Complex & Intelligent Systems (2024) 10:455–468
https://doi.org/10.1007/s40747-023-01150-z

ORIGINAL ARTICLE

Hybrid multi-criteria decision-making technique for the selection of best cryptographic multivalued Boolean function

Nabilah Abughazalah[1] · Majid Khan[2] · Mohsin Iqbal[3]

Received: 23 March 2023 / Accepted: 12 June 2023 / Published online: 25 July 2023

Abstract
Robustness of modern information confidentiality algorithm depends on its individual components. Modern block ciphers highly depend on two components namely confusion and diffusion. These two main characteristics in any modern cipher are achieved by substitution and permutation boxes. In this article, a decision-making algorithm is utilized for the selection of optimum substitution box (S-box), which plays a significant role in the field of information confidentiality. For this purpose, an interval-based Pythagorean fuzzy technique for order of preference by similarity to the ideal solution (IVPF–TOPSIS) method is introduced to get the desired nonlinear confusion component of block cipher namely S-box. In this manner, we performed cryptographic analyses of standard S-boxes namely nonlinearity (NL), strict avalanche criterion (SAC), bit-independent criterion (BIC), absolute indicator (ABI), the sum of square and absolute indicator (SSAI), algebraic degree (AD), algebraic immunity (AI), transparency order (TO), composite algebraic immunity (CAI), robustness (RB), signal to noise ratio (SNR), confusion coefficient of variance (CCV). With these cryptographic characteristics, we have used interval-valued based Pythagorean fuzzy TOPSIS multi-criteria decision-making technique to classify standard S-boxes suitable for construction of modern block ciphers.

Keywords Substitution box · Multi-criteria decision-making · Interval-based Pythagorean fuzzy TOPSIS

Introduction

Decision-making plays an important role in our daily life. A decision is an action of collection or option of one accomplishment from various preferences. The process of selecting an optimum and profitable plan of action from two or more options to attain a preferred result is known as decision-making. Our daily life is all about making decisions. Decisions reinforce the complete management process in any organization. Decision-making is needed for concentrating on main issues and optimized the gains from offered prospects. Appropriate decisions reduce the complication, ambiguity, and variety of administrative situations. Several subjective and objective types of multi-criteria decision-making techniques were developed so far for the selection of best options among different conflicting alternatives. There are individual and group-based decision-making techniques with different weighting mechanism to minimize or maximize various criteria upon which optimum selection of alternatives is based on.

Multi-criteria decision-making (MCDM) techniques deals with various complex problems in various fields of sciences and engineering that cannot be resolved using classical methods due to a large number of uncertainties and vagueness present in their data analysis. To counter these problems, Zadeh [1] presented the idea of a fuzzy set in which a membership value is assigned to every element of a set within a unit interval [0,1]. However, fuzzy sets do not provide a non-membership value which is sometimes necessary to handle uncertain and vague information. To deal with this, Attanassov [2] presented the idea of the intuitionistic fuzzy set (IFS) where both, the membership values and non-membership values are given with the property that their addition does not exceed 1.

✉ Majid Khan
mk.cfd1@gmail.com

[1] Department of Mathematical Sciences, College of Science, Princess Nourah Bint Abdulrahman University, P.O.Box 84428, Riyadh 11671, Saudi Arabia

[2] Department of Applied Mathematics & Statistics, Institute of Space Technology, Islamabad, Pakistan

[3] Department of Mathematics & Statistics, Riphah International University, Islamabad, Pakistan

In real-life problems, interval-based information is sometimes necessary to handle uncertain and vague information. To deal with such a problem, Attanassov and Gargov [3] presented the idea of an interval-based intuitionistic fuzzy set (IVIFS) in which interval-based membership value and non-membership value are given. During the most recent couple of years, IFS and IVIFS have effectively been utilized in numerous fields of life such as disease diagnosis, and face recognition [4–8]. However, in many real-life applications, it is not constantly feasible to provide the preferences under this limitation. For example, an individual may assign a worth 0.7 and 0.5 to an object as a membership value and non-membership value separately, then, at that point 0.7 + 0.5 > 1. Thus (IFS) fails to handle these types of preferences.

To deal with such preferences, Yagar [9, 10] generalized IFS to Pythagorean fuzzy set (PFS) with condition that the square sum of preference values does not exceed 1. In real-life applications, PFS is used where IFS fails to handle the situations. For instance, for the above-mentioned example, it is easily observed that $(0.7)^2 + (0.5)^2 \leq 1$. Thus, PFS better handle those situations where IFS fails. Peng and Yang [11] put forward an idea of an interval-based Pythagorean fuzzy set (IVPFS). We will discuss these concepts in detail in the next section.

MCDM is a commonly applied methodology for solving real-life decision problems effectively. It aims to find the ideal alternatives from the set of possible alternatives, characterized by multiple criteria. Over the past few decades, various techniques have been set up for tackling MCDM issues [12–15]. The most commonly used MCDM techniques includes Analytical hierarchy process (AHP), Fuzzy analytical hierarchy process (FAHP), Entropy method, Weighted aggregated sum (WAS), Weighted aggregated product method (WASPM) and Vise Kriterijumska Optimizacija Kompromisno Revenge (VIKOR).

Among them, TOPSIS [16] is the most effective method that utilizes the idea of choosing an ideal solution that is nearer to a positive ideal solution (PIS) and a long way from a negative ideal solution (NIS). TOPSIS method has effectively been applied by many researchers in a fuzzy environment [17–22]. Zhang and Xu [23] applied (PF) TOPSIS method in decision-making applications. Garg [24] utilizes interval-based data by introducing the IVPF-TOPSIS method. In this work, we use the technique [24] to select the best (S-box).

In the present world, security and confidentiality are the existing challenges for researchers. To overcome these challenges, strong cryptographic algorithms are designed nowadays, keeping the property to resist any differential and linear cryptanalysis attacks. The construction of modern block cipher is based on confusion and diffusion components. These two components are building blocks of any modern information confidentiality mechanisms. The idea to add confusion and diffusion in modern information secrecy techniques is to make it resistant against various cryptographic attacks. These two characteristics can be achieved through substitution box (S-box) and permutation box (P-box). An S-box is generally a nonlinear mapping which is used nowadays in modern ciphers schemes. The ability of encryption depends on the strength of this nonlinear component in manipulating the input information. Many techniques have been introduced in the literature for constructing secure S-boxes [25–42]. Multi-criteria decision-making techniques were already used extensively for various problems in literature [42–49].

Our contributions

In this work, a decision-making algorithm is utilized to select the suitable S-box. Our contributions are summarized as follows:

- We first look into the results by investigating the cryptographic properties of some standard S-boxes.
- Secondly, the TOPSIS method based on the IVPF set is applied to analyze the results to reach the final decision.
- We ranked best nonlinear confusion component of block ciphers which can be utilized in any modern information confidentiality mechanism.

The rest of the article is organized as follows: "Some basic preliminaries" is devoted to background. In "Cryptographic properties of S-boxes", we added standard cryptographic analysis. The IVPF-based TOPSIS method is applied to choose the desired S-box is presented in "Selection of optimum nonlinear confusion component based on interval–valued Pythagorean fuzzy set". In "Results and discussion", we added results and discussions of our proposed method on S-boxes. "Conclusion" is dedicated to conclusion and future recommendations.

Some basic preliminaries

In this section, we will defined some fundamental definitions will be helpful in following sections of our article.

Definition 1. Let G be a ground set. A fuzzy set F in G is defined as

$F = \{(g, \alpha_F(g)) \mid g \in G\}$, where$_F : G \rightarrow [0, 1]$, is the membership value of every element $g \in G$ to F [1].

Definition 2. Let G be a ground set. An intuitionistic fuzzy set (IFS) I in G is defined as.

$$I = \{(g, \alpha_1(g), \beta_1(g)) | g \in G\},$$

where α_I : G → [0, 1] and β_I : G → [0, 1] indicates the membership value and non-membership value of every element $g \in G$ to I, respectively, with the condition $0 \leq \alpha_I$(g) + β_I(g)≤ 1. The indeterminacy value is given by $\rho_I(g) = 1 - \alpha_I(g) - \beta_I(g)$. For simplicity, Yager and Xu called the pair (α_I(g),β_I(g)) an IF number and is represented by I = (α_I, β_I) [2].

Definition 3. Let G be a ground set. An interval-valued intuitionistic fuzzy set (IVIFS) A in G is defined as

$$A = \Big\{\Big(g, \Big[(\alpha_A(g))^l, , (\alpha_A(g))^u\Big], \times \Big[(\beta_A(g))^l, (\beta_A(g))^u\Big]\Big), |g \in G\Big\},$$

where α_A : G → L[0, 1] is the membership interval denoted by[$(\alpha_A(\mathrm{g}))^l$, $(\alpha_A(\mathrm{g}))^u$] with $(\alpha_A(\mathrm{g}))^l \leq (\alpha_A(\mathrm{g}))^u$ and β_A : G → L[0, 1]is the non-membership interval denoted by[$(\beta_A(\mathrm{g}))^l$,$(\beta_A(\mathrm{g}))^u$] with $(\beta_A(\mathrm{g}))^l \leq (\beta_A(\mathrm{g}))^u$ to each element $g \in G$ to A, respectively, with condition $(\alpha_A(\mathrm{g}))^u + (\beta_A(\mathrm{g}))^u \leq 1$. Foreveryg $\in G$, α_A and β_A are the closed subinterval of[0, 1]. For simplicity, the IVIF number is represented by A = ([a_1, b_1], [a_2, b_2]), where $b_1 + b_2 \leq 1$ [3].

Definition 4. Let G be a ground set. A Pythagorean fuzzy set (PFS) P in G is defined as [9]

$$P = \big\{\big(g, \alpha_p(g), \beta_p(g)\big)|\, g \in G, \big\}$$

where $\alpha_P : G \rightarrow$ [0, 1] indicates the membership value and β_P : G → [0, 1] indicates the non-membership value of an element g ∈ G to the set *P*, respectively, with condition $0 \leq (\alpha_P(g))^2 + (\beta_P(g))^2 \leq 1$. The indeterminacy value is given by

$$\rho_P(g) = (1 - \Big((\alpha_P(g))^2 + (\beta_P(g))^2\Big))^{0.5}$$

Zhang and Xu denote the pair (α_P(g), β_P(g)) as PF number and is represented by $P = (\alpha_P,\beta_P)$.

Definition 5. Let G be a ground set. An interval-valued Pythagorean fuzzy set (IVPFS) I_P in G is defined as [11]

$$I_p = \Big\{\Big(g, \Big[\big(\alpha_{I_P}(g)\big)^l, \big(\alpha_{I_P}(g)\big)^u\Big], \times\Big[\big(\beta_{I_P}(g)\big)^l, \big(\beta_{I_P}(g)\big)^u\Big]\Big)|g \in G\Big\}$$

where α_{I_P}G → L[0, 1] ithe membership interval denoted by[$(\alpha_{I_P}(g))^l$, $(\alpha_{I_P}(g))^u$] with $(\alpha_{I_P}(g))^l \leq (\alpha_{I_P}(g))^u$ and $\beta_{I_P} : G \rightarrow$ [0, 1] is the non-membership interval denoted by [$(\beta_{I_P}(g))^l$,$(\beta_{I_P}(g))^u$] with $(\beta_{I_P}(g))^l \leq (\beta_{I_P}(g))^u$ to each element $g \in G$ to I_P, respectively, with condition $((\alpha_{I_P}(g))^u)^2 + ((\beta_{I_P}(g))^u)^2 \leq 1$. For every g $g \in G$, α_{I_P} and υ_{I_P} are the closed subinterval of [0, 1].For simplicity IVPF number is denoted by I_P = ([a_1, b_1], [a_2, b_2]) ${b_1}^2 + {b_2}^2 \leq 1$. The indeterminacy value is given by:

$$\rho_{I_P}(g) = \Big[\Big(1-\big((\alpha_{I_P}(g))^u\big)^2 - \big((\beta_{I_P}(g))^u\big)^2\Big)^{0.5}, \Big(1-\Big(\big(\alpha_{I_P}(g)\big)^l\Big)^2 - \Big(\big(\beta_{I_P}(g)\big)^l\Big)^2\Big)^{0.5}\Big]$$

.

Definition 6. Interval-valued Pythagorean fuzzy numbers can be graded using score function which is given as follows [9]:

$$S(I_P) = \frac{({a_1}^2 + {b_1}^2 - {a_2}^2 - {b_2}^2)}{2}, \tag{1}$$

where I_P = ([a_1, b_1], [a_2,b_2]) be any IVPF number with $-1 \leq$ S (I_P) ≤ 1. However, it is observed in many cases that score function is unable to grade IVPF number. For example, let I_{P1} = [0.4, 0.5], [0.4, 0.5] and I_{P2} = [0.6, 0.7], [0.6, 0.7] be two IVPF numbers, then using Eq. (1), we have S (I_{P1}) = S (I_{P2}) = *0*. Thus, it is unable to find the best between them. To counter this problem an accuracy function [9] is introduced which is defined as:

$$Z(I_P) = \frac{({a_1}^2 + {b_1}^2 + {a_2}^2 + {b_2}^2)}{2} \tag{2}$$

where $0 \leq Z\ (I_P) \leq 1$. If we apply Eq. (2) in above example, we get Z (I_{P1}) = 0.41 and Z (I_{P2}) = 0.85. Here it is clearly observed that $I_{P1} < I_{P2}$. Based on above observation, a comparison method is formulated as follows:

Proposition For any two IVPF numbers, I_{P1} and I_{P2} the following results hold [9],

1. If S (I_{P1}) < S (I_{P2}), then $I_{P1} < I_{P2}$.
2 If S (I_{P1}) > S (I_{P2}), then $I_{P1} > I_{P2}$.
3 If S (I_{P1}) = S (I_{P2}),

(i) If Z (I_{P1}) < Z (I_{P2}), then $I_{P1} < I_{P2}$.

(ii) If Z (I_{P1}) > Z (I_{P2}), then $I_{P1} > I_{P2}$.

(iii) If Z (I_{P1}) = Z (I_{P2}), then $I_{P1} \sim I_{P2}$.

Limitations of existing score and accuracy function

Here, we consider an example which illustrates that, both, the score and the accuracy functions are inadequate to provide the correct information about the IVPF numbers used in the decision process.

Example Let I_{P1}= ([0, 0.5], [0.1, 0.8]) and I_{P2} = ([0.3, 0.4], [0.4, 0.7]) be two IVPF numbers, then using Eq. (1), we have.

$$S\,(I_{P1}) = -0.2\,and\,S\,(I_{P2}) = -0.2$$

Now using Eq. (2), we have.

$$S\,(I_{P1}) = -0.2\,and\,S\,(I_{P2}) = -0.2$$

Therefore, by proposition 2.1 (iii) $I_{P1} \sim I_{P2}$. But it is clear that $I_{P1} \neq I_{P2}$. Hence, both score function and accuracy function are not sufficient to grade IVPF numbers, so there is a need of an efficient score function which addresses this problem.

Improved score function

Garg [22] improved the score function by taking into account the indeterminacy information of an IVPF number which is given by:

$$\mathrm{Q}(I_P) = \frac{(a_1^2 - a_2^2)(1 + (1 - a_1^2 - a_2^2)^{o.5}) + (b_1^2 - b_2^2)(1 + (1 - b_1^2 - b_2^2)^{0.5})}{2} \quad (3)$$

where $-1 \leq \mathrm{Q}\,(I_P) \leq 1$. Garg presented comparison laws based on improved score function which is defined as follows:

If Q (I_{P1}) < Q (I_{P2}), then I_{P1} <I_{P2}.
If Q (I_{P1}) > Q (I_{P2}), then I_{P1} >I_{P2}.
If Q (I_{P1}) = Q (I_{P2}), then $I_{P1} \sim I_{P2}$.

Now, let us check the effectiveness of the proposed score functions. Consider two IVPF numbers defined in Example 2.1 then after applying Eq. (3), we have.

$$Q\,(I_{P1}) = -0.5393 \text{ and } Q\,(I_{P2}) = -0.6558$$

Hence Q (I_{P1}) > Q (I_{P2}) ⇒ I_{P1} >I_{P2}. Garg [22] proved some important results for improved score function which are discussed below:

$$\text{If } I_p = ([1,\ 1],\ [0,\ 0]) \text{ then } \mathrm{Q}\,(I_p) = 1. \quad (4)$$

$$\text{If } \mathrm{I}_p = ([0,\ 0],\ [1,\ 1]) \text{ then } \mathrm{Q}\,(I_p) = -1. \quad (5)$$

The classification of different types of set are given in Figs. 1, 2 shows different types of uncertain parameters in fuzzy numbers. The generalization of fuzzy sets and their corresponding extensions are given in Fig. 3, along with their historical publication years and name of researchers. These classifications are nowadays used in several designs of multi-criteria decision-making schemes for the classification and ranking of given data set.

Multi-criteria decision-making

Multi-criteria decision-making is defined as a mathematical tool permit the comparative investigation of various available situations or alternatives based on several criteria and sub-criteria, often conflicting to direct the policy makers or stakeholders concerning an optimum selection. Mathematically, MCDM is multivalued function defined as:

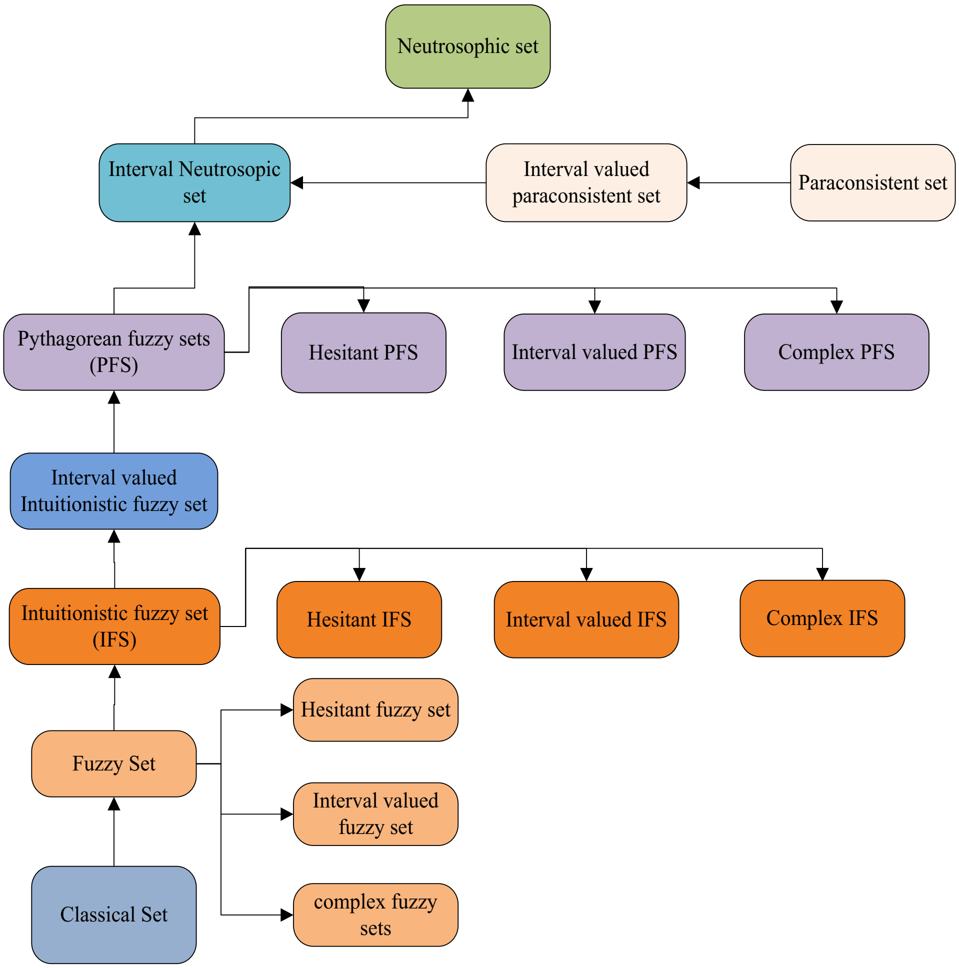
$$f : A \times C \times W \times Ag \to R,$$

where $A = \{A_1, A_2, A_3, \ldots, A_\mathrm{n}\}$ set of possible alternatives, $C = \{C_1,\ C_2,\ C_3, \ldots, C_\mathrm{m}\}$ set of criteria, $W = \{w_1,\ w_2,\ w_3, \ldots, w_\mathrm{m}\}$ set of weights corresponding to each criteria, Ag is aggregation and R is set of ranks after applying aggregation methods. The multi-criteria decision-making scheme comprises of the following fundamental steps for the selection of optimum alternatives among various available conflicting options to be followed (see Fig. 4):

i. Defining the formulation/objective/goal of the decision-making process
ii. Selection of Parameters/Features/Issues/Criteria/Play-off
iii. Selection of the Choices/Options/ Substitutes/ Replacements/Alternatives
iv. Selection of best weighing technique to represent the importance of each criterion
v. Technique to be applied for ranking namely method of aggregation
vi. Ranking/Classification of alternatives based on the aggregation results

MCDM is further classified into subjective and objective information. In subjective techniques we mapped qualitative information to quantitative date set. The subjective MCDM techniques fundamentally depends on the partialities of decision makers or experts. These experts ultimately determine weights for each criterion on which alternatives are to be ranked. Mostly commonly subjective methods based on linguistics terms which consists of degree of agreement or disagreement, respectively. Mostly fuzzy set-based techniques fall in the category of subjective mechanisms for instance, fuzzy AHP, fuzzy ANP, fuzzy TOPSIS, interval-valued fuzzy TOPSIS, Pythagorean fuzzy TOPSIS and interval-valued Pythagorean fuzzy TOPSIS method (see Fig. 5). There are various objective based methods for the selection of best alternatives. The objective MCDM techniques used different

Fig. 1 Classical to fuzzy sets classification



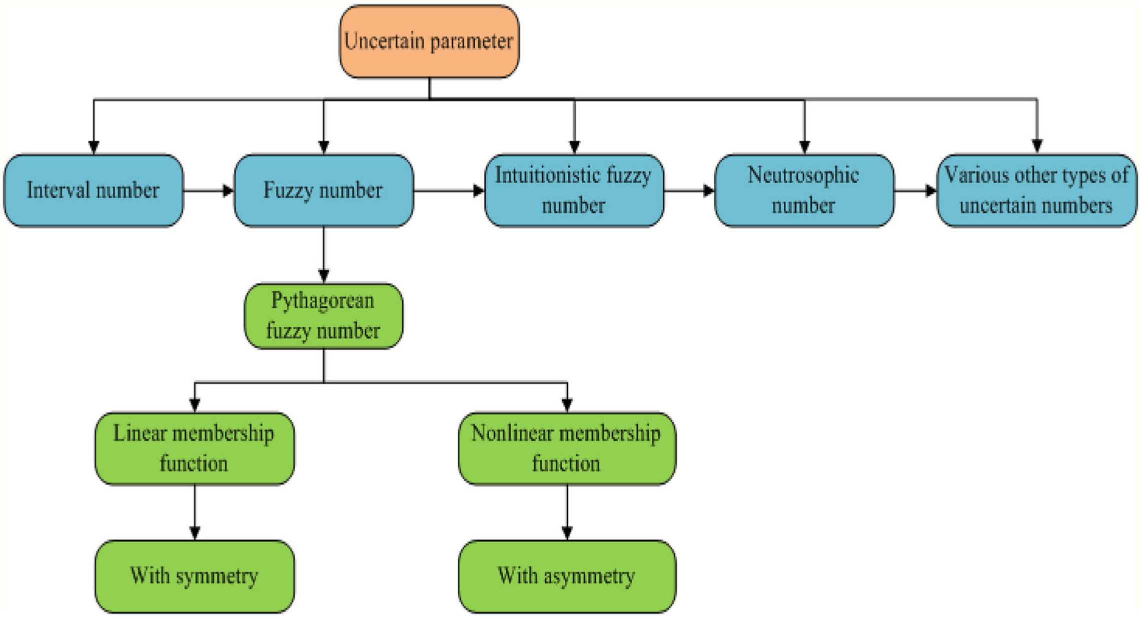

Uncertain parameter
Interval number
Fuzzy number
Intuitionistic fuzzy number
Neutrosophic number
Various other types of uncertain numbers
Pythagorean fuzzy number
Linear membership function
Nonlinear membership function
With symmetry
With asymmetry

Fig. 2 Different types of uncertainty parameters of fuzzy numbers

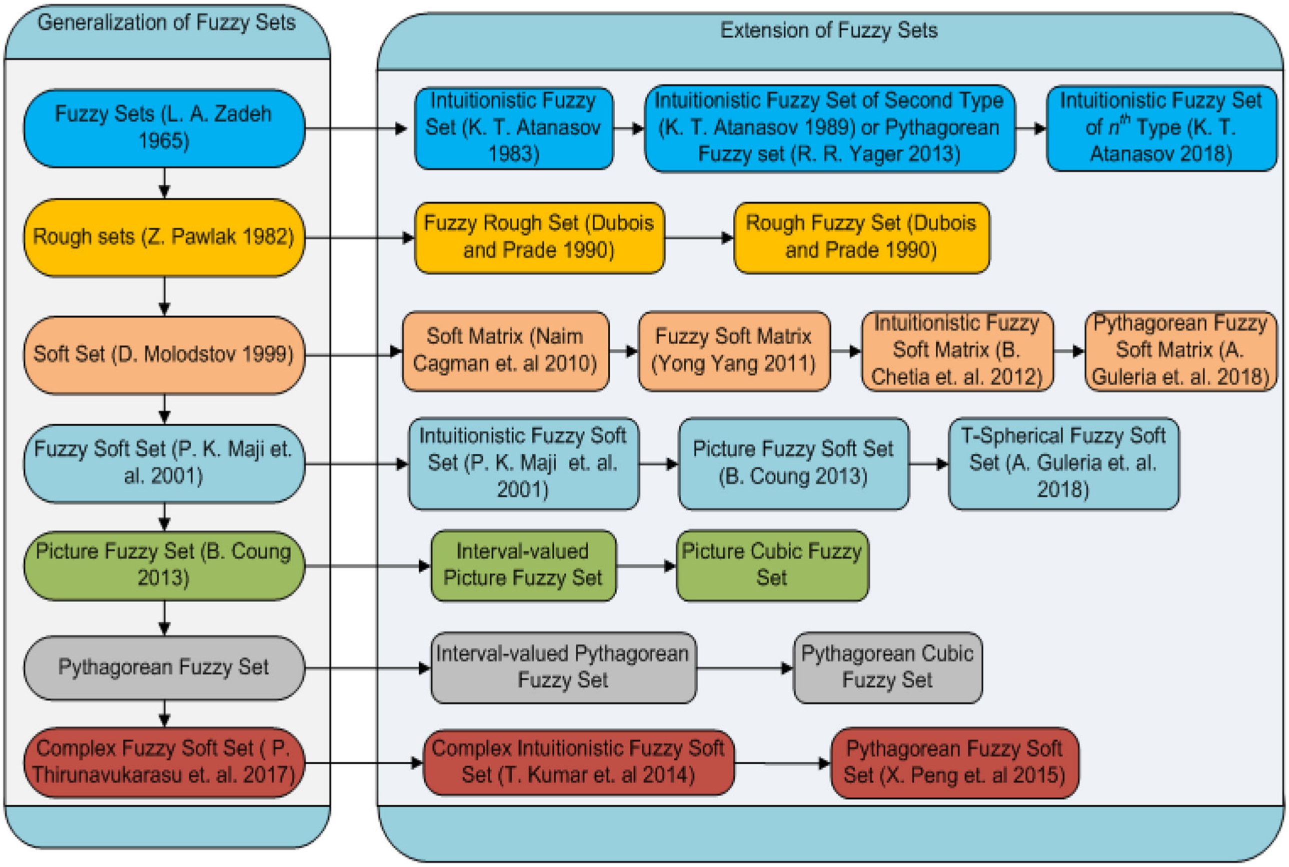

Generalization of Fuzzy Sets
Extension of Fuzzy Sets
Fuzzy Sets (L. A. Zadeh 1965)
Intuitionistic Fuzzy Set (K. T. Atanasov 1983)
Intuitionistic Fuzzy Set of Second Type (K. T. Atanasov 1989) or Pythagorean Fuzzy set (R. R. Yager 2013)
Intuitionistic Fuzzy Set of n^th Type (K. T. Atanasov 2018)
Rough sets (Z. Pawlak 1982)
Fuzzy Rough Set (Dubois and Prade 1990)
Rough Fuzzy Set (Dubois and Prade 1990)
Soft Set (D. Molodstov 1999)
Soft Matrix (Naim Cagman et. al 2010)
Fuzzy Soft Matrix (Yong Yang 2011)
Intuitionistic Fuzzy Soft Matrix (B. Chetia et. al. 2012)
Pythagorean Fuzzy Soft Matrix (A. Guleria et. al. 2018)
Fuzzy Soft Set (P. K. Maji et. al. 2001)
Intuitionistic Fuzzy Soft Set (P. K. Maji et. al. 2001)
Picture Fuzzy Soft Set (B. Coung 2013)
T-Spherical Fuzzy Soft Set (A. Guleria et. al. 2018)
Picture Fuzzy Set (B. Coung 2013)
Interval-valued Picture Fuzzy Set
Picture Cubic Fuzzy Set
Pythagorean Fuzzy Set
Interval-valued Pythagorean Fuzzy Set
Pythagorean Cubic Fuzzy Set
Complex Fuzzy Soft Set (P. Thirunavukarasu et. al. 2017)
Complex Intuitionistic Fuzzy Soft Set (T. Kumar et. al 2014)
Pythagorean Fuzzy Soft Set (X. Peng et. al 2015)

Fig. 3 Extension and generalization of fuzzy set

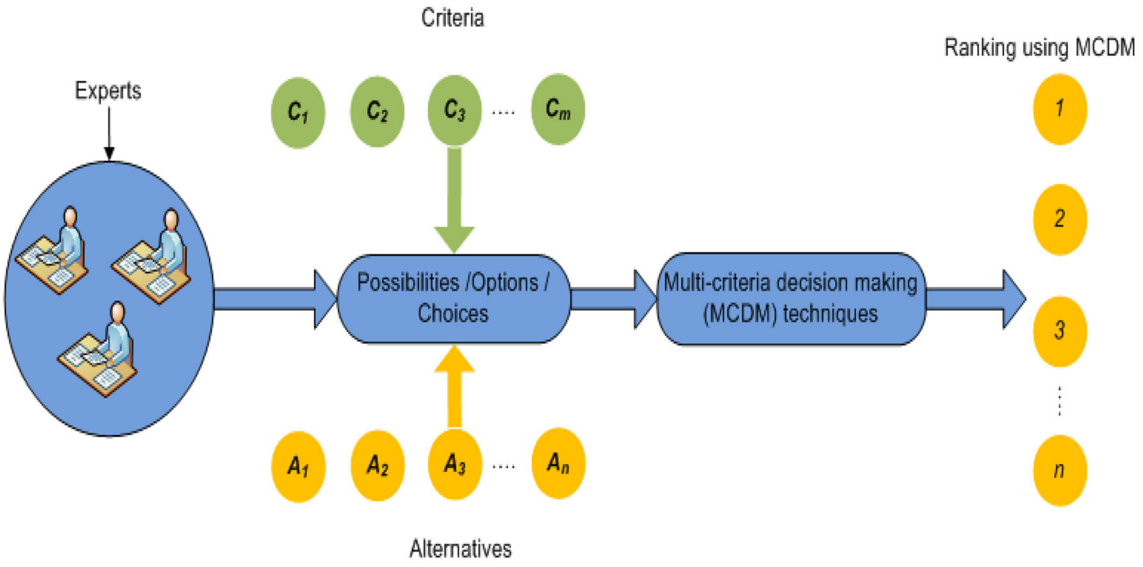

Criteria
Ranking using MCDM
Experts
C1
C2
C3
....
Cm
1
2
3
n
Possibilities /Options / Choices
Multi-criteria decision making (MCDM) techniques
A1
A2
A3
....
An
Alternatives

Fig. 4 Multi-criteria decision-making technique components and process

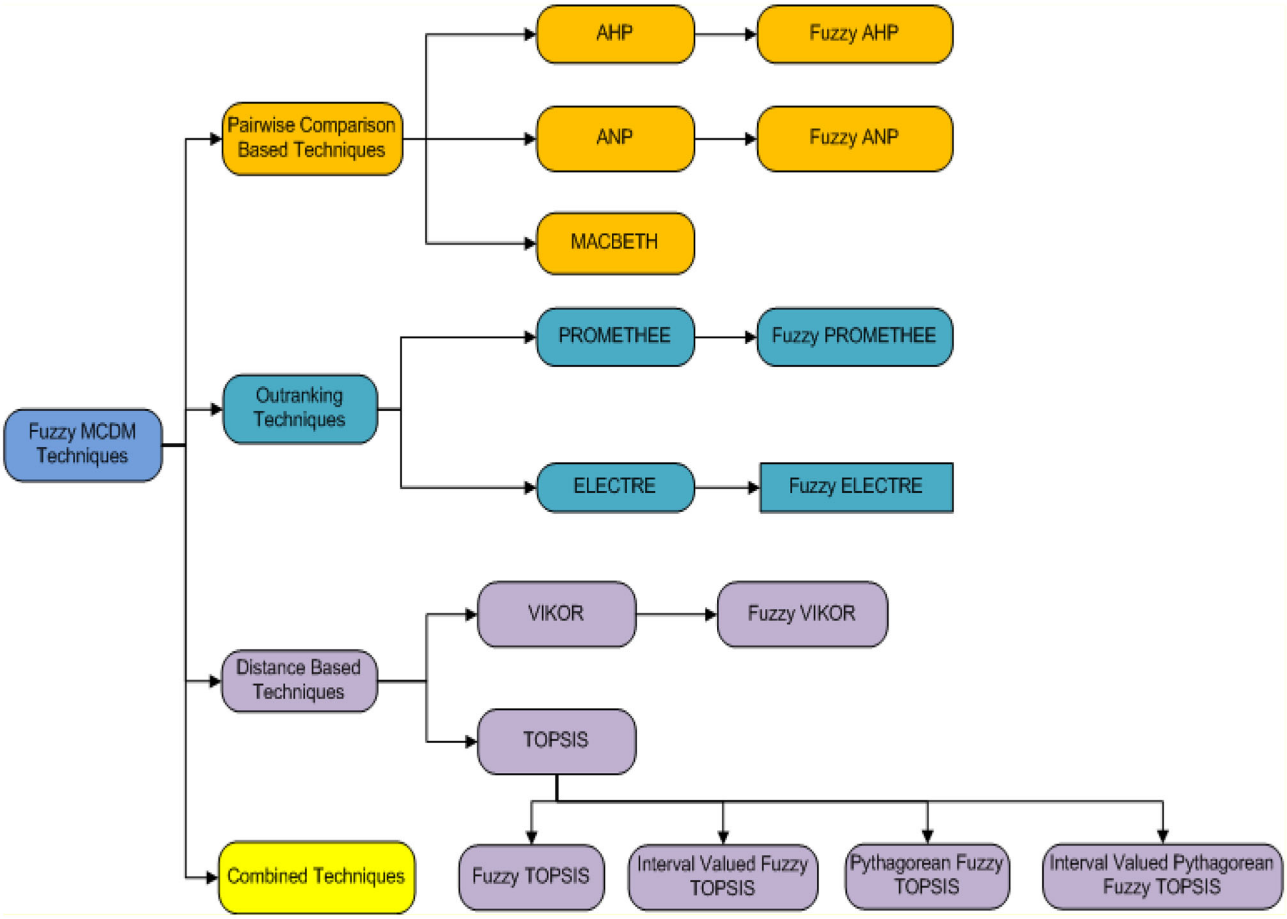


Fig. 5 Fuzzy-based multi-criteria decision-making techniques

aggregation operations or mathematical techniques and there is no role of decision makers to influential the relative importance of criteria. The most common used objective MCDM are TOPSIS, VIKOR, PROMETHEE, ELECTRE and hybrid techniques.

Cryptographic properties of S-boxes

This section mainly deals with some well-known cryptographic properties of nonlinear confusion component of block ciphers.

Nonlinearity

It is defined as minimum hamming distance of any Boolean function h from all affine functions. The mathematical expression for nonlinear of Boolean function h is given as follows:

$$\mathrm{NL}_h = \min_{a\epsilon A_n} \mathrm{d}(h, a),$$

where $a\epsilon A_n$ an affine function, d is the distance between a Boolean function h and set of all affine functions A_n. High value of nonlinearity increases the resistance against any cryptanalytic attack optimum value of nonlinearity is 120 [35].

Strict avalanche criterion (SAC)

It is used to determine the confusion ability of multivalued Boolean function namely S-box. The optimum value of SAC is 0.5.

Bit-independent criterion

Bit-independent criterion (BIC) defines the relationship between bit independent and nonlinearity. It also defines the relationship between bit independent and SAC. It is noticed that if nonlinearity and SAC are satisfied, then BIC is also satisfied [33].

Sum of square and absolute indicator

The absolute indicator is the maximum absolute value of $\delta_H(\mathrm{w})$ ∀ w $\epsilon\{1\ldots 2^{n-1}\}$. The sum of square indicator is denoted by σ_h and is given by $\sum_w (\delta(w))^2$ where $\delta(w)$ is an autocorrelation of n variable Boolean function h.

Algebraic degree

It is defined as the highest number of confusion component in truth table. Low value of algebraic degree decreases the resistance against any cryptanalytic attack [36].

Algebraic immunity

High level of algebraic immunity is required to overcome the algebraic attacks in breaking an encryption system [37].

Transparency order

Low value of transparency order is required to resist against any differential power analysis (DPA) attack [38].

Robustness to differential cryptanalysis

Suppose $F = (f_1, f_2, \ldots, f_s)$ be an $n \times s$ S-box, where h_j ($j = 1,\ldots,s$) is a function on GF (2^n). If L is the highest value of differential characteristic Table on F and k is the number of non-zero values in the first column of the table where the value of 2^n is not calculated in either case [39]. Then, F is ε – robustness against the differential cryptanalysis, where ε is defined by:

$$\varepsilon = \left(1 - \frac{k}{2^n}\right)\left(1 - \frac{L}{2^n}\right)$$

Signal to noise ratio

High value of signal to noise ratio (SNR) is required for strong S-box, which is close to maximum bound [40].

Confusion coefficient variance

The confusion coefficient variance (CCV) indicates the resistance of S-boxes against any cryptanalytic attack. High value of confusion coefficient variance is required, which infers that the S-box output is distinctive [41].

Selection of optimum nonlinear confusion component based on interval-valued Pythagorean fuzzy set

TOPSIS [16] is one of the popular and preferable MCDM methods used to find a solution which is nearer to positive ideal solution (PIS) and a long way from negative ideal solution (NIS). With the passage of time, researchers applied TOPSIS method to solve decision problems in different fuzzy environments.

Chen [21] used TOPSIS method for fuzzy environment, Park in [22] extended it for interval-valued fuzzy environment. All above extensions were not able to handle decision problems using Pythagorean fuzzy information. Therefore, Hang and Xu [23] in 2014 introduced Pythagorean fuzzy TOPSIS method to solve decision problems using PFSs. Further, Garg [24] utilizes TOPSIS method for solving decision problems containing IVPF information by introducing improved score function. The detailed steps of IVPFS-based MCDM are given in [24]. The thirst for searching and construction of ideal S-box is always an interesting problem among cryptographers in literature. Our principal goal here is to use IVPFS-based MCDM for the selection of best nonlinear confusion component of modern block ciphers.

Our aim here is to use IVPFS-based MCDM scheme for the selection of best nonlinear confusion component of block ciphers [24]. For this purpose, let $S = \{S_1, S_2, S_3, S_4, S_5, S_6\}$ be a set of six S-boxes, in which S_1 represents (AES) S-box, S_2 represents APA S-box, S_3 represents Gray S-box, S_4 represents Prime S-box, S_5 represents Skipjack S-box and S_6 represents (XYI) S-box, and $T = \{T_{1,} T_{2,} T_{3,} T_{4,} T_{5,} T_{6,} T_{7,} T_{8,} T_{9,} T_{10,} T_{11,} T_{12,} T_{13}\}$ be a set of criteria, in which T_1 is nonlinearity, T_2 is strict avalanche criterion (SAC), T_3 is bit-independent criterion (BIC-SAC), T_4 is BIC-Nonlinearity, T_5 is absolute indicator, T_6 is sum of square indicator, T_7 is algebraic degree, T_8 is algebraic immunity, T_9 is transparency order, T_{10} is composite algebraic immunity, T_{11} is robustness, T_{12} is signal to noise ratio (SNR), T_{13} is confusion coefficient variance.

The criteria weights, provided by an expert, are given by $W = \{0.0738, 0.0818, 0.0907, 0.0912, 0.0421, 0.0424, 0.0926, 0.0926, 0.0915, 0.0926, 0.0787, 0.0774, 0.0528\}^t$ such that $\sum w = 1$. The S-boxes are examined using IVPF information given by decision maker which satisfies the above-mentioned criteria. The decision maker utilizes the (IVPF) TOPSIS method to select the desired S-box.

The detail of the procedure is given below:

Table 1 Interval-valued Pythagorean fuzzy decision matrix $I_P = (T_m(S_n))_{m \times n}$

$$\begin{bmatrix}
([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.4, 0.6], [0.5, 0.6]) \\
([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.6, 0.8], [0.3, 0.5]) & ([0.6, 0.8], [0.3, 0.5]) \\
([0.7, 0.8], [0.2, 0.4]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) \\
([0.7, 0.8], [0.2, 0.4]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.2, 0.4], [0.7, 0.8]) & ([0.4, 0.6], [0.5, 0.6]) & ([0.4, 0.6], [0.5, 0.6]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.2, 0.5]) & ([0.3, 0.5], [0.6, 0.7]) & ([0.4, 0.6], [0.4, 0.6]) & ([0.3, 0.5], [0.5, 0.6]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.5, 0.6], [0.4, 0.6]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.5, 0.6], [0.4, 0.5]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.5, 0.6], [0.4, 0.6]) & ([0.4, 0.6], [0.5, 0.6]) & ([0.6, 0.7], [0.3, 0.4]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.6, 0.8], [0.3, 0.5]) \\
([0.5, 0.6], [0.4, 0.6]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.6], [0.3, 0.5]) & ([0.4, 0.6], [0.5, 0.6]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.6, 0.7], [0.3, 0.5])
\end{bmatrix}$$

Table 2 Normalized IVPF decision matrix $N = n_{(m,n)}$

$$\begin{bmatrix}
([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.4, 0.6], [0.5, 0.6]) \\
([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.6, 0.8], [0.3, 0.5]) & ([0.6, 0.8], [0.3, 0.5]) \\
([0.7, 0.8], [0.2, 0.4]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) \\
([0.7, 0.8], [0.2, 0.4]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) \\
([0.3, 0.5], [0.6, 0.7]) & ([0.3, 0.5], [0.6, 0.7]) & ([0.3, 0.5], [0.6, 0.7]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.5, 0.6], [0.4, 0.6]) & ([0.5, 0.6], [0.4, 0.6]) \\
([0.3, 0.5], [0.6, 0.7]) & ([0.3, 0.5], [0.6, 0.7]) & ([0.2, 0.5], [0.6, 0.7]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.4, 0.6], [0.4, 0.6]) & ([0.5, 0.6], [0.3, 0.5]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.5, 0.6], [0.4, 0.6]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.5, 0.6], [0.4, 0.5]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.5, 0.6], [0.4, 0.6]) & ([0.4, 0.6], [0.5, 0.6]) & ([0.6, 0.7], [0.3, 0.4]) & ([0.6, 0.7], [0.3, 0.5]) \\
([0.6, 0.7], [0.3, 0.5]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.6, 0.7], [0.3, 0.5]) & ([0.7, 0.8], [0.2, 0.4]) & ([0.5, 0.6], [0.4, 0.5]) & ([0.6, 0.8], [0.3, 0.5]) \\
([0.4, 0.6], [0.5, 0.6]) & ([0.3, 0.5], [0.6, 0.7]) & ([0.3, 0.5], [0.6, 0.6]) & ([0.5, 0.6], [0.4, 0.6]) & ([0.2, 0.4], [0.7, 0.8]) & ([0.3, 0.5], [0.6, 0.7])
\end{bmatrix}$$

Table 3 The score matrix of given information

$$R = \begin{bmatrix} 0.7266 & 0.7266 & 0.7266 & 0.1689 & 0.1689 & -0.0796 \\ 0.7266 & 0.7266 & 0.7266 & 0.1689 & 0.4948 & 0.4948 \\ 0.7266 & 0.4163 & 0.7266 & 0.5893 & 0.4163 & 0.7266 \\ 0.7266 & 0.4163 & 0.7266 & 0.7266 & 0.4163 & 0.7266 \\ -0.4163 & -0.4163 & -0.4163 & 0.7266 & 0.0796 & 0.0796 \\ -0.4163 & -0.4163 & -0.4651 & 0.4163 & 0 & 0.2343 \\ 0.4163 & 0.4163 & 0.4163 & 0.4163 & 0.4163 & 0.4163 \\ 0.4163 & 0.4163 & 0.4163 & 0.4163 & 0.4163 & 0.4163 \\ 0.4163 & 0.4163 & 0.4163 & 0.0796 & 0.1689 & 0.4163 \\ 0.4163 & 0.4163 & 0.4163 & 0.4163 & 0.4163 & 0.4163 \\ 0.1689 & 0.1689 & 0.0796 & -0.0796 & 0.4977 & 0.4163 \\ 0.4163 & 0.1689 & 0.4163 & 0.7266 & 0.1689 & 0.4948 \\ -0.0796 & -0.4163 & -0.3245 & 0.0796 & -0.7266 & -0.4163 \end{bmatrix}$$

Step 1

Initially, a decision matrix is constructed in which all the preferences are given as, IVPF numbers. For this purpose, Let I_{P}= $(T_{\mathrm{m}}(S_n))_{\mathrm{m\times n}}$ = $([a_{\mathrm{m,n}}, b_{\mathrm{m,n}}], [c_{m,n}, \mathrm{d}_{m,n}])_{\mathrm{m\times n}}$ be an IVPF decision matrix as defined in Table 1, where $[a_{m,n}, b_{m,n}]$ denotes the degree of membership of the S-box S_n(n = 1,2…,6) with respect to the criterion T_m (m = 1,2…,13) and $[c_{m,n}, \mathrm{d}_{m,n}]$ denotes the degree of non-membership with $(b_{m,n})^2 + (d_{m,n})^2 \leq 1$.

In Table 1, the element $T_1(S_1)$ = ([0.7, 0.8], [0.2, 0.4]) (first row and first column) corresponding to S_1(AES) and T_1 (Nonlinearity) represents the degree to which an S-box S_1 satisfies the criteria T_1, is expressed as [0.7, 0.8] and the degree to which an S-box S_2 dissatisfies the criteria is expressed as [0.2, 0.4]). The remaining elements in Table 1 represent the same meaning.

Step 2

Normalization of the decision matrix I_P= $(T_m(S_n))_{m\times n}$ is performed in this step, which is defined as

$$N_{m,n} = \begin{cases} T_m(S_n);\ m \in B \\ (T_m(S_n))^c;\ m \in C, \end{cases} \tag{6}$$

where $(T_m(S_n))^c$ represents the complement of $T_m(S_n)$, B and C represents the benefit and cost criteria, respectively. The results are shown in Table 2.

Step 3

Next, we construct a score matrix R, using Eq. (3). The results are presented in Table 3.

Step 4

Separation measure of each alternative, from interval-valued Pythagorean positive ideal solution (IVPIS) and interval-valued Pythagorean negative ideal solution (IVPNIS) is calculated, which is given by the formula

$$D(S_n, s^+) = \left(\sum_m \left\{w_m \left(Q\left(s^+\right) - Q\left(n_{(m,n)}\right)\right)^2\right\}^2\right)^{0.5}, \quad (m = 1, 2, ..., 13) \text{ and } (n = 1, 2, \ldots, 6) \tag{7}$$

$$D(S_n, s^+) = \left(\sum_m \{w_m \left(Q\left(n_{(m,n)}\right) - Q\left(s^-\right)\right)^2)\}^2\right)^{0.5}, \quad (m = 1, 2, \ldots 13) \text{ and } (n = 1, 2, \ldots, 6) \tag{8}$$

where $s^+ = \{[1, 1], [0, 0]\}$ and $s^- = \{[0, 0], [1, 1]\}$ represents IVPPIS and IVPNIS, respectively. Also $Q(s^+) = 1$ and $Q(s^-) = -1$ (from Eqs. (4) and (5)). The calculated results are shown in Table 4. For better understanding, the results are shown geometrically in Fig. 6.

Figure 6 illustrates that the distance of AES S-box and prime S-box from interval-valued Pythagorean PIS is minimum, where the distance of AES S- box and Gray S-box from interval-valued Pythagorean NIS is maximum.

Step 5

Relative closeness coefficient is measured to evaluate the performance score of each S-box. Relative closeness coefficient RC C_i of each alternative from ideal solution is given by:

$$\mathrm{RCC_i} = \frac{D(S_n, s^-)}{D\left(S_n, s^-\right) + D(S_n, s^+)} \tag{9}$$

The results are presented in Table 5.

Step 6

The S-box with high rank is considered as the best S-box, and it is clear from Table 5 that AES S-box box is the desired S-box with respect to above-mentioned criteria. It can be visualized geometrically as shown in Fig. 7.

Results and discussion

The quality of modern information confidentiality mechanism highly depends on its nonlinear confusion component. This nonlinear confusion component which is responsible for adding confusion capability in encryption algorithm. The confusion is used to make relationship between the

Table 4 Separation measure of each alternative from IVPPIS and IVPNIS

	S_1	S_2	S_3	S_4	S_5	S_6
$D(S_n, s^+)$	0.1610	0.1932	0.1823	0.1604	0.2074	0.1615
$D(S_n, s^-)$	0.0965	0.0714	0.0967	0.0794	0.0533	0.081

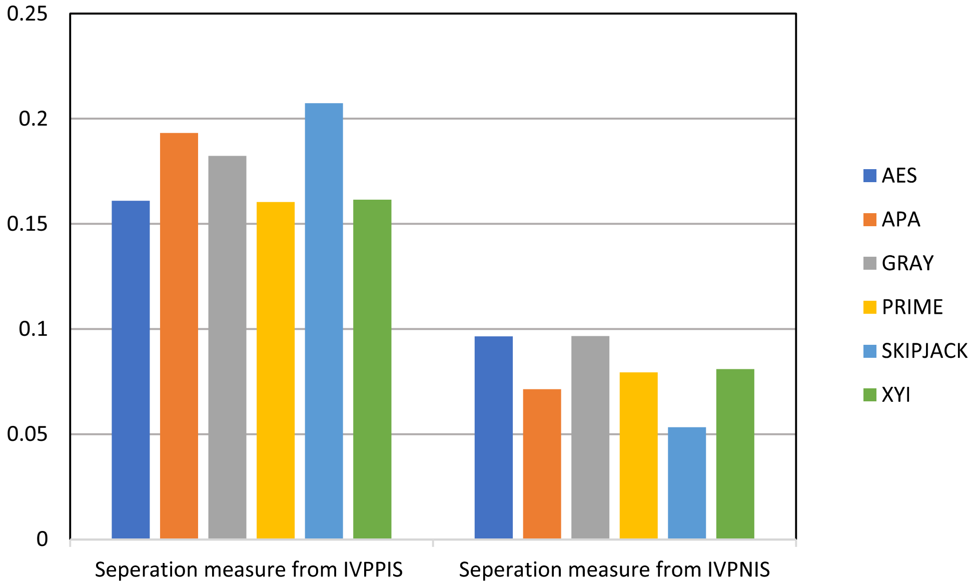


Fig. 6 Distance of each alternative from IVPPIS and IVPNIS

Table 5 Relative closeness coefficient and rank of each S-box

	S_1	S_2	S_3	S_4	S_5	S_6
RCC_i	0.3747	0.2699	0.3467	0.3312	0.2045	0.3358
Rank	1	5	2	4	6	3

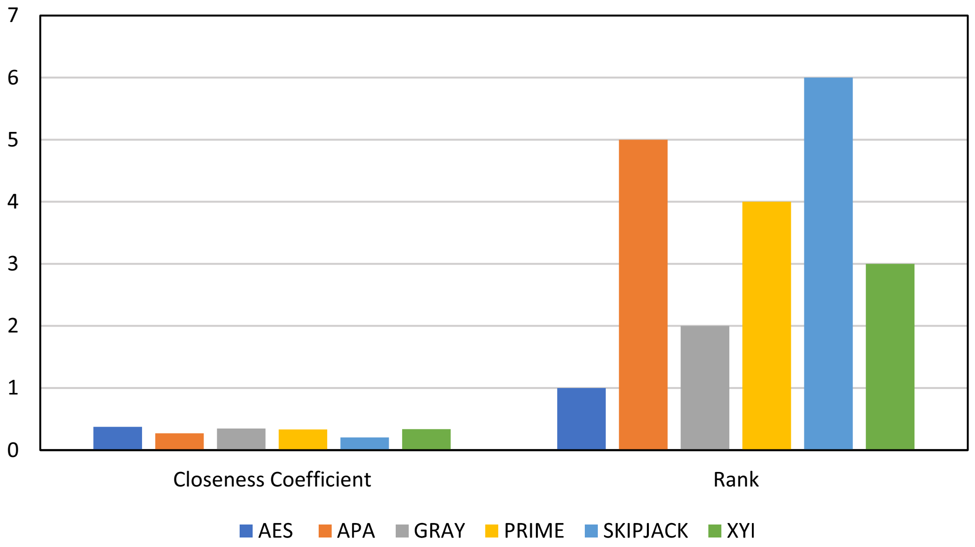


Fig. 7 Relative closeness of each alternative

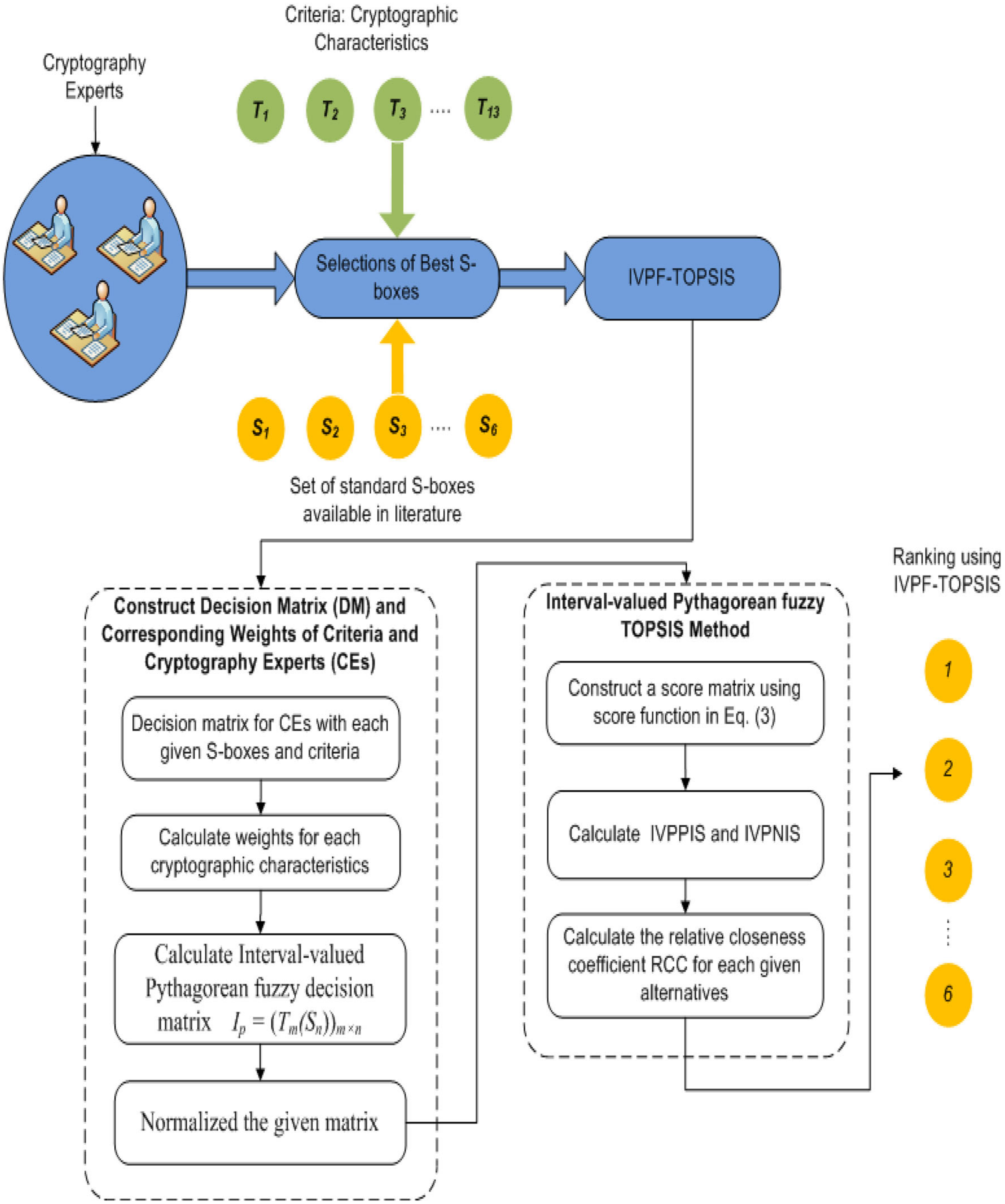

Criteria: Cryptographic Characteristics
Cryptography Experts
T_1
T_2
T_3
....
T_{13}
Selections of Best S-boxes
IVPF-TOPSIS
S_1
S_2
S_3
....
S_6
Set of standard S-boxes available in literature
Ranking using IVPF-TOPSIS
Construct Decision Matrix (DM) and Corresponding Weights of Criteria and Cryptography Experts (CEs)
Decision matrix for CEs with each given S-boxes and criteria
Calculate weights for each cryptographic characteristics
Calculate Interval-valued Pythagorean fuzzy decision matrix $I_p = (T_m(S_n))_{m \times n}$
Normalized the given matrix
Interval-valued Pythagorean fuzzy TOPSIS Method
Construct a score matrix using score function in Eq. (3)
Calculate IVPPIS and IVPNIS
Calculate the relative closeness coefficient RCC for each given alternatives
1
2
3
6

Fig. 8 Proposed optimum S-box selection criteria based on interval-valued Pythagorean fuzzy set

key and the ciphertext as complex as possible in order not to retrieve plaintext. In modern block ciphers, confusion is achieved through substitution box (S-box) which is nonlinear confusion component. With this study, we have studied various standard S-boxes based on their standard cryptographic characteristics. We have studied AES, APA, Gray, Prime, Skipjack and XYI S-boxes, respectively. It is quite evident from Fig. 7, that AES S-box is the best nonlinear confusion component of modern block ciphers. In this article, we fundamentally tested standard six S-boxes based on thirteen cryptographic characteristics (see Fig. 8). We have taken decision matrix based on these thirteen cryptographic characteristics for six standard S-boxes. The relative closeness of AES S-box is high as compared to other standard S-boxes which clearly elucidate its distance from positive idea solution is maximum and negative ideal solution is minimum.

Conclusion

With this investigation, we can easily determine the best S-box which is one of the nonlinear confusion component of modern block cipher mechanism. We have used an interval-valued Pythagorean fuzzy set-based TOPSIS technique to scrutinize the suitable S-box, whereas the preference values of each S-box are taken in the form of IVPF number. This technique can easily be utilized for the classification of encryption algorithms based on various security analyses. These security analyses can be taken as criteria and encryption algorithms are taken to be alternatives.

Acknowledgements This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2023R87), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Funding This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project Number (PNURSP2023R87), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Declarations

Conflict of interest The authors reveal that they have no conflict of interests.

References

1. Bellman RE, Zadeh LA (1970) 'Decision-making in a fuzzy environment.' Manag Sci 17(4):B-41
2. Atanassov K (2016) 'Intuitionistic fuzzy sets.' Int J Bioautomat 20:1
3. Abdullah S, Ayub S, Hussain I, Bedregal B, Khan MY (2017) 'Analyses of S-boxes based on interval valued intuitionistic fuzzy sets and image encryption.' Int J Computat Intell Syst 10(1):851–865
4. Garg H (2016) 'A new generalized improved score function of interval-valued intuitionistic fuzzy sets and applications in expert systems.' Appl Soft Comput 38:988–999
5. Garg H (2016) 'Generalized intuitionistic fuzzy interactive geometric interaction operators using Einstein t-norm and t-conorm and their application to decision making.' Comput Ind Eng 101:53–69
6. Cao YX, Zhou H, Wang JQ (2018) 'An approach to interval-valued intuitionistic stochastic multi-criteria decision-making using set pair analysis.' Int J Mach Learn Cybern 9(4):629–640
7. Zhou H, Wang J, Li XE, Wang JQ (2016) 'Intuitionistic hesitant linguistic sets and their application in multi-criteria decision-making problems.' Oper Res Int Journal 16(1):131–160
8. Garg H (2017) 'Novel intuitionistic fuzzy decision making method based on an improved operation laws and its application.' Eng Appl Artif Intell 60:164–174
9. Yager RR (2013) "Pythagorean fuzzy subsets," In: 2013 joint IFSA world congress and NAFIPS annual meeting (IFSA/NAFIPS), IEEE, pp. 57–61, 2013.
10. Yager RR (2013) Pythagorean membership grades in multicriteria decision making. IEEE Trans Fuzzy Syst 22(4):958–965
11. Peng X, Yang Y (2016) "Fundamental properties of interval-valued Pythagorean fuzzy aggregation operators. Int J Intell Syst 31(5):444–487
12. Greco S, Figueira J, Ehrgott M (2016) ' Multiple criteria decision analysis.' Springer, New York, p 37
13. Hwang CL, Masud ASM (2012) 'Multiple objective decision making—methods and applications: a state-of-the-art survey.' Springer Science & Business Media
14. Tzeng GH, Huang JJ (2011) Multiple 'attribute decision making: methods and applications. CRC Press
15. Çalışkan H, Kurşuncu B, Kurbanoğlu C, Güven SY, Ş. Y, (2013) 'Material selection for the tool holder working under hard milling conditions using different multi criteria decision making methods.' Materials Design 45:473–479
16. Hwang CL, Yoon K (1981) 'Multiple attribute decision making: a state of the art survey. Lecture Notes in Economics and Mathematical Systems.' Springer
17. Yue Z (2014) 'TOPSIS-based group decision-making methodology in intuitionistic fuzzy setting. Informat Sci 277:141–153
18. Torlak G, Sevkli M, Sanal M, Zaim S (2011) 'Analyzing business competition by using fuzzy TOPSIS method: an example of Turkish domestic airline industry.' Expert Syst Appl 38(4):3396–3406
19. Joshi D, Kumar S (2016) 'Interval-valued intuitionistic hesitant fuzzy Choquet integral based TOPSIS method for multi-criteria group decision making.' Eur J Oper Res 248(1):183–191
20. Xu Z, Hu H (2010) 'Projection models for intuitionistic fuzzy multiple attribute decision making.' Int J Informat Technol Decision Making 9(2):267–280
21. Chen CT (2000) ' Extensions of the TOPSIS for group decision-making under fuzzy environment.' Fuzzy Sets Syst 114(1):1–9
22. Park JH, Park IY, Kwun YC, Tan X (2011) (2011), '"Extension of the TOPSIS method for decision making problems under interval-valued intuitionistic fuzzy environment",.' Appl Math Model 35(5):2544–2556
23. Zhang X, Xu Z (2014) 'Extension of TOPSIS to multiple criteria decision making with Pythagorean fuzzy sets.' Int J Intell Syst 29(12):1061–1078
24. Garg H (2017) 'A new improved score function of an interval-valued Pythagorean fuzzy set based TOPSIS method.' Int J Uncert Quantif 7(5):463–474
25. Khan M, Shah T (2015) 'An efficient construction of substitution box with fractional chaotic system.' SIViP 9(6):1335–1338
26. Khan M, Shah T, Batool SI (2017) 'A new approach for image encryption and watermarking based on substitution box over the classes of chain rings.' Multimedia Tools Appl 76(22):24027–24062
27. Munir N, Khan M (2018) "A generalization of algebraic expression for nonlinear component of symmetric key algorithms of any characteristic p," In: 2018 international conference on applied and engineering mathematics (ICAEM), IEEE, p.48–52
28. Daemen J (1999) " aes proposal: Rijndael," aes algorithm submission. http://csrc.nist.gov/encryption/aes/Rijndael.pdf

29. Cui L, Cao Y (2007) ‘ A new S-box structure named affine-power-affine. International Journal of Innovative Computing.’ Inf Control 3(3):751–759
30. Tran MT, Bui DK, Duong AD (2008) “Gray S-box for advanced encryption standard.” In: 2008 International Conference on Computational Intelligence and Security ,IEEE, vol. 1, p. 253–258
31. Abuelyman ES, Alsehibani AAS, Arabia S (2008) S, ‘“ An optimized implementation of the S-Box using residue of prime numbers”,.’ Int J Comp Sci Net Sec 8(4):304–309
32. Skipjack and NIST, KEA algorithm specifications. Online document:http://csrc.nist.(1998),[Online].org/encryption/skipjack/skipjack.pdf
33. Shi XY, Xiao XC, Hu. You, KY Lam (2002) Int, In Conf. Info. Network. Appl, 2: 14
34. Alghafis A (2021) ‘Quantum half and full spinning operator-based nonlinear confusion component.’ IEEE Access 9:31256–31267
35. Hussain I, Shah T (2013) ‘Literature survey on nonlinear components and chaotic nonlinear components of block ciphers.’ Nonlinear Dyn 74(4):869–904
36. Zheng Y, Zhang XM (2000) ‘Improved upper bound on the nonlinearity of high order correlation immune functions.’ International Workshop on Selected Areas in Cryptography. Springer, pp 262–274
37. Nawaz Y, Gupta KC, Gong G (2009) “Algebraic immunity of S-boxes based on power mappings’*,’analysis and construction*. IEEE Trans Inf Theory 55(9):4263–4273
38. Mazumdar B, Mukhopadhyay D, Sengupta I (2013) ‘ Constrained search for a class of good bijective S-boxes with improved DPA resistivity.’ IEEE Trans Inf Forensics Secur 8(12):2154–2163
39. Mazumdar B, Mukhopadhyay D, Sengupta I (2012) “Design for security of block cipher S-Boxes to resist differential power attacks,” In: 2012 25th International Conference on VLSI Design, IEEE, pp. 113–118
40. Guilley S, Hoogvorst P, Pacalet R (2004) Differential power analysis model and some results. Smart card research and advanced applications. Springer, UK
41. Fei Y, Ding AA, Lao J, Zhang L (2014) ‘A statistics-based fundamental model for side-channel attack analysis.’ IACR Cryptol ePrint Arch 2014:152
42. Adams CM, Tavares SE (1993) “Designing S-boxes for ciphers resistant to differential cryptanalysis.” In: Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, p. 181–190
43. Tabatabaei S (2020) A novel fault tolerance energy-aware clustering method via social spider optimization (sso) and fuzzy logic and mobile sink in wireless sensor networks (wsns). Comput Syst Sci Eng 35(6):477–494
44. Khan MAR, Jain MK (2020) Feature point detection for repacked android apps. Intell Automat Soft Comp 26(6):1359–1373
45. Lee S, Ahn Y, Kim HY (2020) Predicting concrete compressive strength using deep convolutional neural network based on image characteristics. Comp, Mater Continua 65(1):1–17
46. Binti N, Ahmad M, Mahmoud Z, Mehmood RM (2020) A pursuit of sustainable privacy protection in big data environment by an optimized clustered-purpose based algorithm. Intell Automat Soft Comput 26(6):1217–1231
47. Gumaei A, Al-Rakhami M, AlSalman H, Rahman SMM, Alamri A (2020) DL-HAR: deep learning-based human activity recognition framework for edge computing. Comp, Mater Continua 65(2):1033–1057
48. Al-Wesabi FN, Alzahrani S, Alyarimi F, Abdul M, Nemri N et al (2021) A reliable NLP scheme for english text watermarking based on contents interrelationship. Comput Syst Sci Eng 37(3):297–311
49. Stojanovic V, Nedic N (2016) Joint state and parameter robust estimation of stochastic nonlinear systems. Int J Robust Nonlinear Control 26(14):3058–3074