해당 하는 문제점의 원인은 차후 연구를 통해 확인해야할 부분으로 보인다. 하지만 본 논문을 통하여 선형 귀환 이동 레지스터의 선형성을 로지스틱 맵으로 대체하여도 난수성에 큰 문제가 없음을 확인하였다. 특히 로지스틱 맵을 활용하여 앞으로 다양한 구조를 설계하고 검증하는 것으로 다양한 카오스 맵을 활용한 연구에 좋은 영향이 될 것이라 생각한다.

감사의 글

이 논문은 2016년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호: NRF-2016R1D1A1B01011908). 또한 부산광역시에서 지원하는 BB21 과제에서 지원받았음.

참고문헌

[1] KiHwan Kim, Mohammed Abdulhakim Alabsi, Hyotaek Lim, HoonJae Lee, "Ping-Pong 256 using the Tap 16 of the LFSR 255/257", MITA, 2016.

[2] 위키백과, 로지스틱 사상, https://ko.wikipedia.org/wiki/%EB%A1%9C%EC%A7%80%EC%8A%A4%ED%8B%B1_%EC%82%AC%EC%83%81

[3] Stallings, William, "Cryptography and network security: principles and practices", Pearson Education India, 2006.

[4] P. Kitsos, N. Sklavos, K. Papadomanolakis and O.Koufopavlou, "Hardware Implementation of Bluetooth Security", IEEE Pervasive Computing, vol. 2, no. 1, pp. 21-29, Jan.-Mar. 2003.

[5] 정성용, 김태식, "카오스 이론을 이용한 암호화 기법.", 한국정보과학회 1998 년도 가을 학술발표논문집, 제25권 제2호, pp45-47, 1998.

[6] 위키백과, "Gamma function", https://en.wikipedia.org/wiki/Gamma_function.

[7] François, Michael, David Defour, and Christophe Negre, "A fast chaos-based pseudo-random bit generator using binary64 floating-point arithmetic", Informatica, vol.38 Issue2, pp115-124, Jun 2014.

[8] AndrewRukhin,JuanSoto,JamesNechvatal,Miles Smid,ElaineBarker,Stefan Leigh,MarkLevenson,Mark Vangel,DavidBanks,AlanHeckert,JamesDray,SanVo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology, April. 2010.