*ISSN: 2278 – 1323*
*International Journal of Advanced Research in Computer Engineering & Technology*
*Volume 1, Issue 4, June 2012*

# Particle Swarm Optimization in Cryptanalysis of DES

**Shweta Pandey, Prof. Megha Mishra**

*Abstract*— **In this paper for the first time Particle Swarm Optimization is applied in the field of cryptanalysis of DES based on their ability to selectively explore the solution space of a given problem. PSO is a robust stochastic optimization technique based on the movement and intelligence of swarms. PSO applies the concept of social interaction to problem solving.**
***It was developed in 1995 by James Kennedy* (social-psychologist) and Russell Eberhart (electrical engineer).**
**It uses a number of agents (particles) that constitute a swarm moving around in the search space looking for the best solution. Each particle is treated as a point in an N-dimensional space which adjusts its "flying" according to its own flying experience as well as the flying experience of other particles. It applies the concept of social interaction to problem solving. A complete problem formulation is explained. Conclusion and References are given as appropriate.**

*Index Terms*— **Cipher Text, Data Encryption Standard Cryptanalysis, Particle Swarm Optimization, Plain Text.**

## I. INTRODUCTION

Cryptology is the art and science of making secret codes and breaking secret codes. Cryptography is the technique to camouflage the message, and only intended recipients can remove the camouflage and read the message. The message we want to send is called plaintext and the camouflage message is called cipher text. The process of converting a plaintext into cipher text is called encryption and the reverse process is called decryption Cryptanalysis is the process of recovering the plaintext and/or key from a cipher.

Cryptanalysis of block cipher is a challenging task due to non-linearity in nature. Many cryptographic systems have a finite key space and, hence, are vulnerable to an exhaustive key search attack. Yet, these systems remain secure from such an attack because the size of the key space is such that the time and resources for searches are not available. Ayman M.B.Albassal and Abdel-Moneim A.Wahdan [1] have used the concept of interpolation attack. Their proposed attack has the benefit of being parallel by nature and can be easily extended to a distributed version. Saptarshi Neil Sinha Supravo Palit, Mostafiz Amin Molla, Atreyee Khanra, Malay Kule [2] presents a cryptanalytic attack on Merkle-Hellman Knapsack cipher using Differential Evolution.

Joseph Alexander Brown, Sheridan Houghten [3] provides a preliminary exploration of the use of Genetic Algorithms (GA) upon a Substitution Permutation Network (SPN) cipher. The purpose of the exploration is to determine how to find weak keys. Mohammad Faisal Uddin and Amr M. Youssef [4] proposed Cryptanalysis of Simple Substitution Ciphers Using Particle Swarm Optimization.Vimalathithan R.and M. L. Valarmathi [5] presents Cryptanalysis of DES using Computational Intelligence by GSO.

In this paper PSO is used to find out the plain text from cipher text. The particle swarm algorithm is initialized with a population of random solutions in the search space and searches for optimum solution by adjusting potential solutions over generations. Cryptanalysis can be done either by transposition or substitution. Here cryptanalysis is done by substitution. By using PSO the optimized solution will be obtained. In PSO there are two types of particles (solution) i.e. **particle best** and **global best**. By using these two the best (optimized solution) will be obtained by finding out the least error rate (Fitness function).Among the particle best the error rate will be calculated by comparing the created cipher text (random value).If the error rate will be high the value of original text will remain otherwise it will be replaced.

## II. PARTICLE SWARM OPTIMIZATION

PSO is a robust stochastic optimization technique based on the movement and intelligence of swarms.PSO applies the concept of social interaction to problem solving. It was developed in 1995 by James Kennedy (social-sychologist) and Russell Eberhart. It uses a number of agents particles) that constitute a swarm moving around in the search space looking for the best solution. Each particle is treated as a point in a N-dimensional space which adjusts its "flying" according to its own flying experience as well as the flying experience of other particles.

Particle swarm optimization [6] is a population based, self-adaptive search optimization technique inspired by social behavior of bird flocking or fish schooling. Like other population-based optimization methods such as genetic algorithm, the particle swarm algorithm is initialized with a population of random solutions in the search space and searches for optimum solution by adjusting potential solutions over generations. In PSO every potential solution are called particles. Each particle keeps track of its coordinates in the search space which are associated with the best solution it has achieved so far. This value is called particle best or *pbest* .Another value is the best value

achieved so far by any particle in the population. This value is called global best or *gbest*.After finding the two best values each particle updates its velocity ( $v_{i,j}$ ) and position ( $P_{i,j}$ ) towards its *pbest* and *gbest* locations as follows:

*Particle velocity update:*

$v_{i,j} = c_0 v_{i,j} + c_1 r_1 (Ppbest_{i,j} - p_{i,j}) + c_2 r_2 (Pgbest_{i,j} - P_{i,j})$

*Particle position update:*

$P_{i,j} = P_{i,j} + v_{i,j}$

Where, $Ppbest_{i,j}$ and $Pgbest_{i,j}$ are the particle best and global best position of the particles respectively.

PSO an attractive optimization technique. By varying these factors, it is possible to use PSO in a wide variety of applications.

In traditional PSO, the particle is encoded as a string of positions, which represent a multidimensional space.

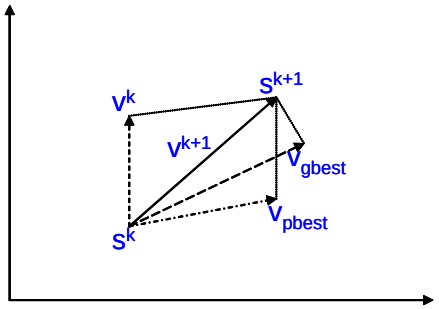


Fig1. Concept of modification of a searching point by PSO

$s^k$: current searching point.
$s^{k+1}$: modified searching point.
$v^k$: current velocity.
$v^{k+1}$: modified velocity.
$v_{pbest}$: velocity based on pbest.
$v_{gbest}$: velocity based on gbest

## III. DATA ENCRYPTION STANDARD

The most widely used encryption scheme is symmetric block cipher called as Data Encryption standard (DES) published by National Institute of standards and Technology (NIST). As with any encryption scheme, there are two inputs to the encryption function: the plaintext to be encrypted and the key. At the encryption site DES takes a 64 bit plan text using 56 bit key and creates a 64 bit cipher text. The encryption process is made of two permutations and sixteen Feistel rounds, where the 64-bit plain text is divided into 32-bit parts, the left part $L_i$ and the right part $R_i$. The round i, $1 \leq i \leq 16$ is defined as follows:

$L_i = R_{i-1}$,

$R_i = L_i \oplus F(R_{i-1}, K_i)$

Where K*i* is the cipher key derived from the **key scheduling algorithm**, which is the 48 bits sub key used in the ith round, and F is a round function. The round function F is the non-linear component of DES and consists of three operations: substitution, permutation and XOR operations. There are eight S-boxes where each one is a substitution mapping 6 to 4 bits. The weakness of DES is out of the 2^56 keys there are four weak keys, six semi weak keys and 48 possible weak keys. The weak key is the one that, after parity drop operation, consist of either of all 0s, all 1s or half zeros and half ones. For example if we take the key '0101010101010101' the actual 56 bit key contains all 0s and the key 'FEFEFEFEFEFEFEFE', the actual 56 bit key is all 1s. A semi weak key creates only two different round keys and a key that creates only four distinct round keys is possible weak keys.

## IV. PROPOSED WORK

By using PSO the optimized solution will be obtained. In PSO there are two types of particles (solution) i.e. **particle best** and **global best**. By using these two the best (optimized solution) will be obtained by finding out the least error rate (Fitness function).Among the particle best the error rate will be calculated by comparing the given cipher text (random value).If the error rate will be high the value of original text will remain otherwise it will be replaced. FA1G02654BCADE56 if this is the key and supposed we have initialized 10 as the number of particles so first the above key will search best means least error rate among itself than among all the 10 particles. So it will take much iteration but will take less time than brute force attack.

.

## V. CONCLUSION

PSO is used for cryptanalysis tool. PSO provides a very powerful tool for the cryptanalysis of DES using a cipher text only attack. One main disadvantage of heuristic optimization a technique (including PSO) is its large sensitivity to parameter variations (e.g., $c_1$ and $c_2$ in PSO). Although fine tuning of these parameters can be done by trial and error, it is interesting to find analytical formula for the optimal regions of these parameters. It is not restricted and can be applied for other block ciphers also. The paper also indicates that it is a much better and efficient technique.

The inclusion of this new technique will force the creation of defenses against it. Differential and linear attacks have lead to the creation of security against them. We believe this being used to break non-classical ciphers to be an interesting, emerging field of research which must be expanded upon in upcoming years.

## REFERENCES

[1] Mohammad Faisal Uddin and Amr M. Youssef"Cryptanalysis of Simple Substitution Ciphers Using Particle Swarm Optimization".
[2] Vimalathithan. R.and M. L. Valarmathi"Cryptanalysis of DES using Computational Intelligence".
[3] Ayman M. B. Albassal and Abdel-Moneim A. Wahdan1993. Neural Network Based Cryptanalysis of a Feistel Type Block Cipher.
[4] Saptarshi Neil Sinha1, Supravo Palit 2, Mostafiz Amin Molla3, Atreyee Khanra4, Malay Kule51997 A Cryptanalytic Attack on Knapsack Cipher Using Differential Evolution Algorithm.

[5] Joseph Alexander Brown, Sheridan Houghten, *Member, IEEE*, and Beatrice Ombuki- Genetic Algorithm Cryptanalysis of a Substitution Permutation.
[6] Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press 1997, ISBN: 0-8493-8523-7.
[7] Howard M. Heys,"A Tutorial on Linear and Differential Cryptanalysis", Cryptologia, vol. **XXVI,** no. 3, pp. 189-221, 2002Cryptologia, vol. XXVI, no. 3, pp. 189-221, 2002
[8] H. Feistel, "Cryptography and Computer Privacy", Scientific American, vol. 228, no. 5, pp. 15-23, 1973.
[9] C. E. Shannon, 'Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, pp. 656-715, 1949.
[10] R. P. Lipmann, "An introduction to computing with neural networks", IEEE ASSP Magazine, pp. 4-22, Apr. 1987.
[11] National Institute of Standards, Advanced Encryption Standard (AES) web site: httD: l/wvw.nist eoviaes
[12] An Introduction to Back-Propagation Neural Networks by Pete McCollum Saipan59@juno.com
[13]Khalil Shihab (2006). "A back propagation neural network for computer network security". *Journal of Computer Science 2*: 710–715.
[14]Shweta pandey(2012)" Cryptanalysis of Feistel cipher using Back propagation Neural Network"Journal of computer science.
[15]Shweta pandey(2012)"Neural cryptanalysis of block cipher"Journal of computer science.

**I Shweta Pandey** received my BTECH degree in IT from IIMT Engineering College, India, in 2006.Pursuing ME degree from SSCET Bhilai, India.My two papers has been published in International journals in 2012. My work is in cryptanalysis using PSO.My first paper was published in IJETAE in the area of Cryptanalysis using Neural network.