International Journal of Advanced and Applied Sciences, 8(3) 2021, Pages: 30-35

Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Application of fuzzy soft sets to analyze the statistical strength of S-boxes

Asima Razzaque [1], Inayatur Rehman [2,*], Shahid Razzaque [3], Muhammad Iftikhar Faraz [4], Muhammad Asif Gondal [2]

[1]*Basic Science Department, King Faisal University, Hofuf, Saudi Arabia*
[2]*Department of Mathematics and Sciences, College of Arts and Applied Sciences, Dhofar University, Salalah, Oman*
[3]*Pakistan Institute of Development Economics, Quaid-e-Azam University Campus, Islamabad, Pakistan*
[4]*Department of Mechanical Engineering, College of Engineering, King Faisal University, Hofuf, Saudi Arabia*

A R T I C L E I N F O

Article history:
Received 20 July 2020
Received in revised form
17 October 2020
Accepted 7 November 2020

Keywords:
Soft set
Fuzzy set
Fuzzy soft set
FS-aggregation operator
S-box
Majority logic criterion

A B S T R A C T

For the evaluation of the substitution boxes, the majority logic criterion is used to analyze the statistical strength of the existing substitution boxes. The main objective of this paper is to make a decision on the analysis and selection of the most appropriate S-box based on a fuzzy soft-aggregation operator. Instead of the usual practice in which a single parameter is considered, we are considering several parameters that will definitely give us a comprehensive analysis of the S-boxes.

1. Introduction

For our imperative understanding, the material world is complex. Many difficulties in various fields such as applied sciences, social sciences, medical skills, computer sciences, and artificial intelligence are generally not precise. The researchers develop a number of tools of certainty that simplify the various uncertain aspects of the tangible world. Regrettably, these mathematical tools are complicated, and we cannot find the precise results. The usual methodologies used to share with these uncertainties are appropriate for certain environments. These may be ascribable to the uncertainties of ordinary environmental phenomena of human consciousness around the actual creation. For instance, vagueness in the boundary between provinces or between urban and rural areas or the precise increase in population in land or making decisions using database information. For that reason, the conventional set theory may not be appropriate to carry out such uncertain problems.

The concept of soft set theory was initiated by Molodtsov (1999). In his work, he gave many important results that are being used to resolve the uncertainty problems in different research areas such as game theory, operation research, probability theory, etc. Basically, soft set theory is considered to be a valuable mathematical tool to cope with the problems of uncertainty. As the soft set theory is based on a number of parameters, so intuitively, this theory is considered to be more comprehensive and effective as compared to other conventional theories. Nowadays, the soft set theory is taking so much attention from the researchers to make its applications in different fields.

In the current decade, the soft set theory is playing a vital role in decision making. For the optimal selection of the objects based on the reduction of parameters, Maji et al. (2002; 2003) used the soft sets in decision making. Chen (2005) defined the soft sets parameterization reduction in another way and compared it with the rough set theory attribute reduction. Soft sets are defined as a class of special information systems by Pei and Miao (2005). The soft sets data analysis approach was investigated by Zou and Xiao (2008). Cagman and Enginoglu (2011) gave the idea of FP-soft sets and discussed their several characteristics, and proposed an algorithm for decision making.

If we look into the literature, we can find a number of proposed encryption methods. These methods seem to be capable, but their effectiveness is not yet installed, and these are preparing to become standards. The most usual methods utilized to study the statistical effectiveness of S-boxes are the differential approximation probability, strict avalanche criterion, correlation analysis, linear approximation probability, and so forth.

* Corresponding Author.
Email Address: irehman@du.edu.om (I. Rehman)
https://doi.org/10.21833/ijaas.2021.03.004
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-6993-945X

The most common S-boxes are APA (Cui and Cao, 2007), Lui (Liu et al., 2005), Gray (Tran et al., 2008), S_8 AES (Hussain et al., 2010), Residue Prime (Abuelyman and Alsehibani, 2008), XYI (Shi et al., 2002) and SKIPJACK (Skipjack, 1998). Many researchers have processed the images encrypted with these S-boxes and examined their features. For the detailed study of S-boxes, image encryption, and soft decision making the readers are referred to Ahmed et al. (2014), Anees et al. (2013; 2014), Hussain et al. (2013), Rehman et al. (2017; 2014), Yaqoob et al. (2013), and Dhiman and Sharma (2020).

In this research article, the fuzzy soft aggregation operator is applied to key out the effectiveness point of S-boxes. The statistical features of S-boxes (average correlation, average entropy, average contrast, average homogeneity, average energy, and an average mean of absolute deviation) have been studied by counting the values of all the analyses of various S-boxes. An algorithm based on a fuzzy soft aggregation operator is applied to select the best S-box among the different S-boxes.

2. Historical perspective of soft sets, fuzzy soft sets, and FS-aggregation operator

We recall some definitions from Molodtsov (1999), Abuelyman and Alsehibani (2008), Acar et al. (2010), Cagman et al. (2011), Maji et al. (2001) and provide an algorithm from Cagman et al. (2011) which are subsequently needed for further discussion.

Throughout this paper, U is considered as the universal set, $P(U)$ represents the power set. The set of parameters is denoted by E while A is considered as a subset of E.

Definition (Molodtsov, 1999): If U denotes the universal set and the set of parameters is E, then consider a function $F: A \rightarrow P(U)$. We call (F, A) a soft set over U, where $P(U)$ denotes a power set, A is a non-empty subset of parametrized set E.

Definition (Maji et al., 2001): (F, A) is said to be a soft subset of (G, B) if,

i. $A \subseteq B$
ii. *For all* $e \in A, F(e) \subseteq G(e)$

Definition (Maji et al., 2001): If *(F, A)* and *(G, B)* are soft subsets of each other, then these are said to be soft equal.

Definition (Maji et al., 2001): *(F, A)* is said to be a Null soft set if $F(\varepsilon) = \varphi$, where each $\varepsilon \in A$.

Definition (Acar et al., 2010): (H, C) is said to be a bi-intersection of *(F, A)* and *(G, B)* if it satisfies:

i. $C = A \cap B$,
ii. For each $z \in C$, $H(z)=F(z) \cap G(z)$,

Definition (Acar et al., 2010): The union of two soft sets *(F, A)* and *(G, B)* is a soft set *(H, C)* satisfying the following:

i. $C = A \cup B$,
ii. For each $x \in C$,

$$H(x) = \begin{cases} F(x) & if\ x \in A - B \\ G(x) & if\ x \in B - A \\ F(x) \cup G(x) & if\ x \in A \cap B \end{cases}$$

Definition (Acar et al., 2010): The support of *(F, A)* is given by $\mathrm{Supp}(F, A) = \{x \in A : F(x) \neq \emptyset\}$.

Cagman et al. (2011) defined fs-aggregation operator on the fuzzy sets, which actually produces a single fuzzy set and is said to be an aggregate fuzzy set of the fs-set. In the following, we recollect some important definitions and algorithms from the work of Cagman et al. (2011).

Definition (Abuelyman and Alsehibani, 2008): Let Γ_A be an fs-set. Γ_A is given by a mapping $\gamma_A : E \rightarrow F(U)$ defined by $\gamma_A(x) = \emptyset$, where $x \notin A$. γ_A is said to be a fuzzy approximate function of Γ_A and $\gamma_A(x)$ is said to be an x-element of the fs-set for every $x \in E$. Consequently, an fs-set Γ_A is represented as follows:

$$\Gamma_A = \{(x, \gamma_A(x)) : x \in E,\ \gamma_A(x) \in F(U)\}.$$

The set of all fs-sets is represented by $FS(U)$.

Definition (Cagman et al., 2011): Γ_A is an fs-subset of Γ_B which is denoted by $\Gamma_A \tilde{\subseteq} \Gamma_B$, *if* $\gamma_A(x) \subseteq \gamma_B(x)$, for every $x \in E$, where $\Gamma_A, \Gamma_B \in FS(U)$.

Definition (Cagman et al., 2011): Let the universal set is $U = \{u_1, u_2, \dots, u_m\}$ and the set of parameters is denoted by $E = \{x_1, x_2, \dots, x_n\}$ where $A \subseteq E$. Table 1 can be constructed.

Table 1: FS-set

Γ_A	x_1	x_2	x_n
u_1	$\mu_{\gamma_A(x_1)}(u_1)$	$\mu_{\gamma_A(x_2)}(u_1)$	$\mu_{\gamma_A(x_n)}(u_1)$
u_2	$\mu_{\gamma_A(x_1)}(u_2)$	$\mu_{\gamma_A(x_2)}(u_2)$	$\mu_{\gamma_A(x_n)}(u_2)$
u_m	$\mu_{\gamma_A(x_1)}(u_m)$	$\mu_{\gamma_A(x_2)}(u_m)$	$\mu_{\gamma_A(x_n)}(u_m)$

where the membership function of γ_A is denoted by $\mu_{\gamma_A(x)}$.

Let $bij = \mu_{\gamma_A(x_j)}(u_i)$, for $i = 1,2, \dots, m$ and $j = 1,2, \dots, n$, then the fs-set Γ_A can be mapped in the following $m \times n$ fs-matrix,

$$[b_{ij}]_{m \times n} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{bmatrix}$$

Definition (Cagman et al., 2011): The cardinal set of Γ_A is defined by $c\Gamma_A = \{\mu_{c\Gamma_A}(x)/x : x \in E\}$. $c\Gamma_A$ is actually a fuzzy set over E. Where $\mu_{c\Gamma_A}$ is a membership function of $c\Gamma_A$ and is defined as:

$\mu_{c\,\Gamma_A}: E \to [0,1], \quad \mu_{c\,\Gamma_A}(x) = \frac{|\gamma_A(x)|}{|U|}$

It is important to note that $|U|$ is the cardinality of the universal set U, and $|\gamma_A(x)|$ is the scalar cardinality of fuzzy set $\gamma_A(x)$.

Moreover, the set of all cardinal sets of fs-sets is denoted by $cFS(U)$. And obviously, $cFS(U) \subseteq F(E)$.

Definition (Cagman et al., 2011): If $\Gamma_A \in FS(U)$ and $c\,\Gamma_A \in cFS(U)$. And $E = \{x_1, x_2, \dots, x_n\}$ where $A \subseteq E$, then Table 2 is contracted to represent $c\,\Gamma_A$,

Table 2: Cardinal matrix

E	x_1	x_2	x_n
$\mu_{c\,\Gamma_A}$	$\mu_{c\,\Gamma_A}(x_1)$	$\mu_{c\,\Gamma_A}(x_2)$	$\mu_{c\,\Gamma_A}(x_n)$

If $b_{1j} = \mu_{c\,\Gamma_A}(x_j)$ for $j = 1,2,\dots,n$, then cardinal set $c\,\Gamma_A$ is represented as

$$[b_{1j}]_{1\times n} = [b_{11} \quad b_{12} \quad \dots \quad b_{1n}].$$

This matrix is called a cardinal matrix over E.

Definition (Cagman et al., 2011): If $\Gamma_A \in FS(U)$ and $c\,\Gamma_A \in cFS(U)$, then the fs-aggregation operator FS_{agg} is defined by,

$$FS_{agg}: cFS(U) \times FS(U) \to F(U), \quad FS_{agg}(c\,\Gamma_A, \Gamma_A) = \Gamma_A^*$$

where, $\Gamma_A^* = \{\mu_{\Gamma_A^*}(u)/u : u \in U\}$ is a fuzzy set over U. Γ_A^* is said to be an aggregate fuzzy set of the fs-set Γ_A. The membership function $\mu_{\Gamma_A^*}$ of Γ_A is given as follows:

$$\mu_{\Gamma_A^*}: U \to [0,1], \quad \mu_{\Gamma_A^*}(u) = \frac{1}{|E|}\sum_{x\in E} \mu_{c\,\Gamma_A}(x)\, \mu_{\gamma_A(x)}(u),$$

where $|E|$ shows the cardinality of E.

Theorem (Cagman et al., 2011): If $\Gamma_A \in FS(U)$ and $A \subseteq E$. Assume that M_{Γ_A}, $M_{c\,\Gamma_A}$ and $M_{\Gamma_A^*}$ are the matrices of Γ_A, $c\,\Gamma_A$ and Γ_A^* respectively. Then,

$$|E| \times M_{\Gamma_A^*} = M_{\Gamma_A} \times M_{c\,\Gamma_A}^T$$

where $|E|$ denotes the cardinality of E and $M_{c\,\Gamma_A}^T$ denotes the transpose of $M_{c\,\Gamma_A}$.

Algorithm: Cagman et al. (2011) proposed a decision-making algorithm which is given in the following:

Step1. Construct an fs-set Γ_A over U,
Step2. Find the cardinal set $c\Gamma_A$ of Γ_A,
Step3. Find the aggregate fuzzy set Γ_A^* of Γ_A,
Step4. Obtain the best alternative from this set that holds the largest membership grade by $\max \mu_{\Gamma_A^*}(u)$.

3. Statistical analysis of S-boxes

It is of the essence to be conversant with the meaning and relationship among the outcomes of several types of analyses. In Tran et al. (2008), the authors employed statistical analysis to define the suitability of an S-box to image encryption application. In reality, the process begins with the correlation analysis. This analysis, under some conditions, does not furnish enough information in deciding the effectiveness of encryption.

Hussain et al. (2012) projected a generalized majority logic criterion, where the authors considered several images. The diversity in image contents made this algorithm more appealing to a wider range of data samples. The generalized majority logic criterion seems to be an alluring option due to its applications and suitability of multiple types of images in the selection of the optimal S-box. Fig. 1 and Fig. 2 give the complete picture of the work of Hussain et al. (2012).

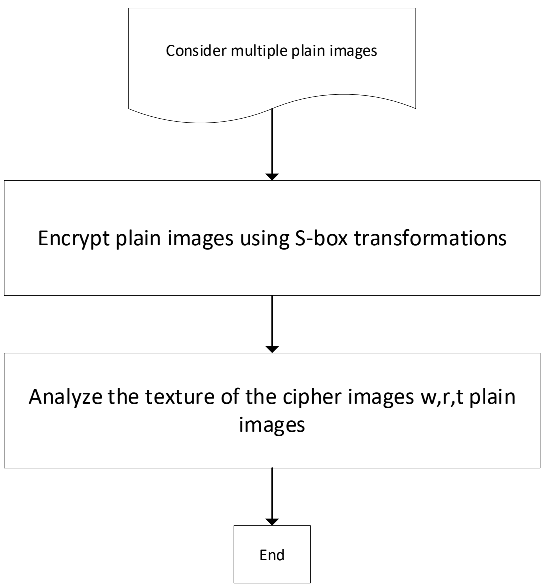

Fig. 1: Generalized majority logic criterion

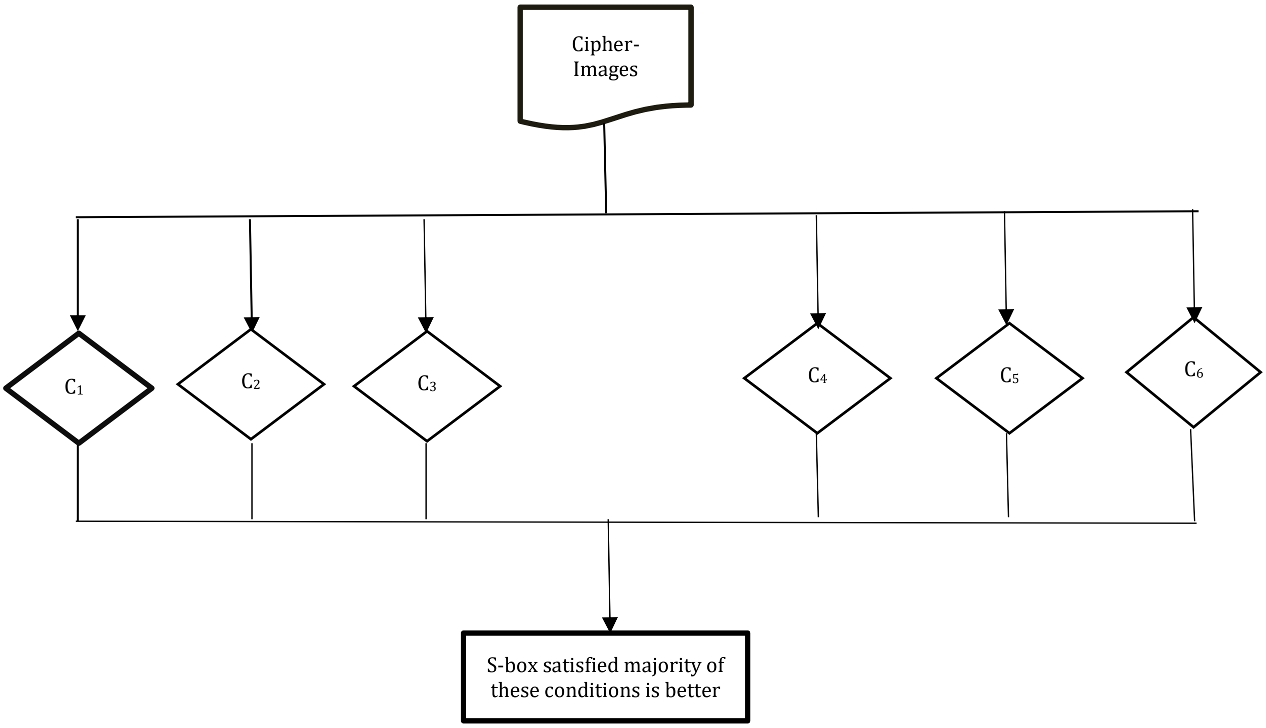

Fig. 2: Details of the generalized majority logic criterion module

[Hussain et al. (2012)](#) used different statistical techniques in their work. Figs. 3-8, represent the graphical detail of the analyses of encrypted images.

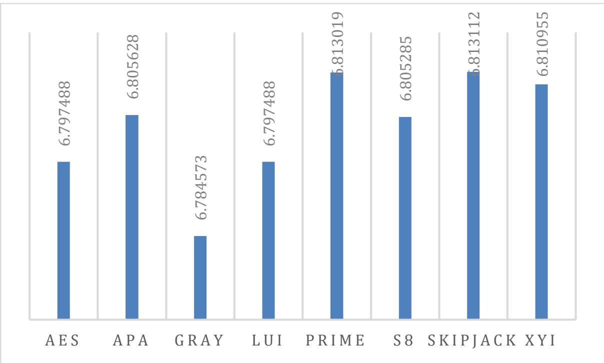

Fig. 3: The result of entropy analysis

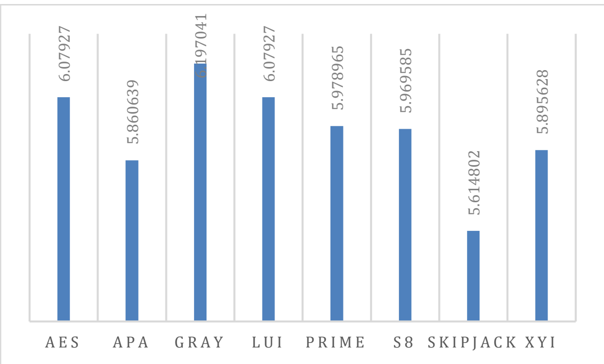

Fig. 4: The result of contrast analysis

If we conclude the work of Hussain et al. (2012), it is evident that S_8 AES S-box has been considered as the best S-box as compared with other S-boxes. This conclusion can be observed in Table 3 obtained from different statistical analyses.

If we look into the current developments in the field of cryptography, many researchers gave different methods to analyze and choose the optimal S-box. On the other hand, it is worth mentioning that the soft set theory has a remarkable contribution to decision-making problems. Here in our discussion, we intend to choose the best S-box by applying an algorithm based on a fuzzy soft set aggregation operator.

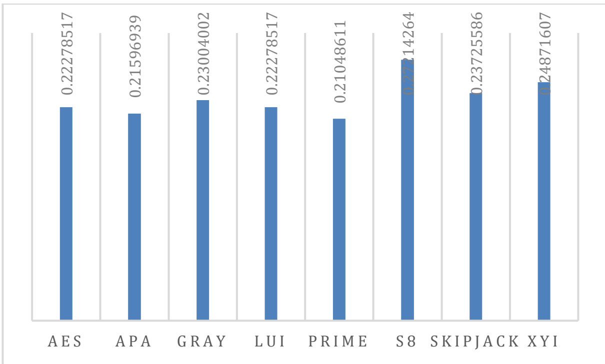

Fig. 5: Results of correlation analysis

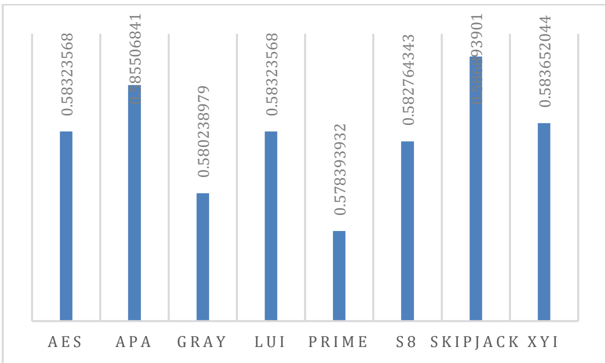

Fig. 6: Homogeneity analysis

Assume that the set of alternatives (AES, APA, Gray, Lui, Gray, Prime, S_8, SKIPJACK and XYI) is denoted by $U = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8\}$, where

u_i $(i = 1, 2, 3, 4, 5, 6, 7, 8)$. To evaluate the S-boxes, let the set of parameters is $E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$, where $i = 1, 2, 3, 4, 5, 6$ and e_i stands for average entropy, average contrast, average correlation, average energy, average homogeneity, and average mean absolute deviation, respectively.

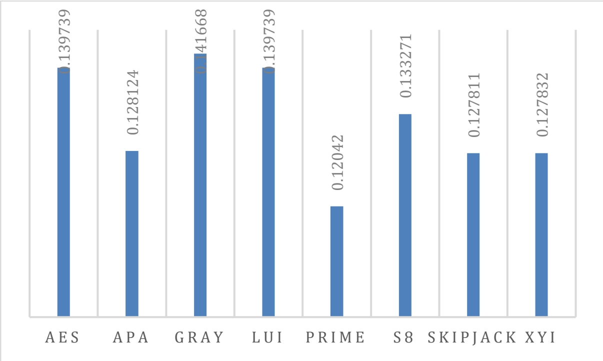

Fig. 7: Energy analysis of cipher-image

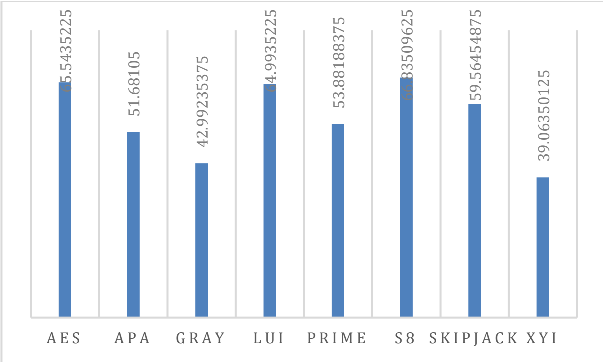

Fig. 8: MAD analysis of cipher-image

After a detailed discussion, we have chosen a subset of parameters $A = E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$. Now, we are in a position to make a decision to analyze S-boxes by using the following steps:

Table 3: Average entropy, average contrast, average correlation, average energy, and average homogeneity of plain image and cipher image

S-boxes	Average Entropy	Average Contrast	Average Correlation	Average Energy	Average Homogeneity	Average MAD
AES	6.797488	6.07927	0.22278517	0.139739	0.58323568	65.5435225
APA	6.805628	5.860639	0.21596939	0.128124	0.585506841	51.68105
Gray	6.784573	6.197041	0.23004002	0.141668	0.580238979	42.99235375
Lui	6.797488	6.07927	0.22278517	0.139739	0.58323568	64.9935225
Prime	6.813019	5.978965	0.21048611	0.12042	0.578393932	53.88188375
S_8	6.805285	5.969585	0.27214264	0.133271	0.582764343	66.83509625
SKIPJACK	6.813112	5.614802	0.23725586	0.127811	0.586893901	59.56454875
XYI	6.810955	5.895628	0.24871607	0.127832	0.583652044	39.06350125

Step1. Foremost, we will build an fs-set Γ_A over U.

$$\Gamma_A = \left\{ \begin{array}{c} \left(e_1, \left\{\frac{0.2}{u_1}, \frac{0.3}{u_2}, \frac{0.9}{u_6}, \frac{0.5}{u_7}\right\}\right), \left(e_2, \left\{\frac{0.1}{u_2}, \frac{0.5}{u_3}, \frac{0.7}{u_4}\right\}\right), \left(e_3, \left\{\frac{0.3}{u_2}, \frac{0.4}{u_4}, \frac{0.6}{u_6}, \frac{0.1}{u_8}\right\}\right), \\ \left(e_4, \left\{\frac{0.2}{u_3}, \frac{0.3}{u_5}\right\}\right), \left(e_5, \left\{\frac{0.1}{u_2}, \frac{0.4}{u_3}, \frac{0.3}{u_4}, \frac{0.2}{u_6}, \frac{0.1}{u_7}\right\}\right), \left(e_6, \left\{\frac{0.2}{u_1}, \frac{0.1}{u_5}\right\}\right) \end{array} \right\}$$

Step2. The calculated cardinal set is,

$$c\Gamma A = \left\{\frac{0.23}{e_1}, \frac{0.16}{e_2}, \frac{0.17}{e_3}, \frac{0.06}{e_4}, \frac{0.13}{e_5}, \frac{0.03}{e_6}\right\}$$

Step3. Using Cagman et al. (2011), we obtained the aggregate fuzzy set,

$$M_{\Gamma_A^*} = \frac{1}{6} \begin{bmatrix} 0.2 & 0 & 0 & 0 & 0 & 0.2 \\ 0.3 & 0.1 & 0.3 & 0 & 0.1 & 0 \\ 0 & 0.5 & 0 & 0.2 & 0.4 & 0 \\ 0 & 0.7 & 0.4 & 0 & 0.3 & 0 \\ 0 & 0 & 0 & 0.3 & 0 & 0.1 \\ 0.9 & 0 & 0.6 & 0 & 0.2 & 0 \\ 0.5 & 0 & 0 & 0 & 0.1 & 0 \\ 0 & 0 & 0.1 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0.23 \\ 0.16 \\ 0.17 \\ 0.06 \\ 0.13 \\ 0.03 \end{bmatrix} = \begin{bmatrix} 0.008 \\ 0.024 \\ 0.024 \\ 0.036 \\ 0.003 \\ 0.055 \\ 0.021 \\ 0.002 \end{bmatrix}.$$

Consequently, we obtained,

$$\Gamma_A^* = \left\{\frac{0.008}{u_1}, \frac{0.024}{u_2}, \frac{0.024}{u_3}, \frac{0.036}{u_4}, \frac{0.003}{u_5}, \frac{0.055}{u_6}, \frac{0.021}{u_7}, \frac{0.002}{u_8}\right\}$$

Step4. From step3, it is obvious that the largest membership grade is $\max\mu_{\Gamma_A^*}(u) = 0.055$. This means that the alternative u_6(S_8 AES) can be considered as the best S-box among all the other S-boxes.

4. Conclusion

In this research work, we tried to analyze the quality and strength of the S-boxes by using an algorithm based on a fuzzy soft aggregation operator to make a decision. This method is effective and appropriate for the selection of the best S-boxes among several S-boxes. In the luminosity of our findings, we may conclude that our study is going to be a good addition to the list of efficient methods to pick the best S-box among various S-box.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abuelyman ES and Alsehibani AAS (2008). An optimized implementation of the S-Box using residue of prime numbers. International Journal of Computer Science and Network Security, 8(4): 304-309.

Acar U, Koyuncu F, and Tanay B (2010). Soft sets and soft rings. Computers and Mathematics with Applications, 59(11): 3458-3463. https://doi.org/10.1016/j.camwa.2010.03.034

Ahmed F, Anees A, Abbas VU, and Siyal MY (2014). A noisy channel tolerant image encryption scheme. Wireless Personal Communications, 77(4): 2771-2791. https://doi.org/10.1007/s11277-014-1667-5

Anees A, Khan WA, Gondal MA, and Hussain I (2013). Application of mean of absolute deviation method for the selection of best nonlinear component based on video encryption. Zeitschrift für Naturforschung A, 68(6-7): 479-482. https://doi.org/10.5560/zna.2013-0022

Anees A, Siddiqui AM, and Ahmed F (2014). Chaotic substitution for highly auto correlated data in encryption algorithm. Communications in Nonlinear Science and Numerical Simulation, 19(9): 3106-3118. https://doi.org/10.1016/j.cnsns.2014.02.011

Cagman N and Enginoglu S (2011). FP-soft set theory and its applications. Annals of Fuzzy Mathematics and Informatics, 2(2): 219-226.

Cagman N, Enginoglu S, and Citak F (2011). Fuzzy soft set theory and its applications. Iranian Journal of Fuzzy Systems, 8(3): 137-147.

Chen D, Tsang ECC, Yeung DS, and Wang X (2005). The parameterization reduction of soft sets and its applications. Computers and Mathematics with Applications, 49(5-6): 757-763. https://doi.org/10.1016/j.camwa.2004.10.036

Cui L and Cao Y (2007). A new S-box structure named Affine-Power-Affine. International Journal of Innovative Computing, Information and Control, 3(3): 751-759.

Dhiman N and Sharma MK (2020). Calculus of new intuitionistic fuzzy generator: In generated intuitionistic fuzzy sets and its applications in medical diagnosis. International Journal of Advanced and Applied Sciences, 7(10): 125-130. https://doi.org/10.21833/ijaas.2020.10.014

Hussain I, Shah T, and Mahmood H (2010). A new algorithm to construct secure keys for AES. International Journal of Contemporary Mathematical Sciences, 5(26): 1263-1270.

Hussain I, Shah T, Gondal MA, and Mahmood H (2012). Generalized majority logic criterion to analyze the statistical strength of S-boxes. Zeitschrift für Naturforschung A, 67(5): 282-288. https://doi.org/10.5560/zna.2012-0022

Hussain I, Shah T, Gondal MA, Khan WA, and Mahmood H (2013). A group theoretic approach to construct cryptographically strong substitution boxes. Neural Computing and Applications, 23(1): 97-104. https://doi.org/10.1007/s00521-012-0914-5

Liu J, Wei B, Cheng X, and Wang X (2005). An AES S-box to increase complexity and cryptographic analysis. In the 19th International Conference on Advanced Information Networking and Applications (AINA'05) Volume 1 (AINA papers), IEEE, Taipei, Taiwan, 1: 724-728. https://doi.org/10.1109/AINA.2005.84

Maji PK, Biswas R, and Roy A (2003). Soft set theory. Computers and Mathematics with Applications, 45(4-5): 555-562. https://doi.org/10.1016/S0898-1221(03)00016-6

Maji PK, Biswas RK, and Roy A (2001). Fuzzy soft sets. Journal of Fuzzy Mathematics, 9: 589–602.

Maji PK, Roy AR, and Biswas R (2002). An application of soft sets in a decision making problem. Computers and Mathematics with Applications, 44(8-9): 1077-1083. https://doi.org/10.1016/S0898-1221(02)00216-X

Molodtsov D (1999). Soft set theory-First results. Computers and Mathematics with Applications, 37(4-5): 19-31. https://doi.org/10.1016/S0898-1221(99)00056-5

Pei D and Miao D (2005). From soft sets to information systems. In the IEEE International Conference on Granular Computing, IEEE, Beijing, China, 2: 617-621. https://doi.org/10.1109/GRC.2005.1547365

Rehman I, Razzaque A, and Shah T (2017). A novel approach to analyze s-boxes in image encryption using fuzzy soft set aggregation operator. Journal of Multiple-Valued Logic and Soft Computing, 28(4-5): 495-510.

Rehman I, Shah T, and Hussain I (2014). Analyses of S-box in image encryption applications based on fuzzy decision making criterion. Zeitschrift für Naturforschung A, 69(5-6): 207-214. https://doi.org/10.5560/zna.2014-0023

Shi XY, Xiao Hu You XC, and Lam KY (2002). A method for obtaining cryptographically strong 8×8 Sboxes. International Conference on Advanced Information Networking and Applications, 2(3):14-20.

Skipjack KEA (1998). Algorithm. Specifications Version, 2(29): 1-23.

Tran MT, Bui DK, and Duong AD (2008). Gray S-box for advanced encryption standard. In the International Conference on Computational Intelligence and Security, IEEE, Suzhou, China, 1: 253-258. https://doi.org/10.1109/CIS.2008.205

Yaqoob N, Akram M, and Aslam M (2013). Intuitionistic fuzzy soft groups induced by (t, s)-norm. Indian Journal of Science and Technology, 6(4): 4282-4289. https://doi.org/10.17485/ijst/2013/v6i4.22

Zou Y and Xiao Z (2008). Data analysis approaches of soft sets under incomplete information. Knowledge-Based Systems, 21(8): 941-945. https://doi.org/10.1016/j.knosys.2008.04.004