Known-Plaintext Attack of DES-16 Using Particle Swarm Optimization

Wafaa G. Abd-Elmonim, Neveen I. Ghali
Faculty of Science, Al-Azhar University,
Cairo Egypt
Email: nev_ghali@yahoo.com

Aboul Ella Hassanien
Faculty of Computers and Information, Cairo University,
Cairo, Egypt
Email: aboitcairo@gmail.com

Ajith Abraham
IT for Innovations, EU Center of Excellence,
Faculty of Electrical Engineering and Computer Science
VSB - Technical University of Ostrava, Ostrava - Poruba, Czech Republic
Machine Intelligence Research Labs (MIR Labs)
Scientific Network for Innovation and Research Excellence, WA, USA
Email: ajith.abraham@ieee.org

***Abstract*—Discovering the root key bits in the cryptanalysis of 16-rounded Data Encryption Standard (DES-160 is considered to be a hard problem. In this paper we present an approach for cryptanalysis of DES-16 based on Particle Swarm Optimization (PSO) using Known-plaintext attack and some equations that deduced from the relationship between sub-key differences and root key information. In Known-plaintext attack the cryptanalyst possesses one or more plaintext/cipher text pairs formed with the secret key and attempts to deduce the root key that used to produce this cipher text. In our approach, PSO is used as optimization technique to collect the optimal effective plaintexts from a plaintext search space according to the proposed fitness function then the set of collected plaintexts and the corresponding cipher texts used to extract the best eight sub-key differences from which most bits of the root key are discovered.**

Keywords-DES; Cryptanalysis; PSO)

I. INTRODUCTION

A cryptosystem is the system which takes unambiguous text message called plaintext as input and produced ambiguous version of the original message called cipher text as output using some secure data called root key. Cryptanalysis is the science of breaking or decoding cipher text into its corresponding plaintext without prior knowledge of the root key or without knowing the real way to decrypt the ciphertext. It is a technique used for searching about the drawbacks in cryptosystems design. It is considered as the one of interest research in the security [3].

Data Encryption Standard differs from the conventional cryptographic algorithms. The major property of DES algorithm is that encryption and decryption are the same processes that are merge substitution and permutation functions but the order of application of the sub-keys is reversed. In this paper we used Known-plaintext attack; in this attack the cryptanalyst possesses a string of plaintext and the corresponding cipher text [2,5].

Many attempts had been performed for attacking the DES. In the previous versions of the attacks on DES some researcher's use of brute force attacks or exhaustive key search. In the brute force attack the attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained, hence the brute force approach may take several days or even years to guess the root key which is used to generate a ciphertext and require high time complexity and less success rate [4,6]. To overcome the above drawbacks, optimization methods have major important in determining optimal solutions for several complex and active troubles.
Laskari et al in [2] used evolutionary computation technique in cryptanalysis of ciphers generated by simplified version of DES. In this contribution PSO was applied as the optimization method and the result indicate that this is a promising approach. Uddin et al in [8] used PSO for the cryptanalysis of simple substitution cipher, based on the experimental results, PSO-based attack proved to be very effective on various sets of encoding keys. Shahzad et al in [4] used binary PSO for the cryptanalysis of four-round DES, the results shown that; it is an effective approach for cryptanalysis of four-rounded DES as compared to the one using Genetic Algorithm.

In this paper we use the Particle Swarm Optimization (PSO) algorithm to address the problem of finding the set of optimal plaintexts from a plaintext search space under the condition that the optimal plaintext having S-boxes input values in the first and the last round are completely different, we focused our attention on S-boxes input values. From the collected optimal plaintexts and the corresponding ciphertexts we infer the correct sub key

978-1-4577-1123-7/11/$26.00 ©2011 IEEE

differences from which most bits of the root key are recovered using some induced equations.

The rest of the paper is organized as follows: Section (II) gives an overview of PSO. Section (III) introduces the Known-plaintext Attack of DES-16 Using Particle Swarm Optimization algorithm. Experimental results are discussed in Section (IV). Finally, Conclusion and Future work are presented in section (V).

II. PARTICLE SWARM OPTIMIZATION

PSO is a population-based optimization technique proposed by Kennedy and Eberhart [1] in 1995 that exploits a population of individuals to search promising regions of the function space. The population is called swarm and the individuals are called particles, each particle is a solution to the problem and moves through the search space with an adaptable velocity according to a certain rule [4]. Each particle has fitness value which is calculated by using proposed fitness function and searches the point that minimizes the evaluation function.

III. DES ATTACK USING PARTICLE SWARM OPTIMIZATION

This section describes the DES-16 attack technique in detail. In the introduced attack S- boxes input values in the first and last round are used to explain the basics of the process of obtaining information on root key. There are two stages of S-boxes input values.

Stage-1: S-boxes input values are equal, this means that

$K_1 \oplus K_{16} = E(R_0) \oplus E(R_{15})$.

For example, let K_1 =101010, K_{16} =111101, $E(R_0)$=011100 and $E(R_{15})$=001011, then S-boxes input has the same values and equal 110110 and $K_1 \oplus K_{16} = E(R_0) \oplus E(R_{15})$ = 010111, for simplify in this example we use 6-bit instead of 48-bit.

Stage-2: S-boxes input values are different, this means that

$K_1 \oplus K_{16} \neq E(R_0) \oplus E(R_{15})$.

The proposed system works as follows:-

Step 1: apply PSO technique in order to collect the optimal plaintexts from the plaintexts search space for which S-boxes input values in the first and last round are completely different, means that which satisfy Stage-2 using Optimization using PSO as described in Algorithm 1.

In traditional PSO, the particle is encoded as a string of positions, which represent a multidimensional space. All the dimensions *D* are normally independent of each other, thus the updates of the velocity and the particle are performed independently in each dimension. In the beginning, particles' positions and velocities are generated randomly [8]. The velocity and position of a particle are updated according to the following rules represented by equation (3) and equation (4) respectively.

$$X_{jd}(t+1) = X_{jd}(t) + V_{jd}(t+1) \quad (1)$$

$$V_{jd}(t+1) = w \times V_{jd}(t) + C_1 r_1 (Pbest_{jd} - X_{jd}(t)) + C_2 r_2 (gbest_d - X_{jd}(t)), \quad (2)$$

Such that $-V_{max} \leq V_{jd} \leq V_{mav}$

Where d = 1, 2, . . .,*D*, j = 1, 2, . . , *N, N* is the population size, *w* is the inertia weight which has the effect of improving the convergence of search by reducing the speed as time progresses C_1 and C_2 are two positive constants, r_1 and r_2 are two random values in the range [0, 1] and $Pbest_{jd}$ and $gbest_d$ are the particle best and global best position of the particles respectively [4].

Step 2: obtaining best sub-key differences from the right hand side of optimal plaintexts and right hand side of corresponding cipher texts using Determine the best eight sub key differences Algorithm (refer to algorithm-2).

Step 3: recovering the root key information using obtained eight sub key differences and some induced equations.

Algorithm 1: Optimization using PSO

Input N, G
Processing: Set initial population randomly
Let number of the collected optimal plaintext M=0
For i =1 to G **Do**
1. Evaluate the fitness function for each particle according to Equation (5)
2. Sort the particles in Descending order according to their Fitness Values.
3. **If** ii equal 1 or 10*n or G (where n is integer number (n=1, 2 …)).
   3.1 Record ***gbest*** position(optimal plaintext).
   3.2 Record the corresponding ciphertext.
   3.3 Let M = M+1
   End if
4. Update *gbest* and *pbest* value.
5. Update particles positions and velocities.

end for
Output: set of optimal plaintext/ciphertexts pairs

Algorithm 2: Determine the best eight sub key differences

Input: the set of optimal plaintext/cipher text pairs
Processing:
For kk=1 to M **do**
Calculate equation (6)
Allocate eight sub key differences
End for
Output: the best 8 sub key differences

A. Fitness Evaluation

The fitness function is the number of the same bits in identical positions between S-boxes input values in first and last round. Particle Swarm Optimization algorithm is randomized procedure that work on the principle of natural evolution. In this paper the cryptanalysis using PSO involves optimal plaintexts search. Each particle represents a plaintext which is a 64 bit binary string. Firstly, the particles positions and velocities take a random values, then the fitness function is evaluate for each particle using equation (3). The optimal plaintext according to minimized the value of fitness function.

$$F(p) = \frac{S}{48} \quad (3)$$

Here, S denotes the number of the same bits in identical positions between S-boxes input values in first and last round. In the other words, between $E(R_0) \oplus K_1$, $E(R_{15}) \oplus K_{16}$.

B. Determine best sub-Key differences

For the collected optimal plaintexts, the S-boxes input values in the first and last round are approximately more different. For each plaintext belong to the optimal plaintexts equation (4) is calculated where PR_0 means right hand side of plaintext and CR_0 means right hand side of its corresponding cipher text, then using the output bits we can obtained to eight sub key differences according to the eight S-boxes then the best eight sub key differences are founded from all the optimal plaintext/cipher text pairs where the best sub key difference has the least frequency among optimal plaintext/cipher text pairs.

$$E(PR_0) \oplus E(CR_0) \quad (4)$$

C. Recovering root key bits

Using obtained best 8 sub key differences that are induced from the previous steps; we can recover most bits in root key from some induced equations. Table (1) illustrates that, the total number of left cyclic shifts is set to 28 bits, which means that (C_0, D_0) and (C_{16}, D_{16}) have the same value, i.e. ($C_{16} = C_0$) and ($D_{16} = D_0$). Based on Key Schedule Algorithm and Left Shifts Schedule, we can deduce table (2) which give the Representation of K_1, K_{16} *in* S-Boxes (S1– S8).The relationship between computed 8 sub-key differences and root key information C, D can be represented using the following two equations (5) and (6). Where RS means right shift bit.

$$K_1 \oplus K_{16} = PC2(C_1) \oplus PC2(C_{16}) = PC2(C_1) \oplus PC2(C_0) = PC2(C_1) \oplus PC2(RS(C_1)) \quad (5)$$

$$K_1 \oplus K_{16} = PC2(D_1) \oplus PC2(D_{16}) = PC2(D_1 \oplus PC2(D_0) = PC2(D_1) \oplus PC2(RS(D_1)) \quad (6)$$

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number of left shifts	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1
Total shifts	1	2	4	6	8	10	12	14	15	17	19	21	23	25	27	28

Table 1: Left Circular Shifts Schedule

Sub-key of first round (K_1)	**Sub-key of last round (K_{16})**
$K_1 = k_1 \| k_2 \| k_3 \| k_4 \| k_5 \| k_6 \| k_7 \| k_8$	$K16 = k_1 \| k_2 \| k_3 \| k_4 \| k_5 \| k_6 \| k_7 \| k_8$
$k_1=C_{1,14} \| C_{1,17} \| C_{1,11} \| C_{1,24} \| C_{1,1} \| C_{1,5}$	$k_1=C_{1,13} \| C_{1,16} \| C_{1,10} \| C_{1,23} \| C_{1,28} \| C_{1,4}$
$k_2=C_{1,3} \| C_{1,28} \| C_{1,15} \| C_{1,6} \| C_{1,21} \| C_{1,10}$	$k_2=C_{1,2} \| C_{1,27} \| C_{1,14} \| C_{1,5} \| C_{1,20} \| C_{1,9}$
$k_3=C_{1,23} \| C_{1,19} \| C_{1,12} \| C_{1,4} \| C_{1,26} \| C_{1,8}$	$k_3=C_{1,22} \| C_{1,18} \| C_{1,11} \| C_{1,3} \| C_{1,25} \| C_{1,7}$
$k_4=C_{1,16} \| C_{1,7} \| C_{1,27} \| C_{1,20} \| C_{1,13} \| C_{1,2}$	$k_4=C_{1,15} \| C_{1,6} \| C_{1,26} \| C_{1,19} \| C_{1,12} \| C_{1,1}$
$k_5=D_{1,13} \| D_{1,24} \| D_{1,3} \| D_{1,9} \| D_{1,19} \| D_{1,27}$	$k_5=D_{1,12} \| D_{1,23} \| D_{1,2} \| D_{1.8} \| D_{1.18} \| D_{1,26}$
$k_6=D_{1,2} \| D_{1,12} \| D_{1,23} \| D_{1.17} \| D_{1.5} \| D_{1,20}$	$k_6=D_{1,1} \| D_{1,11} \| D_{1,22} \| D_{1.16} \| D_{1.4} \| D_{1,19}$
$k_7=D_{1,16} \| D_{1,21} \| D_{1,11} \| D_{1.28} \| D_{1.6} \| D_{1,25}$	$k_7=D_{1,15} \| D_{1,20} \| D_{1,10} \| D_{1.27} \| D_{1.5} \| D_{1,24}$
$k_8=D_{1,18} \| D_{1,14} \| D_{1,22} \| D_{1.8} \| D_{1.1} \| D_{1,4}$	$k_8=D_{1,17} \| D_{1,13} \| D_{1,21} \| D_{1.7} \| D_{1.28} \| D_{1,3}$

Table 2: Representation of K_1 , K_{16}

Using equation (5) and Table (2), we can deduce the following equations and most bits in C_1 can be recovered.

$$K_{1,24} \oplus K_{16,24} = C_{1,1} \oplus C_{1,2} \qquad K_{1,9} \oplus K_{16,9} = C_{1,14} \oplus C_{1,15}$$
$$K_{1,7} \oplus K_{16,7} = C_{1,2} \oplus C_{1,3} \qquad K_{1,19} \oplus K_{16,19} = C_{1,15} \oplus C_{1,16}$$
$$K_{1,16} \oplus K_{16,16} = C_{1,3} \oplus C_{1,4} \qquad K_{1,2} \oplus K_{16,2} = C_{1,16} \oplus C_{1,17}$$
$$K_{1,6} \oplus K_{16,6} = C_{1,4} \oplus C_{1,5} \qquad K_{1,14} \oplus K_{16,14} = C_{1,18} \oplus C_{1,19}$$
$$K_{1,10} \oplus K_{16,10} = C_{1,5} \oplus C_{1,6} \qquad K_{1,22} \oplus K_{16,22} = C_{1,19} \oplus C_{1,20}$$
$$K_{1,20} \oplus K_{16,20} = C_{1,6} \oplus C_{1,7} \qquad K_{1,11} \oplus K_{16,11} = C_{1,20} \oplus C_{1,21}$$
$$K_{1,18} \oplus K_{16,18} = C_{1,7} \oplus C_{1,8} \qquad K_{1,13} \oplus K_{16,13} = C_{1,22} \oplus C_{1,23}$$
$$K_{1,12} \oplus K_{16,12} = C_{1,9} \oplus C_{1,10} \qquad K_{1,4} \oplus K_{16,4} = C_{1,23} \oplus C_{1,24}$$
$$K_{1,3} \oplus K_{16,3} = C_{1,10} \oplus C_{1,11} \qquad K_{1,17} \oplus K_{16,17} = C_{1,25} \oplus C_{1,26}$$
$$K_{1,15} \oplus K_{16,15} = C_{1,11} \oplus C_{1,12} \qquad K_{1,21} \oplus K_{16,21} = C_{1,26} \oplus C_{1,27}$$
$$K_{1,23} \oplus K_{16,23} = C_{1,12} \oplus C_{1,13} \qquad K_{1,8} \oplus K_{16,8} = C_{1,27} \oplus C_{1,28}$$
$$K_{1,1} \oplus K_{16,1} = C_{1,13} \oplus C_{1,14} \qquad K_{1,5} \oplus K_{16,5} = C_{1,28} \oplus C_{1,1}$$

Similarly, Using equation (6) and Table-2, we can deduce the following equations and most bits in D_1 can be recovered.

$$K_{1,31} \oplus K_{16,31} = D_{1,1} \oplus D_{1,2} \qquad K_{1,34} \oplus K_{16,34} = D_{1,16} \oplus D_{1,17}$$
$$K_{1,27} \oplus K_{16,27} = D_{1,2} \oplus D_{1,3} \qquad K_{1,43} \oplus K_{16,43} = D_{1,17} \oplus D_{1,18}$$
$$K_{1,48} \oplus K_{16,48} = D_{1,3} \oplus D_{1,4} \qquad K_{1,29} \oplus K_{16,29} = D_{1,18} \oplus D_{1,19}$$
$$K_{1,35} \oplus K_{16,35} = D_{1,4} \oplus D_{1,5} \qquad K_{1,36} \oplus K_{16,36} = D_{1,19} \oplus D_{1,20}$$
$$K_{1,41} \oplus K_{16,41} = D_{1,5} \oplus D_{1,6} \qquad K_{1,38} \oplus K_{16,38} = D_{1,20} \oplus D_{1,21}$$
$$K_{1,46} \oplus K_{16,46} = D_{1,7} \oplus D_{1,8} \qquad K_{1,45} \oplus K_{16,45} = D_{1,21} \oplus D_{1,22}$$
$$K_{1,28} \oplus K_{16,28} = D_{1,8} \oplus D_{1,9} \qquad K_{1,33} \oplus K_{16,33} = D_{1,22} \oplus D_{1,23}$$
$$K_{1,39} \oplus K_{16,39} = D_{1,10} \oplus D_{1,11} \qquad K_{1,26} \oplus K_{16,26} = D_{1,23} \oplus D_{1,24}$$
$$K_{1,32} \oplus K_{16,32} = D_{1,11} \oplus D_{1,12} \qquad K_{1,42} \oplus K_{16,42} = D_{1,24} \oplus D_{1,25}$$
$$K_{1,25} \oplus K_{16,25} = D_{1,12} \oplus D_{1,13} \qquad K_{1,30} \oplus K_{16,30} = D_{1,26} \oplus D_{1,27}$$
$$K_{1,44} \oplus K_{16,44} = D_{1,13} \oplus D_{1,14} \qquad K_{1,40} \oplus K_{16,40} = D_{1,27} \oplus D_{1,28}$$
$$K_{1,37} \oplus K_{16,37} = D_{1,15} \oplus D_{1,16} \qquad K_{1,47} \oplus K_{16,47} = D_{1,28} \oplus D_{1,1}$$

IV. Experimental Setup and Results

In this section, some experiments have been done to evaluate the performance of the proposed algorithm. This algorithm is performed in Matlab 7.0 and run on Intel P4-m processor. In our experiment the fitness value is calculated using equation (3) and PSO parameters were set as particle size=64bits, $C_1 = C_2 = 2$. The maximum velocity V_{max} of the algorithm was set to 4. The size of population was taken equal to N = 500, the number of iterations G = 200 and the number of Trials T = 15 on three different type of root key.

The given table (3) summarizes the performance results of the proposed attack for sixteen-rounded DES. In 48 deduced equation the number of variables is equal to 56bits(28bits of C, 28 bits of D) which are need to be recovered, from our experimental results we found that Success bits" the number of bits in guessed key that are compared with the original root key" are ranged between 31-39 bits.

V. Conclusion and Future Works

In this paper we have presented a new approach for the cryptanalysis of sixteen-rounded Data Encryption Standard

based on particle swarm optimization System using known-plaintext attack. Using PSO help use to collect the optimal plaintext for which S- boxes input values satisfy the proposed fitness function. From experimental results we found that the proposed system is able to recover most root key bits. The proposed fitness function used here can be applied for other block ciphers also. The future works are extending this approach for attacking other block ciphers.

Exp.no	Type	Number of recovered bits in C	Number of recovered bits in D	Total bits
1	Type1	18	17	35
2		18	17	35
3		18	17	35
4		16	15	31
5		15	17	32
6	Type2	16	15	31
7		16	15	31
8		19	14	33
9		16	15	31
10		16	19	35
11	Type3	19	20	39
12		16	17	33
13		16	16	32
14		16	15	31
15		18	15	33

Table 3: Experimental results

REFERENCES

[1] J. Kennedy and R. Eberhart, "Particle swarm optimization" In Proc of IEEE/ICNN, pp.1942–1948, 1995.

[2] Laskari, E. C., Meletiou, G. C., Stamation, Y. C., and Vrahatis, M. N., "Evolutionary Computation based Cryptanalysis:A first study". Nonlinear Analysis, vol. 63, no. (5-7), pp.823-830, 2005.

[3] Sathya, S. S., Chithralekha, T. and Anandakumar, P. , "Nomadic Genetic Algorithm for Cryptanalysis of DES 16" International Journal of Computer Theory and Engineering, vol. 2(3), pp. 1793-8201, June 2010.

[4] Shahzad,W., Siddiqui, A. B., and Khan, F. A., "Cryptanalysis of Four-Round DES using Binary Particle Swarm Optimization" Genetic and Evolutionary Computation Conference (GECCO). pp. 1757-1758, July 8-12, 2009.

[5] Stallings, W., "Cryptography and Network Security Principles and Practices" Pearson Education, 2004.

[6] Toemer, R., and Arumugam, S., "Breaking Transposition Cipher with Genetic Algorithm". Electronics and Electrical Engineering. vol. 7 No. 79, pp.75 - 78, 2007.

[7] Tsunoo, Y., Saito, T., and Suzaki, T., "Cryptanalysis of DES implemented on computers with cache" proceedings of Workshop on Cryptographic Hardware and Embedded System. Sep 62-76, 2003.

[8] Uddin, M. F., and Youssef, A. M., "Cryptanalysis of simple substitution cipher using Particle Swarm Optimization". Proceedings of IEEE 2006 Congress on Evolutionary Computation, pp. 677-680, July 6-21, 2006.