제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

적응적 임계값을 이용한 개선된 카오스 키 수열 생성 기법

정성용
대구보건대학 컴퓨터정보기술계열
syjung@mail.thc.ac.kr

Improved Keystream Generation Method on Chaos Theory Using Accord Threshold

Sungyong Jung
Department of computer information, Taegu Health Collage

요 약

스트림 암호 시스템에서는 비선형 결합 LFSR 키 수열을 이용하였다. 주기가 존재하고 상관관계 공격에 약한 비선형 LFSR 키 수열의 문제를 개선하기 위해 제안된 카오스 키 수열은 균형성과 랜덤특성을 만족하지 못하고 있다. 따라서, 본 연구에서는 적응적 임계값 적용 방법을 이용하여 균형성과 랜덤특성을 만족하는 카오스 키 수열 생성 기법을 제안하였다.

본 연구에서 제안한 키 수열 생성 기법은 로지스틱 방정식을 이용하여 키 수열 생성을 위한 카오스 신호를 만든 다음 카오스 신호를 적응적 임계값 적용방법을 통해 '0'과 '1'로 양자화하여 키 수열을 생성한다.

제안한 알고리즘으로 생성된 키 수열의 특징을 분석한 결과 균형성과 랜덤특성이 기존의 카오스 키 수열에 비해 개선되었음을 알 수 있다.

1. 서론

비밀키 암호 알고리즘(symmetric cryptography)의 경우 인증, 키 관리, 키 분배 등 몇가지 문제를 갖고 있기는 하지만 공개키 암호 알고리즘(asymmetric cryptography)보다 키의 길이가 짧아 암호화 및 복호화 시간이 짧아지는 이점을 갖고 있다. 반면 공개키 암호 알고리즘은 비밀키 암호 알고리즘에서처럼 키의 관리를 위해 키 분배 센터를 두지 않고도 키를 안전하게 관리 할 수 있는 이점을 갖고 있다[1][2].

스트림 암호 시스템은 블록 암호 시스템에 비해 에러의 확산이 없고, 비도 수준과 관련된 여러 가지 중요한 수치에 대한 정량화가 가능하며, 하드웨어나 소프트웨어로 구현이 용이하고, 통신 지연이 없으며, 고속 통신이 가능한 등 여러 가지 장점을 지니고 있어 안전한 암호 시스템을 설계하기에 적당하다.

일반적으로 암호 시스템의 안전성에 대한 측도로 이용되는 비도(security level)는 키의 크기와 임의성 및 주기성, 선형 복잡도 등에 크게 좌우되는데, 스트림 암호 시스템에서는 키 수열의 발생을 위해 지금까지 선형 귀환 쉬프트 레지스트(Linear Feedback Shift Register; LFSR)가 일반적으로 이용되어 왔다. 그러나, LFSR에의해 2^n-1 주기를 갖는 키 수열은 Berlekamp-massey 알고리즘[3]을 이용한 알려진 평문 공격에 의해 해독된다고 알려져 있으며, 키 수열이 Berlekamp-massey 알고리즘에 의해 해독되는 단점을 개선하기 위해 LFSR에 의해 출력되는 수열을 비선형 결합하여 키 수열을 생성하는 연구가 있어 왔다. 그러나, LFSR에 의해 출력되는 수열이 비선형 결합 함수와 상관관계(correlation)가 있을 경우 이 성질을 이용하면 키 수열을 쉽게 찾을 수 있는 상관 공격법에 의해 해독된다고 알려져 있어[4], LFSR의 비선형 결합을 이용하지 않고 스트림 암호 시스템의 키 수열에 대한 안전성을 높일 수 있는 방법에 대한 연구가 필요하게 되었다.

LFSR의 비선형 결합을 이용하지 않고 상관 공격에 안전한 키 수열 생성 방법의 하나로 최근 비선형 함수의 대표적 알고리즘으로 다양한 분야에서 응용되고 있는 카오스 이론(Chaos Theory)을 이용한 '카오스 암호 시스템'에 관한 연구가 늘어나고 있다.

본 연구에서는 기존의 카오스 키 수열 생성기를 개선하여, 비선형 결합 LFSR 키 수열 생성기가 갖고 있는 주기성과 상관관계 문제를 해결하고, 적응적 임계값 적용을 통해 균형성과 랜덤 특성이 보장되는 개선된 카오스 키 수열 생성 알고리즘을 제안하고자 한다.

2. LFSR 키 수열 생성기

일반적으로 스트림 암호 시스템에서는 대부분 비선형 결합 LFSR 키 수열 생성기를 이용하여 랜덤 특성이 양호하고, 주기와 선형 복잡도가 우수한 것으로 평가된다. 그러나, 이들 키 수열 생성기가 Berlekamp-massey 알고리즘[5]을 이용한 알려진 평문 공격에 의해 해독되는 단점을 개선하기는 하였으나, LFSR에 의해 출력되는 키 수열에 비선형 결합 함수와의 상관관계(correlation)가 존재하므로 이 성질을 이용한 상관 공격법에 의해 해독될 수 있다[6].

따라서, 상관공격에 강한 비선형 결합 LFSR 키 수열 생성기를 개발하기 위한 다양한 형태의 연구가 이루어지고 있다[7][8][9]. 그러나, 이 같은 연구에서 키 수열의 주기와 상관관계가 개선되었지만 여전히 키 수열의 주기와 상관관계로 인한 문제를 갖고 있어, 카오스를 이용한 키 수열 생성 기법을 통해 비선형 결합 LFSR 키 수열 생성기의 문제를 해결할 수 있을 것으로 기대하고 있다.

3. 카오스 암호화

3.1 카오스 이론의 개요

로렌츠(Lolenz)의 로렌츠는 '초기값의 민감한 의존성'에 대해 '나비효과'를[10] 밝힌 이후 자연의 복잡성 속에 숨어 있는 규칙성 및 질서를 찾아내고자 하는 노력이 매우 활발해 지고 있다.

1975년에 요크(York)와 이천암(Li)은 "Period Three Implies Chaos"라는 제목의 논문[11]을 발표하였고, 이 논문에서 카오스는 "결정적 비선형 동적 시스템에서의 복잡한 현상"이라고 정의하였다. 또한 로버트 메이(Robert May)는 1976년에 생물의 개체수 변동을 수학적으로 처리함으로서 카오스의 응용 분야가 더욱 확대되는 기틀을 마련하였다. 네이춰지에 발표된 메이의 논문[12]에서 그는 매우 복잡한 동적 시스템을 간단한 수학적 모델인 로지스틱 방정식을 제안하였고 이 간단하고 단순한 방정식에서 나온 해답이 카오스적인 의미를 갖는다고 하였다. 본 연구에서는 로버트 메이의 로지스틱 방정식을 이용한 키 수열 생성 기법을 제안하고자 한다.

3.2 로지스틱 방정식

로버트 메이가 시간의 변화에 따른 동물의 개체수 변화를 구하는 간단한 식을 통하여 이천암과 요크의 논문의 구체적인 연구 결과를 발표하였다. 이에 의하면 개체수 변화는 현재의 개체수와 증가율, 그리고 자연 감소율 등을 종합해서 다음 단계의 개체수를 계산하는데 다음과 같이 나타낼 수 있다.

$$X_{n+1} = \alpha X_n(1-X_n) \quad 단,\ 1<=\alpha<=4.\ 0<=X_n<=1$$

α는 개체의 증가량을 나타내는 증가율이며, X_n은 현재 개체수, X_{n+1} 은 다음의 개체수이다. 로지스틱 방정식에서 X_n 에서 X_{n+1} 로의 변화를 로지스틱 맵(Logistic Map)이라 한다. α의 값이 크다면 개체수가 적을 때는 빠른 속도로 증가하고 많은 개체는 빠른 속도로 감소함을 나타낸다.

이러한 개체수의 변화는 증가율 α의 값에 따라 다른 양상을 나타내는데, 증가율 α의 범위가 3.5699456... < α < 4 일때 개체수 Xn의 변동은 카오스적으로 나타나는 특성이 있다.

3.3 카오스 암호화

카오스를 이용한 암호 시스템과 암호 응용에 관한 연구는 암호화 통신, 영상 암호화를 비롯한 여러 분야에서 활발하게 진행되고 있으나, 암호 시스템의 안정성을 보장하는 키 수열 생성 알고리즘에 관한 연구는 대부분 암호 시스템 연구의 일부분으로 진행되어 왔으며, Bianco[13], Gao[14], Kohda[15] 등의 알고리즘을 살펴볼 때 키 수열 검증 및 개선의 필요성이 보인다.

4. 개선된 카오스 키 수열 생성 기법

4.1 적응적 임계값 적용방법

본 연구에서는 기존의 방법을 개선한 적응적 임계값 적용방법은 카오스 신호의 이진화에 사용되는 임계값이 이진 단계에서 생성된 키 수열의 특성에 기초하여 적응적으로 변화함으로서, 키 수열의 균형성과 랜덤특성을 개선 할 수 있도록 하는 방법이다. 적응적 임계값 적용방법은 임계값이 알고리즘에 의해 정의되면서도 다음 단계의 키 수열 생성에 필요한 임계값을 최적의 조건에서 설정되도록 할 수 있는데, 적응적 임계값 적용방법에 대해 자세히 살펴보면 다음과 같다.

첫째, 카오스 신호의 일반적인 평균값을 이용하여 카오스 신호를 이진화한다.

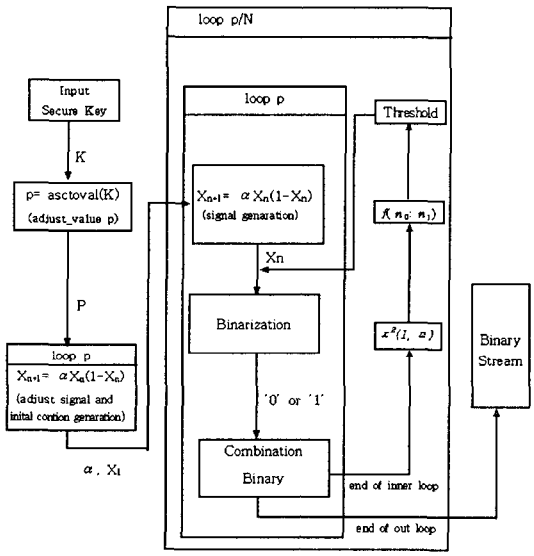
둘째, 다음 단계의 임계값 설정에 중요한 역할을 하게 되는 부분 키 수열의 길이는 안정화 변수 p를 활용하여 처음 p 길이 만큼의 부분 키 수열을 생성한다.

셋째, 생성된 부분 키 수열의 랜덤특성을 평가한다. 이때 랜덤특성이 통계적 검증값을 만족하면 부분 키 수열을 생성할 때 사용된 임계값은 그대로 유지되며, 통계적 검증값을 만족하지 못하면 임계값을 0.05 가감하여 다음 p길이 만큼의 부분 키 수열을 생성하는 과정을 반복하여 전체 키 수열을 생성한다.

넷째, 부분 키 수열의 랜덤특성 검증결과가 기각역에 포함되면 다음단계의 키 수열 생성을 위한 임계값은 적응적

으로 변화한다. 임계값의 적응적 변화량은 시험 통계량 x^2이 기각역 3.841이내일 경우 이전의 임계값을 다음 단계에서 그대로 유지하도록 하고, 기각역 3.841보대 클 경우 '0'과 '1'의 개수에 따라 '0'의 수가 많을 경우 임계값은 0.05감소하고 '1'의 수가 많을 경우 임계값은 0.05증가하여 p길이 만큼의 다음부분 수열을 생성하기 위한 이진화에 적용한다.

적응적 임계값을 적용하여 키 수열을 생성하는 과정을 도식화하면 (그림 4-1)과 같다.



(그림 4-1) 적응적 임계값 적용방법을 이용한 키 수열 생성 과정

4.2 실험 및 평가

제안된 알고리즘이 키 수열이 암호학적으로 좋은 균형성과 랜덤특성을 보이는지를 확인하기 위한 실험은 PC(Pentium IV, 1Ghz)에서 Tubro C를 이용하여 1,048,576 bit의 표본 키 수열을 서로 다른 초기조건 상태에서 키 수열을 생성하였으며, 이를 Rueppel, Bianco, Gao, Kohda 등의 알고리즘과 비교 분석하였다.

본 논문에서 제안된 알고리즘 의존적 임계값 적용방법은 알고리즘 실행시 임의의 임계값을 지정하지 않고 알고리즘에 의존해 설정되므로, 입력값의 수를 줄일 수 있으며, 대부분의 경우 유사한 수준의 균형성과 랜덤특성을 보이고 있어 기존의 방법에서 발생하는 문제점을 개선한 효과가 있음을 알 수 있다.

동일한 조건에서 30회에 걸친 실험에서 Rueppel, Bianco, Gao Zhenyu, Kohda 등의 키 생성 알고리즘과 제안된 알고리즘을 대상으로 실시한 실험결과는 <표 4-1>과 같다.

5. 결 론

LFSR을 이용한 스트림 암호 시스템의 경우 상관 공격법 등에 의해 해독이 가능하여, 최근 LFSR의 비선형 결합을 이용하지 않고 상관 공격에 안전한 키 수열을 생성하기 위한 방법의 하나로 카오스 이론을 이용한 카오스 키 수열 생성 기법에 관한 연구가 늘어나고 있다.

본 연구에서는 기존의 카오스 키 수열 생성기들이 균형성과 랜덤특성에 문제가 있음을 지적하고, 이를 실험을 통해 확인하였으며, 균형성과 랜덤특성을 개선하기 위해 적응적 임계값 적용을 통한 개선된 키 수열을 생성 기법을 제안하고 분석하였다.

횟수	LFSR	기존의 카오스 키 수열 생성기			제안된 방법
	Rueppel	Bianco	Gao Zhenyu	Kohda	
1	0.4992:0.5008	0.3921:0.6079	0.5000:0.5000	0.5464:0.4536	0.5007:0.4993
2	0.4992:0.5008	0.2363:0.7637	0.4396:0.5604	0.5465:0.4535	0.5005:0.4995
3	0.4992:0.5008	0.4112:0.5888	0.4421:0.5579	0.5465:0.4535	0.4996:0.5004
4	0.4992:0.5008	0.4413:0.5587	0.5527:0.4473	0.5464:0.4536	0.4996:0.5004
5	0.4992:0.5008	0.4194:0.5806	0.4709:0.5291	0.5464:0.4536	0.5004:0.4996
6	0.4992:0.5008	0.3484:0.6516	0.3780:0.6220	0.5464:0.4536	0.5006:0.4994
7	0.4992:0.5008	0.4618:0.5382	0.5000:0.5000	0.5464:0.4536	0.5001:0.4999
8	0.4992:0.5008	0.5000:0.5000	0.6667:0.3333	0.5464:0.4536	0.5001:0.4999
9	0.4992:0.5008	0.0625:0.9375	0.5770:0.4230	0.5465:0.4535	0.4999:0.5001
10	0.4992:0.5008	0.2541:0.7459	0.5738:0.4262	0.5465:0.4535	0.4998:0.5002
11	0.4992:0.5008	0.1188:0.8812	0.5833:0.4167	0.5464:0.4536	0.4996:0.5004
12	0.4992:0.5008	0.3306:0.6694	0.5470:0.4530	0.5464:0.4536	0.4995:0.5005
13	0.4992:0.5008	0.3990:0.6010	0.4548:0.5452	0.5464:0.4536	0.5001:0.4999
14	0.4992:0.5008	0.4372:0.5628	0.5482:0.4518	0.5464:0.4536	0.4995:0.5005
15	0.4992:0.5008	0.4836:0.5164	0.4772:0.5228	0.5465:0.4535	0.4998:0.5002
16	0.4992:0.5008	0.2159:0.7841	0.4462:0.5538	0.5465:0.4535	0.5008:0.4992
17	0.4992:0.5008	0.3770:0.6230	0.5024:0.4976	0.5465:0.4535	0.4998:0.5002
18	0.4992:0.5008	0.3812:0.6188	0.3517:0.6483	0.5464:0.4536	0.5009:0.4991
19	0.4992:0.5008	0.4672:0.5328	0.5611:0.4389	0.5464:0.4536	0.5004:0.4996
20	0.4992:0.5008	0.3948:0.6052	0.6667:0.3333	0.5464:0.4536	0.4999:0.5001
21	0.4992:0.5008	0.2828:0.7172	0.3483:0.6517	0.5465:0.4535	0.4994:0.5006
22	0.4992:0.5008	0.3443:0.6557	0.4406:0.5594	0.5465:0.4535	0.4992:0.5008
23	0.4992:0.5008	0.2281:0.7719	0.4031:0.5969	0.5465:0.4535	0.5006:0.4994
24	0.4992:0.5008	0.2637:0.7363	0.5351:0.4649	0.5464:0.4536	0.4997:0.5003
25	0.4992:0.5008	0.2773:0.7227	0.3309:0.6691	0.5464:0.4536	0.4996:0.5004
26	0.4992:0.5008	0.2050:0.7950	0.5439:0.4561	0.5464:0.4536	0.4997:0.5003
27	0.4992:0.5008	0.4194:0.5806	0.5546:0.4454	0.5465:0.4535	0.5002:0.4998
28	0.4992:0.5008	0.4112:0.5888	0.4845:0.5155	0.5465:0.4535	0.5000:0.5000
29	0.4992:0.5008	0.4645:0.5355	0.4331:0.5669	0.5465:0.4535	0.5002:0.4998
30	0.4992:0.5008	0.4413:0.5587	0.5257:0.4743	0.5465:0.4535	0.4997:0.5003
평균	0.4992:0.5008	0.3490:0.6510	0.4946:05034	0.5464:0.4536	0.5000:0.5000

<표 4-1> 실험결과 비교

횟수	LFSR	기존의 카오스 키 수열 생성기			제안된 방법
	Rueppel	Bianco	Gao Zhenyu	Kohda	
1	2.3747	48,813.3789	0.0000	856.7656	2.1059
2	2.7691	291,555.7048	15,295.6989	858.9952	1.1708
3	2.3687	33,069.9908	14,057.0664	858.2520	0.8213
4	2.7691	14,469.9284	11,629.4319	856.7656	0.8213
5	2.3687	27,216.6217	3,546.0629	854.5362	0.7021
6	2.7691	96,426.0182	62,384.8187	855.6509	1.6718
7	2.3747	6,132.2359	0.0000	855.2793	0.0352
8	2.7561	0.0047	116,506.2222	856.7656	0.0352
9	2.3868	892,816.0000	24,851.1824	859.7385	0.0250
10	2.7432	253,594.8622	22,829.9115	859.3668	0.1635
11	2.3928	609,332.7009	29,107.5588	854.9078	0.7554
12	2.7432	120,354.7874	9,257.6720	854.5362	0.9084
13	2.3989	42,815.0458	8,573.6025	853.7932	0.0496
14	2.7367	16,551.4256	9,741.5358	856.7656	1.1539
15	2.3989	1,124.0828	2,175.1667	858.9952	0.1572
16	2.7302	338,639.8880	12,139.9939	857.8804	2.4659
17	2.3989	63,408.5515	23.6705	857.8804	0.2143
18	2.7302	59,200.9727	92,217.7939	854.9078	3.1729
19	2.4110	4,502.3576	15,673.3772	854.5362	0.5625
20	2.7173	46,408.2672	116,507.5556	854.5362	0.0250
21	2.4171	197,918.9790	96,565.5625	857.5088	1.7278
22	2.7238	101,676.2833	14,791.6904	858.6236	2.4782
23	2.4110	309,974.9121	39,378.9917	859.3668	1.6018
24	2.7173	234,286.2510	5,166.2964	854.1647	0.4567
25	2.4110	208,007.2561	119,914.7621	854.1647	0.5422
26	2.7173	365,108.6212	8,068.3903	853.7932	0.2843
27	2.4110	27,253.3668	12,502.4719	857.1372	0.0977
28	2.7302	33,053.6546	1,001.9945	858.9952	0.0000
29	2.4110	5,203.6093	18,749.7393	858.2520	0.0977
30	2.7238	14,473.6878	2,764.4592	858.6236	0.2843
평균	2.5671	145,782.6512	29,514.0893	856.7162	0.8196

키 수열 생성 기법에서 키 수열 생성을 위해 카오스 함수에서 사용 할 수 있는 초기조건 생성 알고리즘을 새로이 제안하였으며, 카오스 신호를 '0' 또는 '1'로 양자화 할 때 적응적 임계값을 적용하는 방법을 이용하여 키 수열의 균형성과 랜덤 특성을 개선하였다. 제안된 기법으로 키 수열을 생성하고, 생성된 키 수열에 대해 균형성과 랜덤 특성을 평가한 결과 균형성은 "0"과 "1"이 0.5:0.5에 가깝게 발생하였으며, 랜덤특성은 유의수준 내에서 시험통계량을 통과하는 우수한 특성이 있음을 확인하였다.

앞으로 카오스 키 수열에 대한 응용 연구와 키 수열의 안전성에 대한 수학적 검정에 대한 연구가 요구된다.

참고문헌

[1] ETRI, *현대 암호학*, 1995.

[2]) 김철, 암호학의 이해, (주)영풍문고, 1996

[3] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Trans. on Infor. Theory*, Vol. IT-15, No. 1, pp. 122-127, Jan. 1969.

[4] T. Siegenthaler, "Cryptanalyst's representation of nonlinearity filtered m-sequences", Lecture Notes in computer Science 219. pp103-110, Berlin : Springer-Verlag, 1985

[5] J. L. Massey, "Shift-Register Synthesis and BCH Decoding," *IEEE Trans. on Infor. Theory*, Vol. IT-15, No. 1, pp. 122-127, Jan. 1969.

[6] T. Siegenthaler, "Cryptanalyst's representation of nonlinearity filtered m-sequences", Lecture Notes in computer Science 219. pp103-110, Berlin : Springer-Verlag, 1985

[7] 이훈재, 문상재, "2비트 메모리를 갖는 개선된 합산 수열 발생기," 한국정보보호학회논문지, 제7권, 제2호, pp. 93-106, 1997년 6월.

[8] 이상진, 지성택, 김용대, 고승철, "상관관계 공격에 안전한 합산 키 수열생기," 한국통신정보보호학회 논문지, 제5권, 제2호, pp. 15-22, 1995년 6월.

[9] 이훈재, 문상재, "다수열 출력 이진 수열 발생기," 한국정보보호학회 논문지, 제7권, 제3호, pp.11-22, 1997년 9월.

[10] 아이하라 키즈유키, '쉽게 읽는 카오스', 한뜻출판사, pp89-100, 1995

[11] T.Y. Li and J.A. Yorke,"Period three implies Chaos", America, Math, Monthly, 82, pp985-992, 1975

[12] R.M. May,"Simple mathematical models with very complicated dynamics", Nature, 261, pp457-461, 1976

[13] Bianco M. E., (et al), *Encryption System based on Chaos Theory*, United States Patent no. 5048086, Sep. 1991

[14] Gao Zhenyu, *Method and apparatus for encrypting and decrypt-ing information using a digital chaos signal* , United States Patent no. 5696826, 9 Dec. 1997

[15] Kohda Tohru, Akio Tsuneda, *Encryption/Decryption appparatus and method incorporating random variable and keystream genetation*, United States Patent, No.6014445, 11. Jan. 2000.