

DOI: 10.37943/GVCR2663

Nursulu Kapalova

Candidate of Technical Sciences, Associate Professor,
Head of the Information Security Laboratory
kapalova@mail.ru, orcid.org/0000-0001-9743-9981
Institute of Information and Computational Technologies, Kazakhstan

Armiyanbek Khaumen

PhD Student, Faculty of Information Technology and Artificial Intelligence
haumen.armanbek@gmail.com, orcid.org/0000-0002-1670-2520
Al-Farabi Kazakh National University, Kazakhstan
Institute of Information and Computational Technologies, Kazakhstan

Kunbolat Algazy

PhD, Associate Professor, Senior Researcher, Information Security Laboratory
kunbolat@mail.ru, orcid.org/0000-0003-3670-2170
Institute of Information and Computational Technologies, Kazakhstan

ADVANTAGES AND DISADVANTAGES OF THE DIFFUSION PROPERTIES OF LIGHTWEIGHT BLOCK CIPHERS BASED ON ROUND-BY-ROUND AVALANCHE ANALYSIS

Abstract: This paper investigates the diffusion properties of lightweight encryption algorithms designed for deployment in resource-constrained systems. Modern schemes intended for environments with strict limitations on computational complexity and energy consumption are evaluated. Particular attention is paid to the analysis of isolated round functions – particularly their behavior prior to the application of round keys. This approach enables the assessment of internal structural properties independently of the key scheduling procedures and identifies basic diffusion characteristics determined exclusively by the employed bitwise transformations. Specifically, the impact of flipping a single bit in the input block on the distribution of changes in the output data is analyzed, facilitating an evaluation of the quality of internal transformations and their resistance to cryptanalytic attacks. For quantitative evaluation, classical measures of avalanche behavior – the Avalanche Effect and the Strict Avalanche Criterion (SAC) – are used to assess how rapidly and uniformly information propagates within a block after the application of round transformations. All algorithms are evaluated using a unified round-by-round experimental procedure under identical conditions. This ensures a consistent and objective comparison of their diffusion characteristics across successive encryption rounds. The results reveal distinct advantages and limitations in diffusion speed, stabilization behavior, and uniformity among the evaluated lightweight cipher constructions. The comparison shows that schemes based on cyclic rotations and bitwise operations exhibit high diffusion rates with minimal computational complexity. This analysis demonstrates the effectiveness of approaches relying on simple bitwise transformations. The obtained results provide valuable practical design insights for the selection or design of lightweight cryptographic primitives for microcontrollers, sensor networks, and other devices with limited computational capabilities.

Keywords: lightweight algorithm, diffusion, avalanche effect, SAC (Strict Avalanche Criterion), Feistel network, RX structure.

Introduction

Digital technologies are increasingly penetrating everyday life. Most of the devices surrounding us – such as smartphones, smartwatches, medical sensors, and smart home systems – constantly exchange data. These data often contain personal or confidential information. Therefore, information security becomes an integral part of the digital environment. At the same time, devices are becoming increasingly miniaturized, while their computational capabilities

remain limited. This creates specific requirements for encryption methods, which must be not only secure but also as simple as possible to implement.

Classical encryption algorithms, such as AES and IDEA, provide a high level of security; however, they require substantial computational resources and energy [1]. Their use in microcontrollers, sensor nodes, and other low-power systems is often inefficient. In response to these constraints, recent years have seen the active development of lightweight cryptographic algorithms. These algorithms are designed to operate under conditions of limited memory, low processor word size, and low energy consumption [2].

Lightweight encryption algorithms rely on various architectural principles, the most common of which include Feistel networks [3], SP-networks [4], as well as ARX (Add–Rotate–XOR) and RX (Rotate–XOR) schemes [5]. Each of these approaches has its own advantages and limitations. SP-networks provide strong diffusion but require the use of substitution tables (S-boxes), which increases memory usage and energy consumption. ARX-based schemes achieve a good balance between security and performance by relying solely on arithmetic and logical operations. RX-based structures, in turn, completely avoid complex computations and use only bitwise cyclic rotations and XOR operations, making them particularly attractive for devices with extremely limited resources.

One of the key quality indicators of any block cipher is its diffusion properties, that is, how rapidly and uniformly changes in the input data propagate throughout the entire output block [6]. In other words, a change of a single input bit should result in changes in approximately half of the output bits. This property is known as the avalanche effect. Strong diffusion ensures that small input modifications lead to significant changes in the output, thereby hindering structural cryptanalysis of the cipher [7].

For the quantitative evaluation of avalanche behavior, measures of the Avalanche Effect and the Strict Avalanche Criterion (SAC) are employed. The former characterizes the proportion of output bits that change when a single input bit is inverted, while the latter reflects how uniformly each input bit influences each output bit. If each output bit changes with a probability close to 0.5, the cipher is considered to satisfy the SAC [8]. These measures enable the comparison of different algorithms independently of their architecture and key parameters.

Despite the substantial body of research on lightweight ciphers, comparative evaluations of the diffusion properties of different architectures remain relatively scarce. Many studies focus primarily on performance, energy consumption, or resistance to specific attacks, while the uniform propagation of input modifications receives comparatively less attention [9]. However, insufficient diffusion may lead to slower propagation of local input changes across the internal state and can reveal structural weaknesses in reduced-round transformations. For this reason, the round-by-round analysis of diffusion behavior provides useful information about how rapidly and uniformly the internal transformations spread input differences. Effective diffusion is therefore an important characteristic in the design and security analysis of lightweight block ciphers [10–11].

In this work, a comparative analysis of the diffusion properties of several well-known lightweight block ciphers is presented, namely SIMON, SPECK, PRESENT, LEA, HIGHT, and TEA, as well as a new algorithm, FEATHER-RX, which is constructed exclusively from simple bitwise operations – cyclic rotations and logical *XOR* and *AND* – without the use of substitution tables or modular addition. All algorithms were implemented within a unified software environment and evaluated using the same experimental methodology.

The main objective of this study is to determine how cipher architecture affects diffusion characteristics and to identify the main advantages and relative limitations of the evaluated constructions. Particular attention is paid to RX-based structures, as they represent a simple and energy-efficient alternative to ARX and SP models. The analysis is conducted using round-by-round avalanche evaluation and classical diffusion measures, providing an objective assessment of diffusion behavior in block ciphers.

The practical significance of this work lies in the fact that the obtained results can be used when selecting cryptographic primitives for Internet of Things devices, embedded systems, medical sensors, and other resource-constrained platforms. The identified relationships between round structure and diffusion characteristics make it possible to formulate guidelines for the design of new lightweight algorithms that achieve a high level of security with minimal hardware overhead.

The main novelty of this study lies in the development of an original lightweight encryption algorithm, FEATHER-RX. The proposed algorithm is built on RAX-like transformations, where the internal structure operates in conjunction with a dynamic parameter. This integration enables enhanced diffusion characteristics while maintaining low computational complexity.

In most existing works, evaluation is performed at the level of the complete encryption algorithm, which makes it difficult to isolate and assess the individual contribution of the round function to the overall diffusion behavior. By addressing this gap, the present study provides a more precise assessment of diffusion at the round-function level.

Thus, the study aims to reveal the relationship between cipher architecture and its ability to uniformly propagate input modifications. A comparison of different structural approaches allows for the identification of promising directions for the further development of efficient cryptographic solutions tailored to resource-constrained environments.

Methodology

Description of the FEATHER-RX algorithm

FEATHER-RX is a new lightweight block cipher developed in the Information Security Laboratory of the Institute of Information and Computational Technologies. The algorithm is designed for systems with limited computational resources and minimal hardware implementation requirements.

The cipher follows a Feistel structure and operates on a fixed 64-bit block size. For implementation efficiency, the block is divided into a left (L) and a right (R) branch, each 32 bits long (Figure 1). This architecture is motivated by the fact that 32-bit operations are natively supported by most microcontrollers, providing an optimal balance between execution speed and simplicity. The name of the algorithm reflects its structural core, which primarily utilizes RX (*Rotate-XOR*) transformations, augmented by bitwise *AND* operations to introduce the required non-linearity.

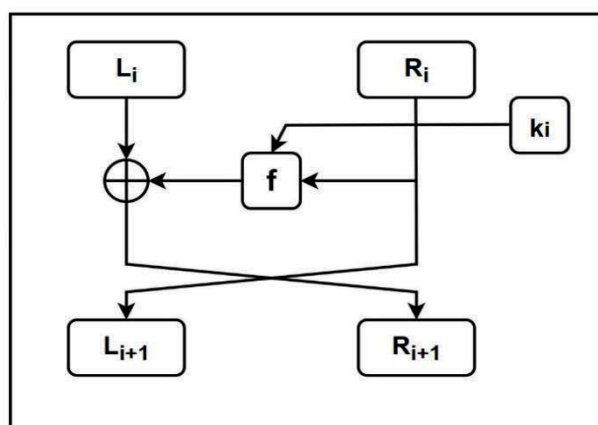


Figure 1. Structural diagram of the FEATHER-RX algorithm

The input block undergoes 48 sequential rounds of transformation. This value was chosen as a compromise between the algorithm's performance and the necessary level of diffusion.

A round is defined as a complete transformation cycle comprising the round function evaluation, mixing with key material, and the subsequent swapping of branches in the Feistel network. Each iteration introduces additional data mixing, increasing the complexity of the

dependency between input and output bits. While an increased number of rounds enhances diffusion and cryptanalytic resistance, it simultaneously raises the computational cost.

In each round, only the right half of the block is transformed. The left half is updated by via an *XOR* operation with the output of the round function, followed by a branch swap. This structure ensures a gradual propagation of changes throughout the entire block with minimal operations.

The structure of the FEATHER–RX round function is shown in Figure 2. The algorithm avoids substitution tables and modular addition, relying instead on three basic primitives: bitwise rotations, *XOR*, and the bitwise *AND*.

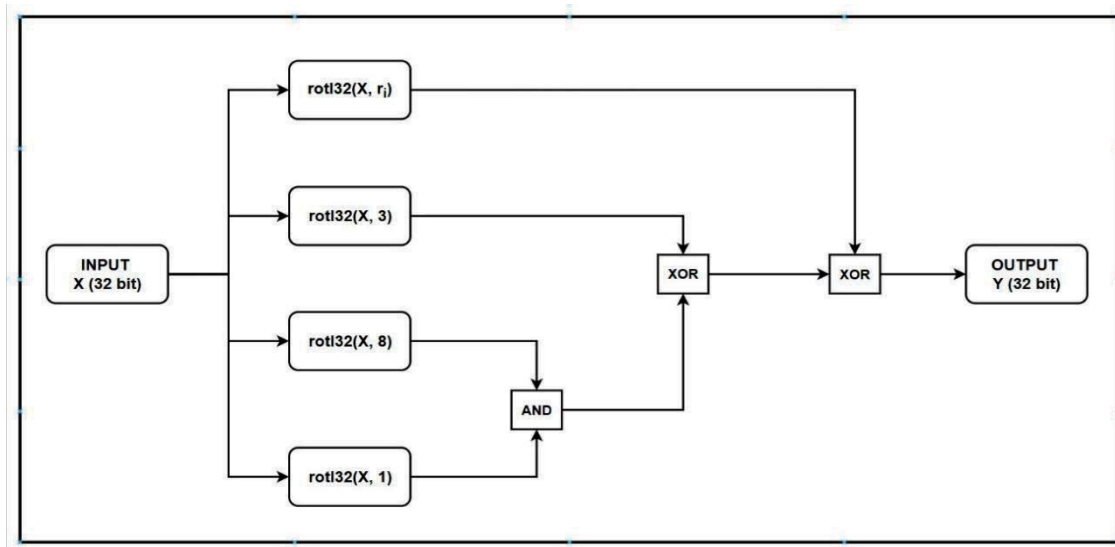


Figure 2. Block diagram of the FEATHER–RX round function

This selection of operations makes FEATHER–RX particularly suitable for extremely resource-constrained devices. Cyclic rotations and *XOR* operations can be implemented in hardware in constant time, without memory access or complex arithmetic units, thereby reducing energy consumption and latency.

The round function is defined as follows:

- The function takes a 32-bit word x and the round index i as inputs.
- A rotation offset is selected from the parameter array $R_CYCLE = (13, 16, 19)$.
- A combination of four cyclic rotations, one *AND* operation, and two *XOR* operations is applied.

In analytical form, the round function is given by

$$r_i = R_CYCLE[i \bmod 3]$$

$$f(x, i) = (\text{rotl32}(x, 1) \& \text{rotl32}(x, 8)) \oplus \text{rotl32}(x, 3) \oplus \text{rotl32}(x, r_i) \quad (1)$$

where $\text{rotl32}(x, j)$ denotes a cyclic left rotation of the 32-bit word x by j bits, $\&$ is the bitwise *AND* operation, $\oplus$ denotes the *XOR* operation (addition modulo 2), and i is the round index. The round function utilizes a combination of fixed rotations $\{1, 8, 3\}$ and a dynamic rotation parameter r_i from the R_CYCLE array.

Thus, each bit in the input word affects multiple positions through varying rotations. The resulting values are combined using the *AND* operation and subsequently mixed via *XOR*. This ensures that even a single-bit change in the input word x propagates rapidly to a large number of bits in the output word y .

The FEATHER–RX round function does not employ table-based nonlinear transformations or modular addition. Nevertheless, the combination of multidirectional cyclic rotations provides a

high level of diffusion, achieving effective change propagation without computationally heavy components. Rotation parameters are selected to avoid symmetric or repetitive structures. The variable parameter r_i changes from round to round, preventing the emergence of stable patterns and improving diffusion uniformity. The *AND* operation introduces essential nonlinear dependencies between bits, while the subsequent *XOR* mixing further strengthens the diffusion effect.

The algorithm supports two master key lengths: 128 and 256 bits. This allows FEATHER–RX to be used in a variety of security scenarios and adapted to the requirements of a specific system. The 256-bit key is intended for environments with higher security requirements, while the 128-bit variant targets devices with stricter memory and energy constraints.

Round keys are derived from the master key with a length of 32 bits. During encryption, a single round key is added to the data in each round. This 32-bit key size is consistent with the internal word size, simplifying implementation on 32-bit architectures.

Within the scope of this study, the key schedule algorithm and the round key addition operation are not analyzed. All experiments focus on evaluating the diffusion properties of the round function itself. This approach isolates the impact of the transformation structure, allowing for an objective assessment of the RAX operations' contribution to the avalanche effect, independent of external factors.

Object and purpose of the study

The object of this study is lightweight block encryption algorithms intended for use in devices with limited computational resources.

The purpose of the work is to conduct a comparative evaluation of diffusion properties and to analyze the behavior of the round transformations that form the core of each considered cipher.

The round function determines how data are transformed within a block at each encryption step. It governs the uniformity of bit-change propagation, the rate at which the avalanche effect emerges, and the structural resistance of the algorithm to linear and differential cryptanalyses. Therefore, studying the round function behavior reveals internal regularities of the cipher and identifies the strengths and weaknesses of its architecture.

The objective of this study is to experimentally demonstrate how the type of round transformation (e.g., SP-, ARX-, or RX-based structures) and the cipher topology (specifically, the Feistel network) affect the degree of diffusion. This facilitates the identification of the most promising approaches for designing new lightweight algorithms. Such results are especially important at the design stage, when it is necessary to select a minimal set of operations that provide adequate security without increasing hardware overhead.

Methods for evaluating diffusion

To evaluate diffusion properties, two classical measures of avalanche behavior were used: the avalanche effect and the Strict Avalanche Criterion (SAC). These measures allow for a quantitative assessment of how significantly and uniformly a small change in the input data (specifically, the inversion of a single bit) is reflected in the ciphertext [12–13].

The methodology was based on the sequential encryption of two closely related blocks differing by only one bit. Let F denote the encryption function, x the original input block, and $x^{(i)}$ the block obtained by inverting the i th input bit. After performing a fixed number of rounds, the number of changed bits was computed as the Hamming distance between the corresponding outputs:

$$d = wt(F(x) \oplus F(x^{(i)})) \quad (2)$$

where $\oplus$ denotes the *XOR* operation and wt is the Hamming weight. Next, the average number of changed bits was determined and compared with the ideal distribution, which corresponds to a 50% change in bits.

The SAC was assessed as a measure of the uniformity of influence exerted by each input bit on each output bit. Mathematically, this is expressed as the probability that the j th output bit changes when the i th input bit is inverted:

$$P_{ij} = P(f_j(x) \oplus f_j(x^{(i)}) = 1) = 0.5 \quad (3)$$

To evaluate the overall diffusion quality, the normalized SAC value was computed as

$$SAC = 1 - \frac{2}{n^2} \sum_{i=1}^n \sum_{j=1}^n |P_{ij} - 0.5| \quad (4)$$

A normalized SAC value close to 1.0 indicates that each input bit affects each output bit with equal probability, which characterizes high-quality diffusion.

Experimental parameters

The experiments were conducted in a unified software environment with all algorithms implemented in Python without platform-specific optimizations. Testing was performed using a unified configuration: 1,000 random input blocks, 16 evaluated rounds, fixed all-zero round keys, and block sizes defined by each cipher specification. A fixed random seed was used to ensure reproducibility.

The analysis focused on the behavior of the round function rather than on the complete cryptographic system. This approach isolates the internal properties of the transformations, allowing for an evaluation of the structural diffusion without the influence of additional components, such as round key addition, external permutations, or final processing stages.

Within the scope of this study, fixed all-zero round keys were used to exclude the influence of the key schedule on the diffusion results. This decision is consistent with the primary objective of analyzing the diffusion properties of the round function itself. This configuration isolates the contribution of the round transformation while maintaining identical key conditions for all algorithms.

Excluding round keys enables the isolation of the intrinsic properties of the transformations. In this case, the observed diffusion is determined solely by the applied bitwise operations, cyclic rotations, and the overall round structure. This approach provides a more direct and objective assessment of the effectiveness of the chosen architecture.

Furthermore, it should be noted that the key schedule algorithms vary substantially across different ciphers, influenced by master key length, the number of rounds, and the specific set of operations employed. In a comparative analysis, such variations could lead to biased results, reducing the validity of comparisons between different schemes.

Fixing or completely excluding key material is a common practice in studies of the diffusion properties of round functions. This approach is typically applied during the early design stages of encryption algorithms to evaluate structural quality independently of key-related parameters.

Thus, omitting round keys in the experimental setup makes it possible to focus on the analysis of the diffusion properties of the round function itself and ensures a correct and consistent comparison of results across all investigated algorithms.

To evaluate the diffusion properties of round functions, a unified experimental methodology was applied to all tested algorithms:

1. Random input data blocks were generated for each round-function variant.
2. Each random block was encrypted, and the output value was recorded.
3. Each input bit was inverted separately while all remaining bits were kept unchanged.
4. The modified block was re-encrypted under identical conditions.
5. The resulting outputs were compared by calculating the number of differing bits to quantitatively assess avalanche behavior.

6. The procedure was repeated for 1,000 randomly generated input blocks at each evaluated round.
7. Based on the averaged results, the avalanche indicator (as a percentage) and compliance with the SAC were evaluated.

The methodology provides an objective comparison of different round functions and identifies designs that ensure efficient change propagation. Intermediate diffusion values were analyzed for each round from 1 to 16, enabling an assessment of both diffusion growth and stabilization.

The study includes seven lightweight block ciphers: SIMON [14], SPECK [15], PRESENT [16], LEA [17], HIGHT [18], TEA [19], and the proposed FEATHER–RX algorithm. Each cipher employs a distinct architectural approach, including permutations, arithmetic operations, logical operations, and cyclic bit rotations.

Results and discussion

The interpretation of the results was based on widely accepted measures of avalanche behavior. An average proportion of modified output bits close to 50% indicates a good level of diffusion, whereas SAC values approaching 1.0 reflect a high degree of uniform influence of input bits on output bits. Values that deviate substantially from these reference levels (in particular, below 0.7) indicate insufficient diffusion and non-uniform propagation of changes [20].

The role of this study is to establish an experimental basis that enables an objective comparison of round functions used in different block ciphers. The obtained results can be applied in the design of new cryptographic primitives, especially for systems in which a balance between security level, performance, and hardware efficiency is required.

The conducted experiments provided comparative round-by-round diffusion data for seven lightweight cipher constructions. Table 1 summarizes the final avalanche characteristics and the round at which stable diffusion was achieved.

Table 1. Diffusion characteristics under the unified experimental methodology

Algorithm	Flips / block	Pairs / round	Stab. round	AE ₁₆ (%)	SD (%)	SAC norm
SIMON64	64	64,000	9	49.9739	0.7692	0.9748
SPECK64/128	64	64,000	5	50.0101	0.7875	0.9745
PRESENT	64	64,000	5	50.0296	0.7860	0.9749
LEA-128	128	128,000	7	49.9834	0.4063	0.9747
HIGHT-style	64	64,000	8	50.0379	0.7595	0.9739
TEA	64	64,000	3	50.0197	0.7767	0.9744
FEATHER-RX	64	64,000	5	49.9599	0.7807	0.9750

Notes: Flips / block – number of single-bit input modifications per random block; Pairs / round – number of original–modified block pairs evaluated at each round; Stab. round – earliest round at which the mean avalanche effect entered the 45–55% interval and remained within this range; AE₁₆ – mean avalanche effect at round 16; SD – standard deviation; SAC norm – normalized SAC quality score. The 95% confidence intervals are presented in the round-by-round diffusion figure.

Table 1 shows that all evaluated constructions achieve final avalanche values close to the ideal 50% level. The main difference lies in the number of rounds required to reach stable diffusion.

For the statistical interpretation of the results, diffusion metrics were analyzed not only as individual values but also in terms of their stability and repeatability across multiple experimental trials. The results indicate that all evaluated constructions achieve comparable final diffusion levels. FEATHER-RX demonstrates stable behavior and the highest normalized SAC score,

although the differences between the algorithms remain small. Consequently, the statistical analysis confirms the practical significance of FEATHER-RX regarding its efficiency in propagating input changes throughout the internal state of the cipher.

While all evaluated constructions approach the ideal final diffusion level, their round-by-round development differs considerably. Figure 3 shows that FEATHER-RX reaches stable diffusion rapidly, while SIMON64 requires more rounds to converge. These differences are determined not only by the number of rounds but also by the type of basic operations used within the round function.

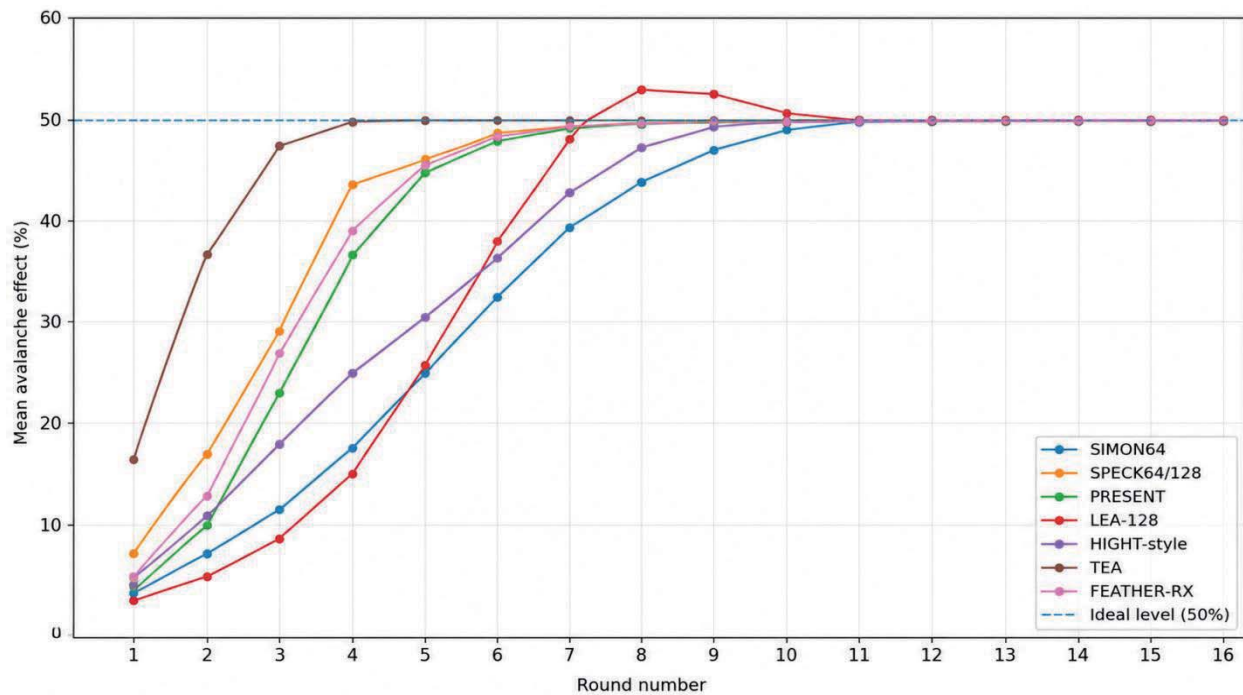


Figure 3. Round-by-round evolution of the avalanche effect for the evaluated lightweight block ciphers

To complement the graphical representation in Figure 3, Table 2 presents the mean avalanche effect values at selected rounds and highlights the differences in diffusion growth across the evaluated constructions.

Table 2. Mean avalanche effect (%) at selected rounds

Algorithm	R1	R3	R5	R7	R9	R16
SIMON64	3.1285	11.4856	26.2057	40.0038	47.7642	49.9739
SPECK64/128	6.6435	28.9476	46.1994	49.9371	49.9817	50.0101
PRESENT	3.9093	24.4525	46.8708	49.8975	49.9595	50.0296
LEA-128	2.4642	9.0759	26.5709	48.4659	51.9108	49.9834
HIGHT-style	4.4082	18.8565	31.3641	43.4602	49.8415	50.0379
TEA	16.3603	47.4505	50.0274	49.9505	49.9512	50.0197
FEATHER-RX	3.9098	26.3496	46.5510	49.9771	49.9589	49.9599

The numerical values confirm that the evaluated constructions differ mainly in the rate of diffusion growth, with all of them approaching the ideal 50% level by round 16.

Below is a generalized characterization of the behavior of each investigated scheme.

SIMON64 exhibits the slowest diffusion development among the evaluated constructions. During the initial rounds, the avalanche effect increases gradually because the round function relies

mainly on rotations, XOR, and bitwise AND operations, which spread input changes more slowly across the state. The algorithm enters the stable 45–55% diffusion interval at round 9 and converges toward the ideal 50% level by round 16. Therefore, although its final diffusion quality is comparable to the other evaluated algorithms, SIMON64 requires a larger number of rounds to achieve this state.

SPECK64/128 shows rapid diffusion progression, reaching the stable range as early as round 5. By round 16, its avalanche effect closely approaches the 50% mark, confirming the effectiveness of combining modular addition, cyclic rotations, and XOR operations.

PRESENT displays swift diffusion increase, entering the stable window at round 5. By round 16, it attains an avalanche effect close to the ideal 50% level, underscoring the efficiency of its substitution and permutation layers. However, relying on S-boxes may increase memory requirements in highly constrained hardware environments.

LEA-128 is an ARX-based cipher designed for efficient implementation on 32-bit processors. The round-by-round results reveal a gradual rise in diffusion during early rounds, followed by stabilization within the 45–55% range at round 7. By round 16, its avalanche effect approaches the ideal 50% benchmark, while the comparatively low standard deviation indicates highly consistent behavior across the tested input blocks. This performance is primarily driven by the joint action of modular addition, cyclic rotations, and XOR operations, which establish strong bit dependencies within the internal state.

The HIGHT-style construction features a progressive diffusion increase during the early rounds, settling into the stable 45–55% window at round 8. By round 16, its avalanche effect converges near the ideal 50% level, reflecting uniform difference propagation across the internal state. This behavior stems from its byte-oriented architecture and the interplay of logical and arithmetic operations. However, these findings characterize the simplified HIGHT-style model evaluated in this experiment rather than the fully standardized HIGHT cipher.

TEA yields the fastest diffusion escalation among all evaluated constructions. Its avalanche effect enters the stable 45–55% interval by round 3 and remains closely aligned with the ideal 50% level throughout the subsequent rounds. This rapid expansion is facilitated by combining modular addition, cyclic shifts, and XOR operations, which induce strong inter-bit dependencies. Consequently, despite its lightweight architecture, TEA delivers highly effective early-round diffusion under the chosen test conditions.

Particular attention is paid to FEATHER-RX, whose round transformation relies on cyclic rotations, XOR, and bitwise AND operations without modular addition or substitution tables. The round-by-round data indicate rapid initial diffusion progression, with the algorithm entering the stable 45–55% window at round 5. By round 16, its avalanche effect reaches near-ideal values close to 50%, while securing the highest normalized SAC score among all evaluated schemes. This robust behavior is attributed to the combined effect of fixed rotations, the round-dependent dynamic rotation parameter, the nonlinear AND operation, and the Feistel branch exchange. These results demonstrate that FEATHER-RX achieves diffusion parity with ARX- and SP-based designs while preserving a lightweight round architecture.

The comparative analysis reveals that while the evaluated constructions reach similar final diffusion levels, they differ noticeably in the number of rounds required to reach them. ARX- and SP-based schemes generally offer rapid early-round diffusion owing to modular addition or substitution layers. FEATHER-RX accomplishes equivalent stabilization using only rotations, XOR, AND, and Feistel branch exchanges, whereas SIMON64 demands a higher round count. This confirms that a carefully selected combination of basic bitwise operations can provide effective diffusion without compromising implementation simplicity.

To summarize the comparative findings, Table 3 presents the main advantages and disadvantages of the diffusion properties observed for each evaluated construction.

Table 3. Advantages and disadvantages of the diffusion properties of the evaluated lightweight cipher constructions

Algorithm	Advantages of diffusion properties	Disadvantages / limitations
SIMON64	Final AE approaches the ideal 50% level; high normalized SAC after sufficient rounds	Slowest diffusion development; stable diffusion is reached only at round 9
SPECK64/128	Rapid diffusion growth; stable diffusion from round 5; final AE close to 50%	Requires several rounds before reaching stable diffusion; early-round diffusion is lower than TEA
PRESENT	Stable diffusion from round 5; final AE close to 50%; high diffusion uniformity	Early-round propagation is slower than TEA; diffusion develops gradually during the first rounds
LEA-128	Final AE close to 50%; lowest standard deviation among the evaluated constructions	Stable diffusion is reached at round 7; temporary overshoot above 50% is observed around round 9
HIGHT-style	Final diffusion approaches the ideal level; uniform propagation after stabilization	Relatively slow stabilization at round 8; results apply to the simplified HIGHT-style model rather than the complete standardized cipher
TEA	Fastest diffusion growth; stable diffusion is reached at round 3; final AE remains close to 50%	Normalized SAC is slightly lower than that of several evaluated constructions
FEATHER-RX	Stable diffusion from round 5; final AE close to 50%; highest normalized SAC score; stable round-by-round behavior	Does not achieve the earliest stabilization among the evaluated constructions; several initial rounds are required before reaching the stable diffusion interval

It should be noted that the conducted experiment was limited to a comparative round-by-round evaluation of diffusion under a unified testing configuration. The obtained results characterize single-bit change propagation and avalanche effect stabilization in the evaluated constructions. However, they do not constitute a comprehensive assessment of cryptographic security, as resistance to differential, linear, related-key, and side-channel attacks was not examined, nor was implementation-specific behavior evaluated across different hardware platforms.

Conclusion

This work presents a unified round-by-round analysis of the diffusion properties of seven lightweight cipher constructions using the avalanche effect and the normalized Strict Avalanche Criterion. The results show that all evaluated constructions approach the ideal final diffusion level, while differing mainly in the number of rounds required to reach stable behavior.

ARX- and SP-based schemes generally exhibit rapid early-round diffusion owing to modular addition, substitution layers, and permutations. TEA reaches the stable diffusion interval earliest, whereas SPECK64/128, PRESENT, and FEATHER-RX stabilize after five rounds. LEA-128 and the HIGHT-style model require more rounds, while SIMON64 displays the most gradual convergence.

Despite this slower stabilization, SIMON64 likewise achieves an avalanche effect approaching the 50% benchmark by round 16. Therefore, the comparison indicates that the principal distinction among the evaluated constructions lies in diffusion speed rather than in the final avalanche level.

The results obtained for FEATHER-RX are of particular interest. Despite relying exclusively on cyclic rotations, XOR, AND, and Feistel branch exchanges, the algorithm reaches

stable diffusion at round 5 and remains near the ideal 50% mark throughout subsequent rounds. Its normalized SAC score is also slightly higher than those of the reference constructions. These findings confirm that carefully selected fixed and dynamic rotation parameters can provide effective diffusion without modular addition or substitution tables.

Overall, the main advantages of the evaluated constructions are associated with rapid diffusion development and stable near-ideal avalanche behavior, whereas their principal limitations are related to slower stabilization or less uniform early-round propagation.

Thus, the results of the study show that a high level of diffusion can be achieved not only by increasing the complexity of the internal structure of a cipher, but also through a rational combination of simple bitwise operations. The RX-based approach proves to be a promising foundation for designing new lightweight cryptographic primitives oriented toward microcontrollers, sensor networks, and Internet of Things devices.

The present findings can be applied in the development and preliminary evaluation of new encryption algorithms at the stage of round function design. In future work, the study will be extended by assessing resistance to differential and linear cryptanalysis and by examining the influence of the key schedule on the diffusion and statistical properties of FEATHER-RX.

Future work

Subsequent research will focus on analyzing the FEATHER-RX key schedule and its influence on plaintext and key avalanche behavior. Particular attention will be paid to the diffusion of round keys and to the interaction between key material and the round-by-round development of the avalanche effect in the complete encryption algorithm.

Additionally, a comprehensive cryptanalytic study of FEATHER-RX is planned. Future investigations will cover differential, linear, and rotational cryptanalysis, as well as an assessment of attacks exploiting the structural properties of RX transformations. These studies will provide a more complete evaluation of the algorithm's cryptographic security and identify directions for further optimization.

Data ethics statement

This study did not involve human participants, animals, personal data, medical records, biometric information, or restricted data sources. All experimental inputs were synthetic binary blocks generated programmatically for cryptographic diffusion analysis. Therefore, ethical approval and informed consent were not required.

Acknowledgments

The research work was funded by the Ministry of Science and Higher Education of Kazakhstan and carried out within the framework of the project BR24993052 "Development and study of cryptographic algorithms for information protection in resource-constrained systems and evaluation of their strength" at the Institute of Information and Computational Technologies.

References:

- [1] Gharat, N., & Jolly, D. (2025). A lightweight, energy-efficient modified AES algorithm for real-time IoT applications. *Indian Journal of Science and Technology*, 18, 2897–2907. <https://doi.org/10.17485/IJST/v18i35.1156>
- [2] Rana, M., Mamun, Q., & Islam, M. R. (2021). Lightweight cryptography in IoT networks: A survey. *Future Generation Computer Systems*, 129. <https://doi.org/10.1016/j.future.2021.11.011>
- [3] Easttom, C. (2022). Feistel networks. In *Modern cryptography: Applied mathematics for encryption and information security* (pp. 139–168). Springer. https://doi.org/10.1007/978-3-031-12304-7_6
- [4] Phadtare, V., & Patil, R. (2025). Distinguisher for substitution–permutation networks. *International Journal for Multidisciplinary Research*, 7. <https://doi.org/10.36948/ijfmr.2025.v07i03.44144>

- [5] Huang, M., Xu, Z., & Wang, L. (2021). On the probability and automatic search of rotational-XOR cryptanalysis on ARX ciphers. *The Computer Journal*, 65. <https://doi.org/10.1093/comjnl/bxab126>
- [6] Yang, J., Li, L., Guo, Y., & Huang, X. (2022). DULBC: A dynamic ultra-lightweight block cipher with high-throughput. *Integration*, 87, 221–230. <https://doi.org/10.1016/j.vlsi.2022.07.011>
- [7] Kapalova, N., Algazy, K., & Haumen, A. (2023). Development of a new lightweight encryption algorithm. *Eastern-European Journal of Enterprise Technologies*, 3(9(123)), 6–19. <https://doi.org/10.15587/1729-4061.2023.280055>
- [8] Pang, K., Abdul-Latip, S., Jamil, N., & Rani, H. (2025). Improved recursive construction of S-box satisfying perfect strict avalanche criterion. *Malaysian Journal of Mathematical Sciences*, 19, 933–959. <https://doi.org/10.47836/mjms.19.3.09>
- [9] Hamarsheh, M., & Salah, S. (2025). MPRESENT: A lightweight cryptographic cipher for optimizing energy efficiency in IoT applications. *Arabian Journal for Science and Engineering*. <https://doi.org/10.1007/s13369-025-10432-2>
- [10] Hediye, N., & Divakar, B. P. (2025). Design of dynamic F-function for lightweight block ciphers. *Defence Science Journal*, 75, 531–538. <https://doi.org/10.14429/dsj.20567>
- [11] Sasikala, T., & Gupta, A. (2025). Lightweight block cipher for security in resource-constrained networks. *International Journal of Electrical and Computer Engineering Systems*, 16, 507–515. <https://doi.org/10.32985/ijeces.16.7.2>
- [12] Yue, X., Li, L., Li, Q., Xiang, J., & Hu, Z. (2024). QLW: A lightweight block cipher with high diffusion. *The Journal of Supercomputing*, 81. <https://doi.org/10.1007/s11227-024-06707-4>
- [13] Mohd Esa, N., Abdul-Latip, S., & Abu, N. (2022). A new design of substitution box with ideal strict avalanche criterion. *Malaysian Journal of Mathematical Sciences*, 16, 697–715. <https://doi.org/10.47836/mjms.16.4.04>
- [14] Leurent, G., Pernot, C., & Schrottenloher, A. (2021). Clustering effect in SIMON and SIMECK. In M. Tibouchi & H. Wang (Eds.), *Advances in cryptology – ASIACRYPT 2021 (Lecture Notes in Computer Science, Vol. 13090)*. Springer. https://doi.org/10.1007/978-3-030-92062-3_10
- [15] Lu, J., Liu, G., Sun, B., Li, C., & Liu, L. (2023). Improved (related-key) differential-based neural distinguishers for SIMON and SIMECK block ciphers. *The Computer Journal*, 67. <https://doi.org/10.1093/comjnl/bxac195>
- [16] Wu, W., & Guo, M. (2024). Improved integral neural distinguisher model for lightweight cipher PRESENT. *Cybersecurity*, 7, Article 65. <https://doi.org/10.1186/s42400-024-00258-0>
- [17] Chaitanya, K., Mishra, Z., Singh, P., & Acharya, B. (2024). Flexible and area-optimised hardware architectures of LEA block cipher for IoT applications. *International Journal of High Performance Systems Architecture*, 12(1), 33–45. <https://doi.org/10.1504/IJHPSA.2024.145714>
- [18] Aguilar, J., Sierra, S., & Jacinto, E. (2015). Implementation of HIGHT encryption algorithm on microcontroller. In *Proceedings of Chilecon 2015* (pp. 937–942). <https://doi.org/10.1109/Chilecon.2015.7404685>
- [19] Hussein, N., Hoobi, M., & Sarab, S. (2025). Enhanced TEA algorithm performance using affine transformation and chaotic Arnold map. *Mesopotamian Journal of Computer Science*, 341–354. <https://doi.org/10.58496/MJCSC/2025/22>
- [20]. Vaughn, R., & Borowczak, M. (2024). Strict avalanche criterion of SHA-256 and sub-function-removed variants. *Cryptography*, 8(3), 40. <https://doi.org/10.3390/cryptography8030040>