CELM 암호화 알고리즘의 성능 비교

박혜련* · 이종혁**

Performance Comparison of the CELM Encryption Algorithm

Hye-ryun Park* · Jong-hyeok Lee**

요 약

본 논문에서는 카오스에 기반을 둔 ELM(Expanding Logistic Map) 암호화 알고리즘을 개선하기 위해 CELM(Cascade ELM)을 제안한다. 제안된 암호화 알고리즘은 3차 방정식에 기반을 둔 ELM의 차수를 증가시켜 키의 범위를 확대하고, 서로 다른 Key 값과 초기 값의 함수를 Cascade연결한 것으로 시뮬레이션 결과 키의 랜덤성이 보장되면서 안정성이 국제 기준에 부합됨을 알 수 있었다.

ABSTRACT

In this paper, we propose CELM(Cascade ELM) to improve stability. We could realize as cascade connected each other key value with N degree equation which has a initial value. And we could know to be improved in stability with the nature of Chaos in simulation result. In efficiency, this CELM algorithm identified size of encrypted code with size of source code and we could know more efficient than existing RSA and ECC. In speed, CELM took average 0.18ms degree to encrypt a file. Although it was slower than DES, it was faster than ECC or RSA.

In security, it took 1.6 x 10^{18}mips/years to decrypt and is suitable for international criterion.

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.[1]

기존의 암호화 알고리즘은 일정한 반복적인 패턴이 있음으로 인해 확률을 이용한 암호문의 해독이 가능하다. 이를 개선하기 위해서 패턴이 없는 랜덤한 값을 이용한 카오스 알고리즘이 제안되었다. 그러나 카오스

*경성대학교 교육대학원 컴퓨터교육

**경성대학교 전기전자 · 컴퓨터공학부 교수

접수일자 2002. 5. 24

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 가능하며, 처리 속도도 매우 빠르지만 안정성 면에서는 국제적인 기준에 미흡하였다.[2]

본 연구에서는 서로 다른 key 값과 초기 값을 갖는 n차 ELM을 cascade 연결한 CELM을 제안하고 기존의 암호화 알고리즘과 성능을 비교해 보고자 한다.

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, ISO에서도 표준안으로 채택되어 널리 사용되고 있는 암호화 알고리즘이다.[1] DES는 64bit의 평문과 키를 가지며, 자리바꿈(Permutation), 치환(Substitution)과 모듈러연산(XOR)을 사용하여 구성된다. 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 규칙적으로 변경해도 암호문에는 영향이 나타나지 않으며, 암호화와 복호화과 쉽다는 장점도 있지만 Key의 관리 및 전송이 어려운 단점이 있다.[3]

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.

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]

2.3 ECC

공개키 암호시스템에서의 타원곡선의 이용은 1985에 Miller와 Koblitz가 독립적으로 제안하였다. 타원곡선 암호시스템은 이산대수에서 사용하는 유한체의 곱셈군을 타원곡선군으로 대치한 암호시스템이다. 타원곡선 암호시스템은 다른 암호시스템에 비해 여러 가지 장점들을 가지고 있다. 첫째, 주어진 소수 에 대하여 유한체의 부분군을 이용하는 경우는 그 후보가 곱셈군 밖에 없는 반면 타원곡선 암호시스템의 경우는 주어진 유한체상에서 정의된 다양한 타원곡선을 선택할 수 있어 풍부한 타원곡선군을 활용할 수 있다. 둘째, 특별한 유형의 타원곡선을 제외하고는 타원곡선 이산대수문제를 푸는 준지수시간 알고리즘(subexponential time algorithm)이 존재하지 않아서 그 안전성을 더욱 보장받고 있다고 볼 수 있으며 안전한 암호시스템의 설계가 용이하다. 셋째, 다른 암호시스템에 비해 더 짧은 키 사이즈로 대등한 안전성을 주고 있다는 것이다. 이러한 장점들 때문에 타원곡선 암호시스템은 스마트 카드나 무선환경에서처럼 상대적으로 작은 키 사이즈와 제한적 대역폭과 메모리가 요구되는 분야에서 각광받고 있는 차세대 암호시스템이다.[4]

2.4 ELM

ELM은 카오스 이론를 기반으로 한 암호 시스템이다. 카오스 이론은 1975년 로버트 메이에 의해 발견되었으며, 랜덤행위를 나타내는 결정론적 시스템(Deterministic System), 초기조건에의 민감한 의존성(Sensitive Dependence on Initial Condition)의 특징가지고 있다.

ELM은 카오스 신호를 만들어내기 위해 사용한 방법은 로지스틱 방정식보다 넓은 진동 범위를 가지는 3차 함수를 이용하였다.

ELM의 특징은 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.

III. CELM(Cascade ELM)

본 연구에서는 ELM의 특징을 모두 포함하며, 안정성 개선을 위해 2가지 제안을 하고자 한다. 첫째, n차 함수의 방정식의 차수를 증가시켜 키의 범위 확대한다. 둘째, 키의 랜덤성을 보장하면서 국제적인 안정도 조건을 만족하기 위하여 n차 함수를 Cascade연결한다. CELM을 이용한 암·복호화 과정을 그림 1에서 나타내었다.

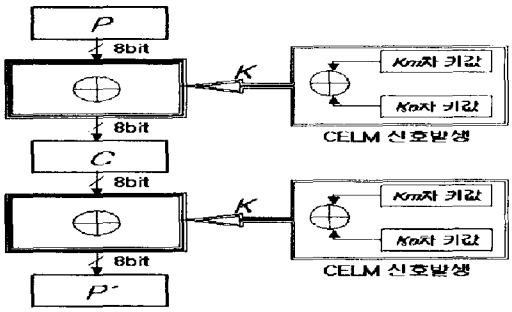

그림 1. 암·복호화 과정

3.1 n차 ELM의 빈도분석

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 암호화하는데 필요한 명령문은 8bit 연산을 하므로 28=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 그림2에서와 같이 -70~+126까지 값만을 암호화에 사용한다. 그러나 최소·최대 값의 범위 안에 한 번도 나오지 않는 값이 있다. 즉, 256 값 중 빈도가 0인 63개의 값은 암호화에 사용할 수 없다는 것이다.

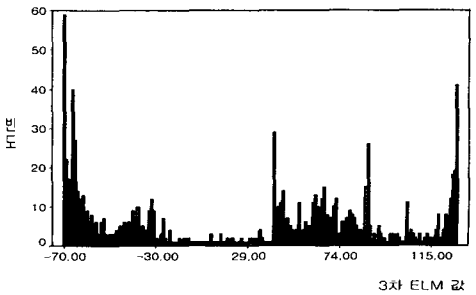

그림 2. 3차 ELM 빈도분석

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 3에 나타내었다.

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

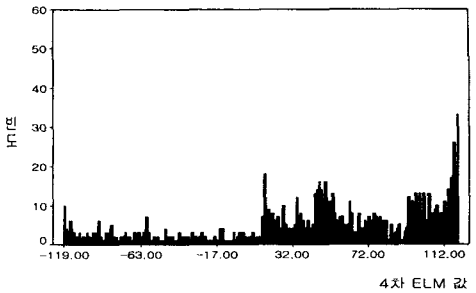

그림 3. 4차 ELM 빈도분석

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 대

한 공격은 최대한 줄어들 것이다.

3.2 n차 ELM의 Cascade

빈도분석에 의한 암호 공격을 최소화하기 위해서 키의 랜덤성을 보장해야 하며 그 방법으로써 카오스의 성질 중 초기 조건에의 민감한 의존성(Sensitive Dependence on Initial Condition)을 이용하였다[5].

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.

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

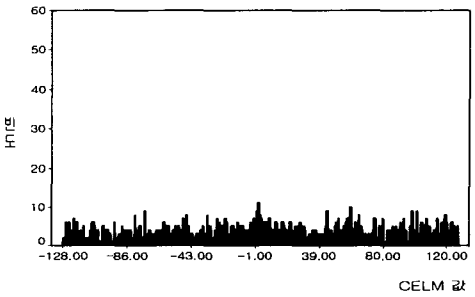

그림 4. 3⊕3 CELM 빈도분석

3차 ELM과 4차 ELM의 Cascade한 결과를 그림 5에 나타내었다. 평균 빈도가 0.79로써 -128~+127까지 값이 매우 random성을 가짐을 알 수 있다.

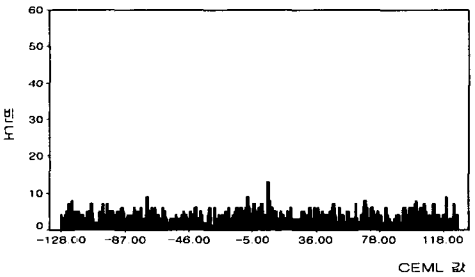

그림 5. 3⊕4 CELM 빈도분석

3.3 성능 비교

3차 ELM에서 사용되는 변수는 초기 값, a, b, c, d, Shift, Gain으로 존재함으로 위 각각의 값을 유효 2자리로 가정한다. 본 암호화 알고리즘은 1 character을 생성하는데 최소 명령문 수는 3차의 경우 21개 명령문이며, 암호해독이 잘 되는가를 알기 위해서는 최소 10 character 정도는 연속으로 맞아야 한다고 가정할 때 한 가지 방법에서 최소한 210명령문이 소요된다.

3차 ELM을 해킹하기 위해서 필요한 총 명령문의 수는 위 식에 대입하여 계산하면 (102)7·21·10 = 2.1×1016 / 365×24×60×60×106 = 2.1×1016 / 3×1013 = 7 × 102 mips-year가 된다. 이는 국제 기준에 매우 미흡하다. 또한 3차 ELM에서 4차 ELM으로 차수를 높여도 102 정도만 증가하기 때문에 국제 기준에 미흡하다. 본 연구에서 제안한 3차 ELM 2개를 Cascade하면 ((102)7)2·450 / 3×1013=1.5×1016 mips-year가 되며 3, 4차 ELM을 Cascade하면 총 명령어 개수는 ((102)7×(102)8)·500 = 5×1032이고 이를 계산하면 5×1032 / 3×1013 = 1.6×1018 mips-year가 된다. 마지막으로 두 개의 4차 ELM은 101만이 증가하였다. 그러므로 국제기준인 1014에 충분하리라 생각한다.

n차 ELM과 각 cascade 간의 mips-year과 기존의 암호화 시스템과의 키 사이즈당 mips-year를 비교한 것을 그림 6, 7에 나타내었다.

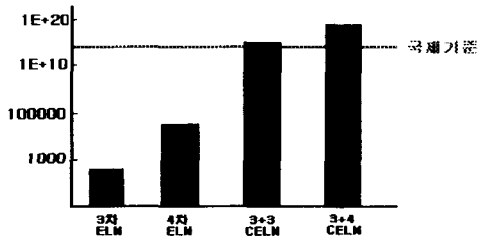

그림 6. 각 알고리즘의 mips-year 비교

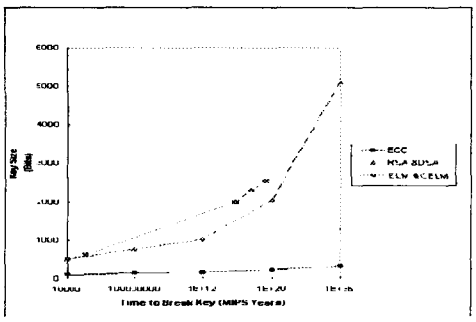

그림 7. 각 암호화 알고리즘의 안전도 비교

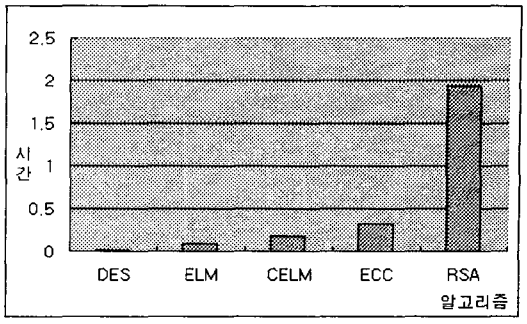

그림 9. 각 알고리즘간 속도 비교

암호화 알고리즘의 조건 중 암호문이 평문에 비해 길어지지 않을 것, 대역폭의 변화가 없는 것을 좋은 알고리즘의 조건이다. 이를 실험하기 위해 1kbyte, 10kbyte, 100kbyte의 평문을 입력하여 기존의 암호화 알고리즘과 CELM과의 코드크기를 비교한 결과를 그림 8에 나타내었다.

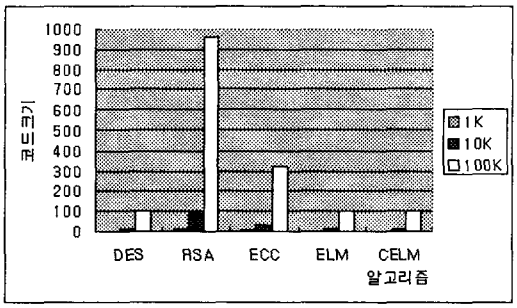

그림 8. 각 암호 알고리즘 간 대역폭 비교

각각의 평문이 암호화 과정을 수행한 후 암호화된 암호문의 크기는 RSA가 가장 크며 ECC가 그 다음으로 본 연구에서 제안한 CELM과 ELM, DES가 효율성이 가장 뛰어난 것으로 나타났다.

그림 9는 각 알고리즘간 영문자로 이루어진 평문을 암호화가 완료되는 시간을 측정하였으며, 각 알고리즘의 iteration단위 별로 나타내었으며, 단위는 ms이다.

3.4 CELM 구현 결과

CELM을 이용한 암·복호화 알고리즘을 구현하였으며 이를 그림10, 11, 12에 나타내었다. 평문은 카오스 신호에 의해 혼동상태를 가지는 코드로 암호화되었으며 암호문은 평문으로 정확하게 다시 복호화 되었다.

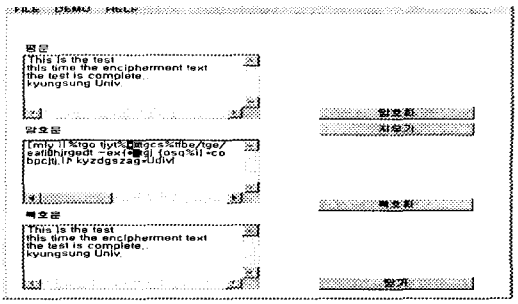

그림 10. 실행한 데모화면

그림 11. image 파일 암호화 전

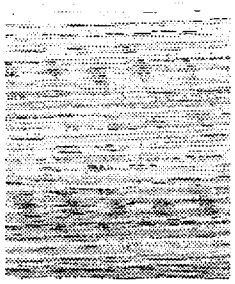

그림 12. image 파일 암호화 후

Ⅳ. 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 확장되며 빈도가 0인 값이 감소되었다. 또한 전체 범위 값이 랜덤성을 가지게 되었다.

n차 방정식의 ELM을 XOR 연산함으로써 암호문과 평문의 길이가 같으며, 비트 연산이기 때문에 고속으로 암·복호화가 이루어지며, 안정성이 국제 기준에 부합됨을 알 수 있었다.

참 고 문 헌

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

저 자 소 개

박혜련(Hye-ryun Park)
1999년 2월 경성대학교 컴퓨터공학과(공학사)
2000년 3월~현재 경성대학교 교육대학원 컴퓨터교육 전공 재학
※관심분야 : 암호화, 네트워크 보안

이종혁(Jong-hyeok Lee)
1975년 2월 부산대학교 전자공학과(공학사)
1980년 2월 부산대학교 대학원 전자공학과(공학석사)
1991년 2월 부산대학교 대학원 전자공학과(공학박사)
1980년 3월~1990년 2월 동의공업대학 전자과 부교수
1990년 3월~현재 경성대학교 전기전자·컴퓨터공학부 교수
1998년 7월~1999년 6월 미국 Beckman Institute, University of Illinois 객원연구원
※관심분야 : 인공지능, 음성인식, 암호화