전방향 신경회로망을 이용한 Feistel 암호 알고리즘 설계

정경권*, 김구영*, 지호진*, 엄기환*
*동국대학교 전자공학과
kihwanum@cakra.dongguk.ac.kr

Feistel Cipher Design using Feedforward Neural Network

Kyung-kwon Jung*, Gu-young Kim*, Ho-jin Jhee*, Ki-hwan Eom*
*Dept. of Electronic Eng., Dongguk University
kihwanum@cakra.dongguk.ac.kr

요 약

본 논문에서는 feistel 암호 알고리즘에서 전방향(feedforward) 신경회로망으로 암호 함수(f)를 구성하는 블록 암호 알고리즘 방법을 제안한다. 신경회로망의 가중치(weight)를 키(key)로 사용하여 암호화 및 복호화를 수행한다. 신경회로망의 비선형적인 특성과 각각의 층을 구성하고 있는 뉴런 간의 방대한 연결로 복잡한 구조이지만, 실제 뉴런은 단순 처리만을 수행하고, 대단위 병렬처리가 가능하다. 은닉층의 구성에 따라 여러 형태의 설계가 가능하다.

I. 서론

현대 사회가 점차 고도 정보화 사회로 발전해 감에 따라 음성, 화상, 데이터 등 다양한 종류의 정보를 교환하고 저장하는 대량 정보 통신 시스템이 구축되어 가고 있다. 이러한 정보 통신 시스템이 사회 전반에 걸쳐 일반화 되기 위해서는 시스템의 신뢰성과 안전성이 필수 불가결한 요건이며, 특히 시스템 내부 또는 각 시스템 상호간 통신에서의 각종 정보에 대한 보호 기술은 중요한 부분으로 자리잡고 있다.

만약 제3자가 결코 획득할 수 없는 전송 수단이 존재한다면 그 정보는 매우 안전하며, 정보를 보호하기 위한 수단의 강구는 필요하지 않을 것이다. 그러나 그러한 전송 수단은 현재 존재하지 않으며, 전송로상의 정보는 항상 제3자가 획득할 수 있다고 가정해야 한다. 이러한 가정에서 정보를 보호할 수 있는 최선의 방법은 암호 시스템을 구성하여 제3자가 정보를 획득하더라도 그 의미를 분석할 수 없도록 하는 것이다. 이것이 바로 암호 시스템을 이용하는 가장 큰 이유라고 할 수 있다.[1][2]

본 논문에서는 feistel 암호 알고리즘에서 전방향(feedforward) 신경회로망으로 암호 함수(f)를 구성하는 블록 암호 알고리즘 방법을 제안한다.

블록 암호 알고리즘은 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변형하는 암호 알고리즘에 의해 암호화 및 복호화 과정을 수행하는 시스템이다. 출력 블록의 각 비트는 입력 블록과 키(key)의 모든 비트에 영향을 받아 결정된다.

DES를 포함한 대부분의 블록 암호 알고리즘은 암호함수 내의 비선형 함수로 S-box를 사용한다. 그러나 이러한 S-box는 DC(differential

cryptanalysis), LC(linear cryptanalysis)에 의한 공격에 취약함을 보이고 있다.[2][3] 따라서 본 논문에서는 비선형 함수로 S-box를 사용하는 암호함수 대신에 대단위 병렬처리가 가능하며, 뉴런간의 방대한 연결과 입출력의 비선형적인 특성이 있는 신경회로망을 암호함수로 사용한다.

II. Feistel 알고리즘

블록 암호 시스템은 고정된 크기의 입력 블록을 고정된 크기의 출력 블록으로 변형하는 암호 알고리즘에 의해 암호화 및 복호화 과정을 수행하는 암호 시스템이다. 출력 블록의 각 비트는 입력 블록과 키(key)의 모든 비트에 영향을 받아 결정된다.[1]

Feistel 알고리즘은 짝수의 블록 크기를 사용하며, 블록의 크기가 2n이라고 하면, 평문 m을 크기가 n인 두 블록으로 나누어 $m=(m_0, m_1)$으로 놓고 다음과 같이 암호화 한다.

라운드 1 :

$$U_0=(m_0, m_1) \rightarrow U_1=(m_1, m_2)$$

⋮

라운드 i :

$$U_{i-1}=(m_{i-1}, m_i) \rightarrow U_i=(m_i, m_{i+1})$$

⋮

라운드 h :

$$U_{h-1}=(m_{h-1}, m_h) \rightarrow U_h=(m_h, m_{h+1})$$

여기서 $m_{i+1}=m_{i-1} \oplus f_{ki}(m_i)$이다. 함수 f_{ki}는 임의로 선택된다.

복호화 과정은 $m_{i-1}=m_{i+1} \oplus f_{ki}(m_i)$이므로 다음과 같다.

라운드 1 :

$$\overline{U}_h=(m_{h+1}, m_h) \rightarrow \overline{U}_{h-1}=(m_h, m_{h-1})$$

⋮

라운드 h+1-i :

$$\overline{U}_i=(m_{i+1}, m_i) \rightarrow \overline{U}_{i-1}=(m_i, m_{i-1})$$

⋮

라운드 h :

$$\overline{U}_1=(m_2, m_1) \rightarrow \overline{U}_0=(m_1, m_0)$$

Feistel 알고리즘은 임의의 함수 f_{ki}에 대해서도 암호화 및 복호화 과정이 수행된다. 특히 f_{ki}의 역함수가 존재하지 않아도 된다. 이 알고리즘은 MDS, Lucifer, DES, FEAL 등의 설계에 기본 개념으로 활용되고 있다.

III. 신경회로망

1957년 미국의 Frank Rosenblatte에 의해 최초의 퍼셉트론이란 신경회로망이 발표된 이후 현재까지 패턴인식, 음성합성, 수중전파탐지, 시스템 모델링 및 제어, 최적화 및 적응제어 등 많은 분야에 응용되고 있다.[4][5]

신경회로망은 단순한 기능을 가진 무수히 많은 신경소자(neuron) 또는 처리소자(PE: processing element)들이 병렬 연결된 연산 구조로 되어 있다. 그 특징은 다음과 같다.

각 신경소자는 다른 신경소자들과 완전히 독립된 기능을 갖는다. 즉, 각 신경소자의 출력은 자신과 연결된 결선을 통하여 직접 전달되는 정보에만 의존할 뿐, 다른 정보들과는 무관하다. 이와 같은 특징으로 인하여 병렬처리가 가능하므로 연산속도가 매우 빠르다.

신경회로망은 무수히 많은 결선을 가지고 잇다. 따라서 정보의 분산 표현 및 처리가 가능하다. 또 중복성(redundancy)이 크므로 일부의 정보로부터 전체를 얻을 수 있는 연상기억(associative memory) 특성을 갖는다.

학습이나 훈련을 통해 결전 강도를 조정함으로써 새로운 정보를 추가하거나 변경할 수 있는 적

응 특성을 가지고 있다.[6]

뉴런의 구조는 그림 1과 같다. 입력패턴이 가중합되어 활성화 함수 f를 거쳐 출력 y가 된다.

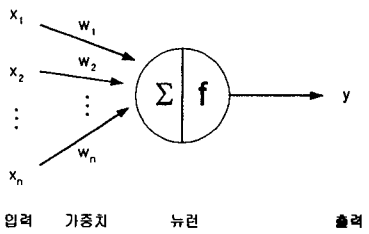

그림1. 뉴런의 구조

뉴런의 연산 기능을 보면 다음과 같다.

$$y = f(\sum_{i=1}^{n} x_i \cdot w_i - \theta) \qquad (1)$$

θ : 임계값

f : 활성함수

활성화 함수의 종류는 그림 2와 같다.

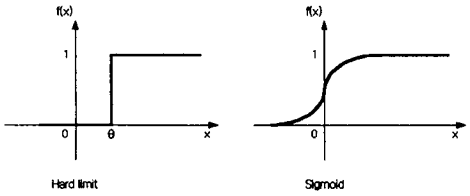

그림2. 활성화 함수의 종류

본 논문에서는 그림2의 Hard limit 형태의 활성화 함수를 사용한다. 임계값 θ는 은닉층의 수에 따라 달리 정하였다.

이와 같이 입력층의 신호가 은닉층을 거쳐 출력층으로 전방향(Feedforward)으로 진행되므로 신경회로망이라 정의한다.

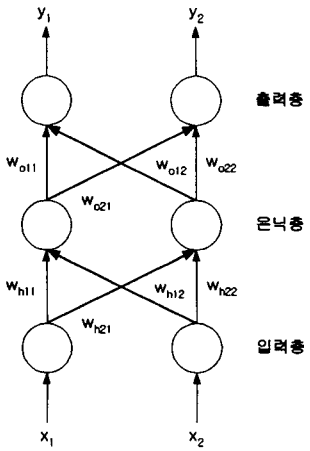

그림3. 전방향 신경회로망

IV. 제안한 암호화 방식

제안한 암호화 방식은 앞에서 소개한 feistel 알고리즘에서 암호화 함수인 f_{ki}를 그림3과 같은 전방향 신경회로망을 사용하여 구성하였다. 전체 구조는 그림4와 같다.

입력은 64비트를 32비트씩 나누어서 m_0와 m_1을 구성하여 feistel 알고리즘을 수행한다. 각각의 연결강도는 0, 1의 값을 갖으며, 입력과 연결강도가 곱해져서 활성화 함수를 통과하여 출력이 된다. 여기서 활성화 함수는 임계값 θ를 8로 하는 hard limit 형태로 사용하였다.

다음은 임의의 입력을 가했을 때 16 라운드 수행 후의 출력이다.

입력

11101111 00000101 10011011 00001110
10010111 00111000 00101011 01101000

출력

00010001 00100011 11001000 11011100
00001011 01111010 00101000 00011000

은닉층의 뉴런수를 32개로 하여 시스템을 구성하였으며, 매 라운드의 연결강도는 같은 값을 사용하였다.

은닉층의 첫 번째 뉴런의 연결강도는 다음과 같다.

00101101101010101110100010011101

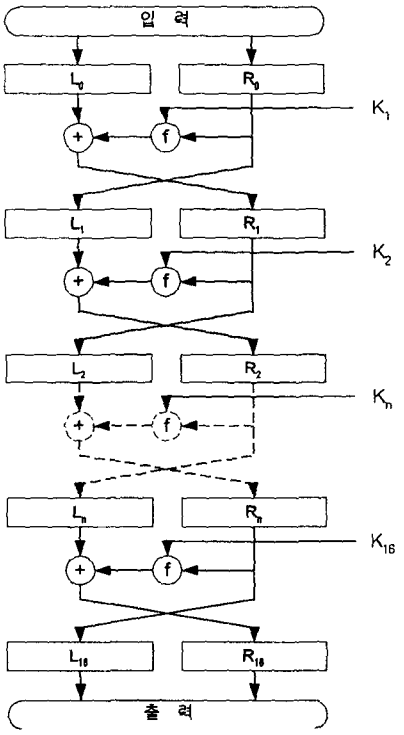

그림4. Feistel알고리즘 구조

V. 결론

Feistel 암호 알고리즘에서 암호 함수를 전방향 신경회로망으로 이용하는 방법을 제안하였다. 신경회로망의 연결강도를 키로 사용하여 암호화 및 복호화를 수행하였다. 신경회로망의 비선형적인 특성으로 암호 함수 구성이 가능하며 신경회로망의 은닉층의 구성에 따라 복잡한 설계도 가능하다.

앞으로 키로 사용되는 연결강도의 비트 크기를 줄이고 실제 하드웨어로 구현하는 등의 연구가 계속되어져야 하겠다.

참 고 문 헌

[1] H. J. Beker, F. C. Piper, "Cipher Systems," John Wiely and Sons, Northwood Publications, 1982

[2] E. Diham, and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," CRYPTO 90, 1990.8

[3] K. Nyberg, "Perfect Nonlinear S-boxes," Advances in Cryptology - EUROCRYPT '91 Proc., Springer-Verlag, pp.378-386, 1991

[4] S. Grossberg, "Adaptive pattern classfication and universal recoding: 1.parrallel development and coding of neural feature detectors," Biological Cybernetic, pp.121-134, 1976

[5] R. P. Lippmann, "An introduction to computing with neural nets," IEEE, ASSP Mag., vol.4, pp.4-22, 1987.4.

[6] B. Widow and M. A. Lehr, "Thirty years of adaptive neural network: Perceptron, Maldaline, and back-propagation," Proc. IEEE, vol.78, no.9, pp.1415-1441, 1990.10.