DESIGN STRONG S-BOXES BASED ON GRAY WOLF OPTIMIZER

Ali Ibrahim Lawah

Electrical and Computer Engineering, Altinbas University, Istanbul, Türkiye

Supervisor Abdullahi Abdu Ibrahim

In this study, a method for robust designs of 8 × 8 substitution boxes (S-boxes) was developed using a metaheuristic approach based on nature-inspired Grey Wolf Optimization algorithm (GWO). The GWO developed as a unique metaheuristic using inspiration from how grey wolves hunt. the GWO's capacity to swiftly explore the search space for the near/optimal feature subsets that maximize any given fitness function. The experiment's findings demonstrated that the proposed S-box architecture has sufficient cryptographic properties.

Keywords: Gray Wolf, S-Box, Cryptography.

Cryptography provides many services to secure the communication and transmission of data such as integrity and security. Encryption systems rely mainly on the s-box cipher properties. In recent symmetric key algorithm, the s-box is considered the important part. The strength of symmetric key cryptosystems is mainly based on their confusion and diffusion (Claude Shannon's properties) attributes [1]. The S-box is typically the only nonlinear component in a symmetric-key cryptosystem which the strength of the algorithm depends it., is important in constructing block ciphers that are cryptographically strong and resilient to common cryptanalysis attacks such as linear and differential attacks [2]. Block ciphers support two main operations known as substitution and permutation hiding the relationship between the cipher text and the secret key is the first characteristic provided by S-box [2]. Currently, there are three generic approaches that are most employed in the construction of S-boxes are the algebraic, random, and metaheuristic-based approaches. Each of these methods has advantages and disadvantages; by way of instance, the random search approach, it typically results in S-boxes with poor cryptographic properties [3]. Although the algebraic method is yields S-boxes with strong cryptographic features, but is not creating S-boxes on a large scale, The metaheuristic-based approach is a great substitute for design S-box, by using the optimization method in general and nature-inspired solutions in particular. in this research A metaheuristic algorithm known as The Grey Wolf Optimizer (GWO) [4]. Recently It was developed as a metaheuristic algorithm to simulated the hunting behavior of grey wolves. The standard version of GWO [5]. Has been used to resolve several global optimization issues. The top three possible solution are "Alpha, Beta, and Delta", which denote the best solution, the second-best solution and the third-best solution. respectively, are primarily dependent upon for the position updating procedure in GWO.The grey wolves frequently live in packs, adhere to a rigid social strong structure Fig. 1.

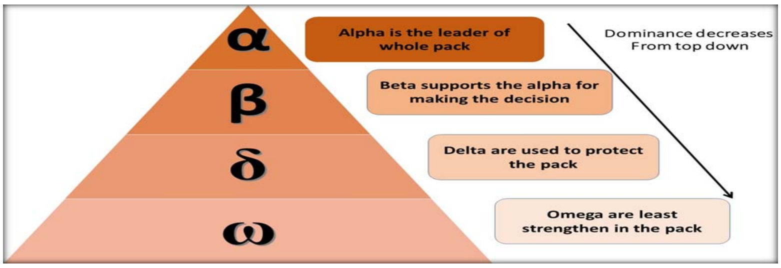
α
β
δ
ω
Alpha is the leader of whole pack
Beta supports the alpha for making the decision
Delta are used to protect the pack
Omega are least strengthen in the pack
Dominance decreases From top down

Fig. 1. Hierarchy of Grey Wolf [4]

The following are the study's main objectives:

i) design and implement GWO algorithm based for s-box generation;

ii) performance testing based on six main criteria.

Grey wolves' three strategy hunting steps are encircling, haunting, and attacking the prey.

Encircling. The grey wolves are encircling the prey in this step, it may be represented as follows:

$$D = \left|C \times X_p(t) - X(t)\right|; \qquad (1)$$

$$X(t+1) = X_p(t) - A \times D. \qquad (2)$$

Where X_p = is the located of the target (prey), X = the hunting wolf location vector, t = the current iteration. The coefficient vectors C and A can be calculated using the formulas below:

$$A = 2 \times A \times r_1 - a(t); \qquad (3)$$

$$C = 2 \times r_2 \qquad (4)$$

where "random vectors in the [0,1] range" are r_1, r_2. During the iteration phase, the vector's components decrease linearly from 2 to 0 by:

$$a(t) = 2 - (2 \times t) \,|\, MaxIter. \qquad (5)$$

Haunting. The mathematical model for the haunting behaviour of wolves is makes the assumption that a, β, and δ further information regarding the location of the target (prey); Therefore, the other wolves follow the location of the a, b, and c as (best solution) ω. The hunting behavior of the wolves is explained by using the following:

$$D_a = \left|C_1 \times X_a - X(t)\right|;$$

$$D_\beta = \left|C_3 \times X_\beta - X(t)\right|; \qquad (6)$$

$$D_\delta = \left|C_3 \times X_\delta - X(t)\right|.$$

Where C_1, C_2 and C_3 are calculated by

$$X_{i1}(t) = X_\alpha(t) - A_{i1} \times D_\alpha(t),$$

$$X_{i2}(t) = X_\beta(t) - A_{i2} \times D_\beta(t)\ , \qquad (7)$$

$$X_{i3}(t) = X_\delta(t) - A_{i3} \times D_\delta(t).$$

Where X_a, X_β and X_δ are the initial three of the iteration best solutions t, A_1, A_2 and A_3 are calculated as in Eq. (3), and D_α, D_β and D_δ are calculated as Eq. (6).

$$X(t+1) = \frac{X_{i1}(t) + X_{i2}(t) + X_{i3}(t)}{3}. \qquad (8)$$

Attacking. When the hunting phase is finished, the wolves begin the attacking phase. The value of a can be used to mathematically control the exploration and exploitation operations. during the course of the repetition procedure, declines linearly. Eq. after each iteration (16), the value of a is updated between the ranges of 2 and 0. Exploitation, according to [6], is devoted to the second half of iterations, which follows seamless change from exploration. (see Fig. 2).

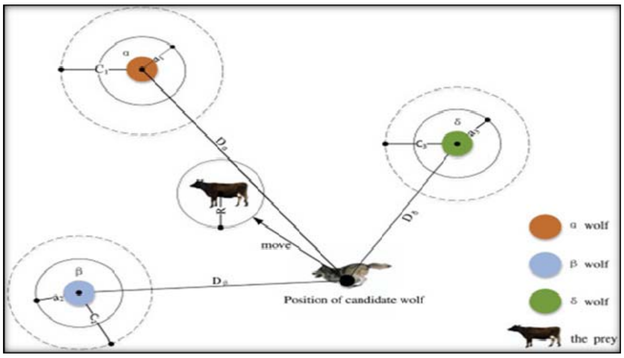

Fig. 2. Update Mechanism of GWO [5]

EVALUATING THE GENERATED S-BOXES

The performance of the proposed S-Box generating algorithm is evaluated based on six main statistical evaluation metrics, as follows:

A. BIJECTIVE CRITERION: it means that there are no unpaired elements, and that every element of one set is matched with another element in another set.

B. NONLINEARITY (*NL*): it is related to plaintext confusion and immunization of block ciphers from linear cryptanalysis. The Walsh spectrum determines the Boolean function $f(x)$ is nonlinear.

C. STRICT AVALANCHE CRITERIA (*SAC*): means that if the input bits of the Boolean function change random. it means the output bits should be equal a probability of half for each bit.

D. BITS INDEPENDENCE CRITERIA (*BIC*): it means that output bits have no association with one another, and that all input-output variables for all avalanche vectors are pairwise independent.

E. DIFFERENTIAL UNIFORMITY (*DU*): the attackers can identify the whole or partial plaintext or key by analyzing these differentials by using (*DU*).

F. LINEAR PROBABILITY: it means the lower LP with the S-box it will be more resistant to this analysis.

Table 1

Gwo Nonlinearity Score for 10Runs

Average Nonlinearity Score		Average Nonlinearity Score	
Run	**GWO**	**Run**	**GWO**
1	105.75	6	106.75
2	106.00	7	106.50
3	106.25	8	106.25
4	106.25	9	108.00
5	106.50	10	106.25

Table 2

The Results of the Six Criteria

	S-Boxes	Nonlinearity			SAC		BIC-NL		BIC-SAC	DP	LP
		Min	*Max*	*Avg*	*Avg*	*Offset*	*Min*	*Avg*	*Avg*	*Max DP*	
Proposed	GWO	106	108	106.45	0.5110	0.02930	96	103.20	0.4995	10	0.1172

References

1. Shannon C. E. Communication Theory of Secrecy Systems*. *Bell Syst. Tech. J.*, oct. 1949, vol. 28, no. 4, pp. 656–715, Oct. 1949. https://doi: 10.1002/j.1538-7305.1949.tb00928.x
2. Adams C., Tavares S. The structured design of cryptographically good s-boxes. *J. Cryptol.*, 1990, vol. 3, no. 1, pp. 27–41, 1990. https://doi: 10.1007/BF00203967
3. Menezes A. Course Outline … Course Outline…. *An Expand. set S-box Des. criteria based Inf. theory its Relat. to Differ. attacks*, november, pp. 1–11, 20AD.
4. Mirjalili S., Mirjalili S. M., Lewis A. Grey Wolf Optimizer, *Adv. Eng. Softw.*, 2014, vol. 69, pp. 46–61. https://doi: 10.1016/j.advengsoft.2013.12.007
5. Gupta S., Deep K. Enhanced leadership-inspired grey wolf optimizer for global optimization problems. *Eng. Comput.*, 2020, vol. 36, no. 4, pp. 1777–1800. https://doi: 10.1007/s00366-019-00795-0
6. BIHAM E. S. Experienced Gray Wolf Optimization Through Reinforcement Learning and Neural Networks. *Gray wolf*, 2018, vol. 29, no. 3, pp. 681–694. https://doi: 10.1109/TNNLS.2016.2634548