

CLEFIA-based Lightweight Encryption for Resource-Constrained Systems: Design, Algorithms and Security Analysis

Sergiy Gnatyuk

Faculty of Computer Science and Technology, State University “Kyiv Aviation Institute”, Kyiv, Ukraine

State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv, Ukraine

E-mail: s.gnatyuk@kai.edu.ua

ORCID iD: <https://orcid.org/0000-0003-4992-0564>

Berik Akhmetov

Department of Computer Science, Yessenov University, Aktau, Kazakhstan

E-mail: berik.akhmetov@yu.edu.kz

ORCID iD: <https://orcid.org/0000-0003-2860-2188>

Dauriya Zhaxygulova*

Department of Automation and Information Technologies, Shakarim University, Semey, Kazakhstan

E-mail: d.zhaksigulova@gmail.com

ORCID iD: <https://orcid.org/0000-0002-2347-9857>

*Corresponding author

Yuliia Polishchuk

Faculty of Computer Science and Technology, State University “Kyiv Aviation Institute”, Kyiv, Ukraine

E-mail: polishchuk.yu.ya@gmail.com

ORCID iD: <https://orcid.org/0000-0002-0686-2328>

Received: 06 June 2025; Revised: 16 August 2025; Accepted: 08 October 2025; Published: 08 December 2025

Abstract: Emerging classes of distributed and embedded systems increasingly require cryptographic mechanisms that provide confidentiality, integrity, and authenticity while operating under strict limitations on computation, energy consumption, memory capacity, and communication bandwidth. Conventional symmetric and asymmetric cryptographic algorithms often fail to meet these stringent requirements. Lightweight cryptography (LWC) offers a promising solution by enabling secure real-time data transmission, command authentication, telemetry encryption, and protection of sensitive information in embedded systems. This paper presents a multicriteria analysis of widely adopted LWC algorithms, identifying the CLEFIA block cipher standardized in ISO/IEC 29192-2 as a balanced choice between security and performance. An enhanced LWC method based on the mentioned cipher is proposed, aiming to improve encryption throughput without compromising cryptographic robustness. Experimental results demonstrate that the proposed method achieves an encryption speedup over the baseline CLEFIA implementation. Furthermore, the improved algorithm successfully passes statistical randomness tests and shows increased resistance to linear and differential cryptanalysis. Notably, the cipher begins to exhibit random substitution characteristics from the third round, reinforcing its suitability for secure deployment in resource-limited environments. The results obtained in this study will be valuable for ensuring confidentiality, integrity, and authenticity in low-power and resource-constrained systems, as well as in modern information platforms where low latency is critical.

Index Terms: Encryption, LWC, CLEFIA, Security, Privacy, IoT, Embedded systems, LMS, NIST STS, Cryptanalysis, Performance, Low-resource Devices, ISO/IEC 29192-2.

1. Introduction

The rapid advances of embedded systems, the Internet of Things (IoT), autonomous sensor networks, and unmanned platforms operating in resource-constrained environments (limited processing power, energy, memory, and bandwidth) have driven the development of new cryptographic methods. Traditional cryptographic algorithms, such as AES or RSA, in their full implementations, are often too resource-intensive for devices running on 8- or 16-bit microcontrollers with only a few kilobytes of RAM and long-term autonomous power requirements. In response, a new generation of lightweight cryptographic (LWC) algorithms has emerged, designed to ensure fundamental information security principles (confidentiality, integrity, and authenticity) without imposing a significant system load [1].

LWC is critical in industries where information security must align with mobility, compact size, and long-term autonomous operation. This is particularly important in aviation and defense, where unmanned aerial vehicles (UAVs), telemetry sensors, navigation, and communication modules operate under complex conditions with a high risk of interception or signal manipulation. Beyond these domains, LWC also finds practical application in learning management systems (LMS) [2] that interact with IoT devices, mobile applications running on low-power or low-budget processors, edge nodes within university infrastructures, and platforms that rely on NFC, RFID, or hardware tokens for security and access control. In these systems, classical solutions are either impossible or impractical due to excessive energy and resource demands. LWC enables secure real-time data transmission, command authentication, telemetry encryption, and protection of confidential information in embedded computing modules. Algorithms such as Ascon, PRESENT, GIFT, Grain, and Trivium have proven effective in highly constrained environments [3-4].

As the number of connected devices continues to grow globally and smart environments (such as smart cities, smart grids, and smart aviation) expand, LWC becomes a fundamental element of cybersecurity. Its application not only protects critical infrastructure but also helps prevent new attack vectors targeting weakly protected system components. The NIST-driven standardization of LWC algorithms, including the selection of Ascon as a competition winner, confirms their global significance. When implemented in hardware, these algorithms offer scalable, cost-effective, and resilient cryptographic solutions for next-generation systems.

2. State-of-the-Art: Analysis of the Modern Cryptographic Algorithms for IoT-based Applications

Symmetric encryption algorithms [5-6] are key components in ensuring data confidentiality and integrity across various applications, including commercial, governmental, military, and embedded systems. AES (Advanced Encryption Standard) [7] is the most widely used algorithm, supporting key lengths of 128, 192, and 256 bits. It is actively used in SSL/TLS, VPNs, Wi-Fi (WPA2/3), cloud storage, and banking systems. Stream ciphers, such as ChaCha20, have gained popularity in mobile devices and modern browsers due to their high efficiency and resistance to bit-level attacks. Authenticated encryption algorithms, such as AES-GCM, are widely used to ensure both confidentiality and integrity. Military and specialized systems often employ certified variants with enhanced resistance, including protection against side-channel attacks. The choice of symmetric algorithms depends on the target environment, performance requirements, resource constraints, and threat levels, which is why modern systems often combine multiple approaches based on application context.

Asymmetric encryption algorithms [8-10] play a crucial role in secure data exchange, user authentication, digital signatures, and key management, especially in open or unstable communication channels. RSA remains widely used in SSL/TLS, VPNs, PKI systems, authentication tokens, and electronic document workflows, primarily due to its simple implementation and broad software support [11]. Elliptic Curve Cryptography (ECC), including ECDSA for digital signatures and ECDH for key exchange, provides stronger security with smaller key sizes, which is critical for mobile devices, IoT, UAVs, and embedded systems [12]. ECC has become the de facto standard in digital currencies and blockchain platforms due to its optimal balance of performance and security. Meanwhile, post-quantum asymmetric algorithms, such as Kyber, Dilithium, NTRU, and FALCON, are being actively developed to counter future quantum computing threats [13-15]. In resource-constrained environments, LWC algorithms are preferred [16]. Examples include Ascon (NIST LWC competition winner), PRESENT, GIFT, Speck, Simon, and others, which offer compact implementations and low power consumption. Notable algorithms include:

Ascon [17] is an authenticated encryption algorithm (AEAD) and hash function that was selected in 2023 as the winner of the NIST Lightweight Cryptography competition for use in resource-constrained devices. It utilizes a sponge-function-based permutation core and features a compact implementation (approximately 2,000-3,000 logic gates), providing robust security while maintaining efficiency in both software and hardware environments. Ascon supports short keys and authentication tags, making it ideal for IoT devices, sensor networks, mobile platforms, and authentication systems. Its cryptographic strength has been validated through extensive cryptanalysis, including assessments of side-channel attacks.

PRESENT [17] is a block cipher and one of the first standardized LWC algorithms (ISO/IEC 29192-2:2019). It follows an SPN (Substitution-Permutation Network) structure with a 64-bit block size and either 80- or 128-bit keys. PRESENT offers excellent hardware efficiency, with approximately 1,570 logic gates, making it suitable for RFID tags, smart cards, embedded modules, and wireless sensors. Although its software performance is limited, it remains a reliable choice when minimal code size and hardware simplicity are critical.

GIFT [18] is a LWC block cipher and the successor to PRESENT, optimized for even higher efficiency while maintaining strong cryptographic strength. The algorithm uses a novel bit permutation technique known as a *bit-sliced structure*, which significantly reduces hardware complexity (down to 700 GE), making it one of the lightest among its peers. GIFT supports a 64-bit block size and a 128-bit key, offering a modern level of security. It is actively researched in projects related to IoT, wearable devices, and distributed sensor networks, although it has not yet undergone formal standardization.

Grain-128a [19] is a stream cipher with built-in message authentication (MAC), developed as part of the eSTREAM project. It offers high processing speed, minimal latency, and reasonable hardware implementation (~3,000 GE), making it suitable for continuous data stream protection, such as in sensor networks, radio modules, or telemetry channels. Grain-128a supports a 128-bit key and features an internal shift register that generates a pseudorandom sequence, thereby complicating cryptanalysis and enhancing resistance to keystream recovery attacks.

Trivium [20] is LWC stream cipher designed for easy hardware implementation with minimal memory usage. A finalist in the eSTREAM competition, it remains popular in devices with limited computational capabilities. Trivium uses an 80-bit key and an 80-bit initialization vector (IV), generating a nonlinear output sequence through three shift registers. Thanks to its simple structure, Trivium is easily implemented on FPGA, ASIC, and microcontrollers used in IoT and real-time systems. However, its relatively short key length is considered insufficient for long-term security, which limits its application in the face of modern threats.

Simon [21] is a block cipher developed by the U.S. National Security Agency (NSA) as LWC alternative to AES. The algorithm supports variable block sizes (32–128 bits) and key lengths (64–256 bits) and uses a simple Feistel network structure, enabling efficient hardware implementation. However, Simon has faced significant criticism from the academic community due to suspected backdoors and lack of design transparency. As a result, it has not been standardized by international organizations and is not recommended for use in security-critical systems.

Speck [22] is another LWC block cipher from the NSA, optimized for software implementation in low-resource environments. It relies on simple bitwise operations (addition, shift, XOR) and achieves high performance even on low-power processors. Like Simon, it offers flexible block and key size configurations. However, due to its opaque development process and potential vulnerabilities, Speck has also not been approved by NIST or ISO, and its use is currently discouraged.

CLEFIA [23] is a block cipher developed by Sony in 2007 as an efficient solution for both hardware and software protection in resource-constrained devices. Its name is derived from the French word *clef*, meaning “key”. It uses a Feistel-type structure with a 128-bit data block and supports variable key lengths (128, 192, or 256 bits), allowing the security level to be scaled according to system requirements. In addition to high performance, CLEFIA features innovative design elements, including a dual Feistel network and an efficient key schedule, which provide strong resistance to known attacks (differential, linear, and algebraic cryptanalysis). It has been standardized under ISO/IEC 29192-2 as a recommended LWC block cipher and remains one of the most balanced options in terms of security and performance for constrained systems.

A comparative analysis of the discussed algorithms in the context of UAV, RFID, and IoT-based applications is presented in Table 1, based on the following criteria: Type (T), Block/Key Length (B/K), Hardware Complexity (HC), Performance (P), Security, Quantum Security (QS), Standardization (St), and Application Area (A).

Table 1. Comparison of modern cryptographic algorithms by various criteria

№	Cipher	T	B/K	HC	P	S	QS	St	A
1	Ascon	LWC	128/128	+	+	+	-	NIST LWC	IoT, UAV
2	PRESENT	LWC	64/80, 128	+	+/-	+/-	-	ISO/IEC	RFID
3	GIFT	LWC	64/128	+	+	+	-	-	IoT
4	Grain-128a	LWC	-/128	+	+/-	+/-	-	eSTREAM	IoT, UAV
5	Trivium	LWC	-/80	+	+	+/-	-	eSTREAM	IoT
6	Simon	LWC	32-128/64-256	+	+	-	-	-	IoT
7	Speck	LWC	32-128/64-256	+	+	-	-	-	IoT
8	CLEFIA	LWC	128/128-256	+	+	+	-	ISO/IEC	Mobile, IoT, RFID
9	AES	SKC	128/128-256	+	+	+	+/-	FIPS 197	VPN, Wi-Fi
10	RSA	PKC	1024-4096+	-	-	+	-	PKCS / X.509	PKI
11	Kyber	PQC	80-1536	+/-	+/-	+	+	NIST PQC	CIIP

The algorithms highlighted in grey in Table 1 are the most optimal for use in resource-constrained systems – this is the key conclusion of the multi-criteria analysis. However, the GIFT algorithm is not yet standardized, whereas Ascon is both standardized and the most extensively studied LWC algorithm. At the same time, CLEFIA represents an optimal compromise between security and performance, supporting longer key lengths compared to Ascon, which gives it greater flexibility and adaptability. Its effectiveness has been demonstrated in practical applications across various fields, including aviation, smart vehicles, and Industry 4.0 systems [24-26].

3. Problem Statement

The CLEFIA algorithm [23], despite its efficiency and standardization (ISO/IEC 29192-2), requires further research and improvement for several key reasons:

- **Architecture complexity** – CLEFIA's structure is more complex than most other LWC block ciphers, which complicates analysis, optimization, and formal verification of its resistance to modern attacks (including differential, algebraic, side-channel, and fault-injection attacks). Unlike newer competitors such as Ascon or GIFT, CLEFIA was developed before the surge in side-channel attacks, and its defenses against SCA, DPA, and CPA require reconsideration and improvement – especially in the context of IoT and embedded systems.
- **Hardware efficiency gap** – Although CLEFIA has a relatively modest hardware footprint (~3,500 GE), there are other algorithms with even smaller footprints and better performance, particularly for ultra-low-power applications. This highlights the need to optimize CLEFIA for modern platforms (e.g., FPGA, ASIC, RISC-V), particularly in multi-core systems or power-constrained environments such as UAVs and RFID.
- **Limited adoption** – CLEFIA has seen limited real-world deployment, which restricts the amount of independent cryptanalysis and integration into contemporary security protocols. Unlike AES or Ascon, CLEFIA is still not part of mainstream cryptographic libraries (e.g., OpenSSL, libsodium), and thus lacks broad validation in open information and communication systems.

In summary, while CLEFIA has strong potential as a secure and well-balanced lightweight cipher, it requires further analysis, adaptation to modern security requirements, and optimization for implementation in the context of embedded, autonomous, and post-quantum systems. Therefore, the goal of this study is to improve the CLEFIA algorithm by increasing the speed of cryptographic transformations while maintaining an adequate level of cryptographic strength.

4. Algorithm CELFIA Analysis

4.1. Encryption

The cipher is based on a generalized Feistel structure, where a 128-bit data block is divided into four 32-bit sub-blocks (denoted as P_0, P_1, P_2, P_3). These sub-blocks undergo 18, 22, or 26 rounds of transformation, depending on the key length. The key length can be 128, 192, or 256 bits. The encryption procedure's structure is illustrated in Figure 1.

Description of the Encryption Procedure:

- Before the first round, partial input whitening is performed – subkey WK_0 is XOR with block P_1 , and subkey WK_1 is XOR with block P_3 : $P_1 = P_1 \text{ XOR } WK_0$; $P_3 = P_3 \text{ XOR } WK_1$;
- In i round ($i = 1, r$) performing the next step:
 - Block P_0 is passed through function F_0 : $P'_0 = F_0(P_0)$;
 - Block P'_0 is passed through block P_1 by operation XOR: $P_1 = P'_0 \text{ XOR } P_1$;
 - Block P_2 is passed through function F_1 : $P'_2 = F_1(P_2)$;
 - Block P'_2 is XOR with block P_3 : $P_3 = P'_2 \text{ XOR } P_3$;
- At the end of each round (except the last), the blocks are rotated as follows: P_0 to P_3 , P_1 to P_0 , P_2 to P_1 , P_3 to P_2 : $(P_0, P_1, P_2, P_3) = (P_1, P_2, P_3, P_0)$.
- After the final round, output whitening is performed, similar to the initial step, using subkeys WK_2 and WK_3 : $P_1 = P_1 \text{ XOR } WK_2$; $P_3 = P_3 \text{ XOR } WK_3$.

4.2. Function F_0 and F_1

The round function of CLEFIA is based on two distinct functions – F_0 and F_1 . Functions F_0 and F_1 follow an SP structure (Substitution–Permutation network).

The advantage of the SP structure is that data processing consists of substitutions and permutations, which are key-dependent. Repeated use of these transformations ensures two essential properties of a secure cipher: diffusion and confusion.

A distinctive feature of CLEFIA's new design approach is that its F-functions utilize the dual substitution-multiplexing (DSM) mechanism, which involves using different diffusion matrices and two separate S-boxes to provide stronger immunity against specific classes of attacks. As a result, the required number of rounds can be reduced. Furthermore, the two S-boxes are based on different algebraic structures, which are expected to enhance the algorithm's algebraic resistance.

The F_0 function processes a 32-bit input block by performing the following steps (see Figure 2):

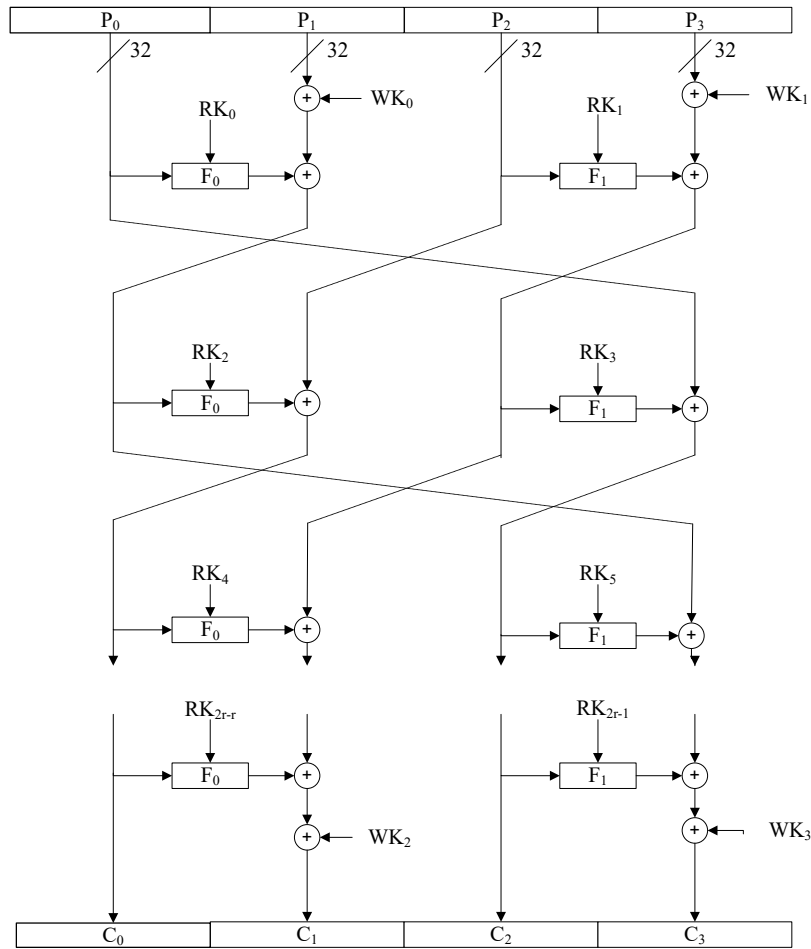
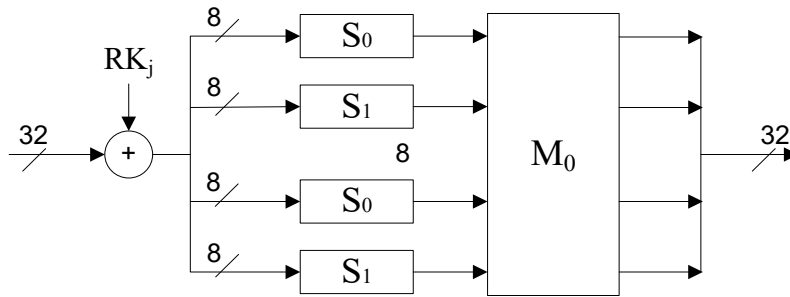


Fig.1. Structure of the encryption process in the CLEFIA cryptographic


 Fig.2. Function F_0 of the CLEFIA algorithm

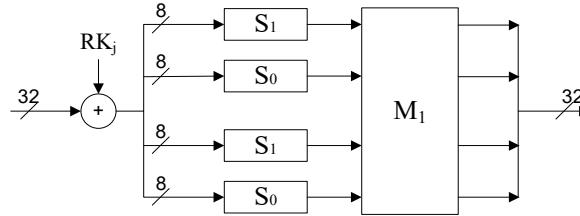
- A 32-bit subkey RK_j is applied to the block using the XOR: $P = P \oplus RK_j$;
- The block is then divided into four 8-bit fragments.
- These fragments are passed through two 8×8 bit S_0 and S_1 . The input/output values for each S-box are provided in [27]. All values in the S-boxes are expressed in hexadecimal format. For an 8-bit S-box input, the upper 4 bits specify the row, and the lower 4 bits specify the column. The input/output values for each S-block are shown in [27].
- The substitution result is multiplied by a fixed matrix M_0 . This multiplication is performed in the finite field $GF(2^8)$ where the defining polynomial is: $z^8 + z^4 + z^3 + 1$.

The matrix M_0 is defined in Table 2 (values are given in hexadecimal).

Table 2. The hexadecimal presentation of the matrix M_0 in the context of realisation F_0

0x01	0x02	0x04	0x06
0x02	0x01	0x06	0x04
0x04	0x06	0x01	0x02
0x06	0x04	0x02	0x01

The F_1 function processes a 32-bit input block by performing the following steps (Figure 3):

Fig.3. Function F_1 of the CLEFIA algorithm

- A 32-bit subkey RK_j is applied to the block using the XOR operation: $P = P \text{ XOR } RK_j$;
- The block is then divided into four 8-bit fragments.
- These fragments are passed through two 8×8 bit substitution boxes S_0 and S_1 . The input/output values for each S-box are provided in [27]. All values in the tables are expressed in hexadecimal format. For an 8-bit S-box input, the upper 4 bits determine the row, and the lower 4 bits determine the column.
- The result of the substitution is multiplied by a fixed M_1 . This multiplication is performed in the finite field $GF(2^8)$ defined by the polynomial: $z^8 + z^4 + z^3 + 1$

The matrix M_1 is defined in Table 3 (values are given in hexadecimal format).

Table 3. The hexadecimal presentation of the matrix M_1 in the context of realisation F_1

0x01	0x08	0x02	0x0a
0x08	0x01	0x0a	0x02
0x02	0x0a	0x01	0x08
0x0a	0x02	0x08	0x01

4.3. Secret Key Expansion Procedure

The CLEFIA algorithm supports 128-, 192-, and 256-bit secret keys. Based on the input secret key, this procedure generates both the whitening keys WK_i ($0 \leq i < 4$) and the round keys RK_j ($0 \leq j < 2r$). The key expansion structure follows the same design as the data processing part of the algorithm, meaning it also uses a generalized Feistel structure.

4.4. Advantages and Disadvantages of CLEFIA

Based on security evaluations, the full-round version of CLEFIA is considered a secure block cipher against all known types of attacks. Various attacks have been studied in relation to CLEFIA, including linear and differential cryptanalysis, impossible differential attacks, and the square attack. Among these, the impossible differential attack has proven to be the most effective.

Table 4 presents data on CLEFIA's resistance to specific types of attacks.

Table 4. CLEFIA's resistance to specific attacks

Attack	Rounds	Data Vol, B	Time, s	Essence of the Attack
Integral attack on CLEFIA 128/192/256	12	2^{113}	$2^{116,7}$	The goal is to predict byte sum values after a certain number of encryption rounds
Integral attack on CLEFIA 192/256	13	2^{113}	$2^{180,5}$	
Integral attack on CLEFIA 256	14	2^{113}	$2^{244,5}$	
Impossible differential attack on CLEFIA 128	12	$2^{118,9}$	2^{119}	An attack implemented using a 9-round impossible differential.
Impossible differential attack on CLEFIA 192	13	$2^{119,8}$	2^{147}	
Impossible differential attack on CLEFIA 256	14	$2^{120,3}$	2^{211}	

Based on the reviewed scientific literature [23-28], the following advantages and disadvantages of the CLEFIA algorithm can be identified. Advantages of CLEFIA include: 1) High level of security – full-round CLEFIA is resistant to all known attacks; 2) Low memory requirements; 3) Efficient hardware implementation in resource-constrained

environments; 4) Encryption and decryption processes are practically identical. Disadvantage of CLEFIA: in software implementations, encryption speed is lower compared to modern lightweight algorithms.

Considering all the aforementioned advantages of the CLEFIA algorithm, as summarized in Table 1 and Table 4, this LWC algorithm has been selected as the baseline for developing a method that ensures confidentiality, integrity, and authenticity in resource-constrained environments.

5. Improved Methods of LWC Algorithms Construction

5.1. Method Description

Since this method is derived from the original CLEFIA cipher [23], it preserves its core structural principles. Nevertheless, several substantial and conceptually significant modifications were introduced, including the following (all modification will be clarified in the next subsections of Section 5):

- Support for increased input data block length;
- Full initial and final whitening of the data block (not partial);
- Use of dynamically changing substitution tables in the F_0 and F_1 functions;
- Modified linear diffusion operation;
- Reworked secret key expansion procedure;
- Reduced number of encryption rounds;
- Introduction of additional operations in each round.

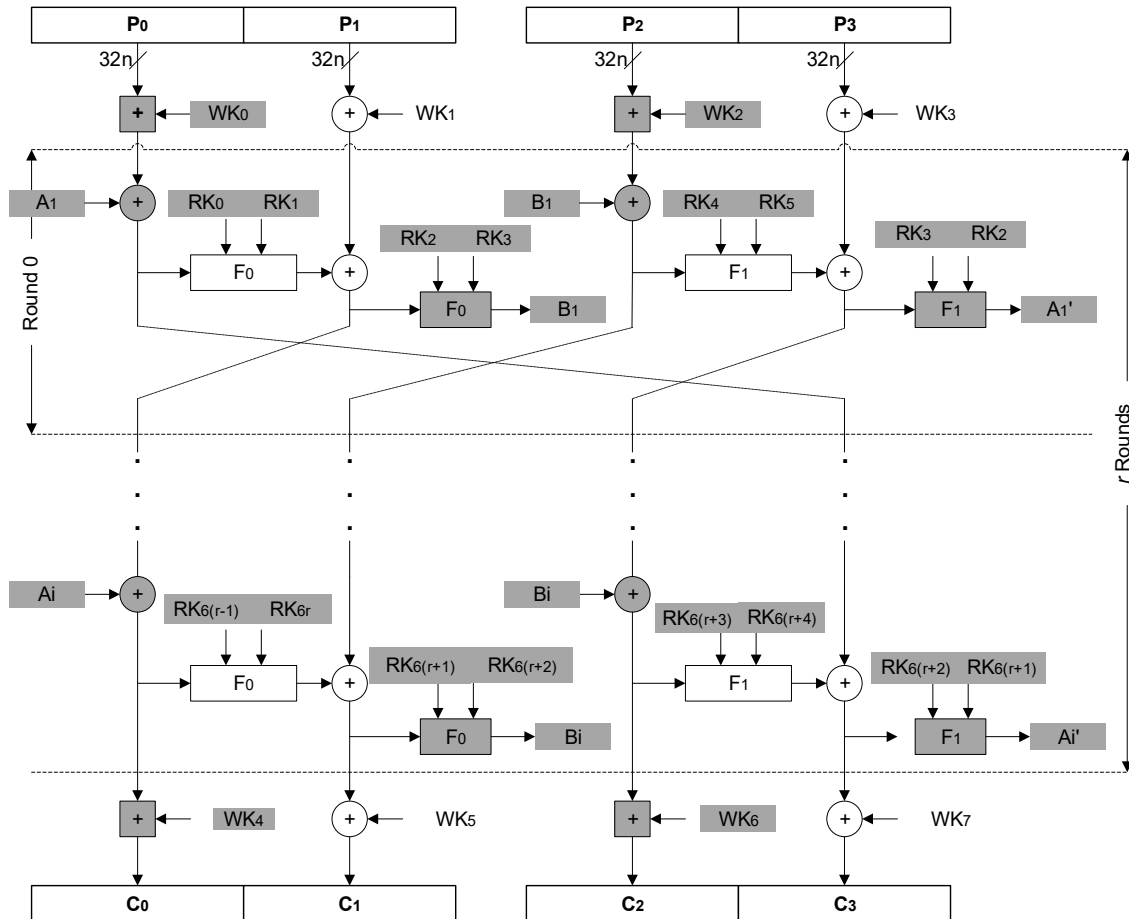


Fig.4. Encryption structure of the improved cryptographic algorithm (all parameters were clarified in Section 5.2)

5.2. Encryption

The method is based on a generalized Feistel structure, where a $128n$ -bit data block ($n \geq 1$) is divided into four $32n$ -bit sub-blocks (denoted as P_0, P_1, P_2, P_3). The key length can vary as $k = 128l$, $k = 256l$, $k = 512l$ bits. Depending on the key length, the number of transformation rounds is defined as: $(r = \max(13, \frac{k}{16}))$.

The structural diagram of the method is shown in Figure 4.

Encryption Procedure Description:

- Before the first round, full input whitening is applied: subkey WK_0 is added to block P_0 , using the «+» operation, subkey WK_1 is XORed with block P_1 , subkey WK_2 is added to block P_2 using the «+» operation, subkey WK_3 is XORed with block P_3 : $P_0 = P_0 + WK_0$; $P_1 = P_1 \text{ XOR } WK_1$; $P_2 = P_2 + WK_2$; $P_3 = P_3 \text{ XOR } WK_3$.
- In the i -th round ($i = 1, r$) the following operations are performed:
 - Temporary value A_1 is XORed with block P_0 : $P_0 = P_0 \text{ XOR } A_1$;
 - Block P_0 is passed through the function F_0 : $P'_0 = F_0(P_0)$;
 - The result P'_0 is XORed with block P_1 : $P_1 = P'_0 \text{ XOR } P_1$;
 - Block P_1 is passed through the function F_0 to produce the variable B_1 : $B_1 = F_0(P_1)$;
 - Variable B_1 is XORed with block P_2 : $P_2 = P_2 \text{ XOR } B_1$;
 - Block P_2 is passed through the function F_1 : $P'_2 = F_1(P_2)$;
 - The result P'_2 is XORed with block P_3 : $P_3 = P'_2 \text{ XOR } P_3$;
 - Block P_3 is passed through the function F_1 to obtain the variable A'_1 : $A'_1 = F_1(P_3)$;
 - At the end of each round (except the last), the blocks are rotated as follows: P_0 to P_3 , P_1 to P_0 , P_2 to P_1 , P_3 to P_2 : $(P_0, P_1, P_2, P_3) = (P_1, P_2, P_3, P_0)$.
- After the final round, output whitening is performed similar to the initial whitening step, using subkeys WK_4, WK_5, WK_6 and WK_7 : $P_0 = P_0 + WK_4$; $P_1 = P_1 \text{ XOR } WK_5$; $P_2 = P_2 + WK_6$; $P_3 = P_3 \text{ XOR } WK_7$.

5.3. Functions F_0 and F_1

The round function in the proposed method is based on two distinct functions: F_0 and F_1 . Both follow an SP-structure. These functions use dynamically changing substitution tables to provide stronger resistance against specific classes of attacks and to reduce the total number of rounds. Additionally, the S-boxes are built on different algebraic structures, which are expected to increase algebraic robustness.

Function F_0 processes a $32n$ -bit input block through the following steps (see Figure 5):

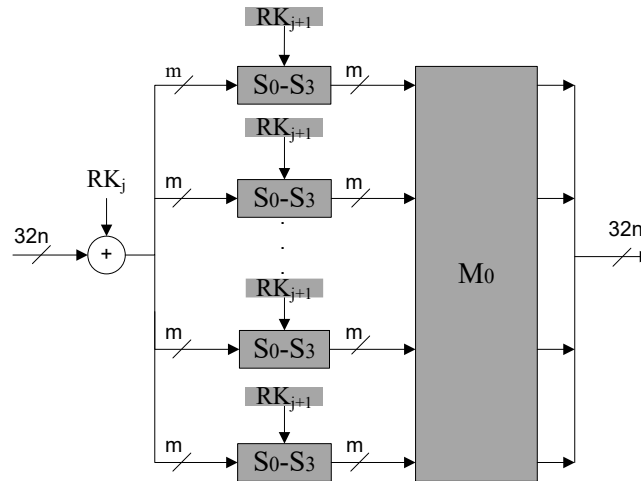


Fig.5. Scheme of function F_0 realisation

- A $32n$ -bit round key RK_j is applied using the XOR operation: $P = P \text{ XOR } RK_j$;
- The block is divided into fragments of length m ($m = 8w, w \in N$). The number of fragments is calculated as: $c = \frac{32n}{m}$;
- Each fragment passes through a set of substitution tables: S_0, S_1, S_2 and S_3 . The choice of S-box depends on the value of the $32n$ -bit round key RK_j .
- The substitution result is multiplied by matrix M_0 . The multiplication is carried out in the finite field $GF(2)$.

Function F_1 processes a $32n$ -bit input block using the same steps as described above, but with different keys and using matrix M_1 instead of M_0 . The multiplication is performed in the finite field $GF(2)$.

6. Experiments

6.1. Speed Analysis

The main objective was to investigate the performance characteristics of the Improved LWC method based on the CLEFIA and compare it with the original CLEFIA. For the experimental study, various hardware platforms (workstations,

WS) were used (WS1: Intel Pentium 4 (2.8 GHz, single-core) with 512 MB DDR of RAM, WS2: Intel Pentium 4 HT (3.0 GHz, single-core / HT) with 1 GB DDR2 of RAM, WS3: Intel Core 2 Duo E7400 / E8400 (dual-core, 2.4–3.0 GHz) with 2 GB DDR3 of RAM, and WS4: Intel Celeron N5100 (quad-core) with 4 GB DDR4 of RAM).

Object of study: The process of cryptographic transformation of information.

Input data: File to be encrypted, encryption key.

Output data: Encryption/decryption speed of the file.

The experiment is conducted using C++ developed software implementations of original CLEFIA and the improved CLEFIA. The results are recorded in Table 5, which will be presented in the next section.

6.2. Security Analysis

The main objectives was to investigate the statistical cryptographic strength characteristics of the Improved LWC method based on the CLEFIA algorithm. Two steps include evaluating the statistical characteristics of the cryptographic strength of the improved CLEFIA algorithm using the NIST STS, as well as assessing the statistical properties of the key expansion method of the improved CLEFIA algorithm using the NIST STS technique.

Object of study: The process of information cryptographic protection.

Input data: Encrypted file (12 MB); Length of the tested sequence; Number of tested sequences; File containing the sequence of generated round keys

Output data: Pass rates for 189 tests.

The experiment is conducted using the console version of the NIST STS application.

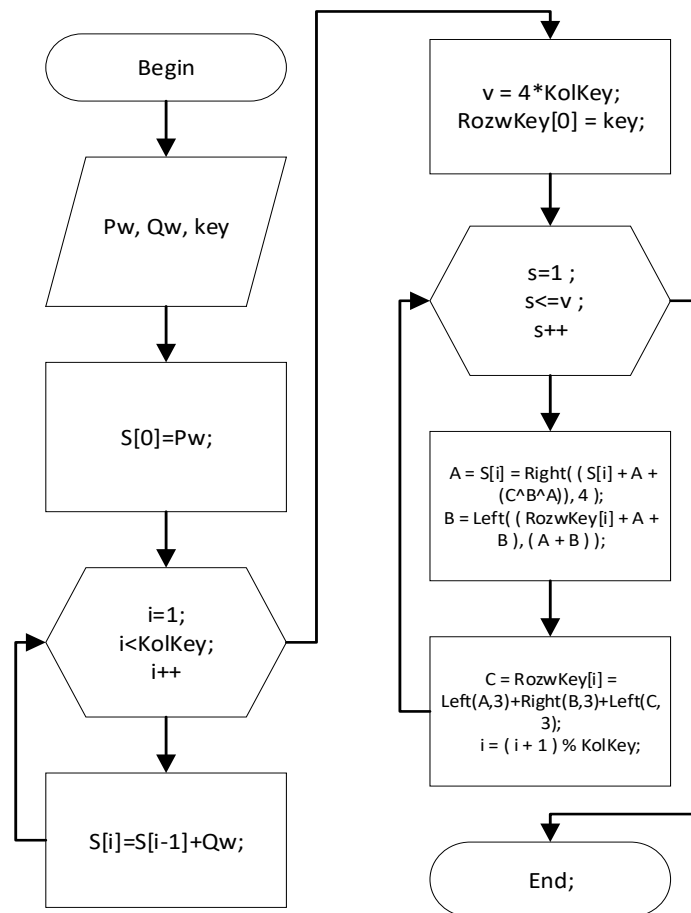


Fig.6. Block diagram of the round key generation algorithm *KeyGen*

6.3. Algorithm and Software Tools

The input data for the software implementation of the improved CLEFIA cryptographic algorithm consists of a file to be encrypted or decrypted, along with a 16-character (128-bit) key. The core of the program consists of three main functions: *KeyGen(kq)* – for generating round keys; *Encryption(FileEnc1, FileDec1)* – for encryption; *Decryption(FileDec2, FileEnc2)* – for decryption

Round Keys Formation

To generate the round subkeys from the original base key, a key expansion procedure is used. The improved CLEFIA cryptographic algorithm requires 50 subkeys, each 32 bits long. The first and last 4 keys are used for whitening operations. Another 14 keys are used to select S-boxes in each round. The remaining 28 subkeys participate in cyclic transformations.

Initially, two pseudorandom constants are generated. These are used to form an array of 50 elements. Based on this array, round keys are generated using chaining mode with the previous values and several other operations. The block diagram of the round key generation algorithm from the base key is shown in Figure 6.

Encryption

The encryption algorithm is an iterative (cyclic) procedure consisting of initial and final whitening, as well as cyclic data transformation. The block diagram of the algorithm is shown in Figure 7.

The input parameters for the Encryption function are the names of two files – one for the plaintext and one for the ciphertext. Data is read in 32-bit blocks and immediately split into four parts (A, B, C, D) of 1 byte each. Before the first round, whitening is performed using a set of expanded keys. The block diagram of the whitening function is shown in Figure 8.

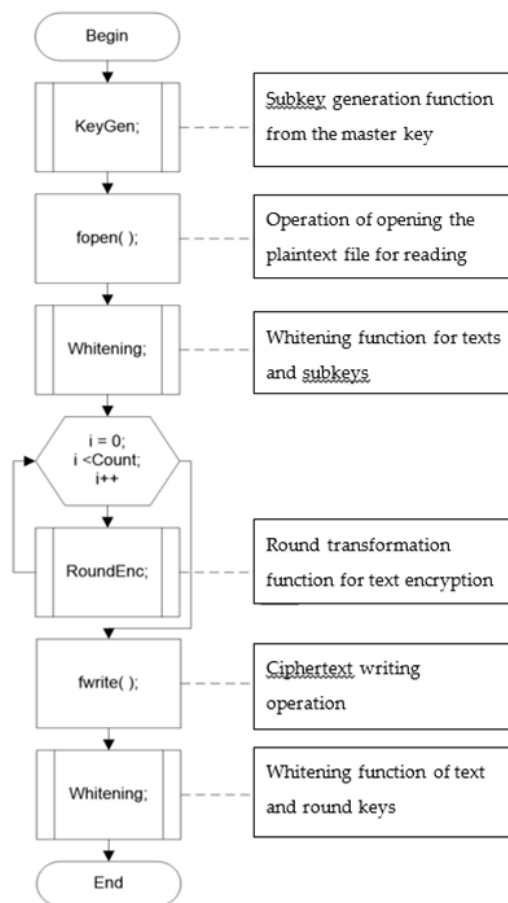


Fig.7. Block diagram of the application algorithm in encryption mode (for the proposed crypto algorithm)

In each round, block A and block B are simply shifted to the right by 64 bits. The remaining blocks require a more detailed description:

- Additional round keys are used to select 2 S-boxes based on a certain scheme.
- Block A and block B pass through the selected substitution tables.
- The outputs of both S-boxes are combined into a single 64-bit sequence, forming a vector of eight characters.
- A fixed extended matrix M of size 8×8 is multiplied by the formed vector. Calculations are carried out in Galois Field $GF(2)^8$ using an irreducible polynomial: $x^8 + x^6 + x^5 + x^3 + 1$.
- The output sequence is then split again into two 32-bit blocks and added modulo 2 to the corresponding round keys.
- The first sequence is added modulo 2 to block C and then cyclically shifted 1 bit to the right. This forms the sequence for the next round of block A.

- The other 32 bits are added modulo 2 to block D (which is cyclically shifted 1 bit to the left), forming the sequence for the next round of block B.

The block diagram of the text round transformation function is shown in Figure 9.

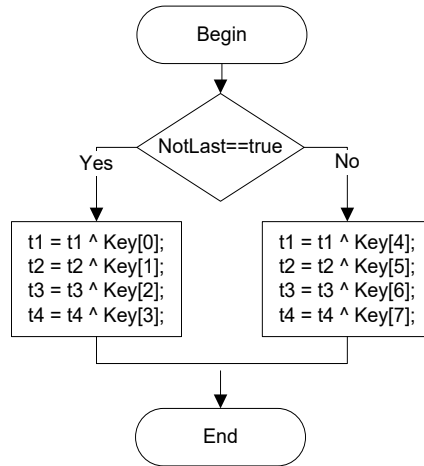


Fig.8. Block diagram of the Whitening function during encryption (for the proposed crypto algorithm)

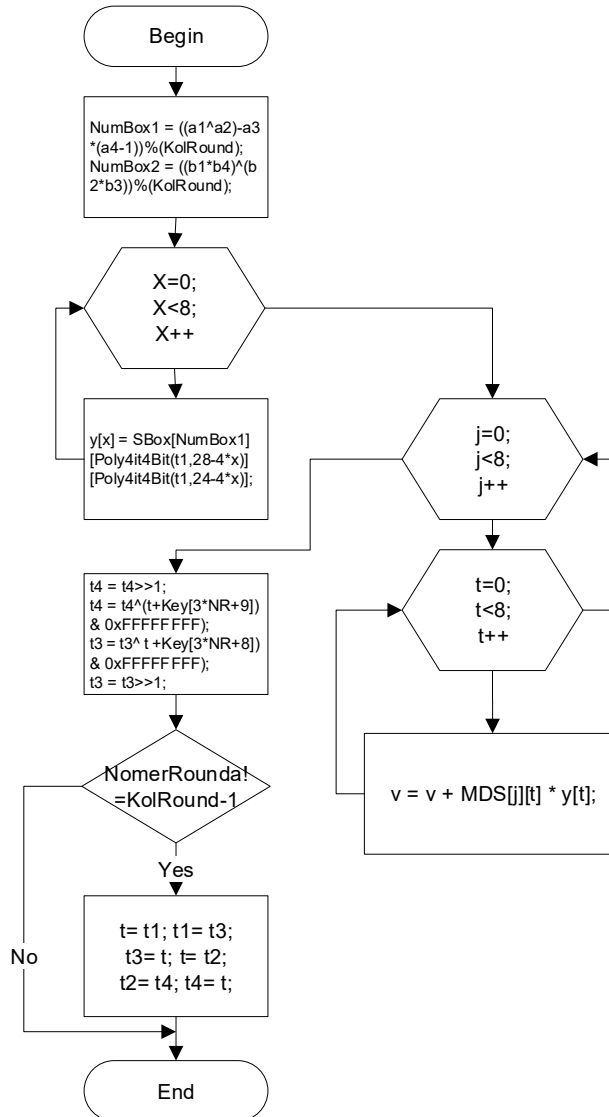


Fig.9. Block diagram of the *RoundEnc* function algorithm (for the proposed crypto algorithm)

Decryption

Given that the encryption algorithm is partially based on elements of a Feistel network, it also has the characteristic that the same sequence of operations is used for both encryption and decryption. Therefore, the decryption process is identical to the encryption process. The only exception is the direction of the cyclic shifts, which are reversed.

7. Results and Discussion

7.1. Performance Analysis: Quantitative Parameters and Comparison

To confirm that the stated objective was achieved, a comparative speed test was conducted between the software implementations of the CLEFIA cryptographic algorithm and the Improved LWC method based on the CLEFIA algorithm. The testing was conducted on four workstations with varying specifications (WS1-WS4). The results of the encryption and decryption speed trials are presented in Table 5.

Table 5. Results of speed testing

Size of file, MB	Time of performance for the CLEFIA, s				Time of performance for the Improved LWC, s			
	WS1	WS 2	WS 3	WS 4	WS 1	WS 2	WS 3	WS 4
1	3,466	4,341	1,062	0,862	0,692	0,764	0,238	0,195
10	31,423	41,633	11,134	7,377	6,73	7,254	2,302	1,854
100	296, 98	399,211	102,46	63,946	65,962	83,461	22,662	18,410
1000	2703,4	3801, 64	1204,368	578,362	601,439	737,45	244,174	167,843

The average speed of the CLEFIA algorithm was 0.77 MB/s, while the speed of the Improved LWC method based on CLEFIA reached 3.18 MB/s. Thus, the developed cryptographic algorithm outperformed the original prototype by a factor of 4.12 in terms of data encryption speed.

7.2. Security Analysis: Statistical Testing

Most modern analytical attacks, primarily linear and differential cryptanalysis, are statistical in nature. During cryptanalysis, a large number of encryption operations are performed, and based on the ciphertexts, possible round key variants are generated. When analysing a sufficiently large sample of ciphertexts produced using the same key, the correct value of certain key bits occurs more frequently than other options.

Clearly, the probability of finding the correct pair that yields a specific key value depends on the statistical properties of the cipher. To increase the complexity of cryptanalysis, the properties of the ciphertext should closely resemble those of a random sequence. Therefore, a necessary (though not sufficient) condition for a cipher's resistance to analytical attacks is ensuring good statistical characteristics of the output sequence (ciphertexts).

To verify the statistical characteristics of the Improved LWC method based on the CLEFIA algorithm, tests were conducted in accordance with the NIST SP 800-22 methodology. The software implementation of the algorithm in cipher block chaining (CBC) mode was subjected to statistical testing using the NIST STS technique.

The following parameters were selected for testing:

- Length of the tested sequence – $n=10^6$ bit;
- Number of tested sequences – $m=100$;
- Significance level $\alpha=0.01$.

Thus, the total volume of the tested sample was $N = 100 \times 10^6$ bits; The number of tests q for different lengths was $q = 189$. Therefore, the statistical profile of the generator includes 18,900 probability values P .

In the ideal case, with the given parameters, only one sequence out of one hundred should be rejected during testing – that is, the passing rate for each test should be 99%. However, such a restriction is considered too strict, so the confidence interval rule based on the value r_k is applied instead. In this case, the lower bound is $r_{min} = 0.96015$. Using this threshold, the results of the testing were analysed for both the encryption algorithm and the key expansion algorithm. The test results based on the ciphertext are shown in Table 6.

Table 6. Results of NIST test pass rates for ciphertexts of the two ciphers

Generator / Cipher	Number of tests in which more than 99% of sequences passed	Number of tests in which more than 96% of sequences passed	Number of tests in which the value of $P < 0,001$	Number of tests in which the value of $P < 0,01$
CLEFIA	134 (71%)	189 (100%)	132 (70%)	189 (100%)
Improved LWC	146 (77.2%)	189 (100%)	140 (74%)	189 (100%)

The diagram of the distribution of coefficients (statistical profile) of ciphertext test passing depending on the test number is shown in Figure 10.

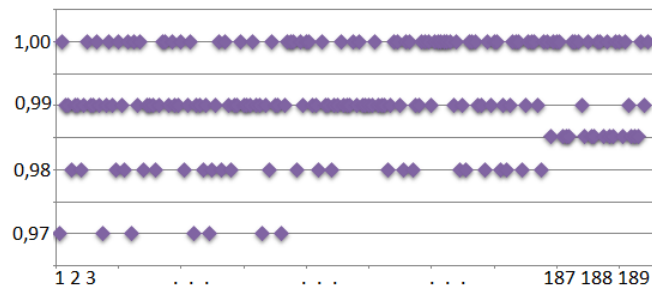


Fig.10. Statistical profile of the Improved LWC method based on CLEFIA passing NIST STS tests

The obtained p-values for all NIST STS tests lie in the range 0.97-1.00, significantly exceeding the standard significance threshold of 0.01. This indicates (Figure 1) that the output sequence demonstrates no statistically detectable deviations from randomness, and therefore passes the entire NIST STS. The concentration of p-values near the upper boundary of the interval is consistent with the behavior of high-entropy cryptographic primitives.

The results of the test with round keys are presented in Table 7.

Table 7. NIST test results for round keys of two ciphers

Generator / Cipher	Number of tests in which more than 99% of sequences passed	Number of tests in which more than 96% of sequences passed	Number of tests in which the value of $P < 0,001$	Number of tests in which the value of $P < 0,01$
CLEFIA	130 (68,7%)	189 (100%)	122 (64,5%)	189 (100%)
Improved LWC	141 (74%)	189 (100%)	136 (72%)	189 (100%)

The distribution diagram of the pass rate coefficients of the round keys depending on the test number is shown in Figure 11.

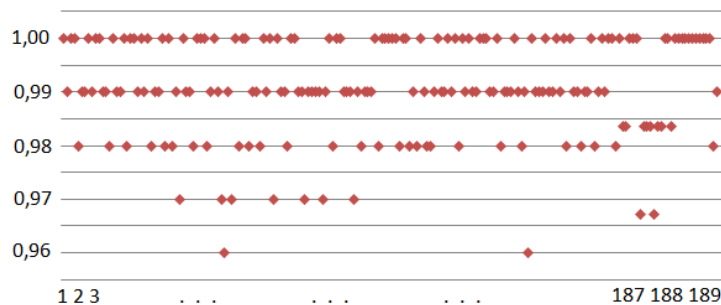


Fig.11. Statistical portrait of the pass rate of the keys of the Improved LWC method based on CLEFIA in NIST STS tests

The second dataset (Figure 11) also passes the entire NIST STS, with all p-values lying in the range 0.96-1.00, significantly exceeding the threshold of 0.01. The distribution of p-values demonstrates a slightly wider spread compared to the first dataset, which corresponds to natural statistical variability and indicates no detectable deviation from randomness. Thus, the analysed sequence can be considered statistically random according to NIST STS criteria.

7.3. Security Analysis: Linear and Differential Characteristics Study

The experiment aims, on the one hand, to use the results of analysing reduced versions of large ciphers to estimate the expected indicators of their full-scale resistance, and on the other hand, to determine the cipher's resistance to differential and linear cryptanalysis. The latter is based on the fact that all such ciphers, after a certain number of rounds – regardless of the specific S-boxes used – begin to exhibit the properties of a random permutation. This holds true in terms of combinatorial metrics, the distribution laws of transitions in XOR difference tables, and the distribution patterns in the linear approximation tables. In essence, their behaviour approximates that of a truly random substitution. The security assessment of the developed block cipher was carried out by estimating its expected resistance indicators to differential and linear cryptanalysis of full-scale ciphers, based on the analysis results of their reduced versions.

The calculated ratios for determining the values of full differentials and the maximum values of linear approximation biases were obtained by applying formulas (1) and (2), which are valid for random substitutions, to ciphers considered as random permutations.

$$DP^f(\Delta x \rightarrow \Delta y) = \frac{|\{x \in GF(2)^n \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}|}{2^n} \quad (1)$$

$$LP^f(\Gamma x \rightarrow \Gamma y) = \left(\frac{|\{x \in GF(2)^n \mid (x * \Gamma x) = f(x) * \Gamma y\}|}{2^{n-1}} - 1 \right)^2 \quad (2)$$

where $\Delta x, \Delta y$ are the input and output differences; $\Gamma x, \Gamma y$ – are the input and output masks; $x * \Gamma x$ – denotes the scalar product of x and Γx ; $f(x) * \Gamma y$ – is the result of the scalar product of $f(x)$ and Γy .

The maximum values of differential and linear probabilities for the key-dependent function f are defined by the following formulas (3) and (4):

$$DP_{max}^f = \max_{\Delta x \neq 0, \Delta y} DP^f(\Delta x \rightarrow \Delta y) \quad (3)$$

$$LP_{max}^f = \max_{\Gamma x, \Gamma y \neq 0} LP^f(\Gamma x \rightarrow \Gamma y). \quad (4)$$

The average differential probability (ADP) of the function $f[k](x)$:

$$ADP^f = \text{ave}_k DP^{f[k]}(\Delta x \rightarrow \Delta y). \quad (5)$$

The average linear hull probability (ALHP) of the function $f[k](x)$:

$$ALHP^f = \text{ave}_k LP^{f[k]}(\Gamma x \rightarrow \Gamma y). \quad (6)$$

The average (over a set of 2^h keys) value of the maximum differential probabilities (AMDP) of the key-dependent function $f[k](x)$:

$$AMDP^f = \text{ave}_k DP_{max}^{f[k]}(\Delta x \rightarrow \Delta y) = \frac{1}{2^h} \sum_{k=1}^{2^h} DP_{max}^{f[k]}. \quad (7)$$

The average (over a set of 2^h keys) value of the maximum differential probabilities (AMLHP) of the key-dependent function $f[k](x)$:

$$AMLHP^f = \text{ave}_k LP_{max}^{f[k]}(\Gamma x \rightarrow \Gamma y) = \frac{1}{2^h} \sum_{k=1}^{2^h} LP_{max}^{f[k]} \quad (8)$$

Root means square value of the maximum differential probabilities ($\sigma(DP)$) of the key-dependent function $f[k](x)$:

$$\sigma(DP) = \sqrt{\frac{1}{h} \sum_{i=1}^h (AMDP_i - \overline{AMDP})^2} \quad (9)$$

where $AMDP_i$ is the i -th value of the maximum differential probabilities; $\overline{AMDP}$ is the arithmetic mean of the $AMDP$ sample; h is the number of rounds.

Root mean square value of the max linear probabilities ($\sigma(LP)$) of linear hulls for the key-dependent function $f[k](x)$:

$$\sigma(LP) = \sqrt{\frac{1}{h} \sum_{i=1}^h (AMLHP_i - \overline{AMLHP})^2} \quad (10)$$

where $AMLHP_i$ is the i -th value of the maximum differential probabilities; $\overline{AMLHP}$ is the arithmetic mean of the $AMLHP$ sample; h is the number of rounds

During the experiments, encryption of 16-bit data blocks was performed using 10 randomly selected keys on mini-versions of the ciphers.

The mini-version of the developed algorithm differs from the original in the following features:

- The input block size is 16 bits;
- Each sub-block (A, B, C, D) is 4 bits;
- Sub-block A is cyclically shifted by 2 bits, instead of 16;
- After concatenating vectors A and B, a table substitution (S-box) of size 4×4 bits is applied;
- Multiplication with the maximum distance separable (MDS) matrix D is done over a field of 4×4 bits;
- The size of the input key is 16 bits;
- The size of the expanded round keys is also 16 bits.

The obtained results were averaged over this number of keys and are presented in Table 8 and Table 9.

Table 8 presents the absolute values of the maximum full differentials (AMDP) for the Improved LWC cipher, along with the root mean square deviations $\sigma(DP)$.

Table 8. Per-round values of max full differentials during encryption of 16-bit blocks using the mini-version of the developed crypto algorithm

Number of Rounds (r)	Max full differentials	Root Mean Square Deviation
1	65536	0
2	3352,23	$\pm 630,312$
3	19,0333	$\pm 1,536$
4	19,0333	$\pm 0,99777$
5	18,8333	$\pm 1,23104$
6	19,1332	$\pm 0,99106$
7	19,2333	$\pm 1,0935$
8	19,1332	$\pm 1,531395$
9	19,0333	$\pm 1,23654$
10	19,3333	$\pm 1,2995$
11	19.4	$\pm 1, 575222$
12	18,8333	$\pm 0,991072$
13	18,8333	$\pm 0,991072$
14	18.9332	$\pm 1,123546$

Table 9 presents the absolute values of the maximum linear hull biases (AMLHP) for the Improved LWC cipher, along with the root mean square deviations $\sigma(LP)$.

Table 9. Per-round values of maximum linear hull biases during encryption of 16-bit blocks using the mini-version of the developed crypto algorithm

Number of Rounds (r)	Maximum Value of Linear Hull Bias	Root Mean Square Deviation
1	0	0
2	8282.27	± 557.454
3	818.267	± 25.8819
4	815	± 28.214
5	818.5	± 18.535
6	815.967	± 21.18
7	831.1	± 33.1887
8	823.143	± 23.5722
9	825.9	± 33.5741
10	827.2	± 25.2885
11	815.6	± 22.3138
12	819	± 27.1125
13	822.5	± 23.7715
14	821.2	± 22.553

The presented results indicate that the Improved LWC method based on CLEFIA, in terms of its differential and linear characteristics, begins to exhibit the properties of random permutations starting from the third round.

8. Conclusions

The analysis of LWC algorithms was conducted in the context of their application in resource-constrained systems, using the following criteria: Type, Block/Key Length, Hardware Complexity, Performance, Security, Quantum Security, Standardization, and Application Area. The analysis identified CLEFIA as an optimal compromise between security and performance. Unlike Ascon, CLEFIA supports longer keys, providing greater flexibility and adaptability, and its effectiveness has been validated in various practical domains. However, despite international standard ISO/IEC 29192-2, CLEFIA still has certain drawbacks – namely, a complex architecture, moderate hardware complexity, and a lack of widespread adoption – indicating the need for further research and refinement.

An Improved LWC method based on CLEFIA was developed, aiming to enhance encryption speed while maintaining sufficient cryptographic strength. The key differences between the improved version and the original algorithm include: support for increased input block sizes; full initial and final whitening of the data block (not partial); use of dynamically changing substitution tables in the round functions F_0 and F_1 a modified linear diffusion operation; a

redesigned key expansion procedure, a reduced number of rounds; additional operations introduced in each round.

Performance evaluations showed that the Improved LWC method based on CLEFIA achieved, on average, 4.12 times higher encryption speed compared to the original. Security analysis focused on two key aspects. Based on the results, the software implementation of the Improved CLEFIA in counter mode, as well as the base key expansion method, successfully passed comprehensive testing using the NIST STS technique.

The statistical evaluation of the generated sequences using the NIST STS demonstrated consistently high p-values across all tests, with all results significantly exceeding the 0.01 significance threshold. Both analyzed datasets exhibited p-values within the ranges 0.97-1.00 and 0.96-1.00, indicating complete compliance with the criteria of statistical randomness. The slightly wider distribution of p-values in the second dataset reflects natural statistical variability and does not reveal any deviations from expected random behavior. Thus, both sequences can be confidently classified as statistically random according to NIST STS, confirming the robustness of the proposed method's output.

An experimental evaluation of the cipher's resistance to linear and differential cryptanalysis, conducted using a reduced-round mini-version, demonstrated a marked strengthening of its security profile. Notably, the enhanced construction begins to exhibit statistically indistinguishable random substitution behavior from as early as the third round, indicating the rapid diffusion and nonlinearity growth essential for thwarting classical analytical attacks. This early emergence of randomness-like properties underscores the effectiveness of the introduced modifications and provides strong evidence of improved cryptographic robustness.

Future research should focus on reducing hardware complexity, developing efficient FPGA/ASIC implementations, assessing side-channel resistance, and exploring integration with modern secure architectures such as zero-trust, authenticated LWC schemes, and hybrid post-quantum protocols. The improved CLEFIA-based method holds strong potential for practical deployment in IoT infrastructures, LMS ecosystems, edge devices, NFC/RFID systems, and access-control mechanisms, enabling high-performance, low-latency protection of confidentiality, integrity, and authenticity in contemporary resource-constrained platforms.

Acknowledgement

This research study is carried out within the framework of research grant №AP22787045 "Development of a prototype of a secure university information system using artificial intelligence methods to detect anomalies in data" (2024-2026), funded by the Ministry of Science and Higher Education of the Republic of Kazakhstan.

References

- [1] Kerimbayeva, A.; Iavich, M.; Begimbayeva, Y.; Gnatyuk, S.; Tynymbayev, S.; Temirbekova, Z.; Ussatova, O. A Lightweight Variant of Falcon for Efficient Post-Quantum Digital Signature. *Information* 2025, 16, 564. <https://doi.org/10.3390/info16070564>.
- [2] F. Jahoor, M. K. Joseph and N. Madhav, "Bibliometric analysis of Cybersecurity in e-learning systems and big data," 2024 Conference on Information Communications Technology and Society (ICTAS), Durban, South Africa, 2024, pp. 57-62, doi: 10.1109/ICTAS59620.2024.10507133.
- [3] S. Q. A. Al-Rahman, S. S. Hamad and D. S. Turkey, "Implementation of Data Transportation Protocol Depending on the Lightweight Cipher Algorithms," 2021 14th International Conference on Developments in eSystems Engineering (DeSE), Sharjah, United Arab Emirates, 2021, pp. 340-345, doi: 10.1109/DeSE54285.2021.9719471.
- [4] N. A. Gunathilake, W. J. Buchanan and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 707-710, doi: 10.1109/WF-IoT.2019.8767250.
- [5] G. Spasova and M. Karova, "A New Secure Image Encryption Model Based on Symmetric Key," 2021 International Conference on Biomedical Innovations and Applications (BIA), Varna, Bulgaria, 2022, pp. 107-110, doi: 10.1109/BIA52594.2022.9831258.
- [6] M. Maragatharajan, L. Sathishkumar, J. Manikandan et al, "A Novel Approach for Data Encryption Based on Vector-Matrix Keys," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 273-278, doi: 10.1109/ICACCS57279.2023.10113061.
- [7] Aljuffri, A.; Huang, R.; Muntenaar, L. et al, The Security Evaluation of an Efficient Lightweight AES Accelerator. *Cryptography* 2024, 8, 24. <https://doi.org/10.3390/cryptography8020024>
- [8] Iavich, M.; Kapalova, N. Optimizing Post-Quantum Digital Signatures with Verkle Trees and Quantum Seed-Based Pseudo-Random Generators. *Computers* 2025, 14, 103. <https://doi.org/10.3390/computers/14030103>.
- [9] D. Gyasi-Nyarko, E. Freeman, M. M. Ujakpa, W. Amponsah and S. O. Amoako, "A Systematic Review of Public Key Cryptography: Implementation, Challenges and Future Opportunities," 2025 IST-Africa Conference (IST-Africa), Nairobi, Kenya, 2025, pp. 1-15, doi: 10.23919/IST-Africa67297.2025.11060567.
- [10] L. Chen, S. Ni, Y. Wang, F. Yu and Y. He, "Content Security Distribution Scheme Based on Certificateless Public Key Cryptography," 2024 IEEE 12th International Conference on Information, Communication and Networks (ICICN), Guilin, China, 2024, pp. 504-508, doi: 10.1109/ICICN62625.2024.10761210.
- [11] Z. Chen, C. Liu, F. Li and S. C. -I. Chen, "Security Analysis of Another Vulnerability to RSA Algorithm," 2023 13th International Conference on Information Technology in Medicine and Education (ITME), Wuyishan, China, 2023, pp. 434-438, doi: 10.1109/ITME60234.2023.00092.

- [12] Hu, Z., Gnatyuk, S., Kovtun, M., Seilova, N. (2019). Method of Searching Birationally Equivalent Edwards Curves Over Binary Fields. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) *Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing*, vol 754. Springer, Cham. https://doi.org/10.1007/978-3-319-91008-6_31.
- [13] D. C. Lawo et al., "Falcon/Kyber and Dilithium/Kyber Network Stack on Nvidia's Data Processing Unit Platform," in *IEEE Access*, vol. 12, pp. 38048-38056, 2024, doi: 10.1109/ACCESS.2024.3374629
- [14] M. Li, J. Tian, X. Hu, Y. Cao and Z. Wang, "High-Speed and Low-Complexity Modular Reduction Design for CRYSTALS-Kyber," 2022 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Shenzhen, China, 2022, pp. 1-5, doi: 10.1109/APCCAS55924.2022.10090253.
- [15] D. Xu, K. Wang and J. Tian, "A Hardware-Friendly Shuffling Countermeasure Against Side-Channel Attacks for Kyber," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 72, no. 3, pp. 504-508, March 2025, doi: 10.1109/TCSII.2025.3528751.
- [16] M. Ahmet, "High-Performance FPGA Implementations of Lightweight ASCON-128 and ASCON-128a With Enhanced Throughput-to-Area Efficiency," 2024 17th International Conference on Information Security and Cryptology (ISCTürkiye), Ankara, Türkiye, 2024, pp. 1-7, doi: 10.1109/ISCTürkiye64784.2024.10779273.
- [17] G. Sravya, M. O. V. P. Kumar, Y. Sudarsana Reddy, K. Jamal and K. Mannem, "The Ideal Block Ciphers - Correlation of AES and PRESENT in Cryptography," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1107-1113, doi: 10.1109/ICISS49785.2020.9315883.
- [18] A. Aljuffri, C. Reinbrecht, S. Hamdioui, M. Taouil and J. Sepúlveda, "Balanced Dual-Mask Protection Scheme for GIFT Cipher Against Power Attacks," 2022 IEEE 40th VLSI Test Symposium (VTS), San Diego, CA, USA, 2022, pp. 1-6, doi: 10.1109/VTS52500.2021.9794230.
- [19] M. Wroński, E. Burek and M. Leśniak, "(In)Security of Stream Ciphers Against Quantum Annealing Attacks on the Example of the Grain 128 and Grain 128a Ciphers," in *IEEE Transactions on Emerging Topics in Computing*, doi: 10.1109/TETC.2024.3474856.
- [20] F. E. Potestad-Ordóñez, E. Tena-Sánchez, J. M. Mora-Gutiérrez, M. Valencia-Barrero and C. J. Jiménez-Fernández, "Trivium Stream Cipher Countermeasures Against Fault Injection Attacks and DFA," in *IEEE Access*, vol. 9, pp. 168444-168454, 2021, doi: 10.1109/ACCESS.2021.3136609.
- [21] B. Degnan, E. Rose, G. Durgin and S. Maeda, "A Modified Simon Cipher 4-Block Key Schedule as a Hash," in *IEEE Journal of Radio Frequency Identification*, vol. 1, no. 1, pp. 85-89, March 2017, doi: 10.1109/JRFID.2017.2764389.
- [22] R. Mohanapriya and V. Nithish Kumar, "Modified SPECK (M-SPECK) Lightweight Cipher Architecture for Resource-Constrained Applications," in *IEEE Access*, vol. 13, pp. 88993-89002, 2025, doi: 10.1109/ACCESS.2025.3570727.
- [23] S. Ahmadi, M. Delavar, J. Mohajeri and M. R. Aref, "Security analysis of CLEFIA-128," 2014 11th International ISC Conference on Information Security and Cryptology, Tehran, Iran, 2014, pp. 84-88, doi: 10.1109/ISCISC.2014.6994027.
- [24] L. Pyrgas and P. Kitsos, "A Very Compact Architecture of CLEFIA Block Cipher for Secure IoT Systems," 2019 22nd Euromicro Conference on Digital System Design (DSD), Kallithea, Greece, 2019, pp. 624-627, doi: 10.1109/DSD.2019.00097.
- [25] F. Mohsin and W. Elmedany, "A Secure Internet of Healthcare Things for tackling COVID-19," 2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), Zallaq, Bahrain, 2021, pp. 98-104, doi: 10.1109/3ICT53449.2021.9581819.
- [26] G. Bansod, N. Raval and N. Pisharoty, "Implementation of a New Lightweight Encryption Design for Embedded Security," in *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 142-151, Jan. 2015, doi: 10.1109/TIFS.2014.2365734.
- [27] P. Saravanan, S. S. Rani, S. S. Rekha and H. S. Jatana, "An Efficient ASIC Implementation of CLEFIA Encryption/Decryption Algorithm with Novel S-Box Architectures," 2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP), Chennai, India, 2019, pp. 1-6, doi: 10.1109/ICESIP46348.2019.8938329.
- [28] Sabri, O.; Al-Shargabi, B.; Abuarqoub, A.; Hakami, T.A. A Lightweight Encryption Method for IoT-Based Healthcare Applications: A Review and Future Prospects. *IoT* 2025, 6, 23. <https://doi.org/10.3390/iot6020023>.

Authors' Profiles



Sergiy Gnatyuk: Vice-rector for research and technology transfer at State University "Kyiv Aviation Institute" (Kyiv, Ukraine). He is the Chief researcher at the State Scientific and Research Institute of Cybersecurity Technologies and Information Protection. He received M.Sc. degree in Information Security as well as Ph.D. / D.Sc. in Engineering (Cybersecurity). Full Professor in Computer Science. Major research interests: Cryptography, Quantum Key Distribution, Network and Internet Security, Incident Response, UAV, Critical Information Infrastructure Protection, AI/ML-based Security Systems.



Berik Akhmetov: Rector of the Yessenov University (Aktau, Kazakhstan), Ph.D., MBA, Associate Professor, Academician of the International Academy of Informatization. Graduated from KazNU named after. Al-Farabi with a degree in Information Systems (M.Sc.). Major research interests: Cybersecurity, Cyber Attacks Detection, Network and Internet Security, Learning Management Systems, Artificial Intelligence and Machine Learning.



Dauriya Zhaxygulova: Master of Science and Technology, Ph.D. student of the East Kazakhstan Technical University named after D. Serikbayev (Ust-Kamenogorsk, Kazakhstan), teacher at the Department of Automation and Information Technologies, Shakarim University (Semey, Kazakhstan). Major research interests are Information Systems, Cryptography, Critical Information Infrastructure Protection, Mathematical Modelling of the Complex Technological Systems.



Yuliia Polishchuk: Master of Science in Cybersecurity, Ph.D. student of the State University “Kyiv Aviation Institute” (Kyiv, Ukraine). Junior researcher at KAI R&D Cybersecurity Lab. Major research interests: Cryptography, Network and Internet Security, Critical Information Infrastructure Protection, AI/ML-based Security Systems, UAV.

How to cite this paper: Sergiy Gnatyuk, Berik Akhmetov, Dauriya Zhaxygulova, Yuliia Polishchuk, "CLEFIA-based Lightweight Encryption for Resource-Constrained Systems: Design, Algorithms and Security Analysis", International Journal of Computer Network and Information Security(IJCNIS), Vol.17, No.6, pp.47-64, 2025. DOI:10.5815/ijcnis.2025.06.04