



SCIENTIFIC OASIS

Spectrum of Engineering and
Management Sciences

Journal homepage: www.sems-journal.org
ISSN: 3009-3309



Intelligent Hybrid Selection of Secure and Energy-Efficient Lightweight Encryption Algorithms for Sustainable Internet of Things

Mian Muhammad Akhtar Hayat¹, Majid Khan^{2,*}

¹ Department of Applied Mathematics & Statistics, Institute of Space Technology, Islamabad, Pakistan

² Department of Mathematics, College of Science and Humanities in Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia

ARTICLE INFO

Article history:

Received 2 September 2026

Received in revised form 22 October 2026

Accepted 26 October 2026

Available online 28 October 2026

Keywords:

Lightweight Cryptography; Internet of Things; Resource-Constrained Devices; Energy-Efficient Computing; Low-Power Internet of Things; Resource Efficiency; Sustainable Digital Infrastructure; Information Confidentiality; Multi-Criteria Decision-Making; CRITIC; CODAS; TOPSIS

ABSTRACT

The rapid growth of Internet of Things (IoT) devices has increased the demand for secure and resource-efficient confidentiality mechanisms in constrained environments. Selecting an appropriate lightweight cipher is challenging because its implementation involves trade-offs among hardware resources, computational performance, memory, and energy requirements. This study presents an objective multi-criteria framework for evaluating well-established lightweight encryption algorithms using eight implementation-critical criteria: chip area, throughput, energy consumption, power consumption, latency, algorithm size, RAM size, and key size. The criteria importance through inter-criteria correlation (CRITIC) method is employed to determine objective criterion weights, while multiplicative exponential weighting (MEW), combinative distance-based assessment (CODAS), and technique for order preference by similarity to ideal solution (TOPSIS) are used for comparative ranking. The proposed CRITIC multi-criteria framework enables systematic selection of lightweight ciphers by jointly considering computational, hardware, memory, and energy efficiency. By promoting low-power operation and efficient utilization of computational resources, the framework may contribute to more sustainable and resilient IoT infrastructures.

1. Introduction

The world has become a global village after the advancement of information technology mechanisms. Several new and intelligent technologies have emerged, which have ultimately advanced the existing world. Various new technologies have been introduced since the Industry 4.0 revolution [1]. The Internet of Things (IoT) generally refers to interrelated connections of various devices, buildings, vehicles, and objects with sensors, with secure connectivity via wire or wireless communication to collect and exchange digital information [2]. IoT has become an important critical part of emerging technologies across several new trends in industrial evolution. The applications

* Corresponding author.

E-mail address: mk.cfd1@gmail.com

<https://doi.org/10.31181/sems41202697>

include smart home automation, industrial IoT, healthcare, agriculture, smart cities, supply chain, logistics, energy management, environmental monitoring, transportation, wearable technology, security and surveillance, waste management, water management, wildlife and conservation [3,4]. These are a few new and emerging applications of IoT. With the evolution of emerging technology, the new applications and opportunities for IoT utilization will become widespread in numerous industries and sectors [5].

IoT, cybersecurity, and blockchain are new emerging technologies. IoT is further classified into various other fields such as Internet of Health Things (IoHTs), Internet of Medical Things (IOMTs), Internet of Drone Things (IoDTs), and Internet of Vehicle Things (IoVTs) [6,7]. These technologies use different types of sensors, hardware, and software that enable the most effective and reliable means of communication with devices available in the nearest source. The utilization of these current emerging technologies surely helps us in various applications [8,9].

The security of digital information, which is passed through these small, constrained environmental devices, is now of utmost importance. The confidentiality of this digital information in IoT devices can be achieved with the help of encryption schemes [10]. These devices range from wearables and sensors to efficient and smart home applications and industrial machinery, which are usually working in various stimulating situations. With the help of lightweight encryption mechanisms, the information remains confidential over IoT devices and cloud-based platforms, which means that if an unauthorized user captures the information, it is impossible for them to decrypt it without the private key [11].

There are several IoT-based applications which comprise of sensitive information, for instance health information of a person or home security automation information. Encryption fundamentally secures this information by preserving the concealment of users' digital information. Nowadays, a new hybrid mechanism has been developed for IoT devices that ensures authentication and integrity of digital information in various applications and implementations [12,13].

IoT devices use lightweight encryption schemes to authenticate their identity and ensure that information remains intact at the time of transmission. This integrity ensures that there is no tampering or modification by an unauthorized person. IoT devices use lightweight encryption schemes for secure bootstrapping processes while initializing or connecting to a network. The trust between constrained environmental devices and networks is fundamentally ensured by the bootstrapping process. The process of bootstrapping over constrained environments prevents the eavesdropper from gaining access. Inspired by the importance of lightweight encryption and constrained environmental devices, which are critical components of the advanced technological landscape. To safeguard digital information and ensure integrity and authentication of digital content transmission, encryption schemes are now enabled to add an additional layer of security against various cryptographic attacks [14,15].

2. Literature Review

The importance of lightweight encryption algorithms increases every day. As technology emerges, devices become smart and efficient with respect to computational complexity and constrained environments. The importance of lightweight encryption algorithms is increasingly important due to its implementation and energy efficiency mode. Lightweight encryption algorithms are classified into three major categories based on design principles, application domains, and cryptographically secure primitives. Modern lightweight encryption algorithms are based on substitution-permutation networks (SP-networks), Feistel networks, and Add-Rotate-XOR (ARX) design principles. SP-network-based block ciphers such as PRESENT and SIMON are based on SP-networks that comprise sequences of substitution and permutation processes over a block of fixed

size. The second classification of lightweight encryption algorithms is with respect to cryptographic primitives, which include block ciphers, stream ciphers, hash functions, and public key encryption mechanisms [16].

Modern lightweight block ciphers use fixed-size blocks of digital information for efficiently and effectively encrypting the given data. The most famous and important lightweight block ciphers include PRESENT, SPECK and SIMON. Grain and Trivium are stream ciphers that generate a bit of keystream to bitwise XOR with the plaintext to produce the ciphertext. For authentication and data integrity, lightweight hash functions such as SPONGENT and PHOTON were designed for constrained environmental devices. Other lightweight public key encryption techniques include FrodoKEM and NTRUEncrypt enable to add confidentiality to digital information and also secure key exchange without excessive computational resources. These modern lightweight mechanisms are frequently utilized nowadays in near-field communication (NFC) and radio-frequency identification (RFID) devices due to their restricted resources and are essential for protected communication. Several other application domains include smart cards, embedded systems, low-power wireless networks, and sensor networks that employ lightweight encryption algorithms to certify the information secrecy and integrity while conserving energy in an efficient way. While implementing these modern lightweight encryption algorithms, we need three types of security levels: low security, balanced security, and high security [17].

These three levels of security fundamentally signify the level of prioritization of user needs with respect to specification, application, and demand. There are some lightweight encryption algorithms that highlight efficiency over the level of security and are suitable for applications where attack models are not extremely confrontational. There are other classes of lightweight encryption algorithms where we need to have a balance between security and efficiency, which makes them appropriate for various embedded systems and IoT devices. It is possible in other scenarios where security is dominant as compared to efficiency, which surely increases resource usage. NIST started efforts to regulate modern lightweight encryption mechanisms to encourage interoperability and security across IoT and embedded systems [18].

2.1 Our Goal

The idea of this article is to investigate the key success factors for designing lightweight encryption algorithms and their ranking based on several criteria such as chip area, throughput, energy consumption, power consumption, latency, algorithm size, RAM size, and key size, respectively. These are key factors while designing any modern lightweight encryption algorithms for constrained environment mode [19-21]. Based on these key factors, we have examined ten famous lightweight encryption algorithms against their eight possible encryption qualities. The following are essential objectives of the current article:

- i. We have investigated various lightweight encryption algorithms and their corresponding characteristics and selected ten famous mechanisms for further study.
- ii. The characteristics that we have studied are chip area, throughput, energy consumption, power consumption, latency, algorithm size, RAM size, and key size, respectively.
- iii. We have examined ten lightweight encryption algorithms, namely PRESENT, SEA, HIGHT, LEA, AES, mCrypton, NOKEON, KLEIN, CAMELLIA, and TEA, against eight possible encryption features [22-24].
- iv. We have developed new multi-criteria decision-making (MCDM)-based techniques for the selection of the best encryption algorithms among these ten famous mechanisms with corresponding features [25-27].

- v. We have utilized MCDM-based techniques CRITIC, MEW, CODAS, and TOPSIS for assigning weights and possible ranking of our investigated lightweight encryption algorithms [28-30].

3. Methodology

The selection of a lightweight encryption algorithm for a resource-constrained IoT environment can be formulated as a finite multi-criteria decision problem involving security, computational performance, hardware utilization, memory requirements, and energy consumption. To establish a consistent mathematical basis for the proposed CRITIC, MEW, CODAS, and TOPSIS framework, the principal concepts are introduced through the following definitions.

Definition 1. Let $\mathcal{A} = \{A_1, A_2, \dots, A_m\}$ be a finite set of feasible alternatives and $\mathcal{C} = \{C_1, C_2, \dots, C_n\}$ be a finite set of evaluation criteria. MCDM is a mathematical decision process in which each alternative $A_i \in \mathcal{A}$ is simultaneously evaluated with respect to multiple, potentially conflicting criteria $C_j \in \mathcal{C}$, and the resulting information is aggregated to establish a preference ordering among the alternatives. An MCDM problem can be represented by

$$\mathfrak{M} = \langle \mathcal{A}, \mathcal{C}, X, W, \tau, \mathcal{G} \rangle \quad (1)$$

where X denotes the decision matrix, W represents the criterion-weight vector, τ specifies the preference orientation of the criteria, and $\mathcal{G}$ denotes the aggregation or ranking mechanism. The decision matrix is given by $X = [x_{ij}]_{m \times n}$, where x_{ij} represents the performance of alternative A_i with respect to criterion C_j .

Definition 2. Let each criterion be represented by a mapping

$$C_j: \mathcal{A} \rightarrow \mathbb{R}, j = 1, 2, \dots, n \quad (2)$$

The multi-criteria decision space is the n -dimensional criterion space

$$\mathcal{D} = \mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_n \subseteq \mathbb{R}^n \quad (3)$$

where $\mathcal{X}_j = \{C_j(A_i): A_i \in \mathcal{A}\}$ denotes the attainable performance set associated with criterion C_j . Each alternative A_i is mapped into the decision space through $\Phi: \mathcal{A} \rightarrow \mathcal{D}$, such that

$$\Phi(A_i) = \mathbf{x}_i = (x_{i1}, x_{i2}, \dots, x_{in}) \quad (4)$$

Thus, every alternative is represented by a point $\mathbf{x}_i \in \mathcal{D}$, and the complete decision problem can be viewed as the finite configuration

$$\Phi(\mathcal{A}) = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m\} \subseteq \mathcal{D} \quad (5)$$

Definition 3. Let $W = (w_1, w_2, \dots, w_n)$ denote the relative importance of the n criteria. A criterion-weighting method is a mapping $\mathcal{W}: \mathcal{I} \rightarrow \Delta^{n-1}$, where $\mathcal{I}$ represents the information used for determining criterion importance and

$$\Delta^{n-1} = \{W \in \mathbb{R}_+^n: \sum_{j=1}^n w_j = 1\} \quad (6)$$

is the admissible weight simplex. Hence, $\mathcal{W}(\mathcal{I}) = W = (w_1, w_2, \dots, w_n)$, subject to

$$w_j \geq 0, \sum_{j=1}^n w_j = 1 \quad (7)$$

The value w_j quantifies the relative contribution of criterion C_j to the overall decision process. The criterion-weighting methods may generally be classified as

$$\mathcal{W} = \mathcal{W}_{\text{sub}} \cup \mathcal{W}_{\text{obj}} \cup \mathcal{W}_{\text{hyb}} \quad (8)$$

where $\mathcal{W}_{\text{sub}}$, $\mathcal{W}_{\text{obj}}$, and $\mathcal{W}_{\text{hyb}}$ denote subjective, objective, and hybrid weighting approaches, respectively.

Definition 4. A subjective weighting method determines criterion importance from decision-maker judgments, preferences, or pairwise assessments. Let $\mathcal{J}$ denote the available preference information supplied by one or more decision makers. A subjective weighting operator is defined as

$$\mathcal{W}_{\text{sub}}: \mathcal{J} \rightarrow \Delta^{n-1} \quad (9)$$

such that $W^{(\text{sub})} = \mathcal{W}_{\text{sub}}(\mathcal{J})$. Thus, the resulting criterion weights depend primarily on elicited preference information rather than solely on the numerical structure of the decision matrix.

Definition 5. An objective weighting method determines criterion importance from the intrinsic information contained in the decision matrix without requiring criterion-importance judgments from decision makers. It is represented by

$$\Phi(\mathcal{A}) = \{\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_m\} \subseteq \mathcal{D} \quad (10)$$

such that $W^{(\text{obj})} = \mathcal{W}_{\text{obj}}(X)$. Hence, $X \xrightarrow{\mathcal{W}_{\text{obj}}} W^{(\text{obj})}$. The objective weighting methods generally derive criterion importance from mathematical properties such as dispersion, contrast, information content, variability, or inter-criterion dependence. In the present framework, CRITIC belongs to this class because its weights are derived from criterion contrast and inter-criterion correlation.

Definition 6. A hybrid weighting method combines subjective and objective information to determine criterion importance. Let $W^{(\text{sub})}$ and $W^{(\text{obj})}$ denote subjective and objective weight vectors, respectively. A hybrid weighting operator can be represented generally as

$$\mathcal{W}_{\text{hyb}}: \Delta^{n-1} \times \Delta^{n-1} \rightarrow \Delta^{n-1} \quad (11)$$

such that $W^{(\text{hyb})} = \mathcal{W}_{\text{hyb}}(W^{(\text{sub})}, W^{(\text{obj})})$. For example, a convex combination may be expressed as

$$w_j^{(\text{hyb})} = \lambda w_j^{(\text{sub})} + (1 - \lambda) w_j^{(\text{obj})}, 0 \leq \lambda \leq 1 \quad (12)$$

Thus, hybrid weighting provides a mathematical mechanism for integrating preference-based and data-driven criterion importance.

Definition 7. Let $R = [r_{ij}]_{m \times n}$ denote the normalized decision matrix and $W \in \Delta^{n-1}$ denote the criterion-weight vector. An MCDM ranking method is a mapping $\mathcal{R}: [0,1]^{m \times n} \times \Delta^{n-1} \rightarrow \mathfrak{S}_m$, where $\mathfrak{S}_m$ denotes the set of all possible permutations of the m alternatives. Accordingly,

$$\pi = \mathcal{R}(R, W) = (A_{(1)}, A_{(2)}, \dots, A_{(m)}) \quad (13)$$

defines the resulting preference ordering $A_{(1)} \succcurlyeq A_{(2)} \succcurlyeq \dots \succcurlyeq A_{(m)}$. Thus, a ranking method transforms multidimensional criterion information and criterion importance into an ordered preference structure over the feasible alternatives.

Definition 8. A score-based ranking method assigns an aggregate scalar preference score to every alternative through an aggregation function $\mathcal{G}: [0,1]^n \times \Delta^{n-1} \rightarrow \mathbb{R}$. For alternative A_i , $S_i = \mathcal{G}(\mathbf{r}_i, W)$, where $\mathbf{r}_i = (r_{i1}, r_{i2}, \dots, r_{in})$. If larger scores represent greater preference, the ranking is induced by $S_p > S_q \Rightarrow A_p \succ A_q$. Consequently, $S_{(1)} \geq S_{(2)} \geq \dots \geq S_{(m)}$ generates the ranking $A_{(1)} \succcurlyeq A_{(2)} \succcurlyeq \dots \succcurlyeq A_{(m)}$.

The MEW method used in the present study can be interpreted within this aggregation-based ranking structure.

Definition 9. Let $\mathbf{v}_i = (v_{i1}, v_{i2}, \dots, v_{in})$ denote the weighted performance vector of alternative A_i , and let $\mathbf{z}$ denote a reference profile in the decision space. A distance-based ranking method evaluates an alternative through a metric $d: \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}_+$, such that $d_i = d(\mathbf{v}_i, \mathbf{z})$.

Depending on the adopted MCDM method, $\mathbf{z}$ may represent an ideal, anti-ideal, or other reference solution. Therefore, ranking is induced from the relative geometric positions of alternatives within the weighted decision space. CODAS and TOPSIS employed in the present framework belong to this general distance-based family, although they use different reference structures and preference rules.

Definition 10. Let $\mathcal{W}$ denote a criterion-weighting operator and $\mathcal{R}$ denote an MCDM ranking operator. An integrated weighting–ranking decision framework is defined by the composite mapping $\mathfrak{F} = \mathcal{R} \circ \mathcal{W}$, or, when normalization is explicitly included, $\mathfrak{F} = \mathcal{R} \circ \mathcal{W} \circ \mathcal{N}$. Accordingly, the overall decision process follows

$$X \xrightarrow{\mathcal{N}} R \xrightarrow{\mathcal{W}} W \xrightarrow{\mathcal{R}} \pi \quad (14)$$

where X is the original decision matrix, R is its normalized representation, W contains the criterion weights, and π denotes the final preference ordering.

Definition 11. Let $\mathcal{A} = \{A_1, A_2, \dots, A_m\}$ be a finite set of candidate lightweight encryption algorithms and $\mathcal{C} = \{C_1, C_2, \dots, C_n\}$ be a finite set of evaluation criteria. A resource-aware lightweight cryptographic decision system is defined as the ordered structure $\mathfrak{D} = \langle \mathcal{A}, \mathcal{C}, X, W, \tau \rangle$, where $X = (x_{ij})_{m \times n} \in \mathbb{R}_+^{m \times n}$ is the decision matrix, x_{ij} denotes the performance of algorithm A_i under criterion C_j , $W = (w_1, w_2, \dots, w_n) \in \Delta^{n-1}$ is the criterion-weight vector (see Figure 1):

$$\Delta^{n-1} = \{W \in \mathbb{R}_+^n: \sum_{j=1}^n w_j = 1\} \quad (15)$$

is the admissible weight simplex. The mapping $\tau: \mathcal{C} \rightarrow \{-1, +1\}$ specifies the optimization orientation of each criterion:

$$\tau(C_j) = \begin{cases} +1, & C_j \text{ is benefit-oriented} \\ -1, & C_j \text{ is cost-oriented} \end{cases} \quad (16)$$

For the present problem [19],

$$\mathcal{C} = \{C_{\text{Area}}, C_{\text{Thr}}, C_{\text{Energy}}, C_{\text{Power}}, C_{\text{Latency}}, C_{\text{AlgSize}}, C_{\text{RAM}}, C_{\text{Key}}\} \quad (17)$$

and hence $n = 8$. Each lightweight cipher is therefore characterized by

$$x_i = (\text{Area}_i, \text{Thr}_i, \text{Energy}_i, \text{Power}_i, \text{Latency}_i, \text{AlgSize}_i, \text{RAM}_i, \text{Key}_i) \in \mathbb{R}_+^8 \quad (18)$$

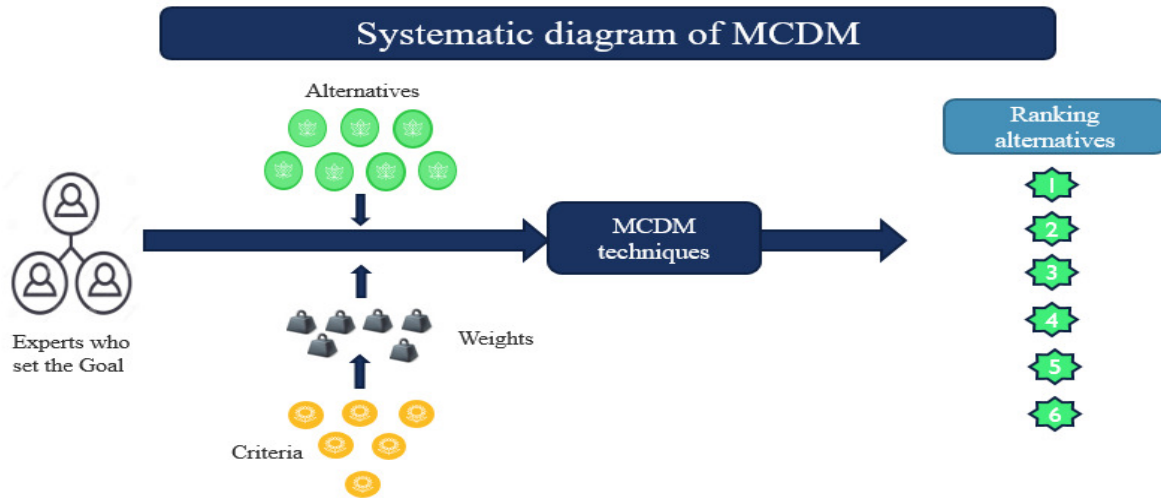


Fig. 1. Systematic diagram of multi-criteria decision making

Definition 12. The criterion space $\mathcal{C}$ is partitioned into the mutually exclusive sets $\mathcal{C} = \mathcal{C}^+ \cup \mathcal{C}^-$, $\mathcal{C}^+ \cap \mathcal{C}^- = \emptyset$, where $\mathcal{C}^+ = \{C_j: \tau(C_j) = +1\}$ denotes the set of benefit criteria and $\mathcal{C}^- = \{C_j: \tau(C_j) = -1\}$ denotes the set of cost criteria. For the considered lightweight cryptographic problem, $C_{\text{Thr}} \in \mathcal{C}^+$, while $\{C_{\text{Area}}, C_{\text{Energy}}, C_{\text{Power}}, C_{\text{Latency}}, C_{\text{AlgSize}}, C_{\text{RAM}}\} \subseteq \mathcal{C}^-$.

Thus, larger throughput is preferred, whereas smaller chip area, energy consumption, power consumption, latency, algorithm size, and RAM requirements are preferred [19].

Definition 13. Let $X = (x_{ij})_{m \times n}$ be the raw cryptographic decision matrix. The preference-oriented normalization operator $\mathcal{N}: \mathbb{R}_+^{m \times n} \rightarrow [0, 1]^{m \times n}$ transforms X into $R = \mathcal{N}(X) = (r_{ij})_{m \times n}$, where for every non-constant criterion,

$$r_{ij} = \begin{cases} \frac{x_{ij} - x_j^{\min}}{x_j^{\max} - x_j^{\min}}, & C_j \in \mathcal{C}^+ \\ \frac{x_j^{\max} - x_{ij}}{x_j^{\max} - x_j^{\min}}, & C_j \in \mathcal{C}^- \end{cases} \quad (19)$$

with $x_j^{\max} = \max_i x_{ij}$ and $x_j^{\min} = \min_i x_{ij}$. Hence, $0 \leq r_{ij} \leq 1$, and $r_{ij} \rightarrow 1$ indicates movement toward a more desirable criterion-level performance.

Definition 14. For criterion C_j , its normalized mean is defined as

$$\bar{r}_j = \frac{1}{m} \sum_{i=1}^m r_{ij} \quad (20)$$

The contrast intensity of C_j is defined by

$$\sigma_j = \sqrt{\frac{1}{m} \sum_{i=1}^m (r_{ij} - \bar{r}_j)^2} \quad (21)$$

The quantity σ_j measures the ability of criterion C_j to discriminate among the candidate lightweight encryption algorithms. In particular, $\sigma_j = 0$ indicates no discriminatory information under criterion C_j .

Definition 15. For two criteria $C_j, C_k \in \mathcal{C}$, their inter-criterion correlation is defined as

$$\rho_{jk} = \frac{\sum_{i=1}^m (r_{ij} - \bar{r}_j)(r_{ik} - \bar{r}_k)}{\sqrt{\sum_{i=1}^m (r_{ij} - \bar{r}_j)^2} \sqrt{\sum_{i=1}^m (r_{ik} - \bar{r}_k)^2}} \quad (22)$$

Since $-1 \leq \rho_{jk} \leq 1$, the associated criterion-conflict measure is defined by $\delta_{jk} = 1 - \rho_{jk}$, such that $0 \leq \delta_{jk} \leq 2$. A smaller δ_{jk} indicates greater informational similarity, whereas a larger δ_{jk} indicates greater non-redundancy between the corresponding implementation criteria.

Definition 16. The CRITIC information measure associated with criterion C_j is defined as

$$\Psi_j = \sigma_j \sum_{k=1}^n (1 - \rho_{jk}) = \underbrace{\sigma_j}_{\text{contrast intensity}} \times \underbrace{\sum_{k=1}^n (1 - \rho_{jk})}_{\text{informational conflict}} \quad (23)$$

The corresponding objective weight is

$$w_j = \frac{\Psi_j}{\sum_{\ell=1}^n \Psi_{\ell}} \quad (24)$$

and therefore $W_{\text{CRITIC}} = (w_1, w_2, \dots, w_n) \in \Delta^{n-1}$. Hence, CRITIC assigns greater importance to criteria that simultaneously exhibit strong discriminatory capability and low informational redundancy.

Definition 17. Let $R = (r_{ij})_{m \times n}$ be the normalized decision matrix and $W = (w_1, \dots, w_n)$ be the CRITIC-derived weight vector. The weighted cryptographic decision matrix is defined as

$$V = R \text{diag}(W) = (v_{ij})_{m \times n} \quad (25)$$

where $v_{ij} = w_j r_{ij}$. The weighted representation of cipher A_i is therefore $v_i = (v_{i1}, v_{i2}, \dots, v_{in})$, and the corresponding weighted decision space is $\mathcal{V} = \{v_1, v_2, \dots, v_m\}$.

Definition 18. For positive normalized values $r_{ij} > 0$, the Multiplicative Exponential Weighting (MEW) preference measure of cipher A_i is defined by

$$S_i = \mathcal{M}(A_i) = \prod_{j=1}^n r_{ij}^{w_j} \quad (26)$$

The MEW preference relation is defined as $A_p \succ_{\text{MEW}} A_q \Leftrightarrow S_p > S_q$. Thus, MEW represents the collective performance of a lightweight cipher through weighted multiplicative aggregation across all considered implementation criteria.

Definition 19. Let $V = (v_{ij})_{m \times n}$ be the weighted preference-oriented decision matrix. The CODAS negative-ideal profile is defined as $\mathbf{v}^- = (v_1^-, v_2^-, \dots, v_n^-)$, where $v_j^- = \min_{1 \leq i \leq m} v_{ij}$. The Euclidean separation of A_i from the negative ideal is

$$E_i = \|\mathbf{v}_i - \mathbf{v}^-\|_2 = \sqrt{\sum_{j=1}^n (v_{ij} - v_j^-)^2} \quad (27)$$

whereas the Taxicab separation is

$$T_i = \| \mathbf{v}_i - \mathbf{v}^- \|_1 = \sum_{j=1}^n |v_{ij} - v_j^-| \quad (28)$$

The pair $\mathcal{D}_i = (E_i, T_i)$ is referred to as the CODAS distance profile of cipher A_i .

Definition 20. For any pair $A_i, A_k \in \mathcal{A}$, the CODAS comparative measure is defined as $h_{ik} = (E_i - E_k) + \psi(E_i - E_k)(T_i - T_k)$, where

$$\psi(x) = \begin{cases} 1, & |x| \geq \theta \\ 0, & |x| < \theta \end{cases} \quad (29)$$

and $\theta > 0$ denotes a prescribed threshold. The overall CODAS assessment score is

$$H_i = \sum_{\substack{k=1 \\ k \neq i}}^m h_{ik} \quad (30)$$

The induced ranking relation is $A_p \succ_{\text{CODAS}} A_q \Leftrightarrow H_p > H_q$.

Definition 21. The positive-ideal cryptographic profile is defined as $\mathbf{v}^+ = (v_1^+, v_2^+, \dots, v_n^+)$, where $v_j^+ = \max_i v_{ij}$, whereas the negative-ideal cryptographic profile is $\mathbf{v}^- = (v_1^-, v_2^-, \dots, v_n^-)$, where $v_j^- = \min_i v_{ij}$. For each cipher A_i , its ideal and anti-ideal distances are respectively defined as

$$D_i^+ = \| \mathbf{v}_i - \mathbf{v}^+ \|_2, \quad D_i^- = \| \mathbf{v}_i - \mathbf{v}^- \|_2 \quad (31)$$

Definition 22. The TOPSIS relative closeness coefficient of cipher A_i is defined as

$$CC_i = \frac{D_i^-}{D_i^+ + D_i^-} \quad (32)$$

where $0 \leq CC_i \leq 1$. The associated preference relation is $A_p \succ_{\text{TOPSIS}} A_q \Leftrightarrow CC_p > CC_q$. Thus, $CC_i \rightarrow 1$ indicates movement toward the ideal implementation profile, whereas $CC_i \rightarrow 0$ indicates movement toward the least desirable implementation profile.

Definition 23. The hybrid CRITIC–MCDM decision operator is defined as the composite mapping

$$\mathfrak{F}: X \xrightarrow{\mathcal{N}} R \xrightarrow{\mathcal{W}_{\text{CRITIC}}} W \xrightarrow{\{\mathcal{M}, \mathcal{C}_{\text{CODAS}}, \mathcal{T}\}} \Pi \quad (33)$$

where $\Pi = \{\pi_{\text{MEW}}, \pi_{\text{CODAS}}, \pi_{\text{TOPSIS}}\}$ is the set of ranking profiles obtained from the three decision mechanisms. Equivalently,

$$\mathfrak{F}(X) = \{\mathcal{M}, \mathcal{C}_{\text{CODAS}}, \mathcal{T}\} \circ \mathcal{W}_{\text{CRITIC}} \circ \mathcal{N}(X) \quad (34)$$

Thus, the overall decision architecture follows $X \rightarrow R \rightarrow \mathcal{W}_{\text{CRITIC}} \rightarrow \{S_i, H_i, CC_i\} \rightarrow \Pi$.

Definition 24. For two candidate ciphers $A_p, A_q \in \mathcal{A}$, A_p is said to weakly dominate A_q , denoted by $A_p \succcurlyeq_c A_q$, if $r_{pj} \geq r_{qj}, \forall j = 1, \dots, n$. The cipher A_p strictly dominates A_q , denoted by $A_p \succ_c A_q$, if $r_{pj} \geq r_{qj} \forall j$ and there exists at least one j^* such that $r_{pj^*} > r_{qj^*}$.

Hence, a dominating cipher is never inferior under any normalized criterion and is strictly superior under at least one criterion.

Definition 25. The lightweight cryptographic criterion space is decomposed as $\mathcal{C} = \mathcal{C}_P \dot{\cup} \mathcal{C}_R \dot{\cup} \mathcal{C}_S$, where $\mathcal{C}_P = \{\mathcal{C}_{\text{Thr}}, \mathcal{C}_{\text{Latency}}\}$ represents operational performance, $\mathcal{C}_R =$

$\{C_{\text{Area}}, C_{\text{Energy}}, C_{\text{Power}}, C_{\text{AlgSize}}, C_{\text{RAM}}\}$ represents implementation-resource consumption, and $C_S = \{C_{\text{Key}}\}$ represents the adopted security-related dimension. Accordingly, each lightweight cipher admits the decomposition $A_i \equiv (P_i, R_i, S_i)$, where P_i , R_i , and S_i denote its performance, resource, and security profiles, respectively.

Definition 26. Let $\mathcal{U}: \mathcal{P} \times \mathcal{R} \times \mathcal{S} \rightarrow \mathbb{R}$ denote an aggregate cryptographic preference functional. A resource-aware lightweight cipher solution is defined as

$$A^* \in \operatorname{argmax}_{A_i \in \mathcal{A}} \mathcal{U}(P_i, -R_i, S_i) \quad (35)$$

Its underlying multi-objective structure is expressed as

$$\operatorname{Max}_{A_i \in \mathcal{A}} P_i, \quad \min_{A_i \in \mathcal{A}} R_i, \quad \text{subject to } \operatorname{Sec}(A_i) \geq s_{\min} \quad (36)$$

where $s_{\min}$ denotes the minimum admissible security requirement.

3.1 Proposed CRITIC-Driven Multi-Method Decision Framework for Lightweight Cipher Selection

This section presents the proposed CRITIC-driven multi-method decision framework (CRITIC-MMDF) for the systematic evaluation and ranking of lightweight encryption algorithms. The framework integrates the objective CRITIC weighting mechanism with three complementary MCDM ranking procedures, namely MEW, CODAS, and TOPSIS. In contrast to treating these methods as separate computational procedures, the proposed formulation establishes a common decision space, a unified criterion orientation, an objective weight vector, and method-specific preference mappings. This is consistent with the original methodology, in which CRITIC determines criterion weights while MEW, CODAS, and TOPSIS perform scoring and ranking. Let $\mathfrak{M} = \langle \mathcal{A}, \mathcal{C}, X_i^j, w_j, \tau^j \rangle$, where $i = 1, \dots, m$ indexes the alternatives and $j = 1, \dots, n$ indexes the criteria. The framework transforms the initial decision tensor X_i^j into method-specific ranking profiles through the following steps.

Step 1. Let $\mathcal{A} = \{A_i\}_{i=1}^m$, $\mathcal{C} = \{C^j\}_{j=1}^n$. Each alternative is embedded into the n -dimensional criterion space through $\Phi: \mathcal{A} \rightarrow \mathcal{D} \subseteq \mathbb{R}^n$, $\Phi(A_i) = x_i^j e_j$, where $x_i^j = C^j(A_i)$. The complete decision information is therefore represented by $X_i^j = [x_i^j]_{m \times n}$, and the feasible decision space is $\mathcal{D}_X = \{x_i^j e_j: i = 1, \dots, m\}$. Thus, X_i^j provides a single common representation of all alternative-criterion evaluations, avoiding reconstruction of the decision matrix for each ranking method. The current draft already establishes this common decision-space formulation.

Step 2. Define the criterion-orientation vector

$$\tau^j = \begin{cases} +1, & C^j \in \mathcal{C}^+ \\ -1, & C^j \in \mathcal{C}^- \end{cases} \quad (37)$$

where $\mathcal{C} = \mathcal{C}^+ \cup \mathcal{C}^-$. For each nonconstant criterion, let $x_{\max}^j = \max_i x_i^j$, and $x_{\min}^j = \min_i x_i^j$. The preference-oriented normalized tensor $R_i^j = \mathcal{N}_\tau(X_i^j)$ is defined as

$$R_i^j = \begin{cases} \frac{x_i^j - x_{\min}^j}{x_{\max}^j - x_{\min}^j}, & \tau^j = +1 \\ \frac{x_{\max}^j - x_i^j}{x_{\max}^j - x_{\min}^j}, & \tau^j = -1 \end{cases} \quad (38)$$

Hence, $0 \leq R_i^j \leq 1$, $R_p^j > R_q^j \Rightarrow A_p \succ_j A_q$. This converts all heterogeneous benefit and cost criteria into a common preference direction.

Step 3. Let the centered normalized tensor be $\tilde{R}_i^j = R_i^j - \bar{R}^j$, and $\bar{R}^j = \frac{1}{m} \sum_{i=1}^m R_i^j$. The criterion contrast and pairwise correlation are respectively

$$\sigma^j = \left[\frac{1}{m-1} \sum_{i=1}^m (\tilde{R}_i^j)^2 \right]^{1/2} \quad (39)$$

and

$$\rho^{jk} = \frac{\sum_{i=1}^m \tilde{R}_i^j \tilde{R}_i^k}{\sqrt{\sum_i (\tilde{R}_i^j)^2} \sqrt{\sum_i (\tilde{R}_i^k)^2}} \quad (40)$$

Defining the conflict tensor $\Delta^{jk} = 1 - \rho^{jk}$, the CRITIC information content becomes

$$\Psi_j = \sigma_j \sum_{k=1}^n \Delta^{jk} = \sigma_j \sum_{k=1}^n (1 - \rho^{jk}) \quad (41)$$

The objective weight covector is then

$$w_j = \frac{\Psi_j}{\sum_{k=1}^n \Psi_k} \quad (42)$$

with $w_j \geq 0$, $\sum_{j=1}^n w_j = 1$. Thus, $\mathcal{W}_C: R_i^j \mapsto w_j$, $\mathbf{w} \in \Delta^{n-1}$. This single step combines the contrast, inter-criterion conflict, and objective-weight calculations that were previously distributed over three separate steps.

Step 4. Let $W_j^k = w_j \delta_j^k$ be the diagonal criterion-weight tensor, where δ_j^k is the Kronecker delta. The weighted normalized decision tensor is obtained by contraction

$$V_i^k = R_i^j W_j^k \quad (43)$$

and therefore $V_i^j = w_j R_i^j$. Each alternative is consequently represented by $v_i = V_i^j e_j$, giving the common weighted decision space $\mathcal{V} = \{v_i\}_{i=1}^m$. The same R_i^j , w_j , and V_i^j are subsequently reused; they need not be reconstructed separately for MEW, CODAS, and TOPSIS.

Step 5. For $R_i^j > 0$, define the MEW preference functional as

$$S_i^{(M)} = \prod_{j=1}^n (R_i^j)^{w_j} \quad (44)$$

The induced preference relation is

$$A_p \succ_M A_q \Leftrightarrow S_p^{(M)} > S_q^{(M)} \quad (45)$$

and therefore $\pi_i^{(M)} = \text{Rank}_{\downarrow} S_i^{(M)}$. Thus, MEW generates the multiplicative ranking profile directly from the CRITIC-weighted preference structure.

Step 6. Let the negative-ideal vector be $v_{-}^j = \min_i V_i^j$, and define the displacement $D_i^j = V_i^j - v_{-}^j$. The Euclidean and Taxicab separations are

$$E_i = (\delta_{jk} D_i^j D_i^k)^{1/2}, T_i = \sum_{j=1}^n |D_i^j| \quad (46)$$

For $A_i, A_k \in \mathcal{A}$, define $h_{ik} = (E_i - E_k) + \psi_\theta(E_i - E_k)(T_i - T_k)$, where

$$\psi_\theta(x) = \begin{cases} 1, & |x| \geq \theta \\ 0, & |x| < \theta \end{cases} \quad (47)$$

The CODAS score and ranking are then obtained simultaneously as

$$H_i = \sum_{\substack{k=1 \\ k \neq i}}^m h_{ik}, \pi_i^{(C)} = \text{Rank}_\downarrow H_i \quad (48)$$

Thus, the negative-ideal construction, two distance measures, pairwise comparison, and final ranking are contained in a single CODAS transformation rather than separate methodological steps.

Step 7. Define the positive and negative ideal vectors of the common weighted space by

$$v_+^j = \max_i V_i^j, v_-^j = \min_i V_i^j \quad (49)$$

The corresponding Euclidean distances are

$$d_i^\pm = [\delta_{jk} (V_i^j - v_\pm^j)(V_i^k - v_\pm^k)]^{1/2} \quad (50)$$

The TOPSIS relative-closeness coefficient is

$$c_i = \frac{d_i^-}{d_i^+ + d_i^-}, 0 \leq c_i \leq 1 \quad (51)$$

which generates $\pi_i^{(T)} = \text{Rank}_\downarrow c_i$. Introducing the method index $\mu \in \{M, C, T\}$, the complete multi-method ranking profile is compactly represented by

$$\Pi_i^\mu = [\pi_i^{(M)}, \pi_i^{(C)}, \pi_i^{(T)}] \quad (52)$$

Accordingly, the proposed CRITIC–MMDF operator is $\mathfrak{F}_{\text{CRITIC-MMDF}}: X_i^j \mapsto \Pi_i^\mu$, with the compact computational chain

$$X_i^j \xrightarrow{\mathcal{N}_\tau} R_i^j \xrightarrow{\mathcal{W}_C} w_j \xrightarrow{w_j^k = w_j \delta_j^k} V_i^k \xrightarrow{\{\mathcal{R}_M, \mathcal{R}_C, \mathcal{R}_T\}} \Pi_i^\mu \quad (53)$$

4. Numerical Case Study: Evaluation of Lightweight Encryption Algorithms

To demonstrate the applicability of the proposed CRITIC-Driven Multi-Method Decision Framework (CRITIC–MMDF), a numerical case study is conducted for the comparative evaluation of ten lightweight encryption algorithms under eight implementation-related criteria. The candidate algorithms are PRESENT, SEA, HIGHT, LEA, AES, mCrypton, NOEKEON, KLEIN, CAMELLIA, and TEA. The numerical analysis follows the mathematical structure established in Section 3, beginning with the construction of the decision space, followed by objective CRITIC weighting and comparative evaluation using MEW, CODAS, and TOPSIS.

4.1 Construction of the Lightweight-Cipher Decision Space

Following Step 1 of the proposed framework, let $\mathcal{A} = \{A_i\}_{i=1}^{10}$ denote the set of candidate lightweight encryption algorithms, where

$$\left\{ \begin{array}{l} A_1 = \text{PRESENT}, \\ A_2 = \text{SEA}, \\ A_3 = \text{HIGHT}, \\ A_4 = \text{LEA}, \\ A_5 = \text{AES}, \\ A_6 = \text{mCrypton}, \\ A_7 = \text{NOEKEON}, \\ A_8 = \text{KLEIN}, \\ A_9 = \text{CAMELLIA}, \\ A_{10} = \text{TEA} \end{array} \right. \quad (54)$$

The criterion set is defined as

$$\mathcal{C} = \{C^j\}_{j=1}^8 = \{C_{\text{Area}}^1, C_{\text{Thr}}^2, C_{\text{Energy}}^3, C_{\text{Power}}^4, C_{\text{Latency}}^5, C_{\text{AlgSize}}^6, C_{\text{RAM}}^7, C_{\text{Key}}^8\} \quad (55)$$

Accordingly, $m = 10$, $n = 8$, and the performance of A_i under criterion C^j is denoted by $x_i^j = C^j(A_i)$. The resulting decision tensor $X_i^j \in \mathbb{R}_+^{10 \times 8}$ is constructed from the implementation data reported in the case study (see Table 1 and Figure 2).

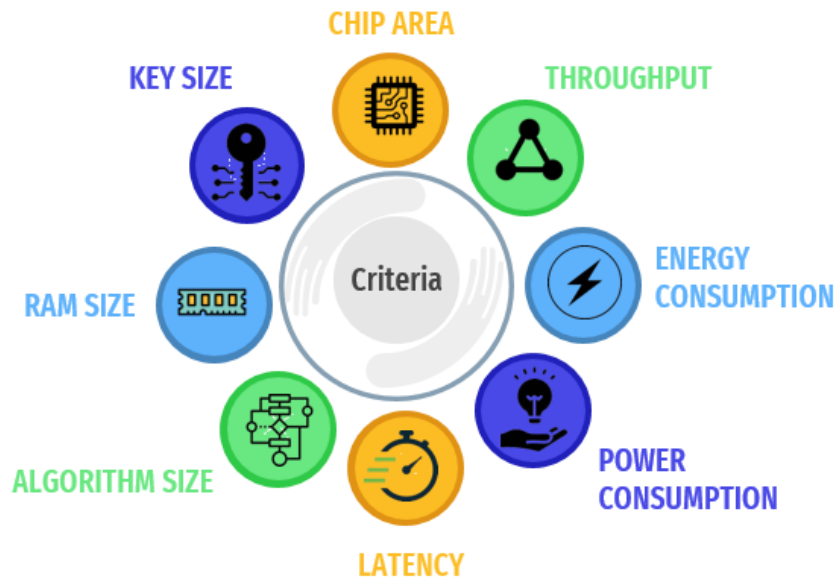


Fig. 2. Criteria for evaluating the alternatives

Thus, the case study is represented by the finite decision configuration

$$\mathcal{D}_X = \{x_i^j \mathbf{e}_j : i = 1, \dots, 10\} \subseteq \mathbb{R}^8 \quad (56)$$

Table 1

Initial decision matrix of the lightweight encryption algorithms [19]

Alternative	Cipher	Area	Throughput	Energy	Power	Latency	Algorithm. size	RAM	Key size
A_1	PRESENT	1075	11.70	1.61	137.81	547	1000	18	80
A_2	SEA	2569	3.29	3.85	1170.50	243	426	24	96
A_3	HIGHT	3048	188.00	5.48	29.14	34	402	32	128
A_4	LEA	3826	76.19	3.82	50.22	168	590	32	128
A_5	AES	2400	56.64	2.40	42.38	226	1659	33	128
A_6	mCrypton	2760	33.51	4.14	122.90	190	3108	24	128
A_7	NOEKEON	2862	3.44	4.30	1247.65	3720	364	32	128
A_8	KLEIN	1478	23.62	2.21	93.87	271	1268	18	80
A_9	CAMELLIA	6511	290.10	9.76	33.57	44	1262	12	128
A_{10}	TEA	2355	100.00	3.53	35.32	64	1354	13	128

4.1.1 Criterion orientation and normalized decision space

Following Step 2, the criteria are partitioned according to their preference directions. In the adopted case study, throughput and key size are treated as benefit criteria, whereas chip area, energy consumption, power consumption, latency, algorithm size, and RAM size are treated as cost criteria. Hence

$$C^+ = \{C^2, C^8\}, C^- = \{C^1, C^3, C^4, C^5, C^6, C^7\} \quad (57)$$

with the orientation vector $\tau^j = (-1, +1, -1, -1, -1, -1, -1, +1)$. The criterion-wise limiting values are $x_{\min}^j = (1075, 3.29, 1.61, 29.14, 34, 364, 12, 80)$ and $x_{\max}^j = (6511, 290.10, 9.76, 1247.65, 3720, 3108, 33, 128)$. Applying the normalization procedure gives a dimensionless decision representation R_i^j . The normalized values reported in the case study are presented in Table 2.

Table 2

Preference-oriented normalized decision matrix

A_i	C^1	C^2	C^3	C^4	C^5	C^6	C^7	C^8
A_1	1.0000	0.0293	1.0000	0.9108	0.8608	0.7682	0.7143	0.0000
A_2	0.7252	0.0000	0.7252	0.0633	0.9433	0.9774	0.4286	0.3333
A_3	0.6370	0.6440	0.5252	1.0000	1.0000	0.9862	0.0476	1.0000
A_4	0.4939	0.2542	0.7288	0.9827	0.9636	0.9176	0.0476	1.0000
A_5	0.7563	0.1860	0.9031	0.9891	0.9479	0.5281	0.0000	1.0000
A_6	0.6900	0.1054	0.6896	0.9231	0.9577	0.0000	0.4286	1.0000
A_7	0.6713	0.0005	0.6699	0.0000	0.0000	1.0000	0.0476	1.0000
A_8	0.9259	0.0709	0.9264	0.9469	0.9357	0.6706	0.7143	0.0000
A_9	0.0000	1.0000	0.0000	0.9964	0.9973	0.6727	1.0000	1.0000
A_{10}	0.7645	0.3372	0.7644	0.9949	0.9919	0.6392	0.9524	1.0000

4.2 CRITIC-based Objective Criterion Weights

Following Step 3, the transformation places the heterogeneous implementation measures on a common dimensionless scale while retaining the adopted preference orientation. The information carried by each criterion is quantified through its contrast intensity and inter-criterion conflict. The dispersion vector obtained from R_i^j is

$$\sigma^j = (0.259817, 0.308914, 0.266313, 0.375991, 0.289157, 0.286909, 0.371795, 0.416333) \quad (58)$$

The correlation tensor ρ^{jk} is subsequently transformed into the conflict tensor $\Delta^{jk} = 1 - \rho^{jk}$, from which the cumulative conflict measure is obtained as

$$\Gamma^j = \sum_{k=1}^8 \Delta^{jk} \\ = (7.820004, 7.017938, 7.823161, 6.035588, 6.173542, 8.223195, 7.080603, 8.121837) \quad (59)$$

The complete correlation and conflict calculations are reported in the source case study. The CRITIC information vector, $\Psi_j = \sigma_j \Gamma_j$, is obtained as

$$\Psi_j = (2.031767, 2.167937, 2.083410, 2.269325, 1.785122, 2.359306, 2.632531, 3.381391) \quad (60)$$

Therefore, $w_j = \frac{\Psi_j}{\sum_{k=1}^8 \Psi_k}$, gives

$$w_j = (0.108588, 0.115866, 0.111348, 0.121284, 0.095406, 0.126093, 0.140696, 0.180719) \quad (61)$$

with $\sum_{j=1}^8 w_j = 1$. These are the CRITIC weights reported for the eight criteria given in Table 3.

Table 3
CRITIC information measures and objective weights

Criterion	σ_j	Γ_j	Ψ_j	w_j
C^1 Area	0.259817	7.820004	2.031767	0.108588
C^2 Throughput	0.308914	7.017938	2.167937	0.115866
C^3 Energy	0.266313	7.823161	2.083410	0.111348
C^4 Power	0.375991	6.035588	2.269325	0.121284
C^5 Latency	0.289157	6.173542	1.785122	0.095406
C^6 Algorithm size	0.286909	8.223195	2.359306	0.126093
C^7 RAM	0.371795	7.080603	2.632531	0.140696
C^8 Key size	0.416333	8.121837	3.381391	0.180719

Among the considered dimensions, C^8 receives the largest objective weight, followed by C^7 and C^6 , whereas C^5 receives the smallest weight. This ordering reflects the combined dispersion and non-redundancy contained in the case-study data rather than an externally assigned subjective importance.

4.2.1 Weighted multi-criteria decision space

Following Step 4, the CRITIC weights are embedded into the normalized decision representation through $W_j^k = w_j \delta_j^k$, yielding $V_i^k = R_i^j W_j^k$. Since W_j^k is diagonal, $V_i^j = w_j R_i^j$. Hence, each candidate cipher is represented by the weighted criterion vector $\mathbf{v}_i = V_i^j \mathbf{e}_j$, and the complete weighted decision space becomes $\mathcal{V} = \{\mathbf{v}_1, \dots, \mathbf{v}_{10}\}$. This representation provides the weighted information required by the subsequent distance-based ranking operations without reconstructing the original decision matrix.

4.3 MEW-based Multiplicative Evaluation

The MEW analysis evaluates each alternative through the weighted multiplicative aggregation defined in Section 3. The numerical implementation reported in the case study produces the score vector:

$$S_i^{(M)} = \begin{pmatrix} 0.334569 \\ 0.219682 \\ 0.637415 \\ 0.446505 \\ 0.414506 \\ 0.312142 \\ 0.170138 \\ 0.367982 \\ 0.551687 \\ 0.573180 \end{pmatrix} \quad (62)$$

The resulting ranking is $A_3 > A_{10} > A_9 > A_4 > A_5 > A_8 > A_1 > A_6 > A_2 > A_7$. Thus, $\pi^{(M)} = (3,10,9,4,5,8,1,6,2,7)$. Within the adopted data and criterion-weight structure, HIGHT (A_3) obtains the highest reported MEW score $S_3^{(M)} = 0.637415$, followed by TEA (A_{10}) and CAMELLIA (A_9).

4.4 CODAS-Based Negative-Ideal Evaluation

Following Step 6, CODAS evaluates the alternatives relative to the negative-ideal profile. The reported negative-ideal vector is

$$v_-^j = (0.017928, 0.001314, 0.018368, 0.002833, 0.000872, 0.014768, 0.051162, 0.112949) \quad (63)$$

The corresponding Euclidean and Taxicab distance vectors are

$$E_i = \begin{pmatrix} 0.142157 \\ 0.105972 \\ 0.208584 \\ 0.123657 \\ 0.126494 \\ 0.085185 \\ 0.134369 \\ 0.106504 \\ 0.204940 \\ 0.163196 \end{pmatrix} \quad (64)$$

$$T_i = \begin{pmatrix} 0.288635 \\ 0.203119 \\ 0.490248 \\ 0.288632 \\ 0.283056 \\ 0.190450 \\ 0.226935 \\ 0.241901 \\ 0.468754 \\ 0.415336 \end{pmatrix} \quad (65)$$

By the application of the CODAS pairwise assessment operator gives

$$H_i = \begin{pmatrix} 0.021277 \\ -0.339837 \\ 0.688032 \\ -0.163643 \\ -0.135267 \\ -0.547128 \\ -0.056497 \\ -0.334787 \\ 0.651175 \\ 0.232164 \end{pmatrix} \quad (66)$$

The resulting ordering is $A_3 \succ A_9 \succ A_{10} \succ A_1 \succ A_7 \succ A_5 \succ A_4 \succ A_8 \succ A_2 \succ A_6$. Thus, $\pi^{(C)} = (3,9,10,1,7,5,4,8,2,6)$. The lightweight cipher, namely HIGHT (A_3) again occupies the first position, followed by CAMELLIA (A_9) and TEA (A_{10}) under the reported CODAS assessment.

4.5 TOPSIS-based Bi-Ideal Evaluation

The TOPSIS analysis characterizes each alternative through its relative position with respect to the positive and negative ideal profiles. The separation measures d_i^+ and d_i^- yield the relative-closeness coefficient $c_i = \frac{d_i^-}{d_i^+ + d_i^-}$. The reported numerical values are summarized below in Table 4.

Table 4

TOPSIS separation measures, closeness coefficients, and rankings

A_i	d_i^+	d_i^-	c_i	Rank
A_1	0.092930	0.154981	0.625147	6
A_2	0.124808	0.133057	0.515994	9
A_3	0.059698	0.167948	0.737758	1
A_4	0.082692	0.155577	0.652947	4
A_5	0.090822	0.149966	0.622814	7
A_6	0.117109	0.135802	0.536955	8
A_7	0.160717	0.099980	0.383510	10
A_8	0.090697	0.154286	0.629783	5
A_9	0.088590	0.168673	0.655644	3
A_{10}	0.068320	0.158614	0.698943	2

Consequently, $A_3 \succ A_{10} \succ A_9 \succ A_4 \succ A_8 \succ A_1 \succ A_5 \succ A_6 \succ A_2 \succ A_7$, giving $\pi^{(T)} = (3,10,9,4,8,1,5,6,2,7)$. The reported TOPSIS results therefore assign the highest relative-closeness value to HIGHT, followed by TEA and CAMELLIA.

4.6 Comparative Multi-Method Ranking Analysis

To examine the consistency of the three ranking mechanisms, let $\mu \in \{M, C, T\}$ represent MEW, CODAS, and TOPSIS, respectively. The resulting ranking information is assembled into $\Pi_i^\mu = [\pi_i^{(M)}, \pi_i^{(C)}, \pi_i^{(T)}]$. The comparative ranking matrix is therefore

$$\Pi_i^\mu = \begin{bmatrix} 7 & 4 & 6 \\ 9 & 9 & 9 \\ 1 & 1 & 1 \\ 4 & 7 & 4 \\ 5 & 6 & 7 \\ 8 & 10 & 8 \\ 10 & 5 & 10 \\ 6 & 8 & 5 \\ 3 & 2 & 3 \\ 2 & 3 & 2 \end{bmatrix} \quad (67)$$

where the columns correspond respectively to MEW, CODAS, and TOPSIS (see Table 5).

Table 5
Comparative ranking profile of the evaluated
lightweight ciphers

Alternative	Cipher	MEW	CODAS	TOPSIS
A_1	PRESENT	7	4	6
A_2	SEA	9	9	9
A_3	HIGHT	1	1	1
A_4	LEA	4	7	4
A_5	AES	5	6	7
A_6	mCrypton	8	10	8
A_7	NOEKEON	10	5	10
A_8	KLEIN	6	8	5
A_9	CAMELLIA	3	2	3
A_{10}	TEA	2	3	2

A notable feature of the resulting profile is the agreement of all three ranking procedures for A_3 :

$$\pi_3^{(M)} = \pi_3^{(C)} = \pi_3^{(T)} = 1 \quad (68)$$

Thus, for the specific dataset, criterion orientations, and CRITIC-derived weights considered in this case study, HIGHT occupies the first position under all three MCDM procedures. MEW and TOPSIS additionally agree on the first four positions; i.e., $A_3 \succ A_{10} \succ A_9 \succ A_4$, whereas CODAS produces $A_3 \succ A_9 \succ A_{10} \succ A_1$.

The differences observed at the intermediate and lower positions arise from the distinct preference structures of the three ranking operators: MEW employs multiplicative aggregation, CODAS emphasizes separation from the negative-ideal profile, and TOPSIS evaluates simultaneous proximity to the positive ideal and separation from the negative ideal. Consequently, the agreement at the leading position indicates ranking consistency across the three reported procedures, while the variation among the remaining alternatives illustrates the sensitivity of comparative ordering to the adopted MCDM mechanism.

5. Robustness, Consistency, and Stability Analysis

To evaluate the reliability of the CRITIC–MMDF beyond the baseline rankings, three complementary validation mechanisms are considered: cross-method consistency, criterion-weight sensitivity, and input-level rank stability. These analyses address different aspects of robustness. The first examines whether MEW, CODAS, and TOPSIS generate compatible preference structures; the second quantifies the effect of controlled changes in CRITIC-derived weights; and the third

investigates whether uncertainty in the original decision information propagates into substantial rank variation. Together, they provide a unified assessment of the numerical stability of the proposed framework.

5.1 Cross-Method Consistency Analysis

The agreement among MEW, CODAS, and TOPSIS is quantified using their alternative-wise rank vectors, $\mathbf{r}^{(M)} = (7, 9, 1, 4, 5, 8, 10, 6, 3, 2)$, $\mathbf{r}^{(C)} = (4, 9, 1, 7, 6, 10, 5, 8, 2, 3)$, and $\mathbf{r}^{(T)} = (6, 9, 1, 4, 7, 8, 10, 5, 3, 2)$. For two ranking procedures p and q , Spearman's rank correlation is defined as

$$\rho_{pq} = 1 - \frac{6 \sum_{i=1}^{10} (r_i^{(p)} - r_i^{(q)})^2}{10(10^2 - 1)} \quad (69)$$

whereas Kendall's coefficient is

$$\tau_{pq} = \frac{N_c - N_d}{\binom{10}{2}} = \frac{N_c - N_d}{45} \quad (70)$$

with N_c and N_d denoting concordant and discordant alternative pairs, respectively. To complement these association measures, the mean absolute rank difference is given by

$$D_{pq} = \frac{1}{10} \sum_{i=1}^{10} |r_i^{(p)} - r_i^{(q)}| \quad (71)$$

The resulting consistency statistics are reported in Table 6.

Table 6

Pairwise consistency among MEW, CODAS, and TOPSIS

Comparison	Spearman ρ	Kendall τ	Mean absolute rank difference
MEW–CODAS	0.6727	0.5111	1.8000
MEW–TOPSIS	0.9636	0.9111	0.4000
CODAS–TOPSIS	0.6727	0.5111	1.8000

The strongest correspondence is observed between MEW and TOPSIS, for which $\rho_{M,T} = 0.9636$, $\tau_{M,T} = 0.9111$. CODAS exhibits a comparatively different ordering of several intermediate alternatives, which explains its lower pairwise coefficients with the other two procedures. To assess collective agreement among all three methods, Kendall's coefficient of concordance is employed:

$$W = \frac{12 \sum_{i=1}^{10} (R_i - \bar{R})^2}{K^2(m^3 - m)} \quad (72)$$

where $K = 3$, $m = 10$, and $R_i = r_i^{(M)} + r_i^{(C)} + r_i^{(T)} = (17, 27, 3, 15, 18, 26, 25, 19, 8, 7)$. Since $\bar{R} = \frac{K(m+1)}{2} = 16.5$, the resulting concordance coefficient is $W = 0.8465$. Thus, the three decision mechanisms exhibit substantial collective agreement while preserving methodological diversity. Most importantly, $r_3^{(M)} = r_3^{(C)} = r_3^{(T)} = 1$, showing complete agreement regarding the leading alternative under the baseline configuration.

5.2 Sensitivity to Criterion-Weight Perturbation

The dependence of the rankings on the exact CRITIC weight configuration is investigated through a deterministic one-factor-at-a-time perturbation scheme. Let the baseline weight vector be $\mathbf{w} = (w_1, \dots, w_8)$. For criterion C^j , its weight is modified by a relative perturbation ε , followed by renormalization

$$\tilde{w}_k^{(j,\varepsilon)} = \frac{w_k(1+\varepsilon\delta_k^j)}{\sum_{\ell=1}^8 w_\ell(1+\varepsilon\delta_\ell^j)} \quad (73)$$

where $\varepsilon \in \{-0.20, -0.10, +0.10, +0.20\}$. For a fixed perturbation magnitude, eight criteria are examined in two directions, giving $8 \times 2 = 16$ configurations. Consequently, the $\pm 10\%$ and $\pm 20\%$ levels together generate 32 perturbed weight scenarios per MCDM procedure. The perturbed ranking $\mathbf{r}^{\mu(s)}$ is compared with its baseline counterpart $\mathbf{r}^{\mu(0)}$ using Spearman's coefficient, Kendall's coefficient, and mean absolute rank divergence

$$D_{\mu,s} = \frac{1}{10} \sum_{i=1}^{10} |r_i^{\mu(0)} - r_i^{\mu(s)}| \quad (74)$$

where $\mu \in \{M, C, T\}$. The numerical results are summarized in Table 7. MEW remains completely unchanged under all examined modifications, $\bar{\rho}_M = \bar{\tau}_M = 1, \bar{D}_M = 0$. TOPSIS retains the baseline first-ranked alternative in every perturbation scenario, although some movement occurs among the remaining alternatives as the perturbation amplitude increases. CODAS is more responsive to relative changes in criterion importance. Its first-ranked alternative is preserved in $13/16 = 81.25\%$ of the scenarios at each perturbation magnitude. The rank changes are associated primarily with increased emphasis on throughput or RAM and reduced emphasis on algorithm size.

Table 7
Sensitivity of the rankings to CRITIC-weight perturbation

Perturbation	Method	$\bar{\rho}$	$\rho_{\min}$	$\bar{\tau}$	$\tau_{\min}$	$\bar{D}$	$D_{\max}$	First-rank retention
$\pm 10\%$	MEW	1.0000	1.0000	1.0000	1.0000	0.0000	0.0000	100.00%
$\pm 10\%$	CODAS	0.9917	0.9636	0.9694	0.8667	0.1375	0.6000	81.25%
$\pm 10\%$	TOPSIS	0.9939	0.9758	0.9778	0.9111	0.1000	0.4000	100.00%
$\pm 20\%$	MEW	1.0000	1.0000	1.0000	1.0000	0.0000	0.0000	100.00%
$\pm 20\%$	CODAS	0.9864	0.9515	0.9528	0.8667	0.2125	0.6000	81.25%
$\pm 20\%$	TOPSIS	0.9780	0.8788	0.9444	0.8222	0.2500	0.8000	100.00%

By aggregating the first-position retention across all procedures and all 32 perturbation scenarios gives $\mathcal{R}_{\text{overall}} = \frac{32+26+32}{96} = 0.9375$. Hence, the baseline leading solution is retained in 93.75% of all method-perturbation combinations.

5.3 Rank Stability Under Input Perturbations

Criterion-weight sensitivity does not capture uncertainty in the original performance measurements. A separate stochastic experiment is therefore conducted by applying bounded perturbations directly to the elements of the original decision array. Let $X = [x_i^j]_{10 \times 8}$ denote the baseline decision matrix. For perturbation radius η_ℓ and realization b ,

$$x_i^{j(\ell,b)} = x_i^j (1 + \delta_i^{j(\ell,b)}) \quad (75)$$

where $\delta_i^{j(\ell,b)} \sim \mathcal{U}(-\eta_\ell, \eta_\ell)$ and $\eta_\ell \in \{0.01, 0.03, 0.05\}$. Each perturbed matrix is propagated through the entire decision architecture. Thus, the CRITIC weights are recalculated, and the three MCDM methods are subsequently executed using their corresponding normalization and aggregation mechanisms. This propagation can be written as

$$X^{(\ell,b)} \rightarrow W^{(\ell,b)} \rightarrow \{r^{M(\ell,b)}, r^{C(\ell,b)}, r^{T(\ell,b)}\} \quad (76)$$

As presented in Table 8, increasing the perturbation radius produces a gradual reduction in rank correlation and a corresponding increase in rank divergence, while the leading alternative remains highly stable across the examined scenarios.

Table 8
Rank stability under bounded perturbations of the decision information

η_ℓ	Method	$\bar{\rho}$	$\rho_{\min}$	$\bar{\tau}$	$\tau_{\min}$	$\bar{D}$	$D_{\max}$	HIGHT retained at rank 1
0.01	MEW	1.000000	1.000000	1.000000	1.000000	0.000000	0.000000	100.00%
0.01	CODAS	0.996615	0.975758	0.987587	0.911111	0.055860	0.400000	100.00%
0.01	TOPSIS	0.999653	0.987879	0.998729	0.955556	0.005720	0.200000	100.00%
0.03	MEW	1.000000	1.000000	1.000000	1.000000	0.000000	0.000000	100.00%
0.03	CODAS	0.992783	0.963636	0.973538	0.866667	0.119080	0.600000	94.47%
0.03	TOPSIS	0.995684	0.975758	0.984173	0.911111	0.071220	0.400000	100.00%
0.05	MEW	0.999982	0.987879	0.999933	0.955556	0.000300	0.200000	100.00%
0.05	CODAS	0.989561	0.939394	0.961853	0.822222	0.171640	0.600000	84.87%
0.05	TOPSIS	0.991945	0.939394	0.971404	0.822222	0.128540	0.600000	100.00%

At the 1% perturbation level, the leading solution is retained in every realization of all three procedures. Increasing the perturbation radius to 3% affects primarily CODAS, for which HIGHT remains first in 94.47% of simulations. At the 5% level, its CODAS retention decreases to 84.87%, with CAMELLIA occupying the leading position in the remaining realizations. MEW and TOPSIS preserve HIGHT throughout all three perturbation regimes. To summarize the collective response, the method-specific means are aggregated as

$$\bar{\rho}^{(\ell)} = \frac{\bar{\rho}_M^{(\ell)} + \bar{\rho}_C^{(\ell)} + \bar{\rho}_T^{(\ell)}}{3}, \quad \bar{\tau}^{(\ell)} = \frac{\bar{\tau}_M^{(\ell)} + \bar{\tau}_C^{(\ell)} + \bar{\tau}_T^{(\ell)}}{3}, \quad \bar{D}^{(\ell)} = \frac{\bar{D}_M^{(\ell)} + \bar{D}_C^{(\ell)} + \bar{D}_T^{(\ell)}}{3} \quad (77)$$

The resulting global stability profile is

$$\begin{cases} \eta_\ell & \bar{\rho}^{(\ell)} & \bar{\tau}^{(\ell)} & \bar{D}^{(\ell)} \\ 0.01 & 0.9988 & 0.9954 & 0.0205 \\ 0.03 & 0.9962 & 0.9859 & 0.0634 \\ 0.05 & 0.9938 & 0.9777 & 0.1002 \end{cases} \quad (78)$$

and therefore

$$\eta_\ell \uparrow \Rightarrow \bar{\rho}^{(\ell)} \downarrow, \quad \bar{\tau}^{(\ell)} \downarrow, \quad \bar{D}^{(\ell)} \uparrow \quad (79)$$

The gradual reduction in correlation together with increasing rank divergence confirms that larger input uncertainty induces greater local rearrangement. However, the cross-method means Spearman

coefficient remains above 0.99 throughout the investigated range. The robustness analysis therefore indicates that the principal selection outcome is comparatively stable, while also revealing that CODAS is more responsive than MEW and TOPSIS to both criterion-weight changes and uncertainty in the underlying implementation measurements.

5.4 Alternative Weighting Mechanisms and Multi-Method Ranking Analysis

To examine the sensitivity of the preference structure to criterion importance, the baseline CRITIC weights were compared with four alternative schemes: Entropy, Equal Weighting (EW), Standard Deviation (SD), and Coefficient of Variation (CV). Each weight vector was integrated separately with MEW, CODAS, and TOPSIS, yielding $5 \times 3 = 15$ weighting–ranking configurations. This design enables the effects associated with criterion weighting to be examined separately from those arising from the choice of MCDM procedure. The data-dependent weights were derived from the preference-oriented normalized decision information, while MEW, CODAS, and TOPSIS retained their respective normalization procedures in the subsequent ranking stage.

5.4.1 Alternative criterion-weighting structures

Let R_i^j denote the preference-oriented normalized performance of alternative A_i with respect to criterion C^j . Under EW, all eight criteria receive identical importance

$$w_j^{(EW)} = \frac{1}{8}, j = 1, \dots, 8 \quad (80)$$

The SD scheme determines criterion importance according to the dispersion of normalized observations:

$$w_j^{(SD)} = \frac{\sigma_j}{\sum_{k=1}^8 \sigma_k} \quad (81)$$

For Entropy weighting, the proportional information associated with criterion C^j is first defined as

$$p_i^j = \frac{R_i^j}{\sum_{i=1}^{10} R_i^j} \quad (82)$$

from which $e_j = -\frac{1}{\ln 10} \sum_{i=1}^{10} p_i^j \ln p_i^j$, and

$$w_j^{(E)} = \frac{1 - e_j}{\sum_{k=1}^8 (1 - e_k)} \quad (83)$$

The CV scheme combines relative dispersion with the mean normalized performance,

$$CV_j = \frac{\sigma_j}{\bar{R}^j}, w_j^{(CV)} = \frac{CV_j}{\sum_{k=1}^8 CV_k} \quad (84)$$

For comparison, the CRITIC coefficient incorporates both criterion dispersion and inter-criterion conflict:

$$w_j^{(C)} = \frac{\sigma_j \sum_{k=1}^8 (1 - \rho^{jk})}{\sum_{\ell=1}^8 \sigma_\ell \sum_{k=1}^8 (1 - \rho^{\ell k})} \quad (85)$$

The resulting weight vectors are summarized in Table 9.

Table 9

Criterion weights generated by alternative weighting mechanisms

Weighting mechanism	C^1	C^2	C^3	C^4	C^5	C^6	C^7	C^8
Entropy	0.061596	0.316177	0.060688	0.096325	0.052906	0.063731	0.219026	0.129551
Equal	0.125000	0.125000	0.125000	0.125000	0.125000	0.125000	0.125000	0.125000
SD	0.100891	0.119956	0.103413	0.146003	0.112284	0.111411	0.144374	0.161669
CRITIC	0.108588	0.115866	0.111348	0.121284	0.095406	0.126093	0.140696	0.180719
CV	0.085038	0.256439	0.083789	0.105044	0.073352	0.087401	0.185107	0.123830

Table 9 reveals appreciable differences in the distribution of criterion importance. Entropy and CV assign their largest coefficients to throughput C^2 , with weights of 0.316177 and 0.256439, respectively. In contrast, CRITIC gives its highest importance to C^8 , while SD distributes importance more evenly across the eight criteria. EW provides a neutral reference configuration in which criterion-specific priority is absent. These differences establish distinct weighting environments for evaluating the sensitivity of the resulting preference orders.

5.4.2 Effect of weighting structure on the MCDM rankings

The five weight vectors were independently propagated through MEW, CODAS, and TOPSIS. The resulting preference orders are reported in Table 10.

Table 10

Ranking comparison under alternative weighting mechanisms and MCDM methods

Weighting mechanism	MCDM method	Ranking order
Entropy	MEW	$A_9 > A_3 > A_{10} > A_4 > A_5 > A_8 > A_6 > A_1 > A_2 > A_7$
Entropy	CODAS	$A_9 > A_3 > A_{10} > A_4 > A_5 > A_1 > A_8 > A_7 > A_6 > A_2$
Entropy	TOPSIS	$A_9 > A_3 > A_{10} > A_4 > A_5 > A_8 > A_1 > A_6 > A_2 > A_7$
Equal	MEW	$A_3 > A_{10} > A_9 > A_4 > A_5 > A_8 > A_1 > A_6 > A_2 > A_7$
Equal	CODAS	$A_3 > A_9 > A_{10} > A_1 > A_7 > A_5 > A_4 > A_8 > A_2 > A_6$
Equal	TOPSIS	$A_3 > A_{10} > A_4 > A_9 > A_8 > A_5 > A_1 > A_6 > A_2 > A_7$
SD	MEW	$A_3 > A_{10} > A_9 > A_4 > A_5 > A_8 > A_1 > A_6 > A_2 > A_7$
SD	CODAS	$A_3 > A_9 > A_{10} > A_1 > A_5 > A_4 > A_7 > A_8 > A_2 > A_6$
SD	TOPSIS	$A_3 > A_{10} > A_9 > A_4 > A_8 > A_5 > A_1 > A_6 > A_2 > A_7$
CRITIC	MEW	$A_3 > A_{10} > A_9 > A_4 > A_5 > A_8 > A_1 > A_6 > A_2 > A_7$
CRITIC	CODAS	$A_3 > A_9 > A_{10} > A_1 > A_7 > A_5 > A_4 > A_8 > A_2 > A_6$
CRITIC	TOPSIS	$A_3 > A_{10} > A_9 > A_4 > A_8 > A_1 > A_5 > A_6 > A_2 > A_7$
CV	MEW	$A_9 > A_3 > A_{10} > A_4 > A_5 > A_8 > A_6 > A_1 > A_2 > A_7$
CV	CODAS	$A_9 > A_3 > A_{10} > A_1 > A_4 > A_5 > A_8 > A_7 > A_2 > A_6$
CV	TOPSIS	$A_9 > A_3 > A_{10} > A_4 > A_5 > A_8 > A_1 > A_6 > A_2 > A_7$

A notable feature of Table 10 is the complete agreement among MEW, CODAS, and TOPSIS regarding the first-ranked alternative within each weighting scheme. HIGHT (A_3) occupies the first position under EW, SD, and CRITIC, whereas CAMELLIA (A_9) becomes first under Entropy and CV. Hence, the identity of the leading alternative changes with the criterion-importance structure, but not with the ranking operator when the weight vector is held fixed. This result suggests that, for the present dataset, the first-rank outcome is more sensitive to the adopted weighting philosophy than to the choice among the three investigated MCDM procedures.

5.4.3 Cross-method concordance

Beyond agreement at the first position, the consistency of the complete ranking vectors was quantified using Kendall's coefficient of concordance. For $m_r = 3$ ranking methods and $n = 10$ alternatives

$$W = \frac{12 \sum_{i=1}^{10} (R_i - \bar{R})^2}{m_r^2 (n^3 - n)} \quad (86)$$

where R_i denotes the sum of the three ranks assigned to A_i , and $\bar{R}$ is the corresponding mean rank sum. The resulting coefficients are reported in Table 11.

Table 11

First-ranked alternative and cross-method concordance

Weighting mechanism	MEW rank 1	CODAS rank 1	TOPSIS rank 1	Kendall W
Entropy	CAMELLIA	CAMELLIA	CAMELLIA	0.9677
Equal	HIGHT	HIGHT	HIGHT	0.8303
SD	HIGHT	HIGHT	HIGHT	0.9030
CRITIC	HIGHT	HIGHT	HIGHT	0.8465
CV	CAMELLIA	CAMELLIA	CAMELLIA	0.9273

The concordance coefficients range from 0.8303 to 0.9677, demonstrating consistently high agreement among the three ranking procedures despite differences in the positions of some intermediate alternatives. The strongest concordance is obtained under Entropy weighting ($W = 0.9677$), followed by CV ($W = 0.9273$) and SD ($W = 0.9030$). CRITIC and EW yield $W = 0.8465$ and $W = 0.8303$, respectively. Thus, none of the examined weighting environments produces substantial disagreement among the three MCDM procedures at the overall ranking level.

5.4.4 Stability of the upper preference region

The robustness of the leading alternatives was further examined by considering their frequency of occurrence within the top three positions across all 15 weighting–ranking configurations. HIGHT (A_3) and TEA (A_{10}) remain within the top three in every configuration, corresponding to a top three inclusion frequency of 15/15 (100%). CAMELLIA (A_9) appears in this region in 14/15 configurations (93.33%); the only exception is the EW–TOPSIS configuration, in which LEA (A_4) occupies the third position and CAMELLIA moves to fourth. All remaining alternatives occur rarely or not at all within this upper preference region. Consequently, the results identify $\{A_3, A_9, A_{10}\} = \{\text{HIGHT}, \text{CAMELLIA}, \text{TEA}\}$ as the principal candidate group across the investigated configurations, while avoiding the stronger and inaccurate assertion that this exact top three set occurs in every case. The transition in first position between HIGHT and CAMELLIA is also consistent with the corresponding weight profiles. Entropy and CV assign substantially greater importance to throughput C^2 , $w_2^{(E)} = 0.316177$, $w_2^{(CV)} = 0.256439$, compared with $w_2^{(C)} = 0.115866$ under CRITIC. In the original decision matrix, CAMELLIA has the highest throughput, $x_9^2 = 290.1$, whereas HIGHT records $x_3^2 = 188$. The movement of CAMELLIA to the first position under Entropy and CV is therefore consistent with the greater emphasis these schemes place on throughput. Conversely, under EW, SD, and CRITIC, where importance is distributed differently across the criterion set, HIGHT occupies the leading position. Taken together, the alternative-weight analysis distinguishes two complementary forms of stability. The identity of the first-ranked cipher is weight-sensitive, shifting between HIGHT and CAMELLIA, whereas the preference structure is comparatively stable, as reflected by Kendall coefficients above 0.83 and the persistent presence of HIGHT, TEA, and, in all but one configuration,

CAMELLIA within the top three regions. These findings support the use of multiple weighting schemes as a robustness check and show that the principal candidate set is considerably less sensitive to modeling assumptions than the first position considered in isolation.

6. Results and Discussions

The results demonstrate a generally stable preference structure across the investigated weighting mechanisms and MCDM methods. Under the baseline CRITIC weights, MEW, CODAS, and TOPSIS consistently identify HIGHT (A_3) as the first-ranked alternative, although some variation occurs among the intermediate positions. This agreement indicates that the leading result is not specific to a single ranking procedure. The alternative-weight analysis further reveals the influence of criterion importance. Across the 15 weighting–MCDM configurations reported in Table 8, HIGHT (A_3) ranks first under Equal, SD, and CRITIC weighting, whereas CAMELLIA (A_9) ranks first under Entropy and CV weighting. The latter two schemes assign comparatively greater importance to throughput, which is consistent with the improved position of CAMELLIA. Thus, for the present dataset, the identity of the leading alternative is more sensitive to the weighting structure than to the choice among MEW, CODAS, and TOPSIS. Cross-method agreement remains high, with Kendall's coefficient of concordance ranging from $0.8303 \leq W \leq 0.9677$. The upper preference region is also stable: HIGHT (A_3) and TEA (A_{10}) occur among the top three in all 15 configurations, while CAMELLIA (A_9) appears in the top three in 14 configurations. The perturbation analysis provides additional evidence of robustness. As the perturbation magnitude increases, mean Spearman and Kendall correlations gradually decrease, while mean rank displacement increases. Nevertheless, the mean Spearman correlation remains above 0.99 over the investigated perturbation range, indicating limited changes in the overall ranking structure. Overall, the results indicate that the proposed framework provides a consistent and robust basis for comparative lightweight cipher evaluation. HIGHT is preferred under the baseline CRITIC configuration, while the HIGHT–CAMELLIA transition under alternative weighting schemes highlights the importance of criterion prioritization. Therefore, the final ranking should be interpreted in relation to the specified weighting structure and resource requirements of the target IoT environment.

7. Conclusion and Future Recommendations

The rapid growth of information technology has increased the need for efficient and reliable methods to select suitable lightweight cryptographic algorithms. In this study, three MCDM techniques, MEW, CODAS, and TOPSIS, are used to evaluate 10 lightweight ciphers under multiple conflicting criteria. The assessment considers chip area, throughput, energy consumption, power consumption, latency, algorithm size, RAM size, and cryptographic key size. The relative importance of these criteria is determined objectively using the CRITIC weighting method. The results obtained from all three MCDM approaches consistently place HIGHT in the first position under the criteria considered and the CRITIC-derived weights. The remaining ciphers are ranked according to their overall performance across the selected implementation, resource, and security-related characteristics. The analysis therefore provides a practical decision support approach for comparing lightweight encryption algorithms in resource-constrained environments.

Acknowledgments

The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/2025/01/33903).

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

The datasets underlying this work can be obtained from the corresponding author upon reasonable request.

Funding

The authors extend their appreciation to Prince Sattam bin Abdulaziz University for funding this research work through the project number (PSAU/2025/01/33903).

AI-Assisted Editing Disclosure

During the preparation of this manuscript, Grammar tools were utilized to potentially enhance linguistic fluency and readability; following the implementation of such tools, the content was thoroughly reviewed, verified, and edited, with the authors assuming full responsibility for the final publication.

References

- [1] Zhang, C., & Chen, Y. (2020). A review of research relevant to the emerging industry trends: Industry 4.0, IoT, blockchain, and business analytics. *Journal of Industrial Integration and Management*, 5(01), 165-180. <https://doi.org/10.1142/S2424862219500192>
- [2] Manavalan, E., & Jayakrishna, K. (2019). A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements. *Computers & Industrial Engineering*, 127, 925-953. <https://doi.org/10.1016/j.cie.2018.11.030>
- [3] Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Gonzalez, E. S. (2022). Understanding the adoption of Industry 4.0 technologies in improving environmental sustainability. *Sustainable Operations and Computers*, 3, 203-217. <https://doi.org/10.1016/j.susoc.2022.01.008>
- [4] Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., & Traore, I. (2022). A survey on IoT-enabled smart grids: emerging, applications, challenges, and outlook. *Energies*, 15(19), 6984. <https://doi.org/10.3390/en15196984>
- [5] Chang, V., Muñoz, V. M., & Ramachandran, M. (2020). Emerging applications of internet of things, big data, security, and complexity: special issue on collaboration opportunity for IoTBDs and COMPLEXIS. *Computing*, 102(6), 1301-1304. <https://doi.org/10.1007/s00607-020-00811-y>
- [6] Hema Rajini, N., & Anton Smith, A. (2023). Osteoarthritis Detection and Classification in Knee X-Ray Images Using Particle Swarm Optimization with Deep Neural Network. In *Interpretable Cognitive Internet of Things for Healthcare* (pp. 91-101). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-031-08637-3_5
- [7] Kamalov, F., Pourghebleh, B., Gheisari, M., Liu, Y., & Moussa, S. (2023). Internet of medical things privacy and security: Challenges, solutions, and future trends from a new perspective. *Sustainability*, 15(4), 3317. <https://doi.org/10.3390/su15043317>
- [8] Akram, J., Umair, M., Jhaveri, R. H., Riaz, M. N., Chi, H., & Malebary, S. (2023). Chained-drones: Blockchain-based privacy-preserving framework for secure and intelligent service provisioning in internet of drone things. *Computers and Electrical Engineering*, 110, 108772. <https://doi.org/10.1016/j.compeleceng.2023.108772>
- [9] Savari, G. F., Krishnasamy, V., Sathik, J., Ali, Z. M., & Aleem, S. H. A. (2020). Internet of Things based real-time electric vehicle load forecasting and charging station recommendation. *ISA Transactions*, 97, 431-447. <https://doi.org/10.1016/j.isatra.2019.08.011>
- [10] Shahzad, K., Zia, T., & Qazi, E. U. H. (2022). A review of functional encryption in IoT applications. *Sensors*, 22(19), 7567. <https://doi.org/10.3390/s22197567>
- [11] Doukas, C., Maglogiannis, I., Koufi, V., Malamateniou, F., & Vassilacopoulos, G. (2012, November). Enabling data protection through PKI encryption in IoT m-Health devices. In *2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE)* (pp. 25-29). IEEE. <https://doi.org/10.1109/BIBE.2012.6399701>
- [12] Munoz, P. S., Tran, N., Craig, B., Dezfouli, B., & Liu, Y. (2018). Analyzing the resource utilization of AES encryption on IoT devices. In *2018 asia-pacific signal and information processing association annual summit and conference (APSIPA ASC)* (pp. 1200-1207). IEEE. <https://doi.org/10.23919/APSIPA.2018.8659779>

- [13] Chatterjee, R., Chakraborty, R., & Mondal, J. K. (2019). Design of lightweight cryptographic model for end-to-end encryption in IoT domain. *IRO Journal on Sustainable Wireless Systems*, 1(4), 215-224. <https://doi.org/10.36548/jsws.2019.4.002>
- [14] Trujillo-Toledo, D. A., López-Bonilla, O. R., García-Guerrero, E. E., Tlelo-Cuautle, E., López-Mancilla, D., Guillén-Fernández, O., & Inzunza-González, E. (2021). Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps. *Chaos, Solitons & Fractals*, 153, 111506. <https://doi.org/10.1016/j.chaos.2021.111506>
- [15] Li, N., Liu, D., & Nepal, S. (2017). Lightweight mutual authentication for IoT and its applications. *IEEE Transactions on Sustainable Computing*, 2(4), 359-370. <https://doi.org/10.1109/TSUSC.2017.2716953>
- [16] Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2024). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, 15(2), 1625-1642. <https://doi.org/10.1007/s12652-017-0494-4>
- [17] Panahi, P., Bayılmış, C., Çavuşoğlu, U., & Kaçar, S. (2021). Performance evaluation of lightweight encryption algorithms for IoT-based applications. *Arabian Journal for Science and Engineering*, 46(4), 4015-4037. <https://doi.org/10.1007/s13369-021-05358-4>
- [18] Naser, N. M., & Naif, J. R. (2022). A systematic review of ultra-lightweight encryption algorithms. *International Journal of Nonlinear Analysis and Applications*, 13(1), 3825-3851. <https://doi.org/10.22075/ijnaa.2022.6167>
- [19] Ning, L., Ali, Y., Ke, H., Nazir, S., & Huanli, Z. (2020). A hybrid MCDM approach of selecting lightweight cryptographic cipher based on ISO and NIST lightweight cryptography security requirements for internet of health things. *IEEE Access*, 8, 220165-220187. <https://doi.org/10.1109/ACCESS.2020.3041327>
- [20] Razaq, A., Ramzan, M., Xin, Q., Alolaiyan, H., & Alghazzawi, D. (2026). From Schreier graphs to secure s-boxes using a group-theoretic design framework. *Scientific Reports*, 16, 26411 (2026). <https://doi.org/10.1038/s41598-026-56441-5>
- [21] Banik, S., Bogdanov, A., Peyrin, T., Sasaki, Y., Sim, S. M., Tischhauser, E., & Todo, Y. (2019). *SUNDAE-GIFT v1.0. NIST Lightweight Cryptography Project*. <https://csrc.nist.gov/Projects/lightweight-cryptography/round-2-candidates>
- [22] Said, L., Alshammari, F.S. & Khan, M. (2026). Chaos-driven design of highly nonlinear S-boxes for secure and efficient lightweight image encryption. *Scientific Reports*, 16, 30175. <https://doi.org/10.1038/s41598-026-58835-x>
- [23] Li, H., Yang, G., Ming, J., Zhou, Y., & Jin, C. (2021). Transparency order versus confusion coefficient: a case study of NIST lightweight cryptography S-Boxes. *Cybersecurity*, 4(1), 35. <https://doi.org/10.1186/s42400-021-00099-1>
- [24] Abughazalah, N., Hayat, M. M. A., & Khan, M. (2024). An intelligent selection of lightweight multivalued cryptographic boolean function based on Multi-criteria decision making. *Multimedia Tools and Applications*, 83(13), 39389-39410. <https://doi.org/10.1007/s11042-023-17145-4>
- [25] Mahmoodi, E., Azari, M., & Dastorani, M. T. (2023). Comparison of different objective weighting methods in a multi-criteria model for watershed prioritization for flood risk assessment using morphometric analysis. *Journal of Flood Risk Management*, 16(2), e12894. <https://doi.org/10.1111/jfr3.12894>
- [26] Zindani, D., Das, G., Bhagwat, V., & Singh, G. (2023). Aggregation multiplicative rule for ranking of Mg-Al-Sn anodic alloys for metal-air batteries. *Materials Today: Proceedings*, 72, 2300-2305. <https://doi.org/10.1016/j.matpr.2022.09.396>
- [27] Dehshiri, S. S. H., & Firoozabadi, B. (2023). A new multi-criteria decision making approach based on wins in league to avoid rank reversal: A case study on prioritizing environmental deterioration strategies in arid urban areas. *Journal of Cleaner Production*, 383, 135438. <https://doi.org/10.1016/j.jclepro.2022.135438>
- [28] Garg, H., Ali, Z., Mahmood, T., & Ali, M. R. (2023). TOPSIS-method based on generalized dice similarity measures with hamy mean operators and its application to decision-making process. *Alexandria Engineering Journal*, 65, 383-397. <https://doi.org/10.1016/j.aej.2022.10.043>
- [29] Awodi, N. J., Liu, Y. K., Ayo-Imoru, R. M., & Ayodeji, A. (2023). Fuzzy TOPSIS-based risk assessment model for effective nuclear decommissioning risk management. *Progress in Nuclear Energy*, 155, 104524. <https://doi.org/10.1016/j.pnucene.2022.104524>
- [30] Corrente, S., & Tasiou, M. (2023). A robust TOPSIS method for decision making problems with hierarchical and non-monotonic criteria. *Expert Systems with Applications*, 214, 119045. <https://doi.org/10.1016/j.eswa.2022.119045>