A REVIEW ON BIOLOGICAL INSPIRED COMPUTATION IN CRYPTOLOGY

Subariah Ibrahim[1] **Mohd Aizaini Maarof[2]**

Department of Communication and Computer System
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia, Skudai 81300, Johore, Malaysia

[1]*Tel: +60-07–557-6160 x 32386, Fax: +60-07–556-5044, E-mail: subariah@fsksm.utm.my*

[2]*Tel: +60-07–557-6160 x 32009, Fax: +60-07–556-5044, E-mail: maarofma@fsksm.utm.my*

Abstract

Cryptology is a field that concerned with cryptography and cryptanalysis. Cryptography, which is a key technology in providing a secure transmission of information, is a study of designing strong cryptographic algorithms, while cryptanalysis is a study of breaking the cipher. Recently biological approaches provide inspiration in solving problems from various fields. This paper reviews major works in the application of biological inspired computational (BIC) paradigm in cryptology. The paper focuses on three BIC approaches, namely, genetic algorithm (GA), artificial neural network (ANN) and artificial immune system (AIS). The findings show that the research on applications of biological approaches in cryptology is minimal as compared to other fields. To date only ANN and GA have been used in cryptanalysis and design of cryptographic primitives and protocols. Based on similarities that AIS has with ANN and GA, this paper provides insights for potential application of AIS in cryptology for further research.

Keywords: Cryptography, Cryptanalysis, Artificial Neural Network, Genetic Algorithm and Artificial Immune System.

1. Introduction

Cryptography is a branch in cryptology that concerned with the construction of schemes that are resilient against malicious attacks. The schemes are designed in such a way as to ensure the security services of confidentiality, authenticity and integrity of messages. Another branch of cryptology is cryptanalysis that delves with the violation of security services to obtain messages. Major works in cryptology are based on number and information theory. The advances in software technology and systems will give more computational power for cryptanalyst to break the cipher. As new computational environment becomes more distributed, more diverse and more global, the transmission of information is becoming more vulnerable to adversary attacks. Thus making the design of cryptographic schemes that can counter new cryptanalysis techniques is becoming harder.

Biological systems can be regarded as sophisticated information processing systems and can provide inspiration for various ideas in engineering and technology. Modern artificial intelligence (AI) employs biological prototypes such as neural networks, genetic code and immune system for AI modeling. Artificial Neural Network (ANN), Genetic Algorithm (GA) and Artificial Immune System (AIS) are AI modeling for neural network, genetic code and immune system respectively. These AI models use the basic elements of the prototypes and their rules of interactions to define computational models

that can be applied to solve problems in various fields [1]. Over the past few decades there has been a growing interest in the use of biology as a source of inspiration for solving computational problems. This area of research is often referred to as Biologically Inspired Computing (BIC) [2].

Techniques taken from BIC, especially GA, ANN and AIS are steadily gaining ground in the area of cryptology and computer security. The goal of this paper is to review major works in the application of BIC in cryptology. Firstly, BIC computational models will be discussed, particularly GA, ANN and AIS. In the next section, the application of BIC in cryptology will be provided and the last section will conclude with some remarks.

2. Biological Inspired Computational Paradigm

Various aspects of biology have always been the inspiration in developing computational models and problem solving methods [3]. Primarily, the motivation of this field is to extract useful metaphors from natural biological systems, in order to create effective computational solutions to complex problems in a wide range of domain areas [2]. However, the actual models of computation used do not really correspond to what actually happens in biology, except at a fairly superficial level. BIC paradigm can be classified into: GA, ANN, AIS, DNA, Cellular Automata (CA) and ant colony. However, the focus of this paper is in GA, ANN and AIS. The more notable development are GA and ANN which has been applied to various fields whereas there have been relatively few applications in AIS [4]. The hybrid of GA, ANN and AIS can also be created in order to benefit the combining strengths of different paradigms [5][6].

2.1 Genetic Algorithm

GA mimics the evolutionary principles rooted in biological evolution inspired by neo-Darwinian theory [2]. Hence, the computational model is based on genetic and evolution. GA has been successfully applied to numerous applications in the field of search and optimization. The computer finds better and better solutions to a problem just as species evolve to better adapt to their environment [7]. GA was developed by Prof. J.Holland and his colleagues at the University of Michigan in 1965 [8]. It is an iterative procedure that consists of a constant-size population of individuals whereby the initial population is generated at random or heuristically. The population evolves by applying three basic operations, selection of solutions, mating of genes and occasional mutation [9]. These operations can be described as follows:

- Selection: Individuals are selected for survival and reproduction according to their fitness.
- Mating: New individuals are created by recombining and/or introducing genetic variation into the selected individuals.
- Mutation: Randomly perturbs a candidate solution for a better individual.

The basic cycle of GA is as shown in Figure 1. The cycle continues until a certain number of generations whereby the surviving individuals represent a solution to the problem (10).

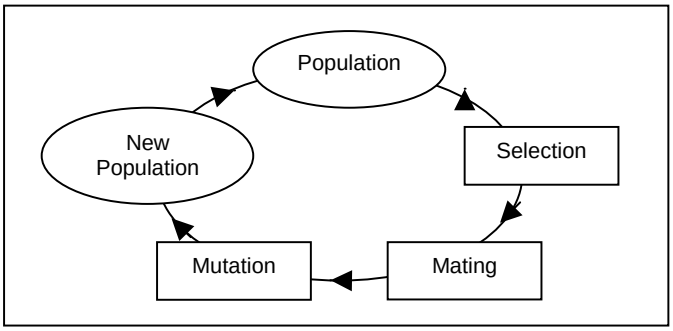

Figure 1: A basic cycle of GA.

2.2 Artificial Neural Network

ANN is a computational model of the brain. The model consists of a number of highly interconnected processors called neurons, which are analogous to the biological neurons in the brain. The neurons are connected by weighted links passing signals from one neuron to another. Each neuron receives several input signals through its connections and produces one output signal [11]. Figure 2 depicts a typical neuron. The manner the neurons are connected determines the flow of information in the network and defines the network model. Amongst the different network models are Multi-Layer Perceptron, Hopfield Networks and Kohonen Networks, each with distinct performance features [12].

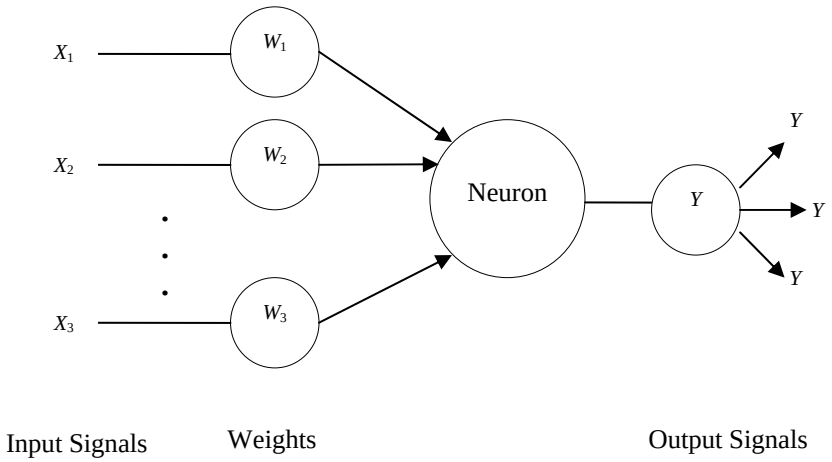

Figure 2: A typical neutron.

ANN is known in their ability to learn and traditionally, there are two types of learning, supervised and unsupervised learning [13][14]. In supervised learning, the network is trained to get expected output by dynamically updating its weight vector, while in unsupervised learning a network receives input and tries to learn about the input distribution [13].

2.3 Artificial Immune System

AIS which is inspired by the immune system represents the new and rapidly growing field of computer science. The approach is expected to give rise to powerful and robust information processing capabilities for complex problems. It possesses all the main properties of an AI system. AIS can learn new information processing, recall previously learned information and perform pattern recognition in highly decentralized fashion. Currently, AIS adopted three immunological principles [15][3]:

- Negative Selection
- Clonal Selection
- Immune Network Theory

The main role of the immune system is to provide defense mechanisms against foreign cells and to remove the malfunctioning cells. In order to perform these functions, the immune system needs to distinguish between good cells (known as self) and bad cells (non-self). The self elements that recognize any element of the self are eliminated. The process creates circulating self elements that react to non-self molecules only and thus is known as negative selection.

Clonal selection is a theory that explains how the immune system fights against non-self elements known as antigens. The system replicates the cells whose receptors can recognize and bind with an antigen. The replication is proportional to their degree of recognition. During the replication, individual cells undergoes a mutation so that it will be more adapted to the antigen recognition [5][15]. A basic algorithm of clonal selection is CLONALG [15][16]. The algorithm has some similarities with GA.

Immune network theory was proposed by Jerne in 1974 where she hypothesized that the immune cells and molecules are capable of recognizing each other in addition to recognizing invading antigens [5][15]. This endows in a network of communication between immune cells. When an immune cell recognizes an antigen or another immune cell, it is stimulated resulting in cell proliferation, cell activation and antibody secretion. However, when the cell is recognized by another immune cell, it is suppressed [15].

The computational model of AIS has been applied in various fields such as pattern recognition and classification, data analysis, computer security, robotics and optimization, information security and fault detection. In the field of information security, AIS is exploited in intrusion and detection system [17][18], virus detection [19] and steganography [20]. In fact, the analogy between computer security problems and biological processes was recognized as early as 1987, when the term “computer virus” was introduced by Adelman [21]. The role of the immune system may be considered analogous to that of computer security systems [22].

3.0 Review on Biological Intelligence Application in Cryptology

In this section, the application of BIC in cryptology will be presented. Literature review shows that GA, ANN, DNA, CA and ant colony have been exploited in cryptology. The review focuses mainly on works done using GA and ANN, however the works on DNA, CA and ant colony will be mentioned briefly for readers awareness.

3.1 Genetic Cryptology

Major works that involves GA focuses on cryptanalysis of cryptographic algorithms and design of cryptographic primitives. Most cryptanalytic research using GA was done on classical ciphers. An initial attempt was conducted by Spillman *et al.*, whereby GA is exploited to cryptanalyse simple substitution ciphers [23]. Since known cryptanalytic attack for simple substitution ciphers employs frequency distribution of characters in the message [24], Spillman derived a cost or fitness function based on single-character and digram frequency distributions in his work. His attempt was fruitful as GA was proven to be highly successful in this cryptanalysis. He suggested the use of trigram frequency distribution and variations on crossover and mutation procedures as future research. Spillman continues his work and illustrated that GA can also be used in the cryptanalysts of public key cryptosystem, the knapsack ciphers [25]. The encryption scheme for knapsack ciphers is based on the NP-complete problem, which is a hard problem.

Another initial attempt conducted by Matthews [26] investigated the use of GA in cryptanalysis of transposition ciphers. In this work the fitness function is based on the message length, frequency distribution of digrams and trigrams tested for, the number of digrams and trigrams checked for and the likelihood of occurrence in successful deciphered messages.

An extensive research on classical cipher cryptanalysis was investigated by Clark in his PhD work [27] and Bagnall [28]. Clark's cryptanalytic attack work covers a variety of classical ciphers that include simple substitution, transposition as well as poly-alphabetic ciphers. He proposed new attacks on these ciphers, which utilize simulated annealing and the tabu search. Existing attacks which make use of the genetic algorithm and simulated annealing are compared with the new simulated annealing and tabu search techniques. A comparison of search techniques of GA, simulated annealing and tabu search on cryptanalytic attack on simple substitutions was presented in a journal paper [10]. He showed that the tabu search outperformed the other techniques when used in the cryptanalysis of these ciphers. A parallel GA was proposed for attacking the poly-alphabetic substitution cipher by solving each of the key positions simultaneously. Through experimental evidence, he showed that parallel GA is highly efficient in solving poly-alphabetic ciphers even with a large period. On the other hand, Bagnall concentrates his work on cryptanalysis of Rotor machine [28]. He used a fitness function based ont the phi test for non-randomness of text and showed that an unknown three rotor machines can be cryptanalysed with about 4000 letters of ciphertext.

The research using GA approach in cryptanalytic attack is gaining popular in the 2^{nd} millennium. Further work on cryptanalytic attack on classical cipher is still taking place [29][30][31][32][33] while the work on modern ciphers emerges. Hernandez did the attack on two rounds TEA cipher [34] while Ali worked on RSA timing attack [35].

Another major application of GA in cryptology is in the design of Boolean functions and S-Boxes. The Boolean function is the linear combinations of S-box columns, which is an important cryptographic primitive for block and stream ciphers. The choice of Boolean functions used must be carefully considered when designing cryptosystems so that the cipher is not vulnerable to cryptanalytic attacks. Boolean functions for ciphers must be highly non-linear and balanced [36]. The conventional methods of Boolean function design are random generation and direct construction. By

using random generation, it is difficult to find functions with truly excellent properties due to the vast size of the search space while direct constructions may only meet certain design criteria. Millan enhanced his earlier work in designing balanced Boolean function using GA by combining it with the two-step hill climbing algorithm [37]. The hill climbing technique has improved the performance of GA in generating highly non-linear and balanced Boolean functions. Dimovski employs similar techniques but only tested for non-linearity criteria and compared it with random search which proved to be more powerful technique [38]. Finally, other application of GA in cryptology is the design of security protocols. Clark showed how simulated annealing and GA can be used to evolve efficient and provably correct protocols [39].

3.2 Neural Cryptology

ANN application in cryptology can be categorized in two sub-fields, that is cryptanalysis and key-exchange. Neural cryptanalysis work was conducted by Ramzan [40]. The aim of the research is to introduce new cryptanalytic techniques based on principles from machine learning, particularly ANN. He used Unix Crypt cryptosystems as a test bed and the results showed that ANN can accurately predict many of the plaintext bits with high probability even though the transfer function chosen for the network was rather naive. This proved that ANN can be trained to do cryptanalytic attack.

The work on neural key exchange is rather a new research area. The work in this area is performed by a research group from Institute for Theoretical Physics in Wurzburg, Germany and Minerva Center, Bar-Ilan University in Ramat-Gan, Israel [41][42]. Key exchange protocol is a cryptographic protocol that enables two users to exchange a key which will then be used for subsequent encryption of messages in a secure manner through public channel [24]. The first published protocol for this exchange is Diffie-Hellman key exchange whereby the security of the protocol is based on the difficulty of computing discrete log over a finite field GF(q)[43].

The neural key-exchange protocol does not employ number theory but is based on a synchronization of neural networks by mutual learning [41]. The architecture used is a two-layered perceptron, exemplified by a parity machine with K hidden units. The secret information of each entity is the initial values for the weights which are secret. Each network is then trained with the output of its partner. The work was extended to multilayer networks, parity machines [42]. When neural cryptography is combined with chaotic synchronization, the synchronization of neural networks accelerates [44]. A feedback mechanism is added to neural cryptography and is capable of enhancing the security of the system [45].

3.3 Other Biological Approaches in Cryptology

Other BIC approaches that are applied in cryptology are DNA, CA and ant colony. The basic element of CA is a biological cell which has a fixed set of states and a fixed position within the node of a spatial grid. It uses a simple mathematical abstraction of the principles of interaction between biological cells. Toffoli and Margolus showed that CA leads to the definition of a computing medium whose computational power is equivalent to the Turing machine [1]. CA has been applied in block and stream ciphers and these ciphers are implemented in hardware [46]. In fact the application of CA in cryptography came as early as 1980's [47].

Cryptography based on one-time-pads was constructed using DNA due to its ultra-scale computation and ultra compact storage, thus only a small amount of DNA is needed for huge one-time-pads [48]. Finally, Bafghi performed a differential cryptanalysis on Serpent using ant colony and claimed that it can be used for any block cipher [49]. Ant colony algorithms are multi-agent systems where the behaviour of each single agent, the ants, is inspired by the behaviour of real ants [15]. *Table 1* summarizes the work done on applications of BIC in cryptology.

Table 1: Biological approach applications in cryptology

Biological Approach	**Cryptology Sub-Field**	**Research Details**	
GA	Cryptanalysis	Classical Cipher	Simple Substitution, Transposition, Polyalphabetic, Rotor Machine, Knapsack
		Modern Cipher	TEA, RSA
	Cryptographic Primitive	Boolean Function and S-Box	
	Cryptographic Protocols	Protocol Design	
NN	Cryptanalysis	Unix Crypt	
	Cryptographic Protocols	Key Exchange	
DNA	Cryptographic Algorithm	Encryption	
CA	Cryptographic Algorithm	Encryption for Stream and Block Cipher	
Ant Colony	Cryptanalysis	Encryption for Block Cipher	

4. Immune Cryptology

Analysis from the literature shows that AIS has some similarities with GA and ANN [12][15][50]. GA can be used for solving hard problems [9], thus sharing the same major characteristic with cryptology [39]. In cryptology, GA is used to heuristically design cryptographically strong balanced Boolean function, cryptographic protocols and techniques of cryptanalysis of several cryptographic algorithms [26][28][29][30][38][51]. The clonal selection algorithm of AIS computational model is similar to GA [15][16]. Cziko noted that the clonal selection can be interpreted as a Charles Darwin's law of evolution, with the three major principles of repertoire diversity, genetic variation and natural selection [16]. Hence, it is in our opinion that this algorithm may be applied in the same cryptology subfield where GA was applied.

As discussed in section 3.2, ANN has been exploited to do key exchange protocol and cryptanalysis. ANN is a computational tool originally designed to model the human brain aiming at producing an "intelligent behaviour". Castro and Zuben performed theoretical and empirical comparisons between ANN and aiNET, the artificial immne

network model and found that there are many similarities between them [52]. Immune network models have been used for the improvement of ANN models [5][53]. Castro and Zuben applied an immunological approach to initialize feed-forward neural network weights [53]. Tarakanov, in his paper [54] showed the principal possibility of using Formal Immune Network (FIN) for encryption but to date no work has been pursued. In order to prove that FIN is suitable, a rigorous mathematical model based on FIN that can be used for encryption need to be explored.

The discussion in this section suggests that application of AIS in cryptology is open to further investigations and innovations. A hybrid of BIC paradigms may also be explored to enhance the performance of the existing work.

5. Conclusion

This paper summarizes the work done in cryptology that employed BIC paradigm. A survey of literature shows that only a few research works exploits BIC in cryptology. However, there is a growing interest from the computer security community towards GA and ANN approach in cryptology in the second millennium. The potential utilization of ANN and GA has been shown useful in the design and analysis of cryptographic primitives, cryptographic protocols and cryptanalysis. However no work has been done in cryptology using the new emerging field of AIS. Since AIS shares some similarities with ANN and GA, thus it may have potential application in cryptology. A hybrid of AIS, ANN and GA for the application in cryptology may also be tackled for future research.

References

[1] Tarakanov, A.O., Skormin, V.A. and Sokolova, S.P. (2003). *Immunocomputing: Principles and Applications*. Springer-Verlag, New York.

[2] Castro, L.N. and Timmis, J. (2002). *Artificial Immune System: A New Computational Intelligence Approach*. Springer-Verlag, New York.

[3] Dasgupta, D., Ji, Z. and Gonzalez, F. (2003). Artificial Immune System (AIS) Research in the Last Five Years. *In Proceedings of Conference on Evolutionary Computation*, 8-12 December. Canberra, Australia.

[4] Dasgupta, D. and Attoh-Okine, N. (1997). Immunity-Based Systems: A Survey. *In the Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, Orlando, USA.

[5] Castro, L.N. and Timmis, J.I. (2003). Artificial Immune System as a Novel Soft Computing Paradigm. *Soft Computing Journal*, 7(7): 526-544.

[6] Bonissone, P.P., Chen, Y., Goebel, K. and Khedkar, P.S. (1999). Hybrid Soft Computing Systems: Industrial and Commercial Applications. *In Proceedings of The IEEE,* 87(9):1641-1667.

[7] Munakata, T. (1998). *Fundamentals of the New Artificial Intelligence: Beyond Traditional Paradigms*, Springer, New York.

[8] Deb, K. (1998). Genetic Algorithms in Search and Optimization: The Technique and Applications. *Proceedings of International Workshop on Soft Computing and Intelligent Systems*, pp. 58-87, Calcutta, India: Machine Intelligence Unit, Indian Statistical Institute.

[9] Tomassini, M. (1996). Evolutionary Algorithms. *In Proceedings of International Workshop: Towards Evolvable Hardware, LNCS 1062*, Springer-Verlag.

[10] Clark, A., Dawson, E. (1998). Optimisation Heuristics for the Automated Cryptanalysis of Classical Ciphers. *JCMMCC*, 28:63-86.
[11] Negnevitsky, M. (2002). *Artificial Intelligence: A Guide to Intelligent System*. Addison-Wesley, Harlow, England.
[12] Dasgupta, D. (1997). Artificial Neural Networks and Artificial Immune Systems: Similarities and Differences. *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*, Orlando, USA.
[13] Rosen-Zvi, M., Klein, E., Kanter, I. And Kinzel, W. (2002). Mutual Learning in a Tree parity Machine and its Application to Cryptography. *Phys. Rev. E*.66.
[14] Bailey, D. and Thompson, D. (1990). How to Develop Neural Network. *AI Expert*, June Issue, pp. 38-47.
[15] Castro, L.N. (2002). Immune, Swarm and Evolutionary Algorithms, Part I: Basic Models, *Proc. of the Int'nal Conf. On Neural Information Processing, Workshop in Immune Systems*, 3:1464 - 1468, Singapore.
[16] Castro, L.N. and Zuben, F.J.V. (2002). Learning and Optimization Using the Clonal Selection Principle. *IEEE Trans. On Evolutionary Computation, Special Issue on Artificial Immune System*, 6(3):239-251.
[17] Kim, J.W. (2002). Integrating Artificial Immune Algorithms for Intrusion Detection. *PhD Dissertation*, Department of Computer Science, University College London.
[18] Esponda, F., Forrest, S.and Helman, P. (2003). A Formal Framework for Positive and Negative Detection Scheme. *IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics 1*.
[19] Goel, s. and Bush, S.F. (2003). Kolmogorov Complexity Estimates for Detection of Viruses in Biologically Inspired Security System: A Comparison with Traditional Approach. P*roceedings in Adaptive and Resilient Computing Security Workshop*. Santa Fe.
[20] Jackson, J.T., Gunsch, G.H., Claypoole, R.L., Lamont, G.B. (2003). Blind Steganography Detection Using a Computational Immune System: A Work in Progress, *International Journal of Digital Evidence*, 4(1).
[21] Cohen, F. (1987). Computer Viruses. *Computers & Security*, 6:22-35.
[22] Forrest, S., Perelson, A. S. Allen, L. and Cherukuri, R. (1994). Self-nonself Discrimination in A Computer. *Proceedings of IEEE Symposium on Research in Security and Privacy*, Los Alamos, CA. IEEE Computer Society Press.
[23] Spillman, R., Janssen, M., Nelson, B. and Kepner, M. (1993). Use of Genetic Algorithms in the Cryptanalysis of Simple Substitution Ciphers. *Cryptologia*, XVII(1):31-43.
[24] Stallings, W. (2003). *Cryptography and Network Security: Principles and Practices*, 3rd Edition. Upper Saddle River, New Jersey: Prentice Hall.
[25] Spillman, R. (1993). Cryptanalysis of Knapsack Ciphers Using Genetic Algorithms. *Cryptologia*, XVII(4):367-377.
[26] Clark, J.A. (2003). Nature-Inspired Cryptography: Past, Present and Future. In *Proceedings of Conference on Evolutionary Computation*, 8-12 December. Canberra, Australia.
[27] Clark, A. (1998). Optimization Heuristics for Cryptology. *Ph.D. Dissertation*, Faculty of Information Technology, Queensland University of Technology, Australia.
[28] Bagnall, A.J. (1996). The Applications of Genetic Algorithms in Cryptanalysis. *M.Sc. Thesis*. School of Information System, University of East Anglia.
[29] Dimovski, A., Gligoroski, D. (2003). Attack on the Polyalphabetic Substitution Cipher Using a Parellel Genetic Algorithm. *Technical Report, Swiss-Macedonian Scientific Cooperation through SCOPES Project, March 2003*, Ohrid, Macedonia.
[30] Dimovski, A., Gligoroski, D. (2003). Attacks on Transposition Cipher Using Optimization Heuristics. *In Proceedings of ICEST 2003*, October, Sofia, Bulgaria.

[31] Morelli, R.A. and Walde, R.E. (2003). A Word-Based Genetic Algorithm for Cryptanalysis of Short Cryptograms. P*roceedings of the 2003 Florida Artificial Intelligence Research Symposium* (FLAIRS – 2003), pp. 229-233.

[32] Morelli, R.A., Walde, R.E., Servos, W. (2004). A Study of Heuristic Search Algorithms for Breaking Short Cryptograms. *International Journal of Artificial Intelligence Tools (IJAIT)*, Vol. 13, No. 1, pp. 45-64, World Scientific Publishing Company.

[33] Servos, W. (2004). Using Genetic Algorithm to Break Alberti Cipher. *Journal of Computing Science in Colleges*, Vol. 19(5): 294-295.

[34] Hernandez, J.C., Sierra, J.M., Isasi, P., Ribagorda, A. (2002). Genetic Cryptanalysis of Two Rounds TEA. *ICCS 2002*, *LNCS 2331*, 1024 – 1031, Springer-Verlag Berlin Heidelberg.

[35] Ali, H. and Al-Salami, M. (2004). Timing Attack Prospect for RSA Cryptanalysis Using Genetic Algorithm Technique. *The International Arab Journal of Information Technology*, 1(1).

[36] Millan, W., Clark, A. and Dawson, E. (1997). Smart Hill Climbing Finds Better Boolean Functions. *Proceedings of. 4th Annual Workshop on Selected Areas in Cryptography*, Aug. 11-12, SAC 1997.

[37] Millan, W., Clark, A. and Dawson, E. (1998). Heuristic Design of Cryptographically Strong Balanced Boolean Functions. *Advances in Cryptology – EUROCRYPT '98, LNCS 1403*, 489-499, Springer-Verlag, Berlin Heidelberg.

[38] Dimovski, A., Gligoroski, D. (2003). Generating Highly NonLinear Boolean Functions Using a Genetic Algorithm. *In Proceedings of 1st Balcan Conference on Informatics*, November, Thessaloniki, Greece.

[39] Clark, J. A. (2000). Metaheuristic Search as a Cryptological Tool. *Ph.D. Dissertation*, Department of Computer Science, University of York, United Kingdom.

[40] Ramzan, Z. (1998). On Using Neural Networks to Break Cryptosystems. *Manuscrip*t, MIT.

[41] Kanter, I., Kinzel, W. andKanter, E. (2002). Secure Exchange of Information by Synchronization of Neural Networks. *Europhys. Lett.* 57, pp. 141 – 147.

[42] Kinzel, W. and Kanter, I. (2002). Interacting Neural Networks and Cryptography. *Advances in Solid State Physics* 42, ed. By Kramer, B., pp.383.

[43] Diffie, W. and Hellman, M. (1976). *New Directions in Cryptography*. *IEEE Transactions on Information Theory*, 22(6): 644-654.

[44] Mislovaty, R., Klein, E., Kanter, I. And Kinzel, W. (2003). Public Channel Cryptography by Synchronization of Neural Networks and Chaotic Maps. *Phys Rev. Lett*. 91.

[45] Ruttor, A., Shacham, L., Kinzel, W., Kanter, E. (2003). Neural Cryptography with Feedback.

[46] Nandi, S., Kar, B.K. and Chauduri, P.P. (1994). Theory and Application of Cellular Automata in Cryptography. *IEEE Transaction on Computers*, 43(12).

[47] Wolfram, S. (1986). Cryptography with Cellular Automata. *Advances in Cryptology – Crypto 85, LNCS 218*, 429-432. Springer-Verlag

[48] Gehani, A., LaBean, T. and Reif, J., (2000). DNA-Based Cryptography, *Discrete Mathematics and Theoretical Computer Science*, 54:233-249.

[49] Bafghi, A.G. and Sadeghiyan, B. (2003). Differential Model of Block Cipher with Ant Colony Technique. *In Proceedings in Workshops on Coding, Cryptography and Combinatorics*, Yellow Mountain.

[50] Castro, L.N. (2002). Immune, Swarm and Evolutionary Algorithms, Part II: Philosophical Comparisons, *Proc. of the Int'nal Conf. On Neural Information Processing, Workshop in Immune Systems*, 3:1469-1473, Singapore.

[51] Chen, H., Clark, J.A. and Jacob, J.L. (2003). Automated Design of Security Protocols. *Conference on Evolutionary Computation. Special Session on Evolutionary Computation in Computer Security and Cryptography*. Canberra 8-12 Dec. 2003.

[52] Castro, L.N. and Zuben, F.J.V. (2001). Immune and Neural Network Models: Theoretical and Empirical Comparisons. *Int. Journal of Computational Intelligence and Applications*, 1(3): 239-257.

[53] Castro, L.N. and Zuben, F.J.V. (2001). An immunological Approach to Initialize Feedforward Neural Network Weights. *Proc. of Int. Conf. On Artificial Neural Networks and Genetic Algorithms*, 126-129, Prague.

[54] Tarakanov, A.O., (2001). Information security with formal immune networks. *Information Assurance in Computer Networks* (eds. V.I.Gorodetski, V.A.Skormin and L.J.Popyack), *LNCS 2052*. 115-126, Springer-Verlag, Berlin.