International Journal of Soft Computing 4 (3): 131-135, 2009
ISSN: 1816-9503

Cryptanalysis of a Feistel Type Block Cipher by Feed Forword Neural Network Using Right Sigmoidal Signals

[1]K.V. Srinivasa Rao, [2]M. Rama Krishna and [1]D. Bujji Babu
[1]Prakasam Engineering College, Kandukur, Prakasam Dt. A.P., India
[2]Department of Information Technology, Vellammal Engineering College, Chennai, A.P. Tamil Nadu, India

Abstract: In this study, we introduced right sigmoidal signal as an activation function for block cipher to perform an approximation problem. We used right sigmoidal signal activation function for feed forward neural network used as a cryptanalysis tool for a Fiestel type block cipher problems.

Key words: Activation function, approximation problem, block cipher, cipher text, cryptanalysis, feedforword neural network, neuron, plain text, sigmoidal signal

INTRODUCTION

Information security is one of the major concerns in cipher age. Cryptology is extremely vital for information security. It has wide applications in defence. Cryptanalysis refers to the study of ciphers, cipher text, or cryptosystems with a view to finding weaknesses in them that will permit retrieval of the plaintext from the cipher text, without necessarily knowing the key or the algorithm. This is known as breaking the cipher, cipher text, or cryptosystem. Cryptanalysis plays an important role in the development of strong cryptographic algorithms. It helps researchers in identifying the vulnerability of the cipher system. With advancement in computing technology and mathematical sciences, cryptographic algorithms have to be made more sophisticated so that the computational complexity and the time required to break into cipher systems is too large. In this study, we used right sigmoidal signal as an activation function for feed forward neural network that perform a new attack for block cipher right sigmoidal signal is introduced for approximation problems (Allan, 1999).

MATERIALS AND METHODS

Feistel block ciphers: Feistel networks were invented by IBM cryptography researcher Horst Feistel and 1st commercially seen in IBM's Lucifer cipher, designed by Feistel and Don Coppersmith. Feistel networks gained respectability when the US Federal Government adopted the DES (a cipher based on Lucifer, with improvements made by the NSA) (Feistel, 1973). Like other components of the DES, the iterative nature of the feistel construction makes implementing the cryptosystem in hardware easier (particularly on the limited hardware available at the time of DES' design). Most modern (non-military) symmetric block ciphers are based on feistel networks and the structure and properties of feistel ciphers have been extensively explored by cryptographers.

Split the plaintext block into 2 equal pieces (L_0, R_0) For each round i =1, 2,.., n, compute

$$L_i = R_{i-1}, R_i = L_{i-1} \text{ XOR } f(R_{i-1}, K_i)$$

where:

f = The round function
K_i = The sub-key
XOR = Exclusive OR operation

Then the cipher text is (L_n, R_n). Regardless of the function f, decryption is accomplished via $R_{i-1} = L_i$, $L_{i-1} = R_i$ XOR f (R_{i-1}, K_i). The Fig. 1 shows both encryption and decryption of Fiestel.

Differential cryptanalysis: Differential cryptanalysis is a potent cryptanalytic technique introduced by Biham and Shamir (2002). Differential cryptanalysis is designed for the study and attack of DES-like cryptosystems. A DES-like cryptosystem is an iterated cryptosystem, which relies on conventional cryptographic techniques such as substitution and diffusion. CA cryptosystems are clearly in this category, so one might expect them to yield to a differential cryptanalytic attack. Yet, due to their probabilistic nature, CA cryptosystems resist automatic application of Biham and Shamir's (2002) techniques.

Corresponding Author: K.V. Srinivasa Rao, Prakasam Engineering College, Kandukur, Prakasam Dt A.P., India

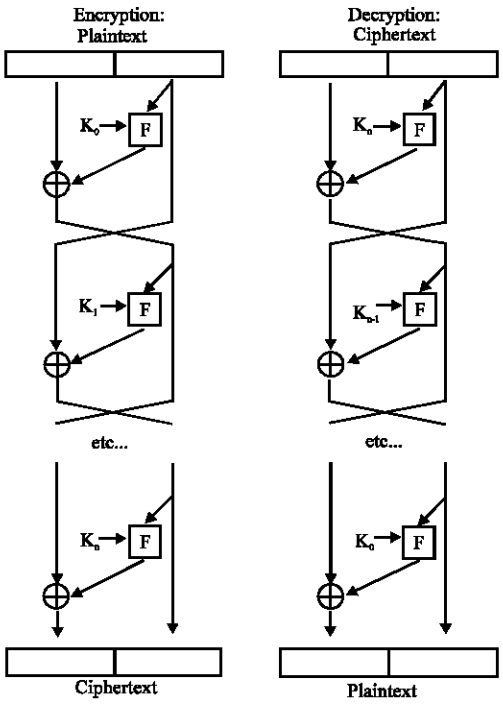

Fig. 1: Feistel structure

Differential cryptanalysis is a chosen-plaintext/ chosen-cipher text cryptanalytic attack. Cryptanalysts choose pairs of plaintexts such that there is a specified difference between members of the pair. They then study, the difference between the members of the corresponding pair of cipher texts. Statistics of the plaintext pair-cipher text pair differences can yield information about the key used in encryption. All of the cryptosystems thus, far studied using differential cryptanalysis are non-probabilistic cryptosystems in which each plaintext corresponds to a unique cipher text, i.e. block vs. block-link cryptosystems (William, 2003). In a block-link, cryptosystem differences in the link as well as differences in the block can be considered. We will first consider fixing the link and producing differences in the block and then consider fixing the block and producing differences in the link.

Artificial neuron model: The transmission of a signal from 1 neuron to another through synapses is a complex chemical process in which specific transmitter substances are released from the sending side of the junction. The effect is to raise or lower the electrical potential inside the body of the receiving cell. If this potential reaches a threshold, the neuron fires. It is this characteristic that the artificial neuron model proposed by McCulloch and Pitts (1943), attempt to reproduce. The neuron model shown in Fig. 2 is the one that is widely used in artificial neural networks with some minor modifications on it.

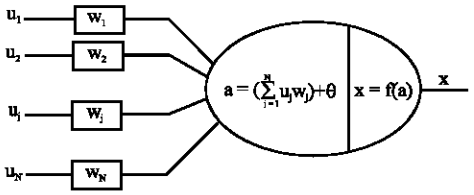

Fig. 2: Neuron of McCulloch and Pitts (1943) model

Once the input layer neurons are clamped to their values, the evolving starts: layer by layer, the neurons determine their output. This ANN configuration is often called feed-forward because of this feature.

The dependence of output values on input values is quite complex and includes all synaptic weights and thresholds (Ling, 1999; McCulloch and Pitts, 1943).

Activation function: The artificial neuron given in Fig. 2 has N inputs, denoted as u_1, u_2, .. u_N. Each line connecting these inputs to the neuron is assigned a weight, which are denoted as w_1, w_2,.., w_N, respectively. Weights in the artificial model correspond to the synaptic connections in biological neurons. If the threshold in artificial neuron is to be represented by θ, then the activation is given by the formula:

$$a = \left(\sum_{j=1}^{N} w_j u_j \right) + \theta$$

The inputs and the weights are real values. A negative value for a weight indicates an inhibitory connection, while a positive value indicates an excitatory one. Although, in biological neurons, θ has a negative value; it may be assigned a positive value in artificial neuron models. If θ is positive, it is usually referred as bias. For mathematical convenience, + sign is used just before θ in the activation formula. Sometimes, the threshold is combined for simplicity into the summation part by assuming an imaginary input u_0 having the value +1 with a connection weight w_0 having the value. Hence, the activation formula becomes output (Ling, 1999; McCulloch and Pitts, 1943).

Output function: The output value of the neuron is a function of its activation and it is analogous to the firing frequency of the biological neurons:

$$x = f(a)$$

Originally the neuron output function f (a) in McCulloch Pitts model is proposed as unit step function (Ling, 1999; McCulloch and Pitts, 1943). However, the artificial neuron model has been expanded to include other functions such as the sigmoid, piecewise linear and

Gaussian. The identity function is the simplest possible activation function; the resulting unit is called a linear associator (Ling, 1999; McCulloch and Pitts, 1943).

Feedforward neural networks: In feed forward neural networks, the neurons are organized in the form of layers. The neurons in a layer get input from the previous layer and feed their output to the next layer. In this kind of networks, connections to the neurons in the same or previous layers are not permitted. The last layer of neurons is called the output layer and the layers between the input and output layers are called the hidden layers. The input layer is made up of special input neurons, transmitting only the applied external input to their outputs. In a network, if there is only the layer of input nodes and a single layer of neurons constituting the output layer, then it is called single layer network. If there are 1 or more hidden layers, such networks are called multilayer networks (Baurn, 1988). The structures, in which connections to the neurons of the same layer or to the previous layers are allowed, such networks are called recurrent networks. For a feed forward network, there always exists an assignment of indices to neurons, so that the weight matrix is triangular, indicating these neurons with smaller indices. Furthermore, if the diagonal entries are zero, which indicates that there is no self-feedback on the neurons (Fig. 3).

Approaximation problem: The approximation problem can then be stated formally as:

$$\rho (F (W^*, X), f (X)) \leq \rho (F (W, X), f (X))$$
$$\text{for all } W \text{ in the set } \rho$$

where:

f (X) = A continuous function defined on set X

F (W, X) = An approximating function that depends continuously on $W \in \rho$ and X, the approximation problem is to determine the parameters W*

A solution to this problem, if it exists, is said to be a best approximation. The existence of a best approximation depends ultimately on the class of functions to F (W, X) (Baurn, 1988; Barron, 1993; Allan, 1999).

Some common choice for activation functions σ from Allan (1999).

- The Heaviside function mentioned above is $\sigma_{(t)} = X_{(0,\infty)}$ (t). This is sometimes referred to in the neural network literature as the threshold function
- The logistic sigmoidal function is given by

$$\sigma_{(t)} = \frac{1}{1+e^{-t}}$$

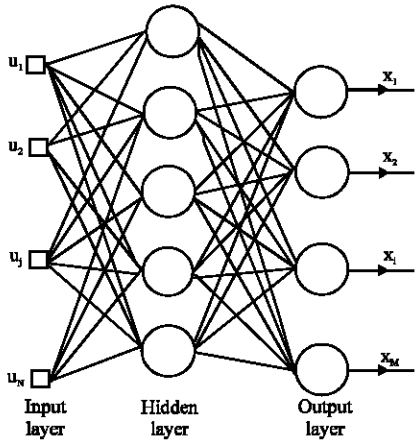

Fig. 3: Layered feed forward neural network

- $\sigma_{(t)} = \tan h_{(1/2)}$, which is logistic sigmoidal function
- The piecewise linear function is of the form

$$\sigma_{(t)} = \begin{cases} 0, & t \leq -1, \\ (t+1)/2 & -1 \leq t \leq 1, \\ 1, & t \geq 1 \end{cases}$$

- The Gaussian sigmoid is given by

$$\sigma_{(t)} = \frac{1}{(2\pi)^{(1/2)}} \int_{-\infty}^{t} e^{-y^2/2} dy$$

- The arctan sigmoid is given by

$$\sigma_{(t)} = \frac{1}{\pi} \arctan_{(t)} + \frac{1}{2}$$

The universal approximation theory is directly applicable to the feed forward neural network with back propagation algorithm (Barron, 1993). The same way, we used to approximate any block cipher, which is n by n discrete mapping between the plain text space and out put cipher text space using right sigmoidal signal as an activation function for feed forward neural networks.

The following definitions of generalized sigmoidal signal and certain approximation theorems are used in the problem (Fig. 4).

Definition 1: $\sigma: R \to R$ is called a generalized sigmoidal function, if

$$\lim_{x \to -\infty} \sigma(x) = 0 \quad \text{and} \quad \lim_{x \to +\infty} \sigma(x) = 1$$

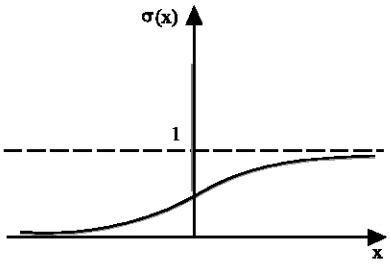

Fig. 4: Generalized sigmoidal signal

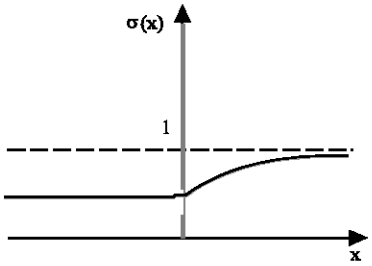

Fig. 5: Right sigmoidal signal

Example: σ: R → R is defined by

$$\sigma(x) = \frac{1}{1+e^{-\alpha x}},\ \alpha>0$$

is generalized sigmoidal function.

Definition 2: The function σ: R→ R is said to be right sigmoidal, if

$$\lim_{x\to+\infty} \sigma(x)=1$$

(Ramakrishnan *et al*., 2006).

Example: σ: R→ R is defined by

$$\sigma(x)=\begin{cases}1-e^{-\alpha x}, & \text{for } x>0,\ \alpha>0\\ \beta, & \text{for } x<0,\ \beta>0\end{cases}$$

is a right sigmoidal function.

The following theorem shows that a left and right sigmoidal signals can be pasted to form a generalized sigmoidal signals (Fig. 5).

Neural network attacks with right sigmoidal signal as an activation

Theorem: Consider an iterated block cipher with block size m. Express the output of the round just before the last as an m-m mapping and use a feed forward neural network with rig ht sigmoidal signal as an activation function to approximate this mapping using a set of known plain text-partially decoded cipher text pairs obtained from a guessed value of the last round key. Further assume that the trained multilayer feed forward neural network with right sigmoidal signal as an activation function obtained from a wrongly guessed value of the last round key will produce a random output and uniformly distributed over the output bits when tried with other known plain text-partially decrypted text pair, then there exist a feed forward neural network with right sigmoidal signal as an activation function attack to the cipher at hand such that the last round key is obtained by dropping out the values of the wrong key.

RESULTS AND DISCUSSION

Proof: Let y be the output of the cipher given a particular input x and y_1 be the partially decrypted cipher text with the correct value of the key K and y_1 be the obtained by a wrong guess of the key.

We assume that the last round function mapping is g (.), then y_1 is the inverse of g (k, y).

Therefore, y_1 is the inverse of g (k, y) and is equal to inverse of g (k_1, g (k. y_1)), a trained feed forward neural network with right sigmoidal signal as an activation function with wrong guessed key value will actually be a random mapping that is not likely to guess values that are not trained by in a uniformly distributed environment.

CONCLUSION

Feed forward neural network with sigmoidal signal as an activation function gives better performance than generalized sigmoidal signal in universal approximation. We used right sigmoidal signal activation function for feed forward neural network used as a cryptanalysis tool for a Feistel type block cipher problems. Future research is to find a new kind of sigmoidal signal for feed forward neural network for cryptanalysis.

ACKNOWLEDGEMENTS

We are grateful to medwell journals for providing the opportunity to publish this article. We would like to thank our research supervisors Prof. M.M. Naidu, Principal, SVU College of Engineering, Thirupathi A.P., India and Dr. R. Sivaramprasad, Associate Professor, ANU College, Acharya Nagarjuna University, Guntur, A.P. India for their guidance, support and understanding throughout this article. We are extremely thankful to Dr. Kancharla Ramaiah, secretary and correspondent, Prakasam

Engineering College, Kandukur, Prakasam (Dt) A.P. India for providing the research environment and inspiration. Finally, we would like to thank our friends and our family members for their love and support.

REFERENCES

Allan, P., 1999. Approximation theory of the MLP model in neural networks. Acta Numerica, 8: 143-195.

Barron, A.R., 1993. Universal approximation bounds for super positions of a sigmoidal function. IEEE. Trans. Inform. Theory, 39 (3): 930-945.

Baurn, E.B., 1988. On the capabilities of multilayer perceptrons. J. Complex., 4: 193-215.

Biham, E. and A. Shamir, 2002. Differential cryptanalysis of DES-like cryptosystems. J. Cryptologsis, 36 (3): 189-221.

Feistel, H., 1973. Cryptography and computer privacy. Scientific Am., 228: 15-23.

Ling, Z.B.Z., 1999. A geometrical representation of McCulloch-Pitts neural model and its applications neural networks. IEEE. Trans. Neural Networks, 10 (4): 925-927.

Ramakrishnan, M., C.M. Velu, N. Prabakaran, K. Ekambavanan, P. Thangavelu and P. Vivek-anandan, 2006. Function approximation using feedforward Neural Networks with sigmoidal signals. Int. J. Soft Comput., 1 (1): 76-82.

McCulloch, W.S. and W. Pitts, 1943. A logical calculus of the ideas immenent in nervous activity. Bull. Mathe. Biophysic., 5: 115-133.

William, S., 2003. Cryptography and Network Security. 3rd Edn. Prentice Hall.