카오스 암호화 알고리즘의 안정성 개선

박혜련* · 정갑식*· 이윤수**· 이종혁*

*경성대학교 컴퓨터공학과

**국제과학문화연구소

Stability Improvement of the Chaos Encryption Algorithm

Hye-ryun Park* · Gab-sic Jung*· Yun-Soo Lee**· Jong-Hyeok Lee*

*Kyungsung University

**Institute of International Science & Culture

E-mail : love2di@star.ks.ac.kr

요 약

본 논문에서는 카오스에 기반을 둔 ELM(Expanding Logistic Map) 암호화 알고리즘을 개선하기 위해 CELM(Cascade Expanding Logistic Map)을 제안한다. 제안된 암호화 시스템은 3차 방정식에 기반을 둔 ELM의 차수를 증가시켜 키의 범위를 확대하고, 서로 다른 Key 값과 초기 값의 함수를 Cascade연결하여 안정성을 높일 수 있었다.

키워드

카오스, 암호화, 복호화, 로지스틱, 빈도분석

Ⅰ. 서 론

오늘날 정보화 사회에 살고 있는 우리는 급속하게 발전하는 컴퓨터와 통신 기술에 의존한 정보 교류를 하고 있다. 정보 교류가 활발해 질수록 안전한 정보 교류 기능을 서비스하는 정보 보호 기술은 매우 중요하다. 정보를 보호하기 위해서는 저장과 교류의 대상이 되는 정보의 직접적인 보호가 가장 기본적이다. 평이한 정보를 암호화된 정보로 만드는 암호시스템(Cipher System)이 직접적인 보호 방법으로 이용되고 있다.[3]

기존의 암호화 알고리즘은 일정한 반복적인 패턴이 있음으로 인해 확률을 이용한 암호문의 해독이 가능하다. 이를 개선하기 위해서 패턴이 없는 랜덤(Random)한 값을 이용한 카오스 알고리즘이 제안되었다. 그러나 카오스 이론에 기반을 둔 암호화 알고리즘의 대부분이 2차 방정식을 기반한 로지스틱맵(Logistic Map)을 이용하므로 멀티미디어 정보 등의 적용에는 제한이 따른다.

로지스택 맵의 제한된 대역폭을 개선하고자 3차 방정식에 기반을 둔 ELM(Expanding Logistic Map)이 제안되었다. ELM은 텍스트뿐만 아니라 멀티미디어 정보에서도 암호화가 용이하며, 처리 속도도 매우 빠르지만 안정성 면에서는 국제적인 기준에 미흡하였다.[3]

본 연구에서는 안정성을 개선하기 위해서 CELM(Cascade ELM)을 제안하고자 한다. CELM은 서로 다른 key 값과 초기 값을 갖는 n차 함수를 Cascade 연결하므로 구현할 수 있었으며, 시뮬레이션 결과 카오스의 성질을 갖고 있으면서도 안정성 면에서는 매우 개선됨을 알 수 있었다.

Ⅱ. 현대 암호화 알고리즘

2.1 DES

DES(The Data Encryption Standard)는 1974년 미국 IBM에서 개발되었으며 1977년에는 미국정부의 표준 암호화 방식으로 채택된 이후 ANSI(American National Standards Institute), ISO(International Standards Organization)에서도 표준안으로 채택되어 널리 사용되고 있는 암호화 알고리즘이다.[1] DES는 64bit의 평문과 키를 가지며, 자리바꿈(Permutation), 치환(Substitution)과 모듈러연산(XOR)을 사용하여 구성된다.[5] 1라운드를 16번 반복하는 구조로 구성되어 있으며, 암호화는 라운드의 동일한 동작 과정의 반복으로 이루어진다. 복호화는 암호화 과정과 동일하나 사용되는 키만 역순으로 적용하면 된다. DES는 운영, 관리가 쉽고 Key의 설정이 용이하여 규칙적

으로 변경해도 암호문에는 영향이 나타나지 않으며, 암호화와 복호화과 쉽다는 장점도 있지만 Key의 관리 및 전송이 어려운 단점이 있다.

2.2 RSA

RSA는 1977년 Rivest, Shamir, Adleman이 제안한 RSA 공개키 암호 시스템을 이용한 전자서명 방식으로 공용키/비밀키를 가지는, 비대칭 키 암호화 알고리즘이며 현재 암호키의 안전한 분배 및 관리문제를 해결하기 위해 널리 이용되는 알고리즘이다. 암호화 방식은 서로 다른 두 소수 p, q (n=pq)를 이용한 암호 방법이다. RSA 공개키 암호의 안전성은 n = p*q을 소인수 분해하는 문제의 어려움에 의존한다. 입력은 블록 단위로 이루어지며, 블록 사이즈는 2^k고 n이라는 숫자의 범위는 $2^k < n < 2^{k+1}$이다. 사용자는 mod $\phi(n)$ =(p-1)(q-1) 에 관해 서로소인 e를 개인 공개키로 선택하고 e와 n을 공개한다. 사용자가 p, q를 알고 있다면, e*d ≡1(mod (p-1)(q-1))인 정수d를 개인 비밀키로 택할 수 있고, 이들을 이용하여 암호화와 복호화를 하는 방법이다. 일단 개인키가 노출이 되면 그 개인키 소유자에게 보내어지는 모든 메시지들은 복호화 될 수가 있게 된다. RSA는 강력한 암호화를 지원하고 DES의 가장 큰 문제점중 하나였던 키 관리 문제를 해결하였다. 그러나 기본 연산알고리즘이 곱셈이기 때문에 DES에 비하여 약 100배 이상 느리다는 문제점이 있다.[1]

III. ELM(Expanding Logistic Map)

3.1 카오스이론의 개요

카오스 이론은 1960년대 등장한 이후 계속적인 연구를 통해 현대과학의 새로운 장을 열어가고 있다. 카오스 이론은 자연계에 존재하는 일정한 규칙을 가진 불규칙해 보이는 현상을 연구하는 학문이다. 1975년에 로버트 메이(Robert May)는 생물의 개체수 변동을 수학적으로 처리함으로서 카오스 공학을 가전제품이나 전기 기기 등에 이용하기 시작하였다.

카오스 시스템은 랜덤행위(Random Behavior)를 나타내는 결정론적 시스템(Deterministic System)이라고 할 수 있다. 최근에 카오스는 비선형 시스템 연구분야의 가장 흥미있는 분야의 하나가 되고 있다. 특히 초기조건에의 민감한 의존성(Sensitive Dependence on Initial Condition)으로 대표되고 있다.[2]

3.2 Logistic map

로버트 메이는 시간의 변화에 따른 동물의 개체수 변화를 구하는 간단한 식을 통하여 구체적인 연구결과를 발표하였다.

$X_{n+1} = \alpha X_n(1 - X_n)$---------- (1)

α=개체수의 증가량, X_n=금년의 개체수, X_{n+1}= 내년의 개체수이다. 위의 로지스틱 방정식에서 X_n에서 X_{n+1}로의 변화를 논리사상(Logistic map)이라 한다. α의 값이 크다면 개체수가 적을 때는 빠른 속도로 증가하고 작다면 빠른 속도로 감소함을 나타낸다.[4]

3.3 ELM

ELM은 카오스 신호를 만들어내기 위해 사용한 방법은 로지스틱 방정식보다 넓은 진동 범위를 가지는 3차 함수를 이용한 것이다. ELM의 일반형은 다음과 같다.

$$X_{n+1} = a X_n^3 + b X_n^2 + cX_n + d \ (a \neq 0)\text{---- (2)}$$

ELM의 특징은 바로 최대값과 최소값을 갖는다는 사실이다. 삼차함수는 a가 0이 아니라면 언제나 최대값과 최소값을 다 가지게 되기 때문에, 그만큼 암호화에 사용할 수 있는 키의 범위가 넓어지게 된다. 이 최대값과 최소값을 기점으로 암호화에 이용되는 키 값의 범위가 정해진다. a의 값은 그래프의 폭을 결정한다. a의 값이 0에 가까울수록 폭이 넓어지고, 0에서 멀어질수록 폭이 좁아지며 구하고자 하는 a의 값에는 제한이 있다. 그러므로 a의 조건은, 0에 가장 가까운 0이 아닌 수가 가장 최적이다. 이는 a의 값만을 생각했을 때고 나머지 b, c의 값을 고려하면 키 값의 범위가 달라질 수 있다. 그리고 c와 a의 부호가 같다면 b의 값이 월등하게 크지 않은 이상, 그래프는 최대점과 최소점을 가지지 않기 때문에 c는 a와 같은 부호값을 가지지 않는 경우가 일반적이다.

식 2에서 초기 값을 0.5, 적당한 키 값을 입력하였을시 ELM의 출력 값의 변화를 그림 1에 나타내었다. 출력 값이 불규칙하게 진동함을 알 수 있었다.[2]

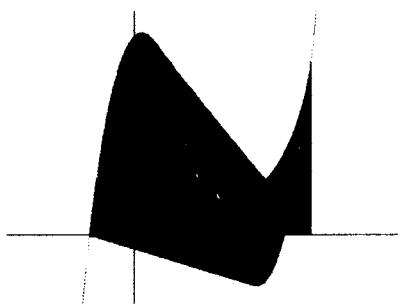

그림 1. 카오스 신호 값의 변화

IV. CELM(Cascade ELM)

4.1 CELM의 구현

본 연구에서는 ELM의 특징을 모두 포함하며, 안정성 개선을 위해 2가지 제안을 하고자 한다. 첫째, n차 함수의 방정식의 차수를 증가시켜 키의 범위 확대한다.

둘째, 키의 Random성을 보장하면서 국제적인 안정도 조건을 만족하기 위하여 n차 함수를 Cascade 연결한다. CELM을 이용한 암호화 및 복호화 과정을 그림 2에서 나타내었다.

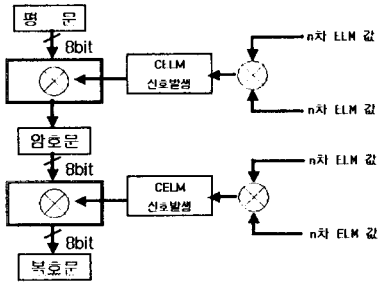

그림 2. 암·복호화 과정

4.2 CELM의 빈도분석 및 안정성

ELM에서 진동 폭이 큰 임의의 3차 방정식을 구하기 위하여 시뮬레이션 프로그램을 구현하여 제안한 초기 값과 a, b, c, d 값을 이용하여 키의 범위를 알아보고자 한다. 시뮬레이션을 통한 3차 방정식의 값을 정수화 된 값으로 변환하기 위해 shift와 확장을 하게 된다. 정수화 된 값의 범위는 한 문자를 암호화하는 데 필요한 명령문은 8bit 연산을 하므로 2^8=256의 범위를 가진다. 즉 -128 ~ +127 까지의 범위를 가지게 된다. 그러나 실제 키의 범위는 유효키만이 사용된다. 유효키는 전체 범위인 -128~+127 중 암호화에 사용 가능한 키를 말한다. ELM에서 제안한 3차 방정식의 최소·최대 값의 범위는 그림3에서와 같이 -70~+126까지 값만을 암호화에 사용한다.

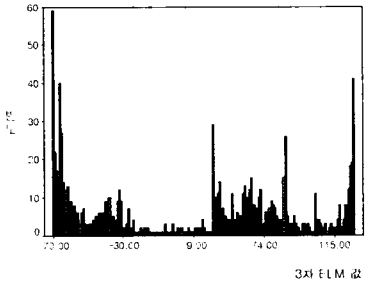

그림 3. 3차 ELM 빈도분석

그러나 최소·최대 값의 범위 안에 한 번도 나오지 않는 값이 있다. 즉, 256값 중 빈도가 0인 63개의 값은 암호화에 사용할 수 없다는 것이다.

ELM과 같은 시뮬레이션으로 암호화에 이용될 수 있는 4차 함수의 값 중에서 초기값= 1.5, a= -0.469, b= -0.75, c= 1.0, d= 1.47599, e= 0.4599인 빈도 분석이며 그림 4에 나타내었다.

4차 방정식의 최소·최대 범위는 -119~+119로 확대되었다. 또한 값이 0인 것은 35개로 ELM보다 10.9% 낮아졌다.

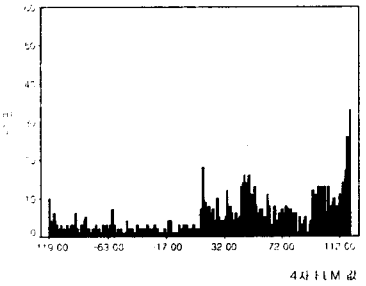

그림 4. 4차 ELM 빈도분석

3차 ELM에 비해 Key 범위는 확대되었지만 암호해독에 있어 키의 빈도는 매우 중요하다. 그래프와 같이 특정 값이 많이 나오면 단순 대체 암호화 알고리즘과 같이 빈도분석(Frequency analysis)을 통한 암호 공격이 가능하게 된다. 즉 빈도수가 낮은 key와 높은 key를 비교한 다음 높은 key부터 공격을 할 것이다. key 값이 카오스의 불규칙하게 진동한다면 빈도분석에 대한 공격은 최대한 줄어들 것이다.

빈도분석에 의한 암호 공격을 최소화하기 위해서 키의 Random성을 보장해야 하며 그 방법으로써 카오스의 성질 중 초기 조건에의 민감한 의존성(Sensitive Dependence on Initial Condition)을 이용[2]하였다.

앞서 ELM에서 제안한 초기 값과 a, b, c, d 값은 특정 값이 높은 빈도 발생으로 최적의 값이 되지 못하기 때문에 시뮬레이션을 통한 값의 범위를 재계산하여 -123~+116 확대하고 이에 n차 방정식과 Cascade를 한다.

그림5는 기존 3차 ELM 값과 초기 값만 0.5 변화시킨 3차 ELM값을 Cascade한 결과이다.

3차 CELM의 빈도 분석하면 최소·최대 값의 범위는 -128~+127까지며 평균 빈도는 5.0으로 0인 값은 전체의 3%만을 가진다.

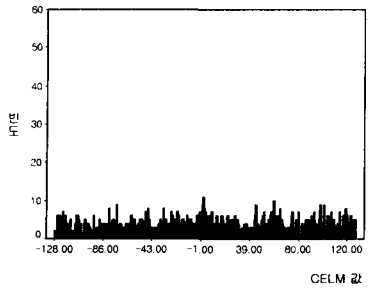

그림 5. 3⊕3 CELM 빈도분석

3차 ELM과 4차 ELM의 Cascade한 결과를 그림 6에 나타내었다. 평균 빈도가 0.79로써 -128 ~ +127까지 값이 매우 random성을 가짐을 알 수 있다.

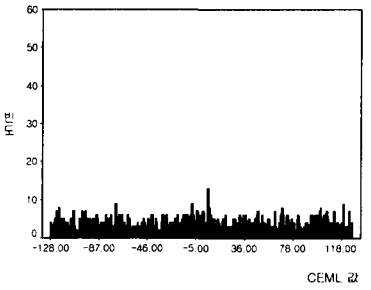

그림 6. 3⊕4 CELM 빈도분석

3차 ELM에서 사용되는 변수는 초기 값, a, b, c, d, Shift, Gain으로 존재함으로 위 각각의 값을 유효 2자리로 가정한다. 본 암호화 알고리즘을 1 character을 생성하는데 최소 명령문 수는 3차의 경우 15명령문이며 암호해독이 잘 되는가를 알기 위해서는 최소 10 character 정도는 연속으로 맞아야 한다고 가정할 때 한 가지 방법에서 최소한 150명령문이 소요된다. 그러므로 3차 ELM을 해킹하기 위해서 필요한 총 명령문의 수는 $(10^2)^7 \cdot 150=1.5\times10^{16}/3\times10^{13}=5\times10^2$ mips/year가 된다. 이는 국제 기준에 매우 미흡하다. 또한 3차 ELM에서 4차 ELM으로 차수를 높여도 10^2 정도만 증가하기 때문에 국제기준에 미흡하다. 본 연구에서 제안한 3차 ELM 2개를 Cascade하면 $(1.5\times10^{16})^2=2.25\times10^{32}$ 명령문이 소요되며 $2.25\times10^{32}/3\times10^{13}=7.5\times10^{18}$ mips/year가 된다. 그러므로 국제기준인 10^{14}에 충분하리라 생각한다.

4.4 CELM의 결과

CELM을 이용한 암·복호화 알고리즘을 구현하였으며 이를 그림7에 나타내었다.

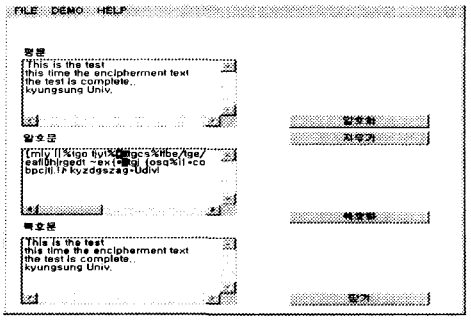

그림 7. 실행한 데모화면

그림 7에서 보이는 것과 같이 평문은 카오스 신호에 의해 혼동상태를 가지는 코드로 암호화 되었으며 암호문은 평문으로 정확하게 다시 복호화 되었다.

V. 결 론

본 연구에서는 안정성 향상을 위하여 2개의 n차 ELM을 Cascade한 CELM 모델을 제안하였다.

제안한 CELM은 카오스의 성질인 혼동상태를 유지하며, 암호화에 사용할 수 있는 유효한 값의 범위가 확장됨과 빈도가 0인 값을 감소되었다. 또한 초기 조건에의 민감한 의존성의 성질을 이용하여 전체 범위 값이 random성을 가지게 되었다. n차 방정식의 ELM XOR 연산함으로써 암호문이 평문에 비해 길어지지 않으며, 비트 연산이기 때문에 고속으로 암·복호화가 이루어지며, 안정성이 국제 기준에 부합됨을 알 수 있었다.

참고문헌

[1] 김철, 암호학의 이해, 영풍문고, 1997.
[2] 이윤수, "카오스에 기반을 둔 암호화 알고리즘의 구현", 경성대 멀티미디어정보예술대학원 석사학위 논문, 2001.
[3] 한국전자통신연구원, "암호학의 기초", 경문사, 1999.
[4] 정성용, 김태식, "카오스 이론을 이용한 암호화 기법", 한국정보과학회 가을 학술발표 논문집 Vol.25, 1998.
[5] 이윤아, DES알고리즘의 FPGA 구현 한남대학교 석사학위 논문, 1999.