카오스 특성을 이용한 스트림 암호 시스템의 키 수열 생성 기법

정성용 (계명대학교 대학원 컴퓨터공학과)
김태식 (계명대학교 공과대학 컴퓨터전자공학부 교수)

1. 개 요

카오스 이론은 짧은 역사 속에서 관련된 분야의 학자들이 많은 연구를 하여 왔으며, 그 응용분야가 점차 확대되어 가고 있다. 최근 컴퓨터의 처리 능력 향상과 인공지능의 학문적인 이론 및 응용기술의 발달은 카오스 이론이 공학 분야에 새롭게 등장 할 수 있도록 하였다. 카오스 이론의 응용분야로는 비선형 회로에서의 카오스, 유체와 기체의 진동에서 발견되는 카오스(Acoustic Chaos), 광학에서의 카오스, 맥파, 뇌파, 심전도 등과 같은 생체 카오스, 주가지수와 같은 경제학에서의 카오스 등 매우 다양하다.

카오스 이론의 공학적인 응용 또한 활발히 이루어지고 있으며, 카오스 이론과 신경 회로망(Neural Networks)의 결합이나 유전자 알고리즘(Genetic Algorithms)과의 결합을 시도하는 연구로 순회 방문 세일즈맨 문제와 같은 NP문제와 화상처리 등 새로운 분야에 대한 카오스 이론의 응용 사례가 늘어나고 있는 실정이다[1].

카오스 현상은 복잡하고 불규칙해 보이는 현상 속에 의외로 단조로운 모델로 나타날 수 있는데, 이 같은 점이 카오스 이론에 대한 응용 분야의 확대, 특히 공학적 이용가치를 한층 더 높이는 근거가 되고 있으며, 최근 암호화에 관련된 연구 또한 지속적으로 증대되고 있다[2,3,4,5,6].

카오스 이론의 새로운 응용분야로 대두되고 있는 카오스 암호 기술은 카오스 신호를 이용하여 정보를 암호화하는 기술로서 암호화 및 복호화 단계가 카오스적이라는 본질적 이유 때문에 수학적 방식으로는 풀리지 않는다고 알려져 있으며, 카오스 암호 기술이 보다 안전하다는 예측을 하고 있다[7].

일반적으로 암호 시스템의 안전성에 대한 측도로 이용되는 비도(security level)는 키의 크기와 임의성 및 주기성, 선형 복잡도 등에 크게 좌우되는데, 스트림 암호 시스템은 특히 키의 영향을 많이 받는 암호 시스템중의 하나이다. 따라서, 안전한 스트림 암호 시스템을 위한 키 수열 생성 알고리즘 설계에 대한 연구가 있어 왔다[8.9].

초기 조건에 민감한 의존성을 보이고 있는 카오스는 그 특성상 주기가 존재하지 않을 뿐 아니라 예측할 수 없는 형태를 보이므로 카오스 특성을 암호 시스템에 적용한다면 암호 시스템의 비도를 높일 수 있는 효과적인 수단이 될 수 있을 것이다. 본 연구에서는 카오스 이론과 카오스 특성에 대해 고찰하고,, 카오스 특성을 이용한 스트림 암호 시스템을 위한 키 수열 생성 기법을 제안하고자 한다.

2. 스트림 암호 시스템

2.1 스트림 암호 시스템의 특징

일반적으로 암호 알고리즘은 암·복호화에 사용되는 키의 특성에 따라 암·복호화 키가 같은 비밀키 암호 알고리즘과 암·복호화 키가 서로 다른 공개키 암호 알고리즘으로 크게 구분할 수 있다. 비밀키 암호 알고리즘은 데이터 처리 형식에 따라 스트림 암호 알고리즘과 블록 암호 알고리즘으로 나눌 수 있다. 공개키 암호는 비밀키 암호에서의 문제점들을 해결하고자 하는 시도로부터 발전된 개념이다.

현재 가장 널리 사용되는 비밀키 암호 기법은 1977년 미국 표준국(NBS : National Bureau of Satandard, 현 NIST의 전신)에 의해 미 연방정보처리표준46(FIPS PUB46)으로 채택된 DES[10]에 기초를 두고 있다. 그리고 공개키 암호의 가장 대표적인 RSA[11] 암호는 MIT의 R. Rivest, A. Shamir, 그리고 L. Adleman에 의해 1978년에 개발되었다. RSA 암호는 현재 가장 널리 사용되고 있는 공개키 암호로 알려져 있다.

비밀키 암호 알고리즘의 하나인 스트림 암호는 블록 암호에 비해 에러의 확산이 없고, 비도 수준에 대한 정량화가 가능하며, 하드웨어나 소프트웨어로 구현이 용이하고, 통신 지연이 없으며, 고속 통신이 가능한등 여러 가지 장점을 지니고 있다. 스트림 암호 시스템중 동기식 스트림 암호 시스템은 키 스트림이 평문과 관계없이 생성되는 것으로 암호문에 들어 있는 키 스트림과 암호문의 독립성으로 인하여 암호 공격에 매우 강하며, 이들은 대부분 키 스트림이 주기를 갖는 주기적 스트림 암호 시스템이다[12].

2.2 스트림 암호 시스템의 비도

스트림 암호 설계시 키 생성에서의 비도가 최우선적으로 고려해야 할 사항이다. 일반적으로 스트림 암호에서의 비도는 여러 종류의 암호 공격에 얼마나 강한 키 수열을 생성할 수 있는가에 달려 있으며, 이는 선형 복잡도, 주기, 랜덤 특성, 상관면역도, 키 수열의 길이 등에 의해 결정된다 할 수 있다. 특히, 스트림 암호 시스템에서는 무엇보다 암호 키 수열이 갖는 비도가 안전한 암호 시스템을 위해 가장 중요한 요소로 인식되어 비 선형 키 수열 생성에 관한 연구가 관심을 끌고 있다[13,14].

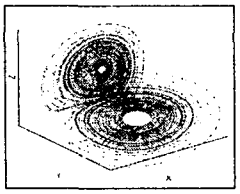
동기식 스트림 암호시스템은 대부분 주기를 갖는 문제를 해결하기 위해 비 주기적 스트림 암호 시스템의 장점을 결합하는 방법으로 비 선형 키를 생성하여 응용되기도 한다.

3. 카오스 이론과 특성

3.1 카오스 이론의 개요

자연현상에서 흔히 관찰되는 여러 가지 현상들이 오랜 노력에도 불구하고 규명하기 곤란했었으나, 로렌츠(Lolenz)의 연구이후 자연의 복잡성 속에 숨어 있는 규칙성 및 질서를 찾아내고자 하는 노력이 매우 활발해 지고 있다. 로렌츠는 '초기 값의 민감한 의존성' 즉 <그림 1>과 같은 '나비효

과'를 발견하였다.



$$x_1 = a(x_2 - x_1)$$
$$x_2 = rx_1 - x_2 - x_1x_3$$
$$x_3 = -\beta x_3 + x_1x_2$$

<그림 1> 로렌츠 방적식과 로렌츠 어트렉트

또한, 1975년에 요크(York)와 이천암(Li)은 '카오스'를 결정적 비 선형 동적 시스템에서의 복잡한 현상이라고 정의하였고[15], 로버트 메이(Robert May)는 1976년에 생물의 개체 수 변동을 수학적으로 처리함으로서 카오스의 응용 분야가 더욱 확대되는 기틀을 마련하였다[16].

특히. 로버트 메이는 시간의 변화에 따른 동물의 개체 수 변화를 구하는 간단한 (식 1)을 발표하였다.

다음의 개체 수 = 번식률×(1-현재의 개체 수)×현재의 개체 수 (식 1)

이러한 개체 수를 모델화할 때에는 계의 상태를 0과 1사이로 나타내는데 1은 개체 수의 최대를 나타내고 0은 전멸을 나타낸다.

이 공식에서 (1 - 현재의 개체 수) 라는 새로운 항을 통하여 개체 수의 변화법칙에 있어서 비선형성이 있음을 알 수 있다. 즉, 단순히 '다음의 개체 수 = 번식률 × 현재의 개체 수' 라고 한다면, 번식률이 1보다 클 경우에는 개체 수가 무제한으로 증가할 것이고, 1보다 작은 경우는 개체 수가 0으로 수렴하는 극단적인 결과가 나타나게 된다. 그러므로 '번식률 × (1- 현재의 개체 수)'를 곱함으로써, 다음의 개체 수는 현재의 개체 수에 의존하여 결정된다는 것을 알 수 있다.

3.2 카오스의 특성

카오스 이론은 자연계에 존재하는 일정한 규칙을 가진 불규칙해 보이는 현상을 연구하는 학문으로서 일반적인 정의를 규정하기가 쉽지 않지만 보통 다음과 같은 정리한다.

① 어떤 동력학계의 복잡하고 비 주기적이며 유인적인 궤도

② 주기성이 없는 일종의 질서

③ 새롭게 인식된 보편적인 자연현상

④ 결정론적인 비 선형 동력학계에 나타나는 불규칙적이고 예측 불가능한 형태 등으로 표현

그러나, 이 같은 카오스 이론의 일반적 성질은 몇 가지 점에서 암호화를 위한 상당한 의미를 제공하게 된다. GCC카오스 암호의 이론과 특징[6]에서 밝힌바와 같이 카오스 특성은 암호 시스템에 매우 효과적으로 이용 될 수 있으리라 기대된다. 암호와 관련된 카오스의 특성을 요약하면 다음과 같다.

①범위가 불안정한 어트렉트

로렌츠 어트렉트와 로지스틱 방정식등에서 나타나는 혼돈 현상이나 스트레인지 어트렉트는 유계영역 안에서 불안정한 상태를 보이며, 예측할 수 없는 성질을 가진다.

② 초기값에 민감한 성질

어트렉트를 이루는 초기값에 대한 민감성은 어트렉트를 나타내는 카오스의 가장 대표적인 성질로 어트렉트나 혼돈 상태를 이루기 위한 초기 값이 0.00001 정도의 차이만 가지더라도 향후 예측할 수 없는 상태를 보이게 되는 성질을 말한다. 특히, 카오스 암호화에서는 이 같은 성질을 이용함으로서 해독이 어려운 암호화 기법을 연구하는데 그 목적이 있다.

한편, 이 같은 성질은 암호화 및 복호화 과정에 존재 할 수 있는 오차를 확대시키는 문제를 안고 있어 한편으로 이를 극복할 연구가 필요하다.

③ 일방향성 성질

카오스는 역사상을 가지지 않는 일방향성을 유지한다. 이는 카오스가 주기를 가지지 않으며, 비 선형성을 지니고 있음을 의미하는 것이다. 이 같은 성질은 특히 스트림 암호 시스템과 같이 비도가 주기성에 의존하는 성질이 높을수록 유용하게 응용 할 수 있을 것이다.

4. 키 수열 생성

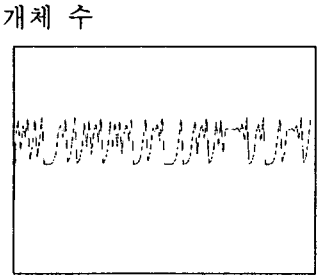
4.1 카오스 신호의 발생

키 수열을 생성하기 위한 카오스 신호 발생을 위해 본 연구에서는 로버트 메이의 연구에 의해 밝혀진 개체 수의 변화를 수학적으로 방정식으로 표현한 로지스틱 방정식을 이용한다. 로버트 메이의 로지스틱 방정식은 (식 2)과 같이 나타낼 수 있다.

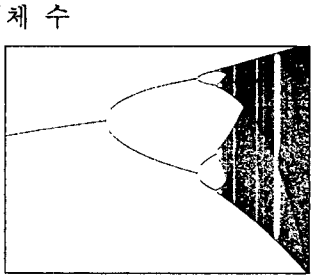
$$X_{n+1} = \alpha X_n(1-X_n) \qquad \text{(식 2)}$$

단, $1 <= \alpha <= 4$. $0 <= X_n <= 1$

α는 증가량을 나타내는 증가율이며, Xn은 현재 개체 수, X_{n+1} 은 다음의 개체 수이다. 위의 로지스틱 방정식에서 X_n 에서 X_{n+1} 로의 변화를 논리사상 (logistic map)이라 한다. α의 값이 크다면 개체 수가 적을 때는 빠른 속도로 증가하고 작다면 빠른 속도로 감소함을 나타낸다. 이러한 값의 변화는 증가율 α의 값에 따라 다른 양상을 타나낸다. 다음 <그림 2>는 X_1=0.04에서의 시간의 변화에 따른 변화를 보이는 Logistic Map을 나타내고 있으며, <그림 3>은 개체 수 X_1=0.04, 증가율 α=1.5~4에서의 개체 수의 변화를 쉽게 알 수 있도록 나타낸 Feigenbaum 분기도이다.



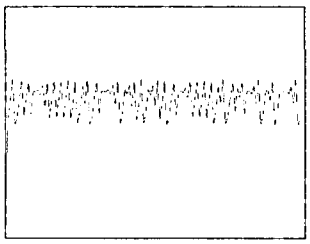
<그림 2> Logistic Map



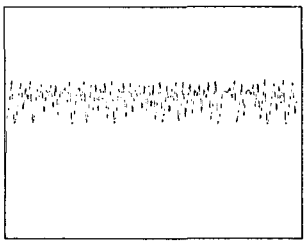
<그림 3> Feigenbaum 분기도

로버트 메이의 논리 차이 방적식(Logistic difference equation)을 이용하여 얻은 Logistic Map은 증가율 α의 값이 일정한 범위 내에 있으면 수렴하거나 진동하게 되지만 그렇지 않을 경우 혼돈 상태를 유지하게 된다. 카오스 이론은 기본적으로 초기조건에 민감한 의존성을 보인다고 알려져 있고, 이는 초기 값의 미세한 차이가 전체 개체 수의 변화에 매우 큰 영향을 줄 수 있다는 것을 의미하는 것이다. 따라서, 초기 값 X_1, 증가율 α는 매우 중요한 의미를 갖는다.

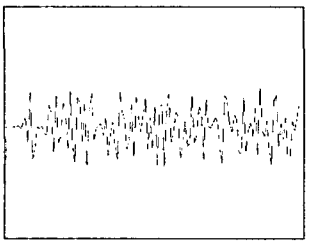
다음 <그림 4>는 X_1=0.04일 때 나타나는 카오스 신호를 Logistic Map으로 보이고 있고, <그림 5>는 X_1=0.041일 때 나타나는 카오스 신호를 Logistic Map으로 보이고 있으며, <그림 6>을 통해 두 Logistic Map의 변화량의 차이를 볼 수 있다.



<그림 4> X_1=0.04



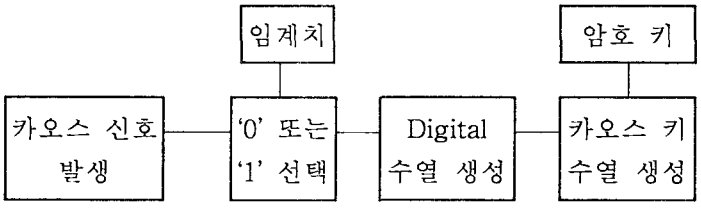
<그림 5> X_1=0.041



<그림 6>차이값 변화량

4.2 키 수열 생성 알고리즘

본 연구에서 제시하는 키 수열 생성 알고리즘은 <그림 5>와 같이 나타낼 수 있다. 먼저 로버트 메이의 논리 차이 방정식을 이용한 카오스 신호를 생성하고, 이 신호를 '0' 또는 '1'의 Digital 값으로 변환한다. 따라서 로버트 메이의 논리차이 방정식으로부터 발생한 카오스 신호는 Digital 수열로 바뀌게 되는 것이다. 여기서 얻어진 Digital 수열을 입력으로 외부로부터 입력받은 암호 키를 이용하여 선택적으로 출력을 얻어냄으로서 스트림 암호 시스템을 위한 키 수열을 생성하게 된다.



<그림 5> 스트림 키 생성 알고리즘

제안하는 키 수열 생성 알고리즘은 처음 카오스 신호를 생성할 때 일정한 시간이 경과한 후로부터의 신호 값을 취함으로서 신호에 대한 랜덤 특성을 높일 수 있고, Digital로 바꾸는 과정에서의 임계값을 임의로 조정하여 상관 면역도 및 랜덤 특성을 높일 수 있다. 또한 외부로부터 입력받은 암호 키를 이용하여 새로운 키 수열을 생성함으로서 특정 함수나 알고리즘으로부터 발생할 수 있는 주기성 및 임의성을 제거하여 안전한 키를 생성 할 수 있다.

4.3 실험 및 결과

키 수열 생성을 위한 실험은 다음과 같이 실시하였다. 실험은 Windows98을 운영체제로 하는 펜티엄 166Mhz/64Mbyte PC에서 Visual C++ 6.0으로 구현되었으며, 카오스 신호의 발생을 위한 로버트 메이의 논리차이 방정식에서의 초기조건과 증가율을 변화시키면서, 암호 키의 차이에 따른 카오스 키 수열 발생을 비교하였다.

카오스 신호 발생을 위한 초기 조건, 암호 키에 따른 실험 결과를 요약하면 다음 <표 1>와 같다. 여기서 카오스 키 수열의 비교를 위해 64bit의 키 수열과 키 수열내의 '0'과 '1'의 개수를 나타내었다.

<표 1> 카오스 키 스트림 생성 실험 결과

no	X_1	α	암호키	카오스 키 수열	'0'	'1'
1	0.11	3.89	chiper	1000011110110000101011111101111111100111111101111101011101000000	24	40
2			chipe	1000000001100000010011111101111101000000111111111111111000111111	27	37
3	0.12	3.89	chiper	1011100011001111110110001110111101001000001000000101100000010011110	33	31
4			chipe	1011111111110000101000001011111111111111100101111100011111010111110	21	43
5	0.12	3.88	chiper	0100000010110000111101111011100000111111111111111011000000011100001	30	34
6			chipe	0100000001000000011111111100000011110000111111111011111101111111	27	37

실험결과 초기조건과 암호 키의 변화에 따라 발생한 카오스 키 수열은 64Bit 내에서 특별한 패턴을 나타내지 않았을 뿐 아니라, 카오스의 특성상 64Bit 이후의 키 수열에서 역시 패턴을 가지지 않을 것으로 기대된다. 또한, 같은 초기조건하에서 발생한 카오스 신호를 이용한 실험에서도 암호 키의 작은 차이('chiper' 과 'chipe')가 키 수열에 매우 큰 영향을 미치는 것을 알 수 있어, 카오스 특성이 키 수열의 생성에 적극 반영되었다고 볼 수 있다.

각 키 수열에 나타난 '0' 또는 '1'의 개수는 각각 27(42%),37(58%)개로 특정 문자에 편중되지 않음을 보이고 있다. 물론 각각의 빈도가 50%에 가깝게 나타나도록 하기 위해 본 연구에는 임계치를 사용할 수 있는 알고리즘을 제안하였다. 실험에서는 임계치를 0.5를 이용하였으나, 향후 연구를 통해 임계치를 조정함으로서 각각의 빈도를 50%를 만족할 수 있을 것이라 사료된다.

5. 결 론

본 연구에서는 카오스 특성을 이용한 스트림 암호 키 수열 생성을 위해 카오스 신호를 생성하고, 카오스 특성을 갖는 키 수열 생성 알고리즘을 제안하였으며, 제안된 알고리즘을 이용하여 키 수열을 생성한 후 생성된 키가 어떠한 특성을 갖는지를 평가하였다.

본 연구에서는 초기조건에 민감한 성질을 갖는 카오스 신호를 생성하고 이를 '0' 또는 '1'로 Digital화 시킨 후 외부로부터 입력된 암호 키를 이용하여 카오스 키 수열을 생성함으로서 카오스 특성이 부가된 키 수열을 생성 할 수 있음을 밝혔다. 따라서 카오스 성질을 갖는 암호 키를

이용한 암호화 시스템에서 발생한 암호문은 카오스적인 어트렉트를 보이므로 불분명한 범위를 나타내어 예측이 어렵고, 초기조건의 미세한 차이에 대해 민감한 성질이 있어 패턴을 이용한 해독이 불가능하며, 신호 발생에 대한 변수가 많이 존재하므로 확률적인 해독이 어려울뿐 아니라, 암호화 알고리즘이 단순하여 속도가 매우 빠르다는 장점을 갖게 될 것으로 기대된다.

향후 키의 안전성에 대한 검증과 키를 이용한 암호화 연구 및 알고리즘의 표준화 문제 등에 관한 연구가 계속 되어야 하며, 아울러 시스템 보안 및 파일 보안, 인터넷 정보의 보안, 전자 상거래 시스템의 정보 보호에 이용 될 수 있도록 노력함으로서 국내 암호화 기술 수준을 제고하고 새로운 국산 암호화 알고리즘의 개발을 기대 할 수 있을 것이다.

6. 참고문헌

[1] 合原一幸, "応用 カオス", サイエソス社, p121~p148, 1994

[2] Hajime Takakubo and Katsufusa Shono, "Digital Cyphering System using Chaos Time Series", SPIE Vol.2612, pp64-pp75, 1995

[3] 정성용, 김태식, "카오스 이론을 이용한 암호화 기법", 한국정보과학회 추계 학술대회 논문집, pp45~47, 1998.10

[4] SuYong, HanZhen, LuoSiwei, "A new method of the Chaos Encryption", Proceedings of ICSP , pp233~236, 1998

[5] Tao Yang, Chai Wah Wu, Leon O. Chua, "Cryptography Based on Chaotic System", IEEE Trans. on Circuits and system, vol. 44. no. 3, pp469~472, 1997.3

[6] 高振宇, "GCC カオス 暗号の 原理と 特徴", 月號抜刷 インターフェース, 1997.6

[7] http://www.iisi.co.jp

[8] 이훈재, 문상재, "고신뢰도 동기식 스트림 암호 시스템", 통신정보보호학회 논문지 제8권 제1호, pp53~64, 1998.3

[9] V. S. Pless, "Encryption schemes for computer confidentiality", IEEE Trans. Comp., vol. c-26, pp1133~1136, 1977.11

[10] NBS, Data Encryption Standard, FIPS pub-46, 1997

[11] R. L. Rivest, A. Shamir, L. Adleman, "A method for obtaining digital signatures and public key cryptosystems", Communications of Association of Computer Manufactures, vol.21, no.2, pp120~126, 1978.2

[12] 김철, 암호학의 이해, (주)영풍문고, pp87-88,1996

[13] P.R. Geffe "How to project data with ciphers that are really hard to break." Electronics, Jan. 4, 1974

[14] S.M. Jennings,"Multiplexed sequences : Some properties of the minimum polynomials.", Lecture Notes in Computer Seience 149, pp.189-206, Berlin:Springer-Verlag, 1983

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

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