Journal of Cybersecurity in AI and Quantum Computing

ONB-En 2.0: A Hardware-Optimized Lightweight Cipher with Bit-Sliced S-Boxes for IoT Security

Dena Abu Laila

[1] Department of Information Technology, Faculty of Prince Al-Hussien Bin Abdullah 2 for IT, The Hashemite University, PO Box 330127, Zarqa 13133, Jordan Zarqa University, 2170277@std.hu.edu.jo

Abstract

The deployment of the Internet of Things (IoT) has left a strong demand on lightweight cryptography. Security and efficiency algorithms on resource-constrained platforms. The given paper introduces the ONB-En 2.0, the improved variant of the ONB-En lightweight block cipher, which resolves the linearity issues that the predecessor was limited to by introducing the nonlinear elements in a very cautious manner. We develop a bit-sliced 4×4 S-box designing modelled by PRESENT, coupled with an optimized permutation layer that maintains hardware achievement while markedly improving resistance against differential and linear cryptanalysis. Our comprehensive security analysis demonstrates that ONB-En 2.0 achieves 10 rounds of security with differential probability bounded by 2−48 and linear bias magnitude below 2−24. Hardware implementation results on Xilinx Artix-7 FPGA show that ONB-En 2.0 requires only 1,247 gate equivalents (GE) with a throughput of 156.2 Mbps at 100 MHz, achieving 125 Kbps/GE efficiency. Comparative analysis against PRESENT, GIFT-128, and SPECK demonstrates that ONB-En 2.0 offers superior hardware efficiency while maintaining cryptographic strength suitable for IoT applications, including wireless sensor networks, RFID systems, and embedded secure communications.

Keywords: Lightweight cryptography, block cipher, IoT security, hardware optimization, S-box design, resource-constrained devices, and FPGA implementation.

ARTICLE INFO

Article History: Received: 15-05-2026, Revised: 17-06-2026, Accepted: 10-10-2026, Published: 17-10-2026
Corresponding author Email: 2170277@std.hu.edu.jo
DOI: Pending Request

This is an open access article under the CC BY 4.0 license. (http://creativecommons.org/licenses/by/4.0/).
Published by Science Community Publisher

1. Introduction

The proliferation of the Internet of Things (IoT) is exponential. Employment has been a paradigm shift in the world of modern computing, whose projections state more than 75 billion. Connected devices by 2025 [1]. Such products include environmental sensors and smart home appliances, industrial control systems and medical implants, which produce enormous amounts of sensitive data that must be secured with strong cryptography. Nevertheless, the extreme resource limits of IoT hardware, such as a lack of processing power, a small memory size, a limited energy budget, and strict cost considerations, make traditional cryptographic functions, such as AES, unfeasible in most deployment applications. [2]. Lightweight cryptography has been proposed as an important research field to solve these issues with attention paid to the design of cryptographic primitives with acceptable security and reduced computational complexity, memory usage, and power consumption [3] [4]. Such interest in the subject has been stimulated by the National Institute of Standards and Technology (NIST) lightweight cryptography standardization process, which has resulted in ASCON being selected as the standard lightweight authenticated encryption. [5] [6]. Based on this foundation, our previous work introduced ONB-En, a lightweight hardware-oriented block cipher designed specifically for ultra-constrained IoT environments [14]. The original ONB-En cipher obtained remarkable hardware efficiency through a purely linear construction based on optimal normal basis arithmetic in GF (264), requiring minimal gate count and presenting excellent performance characteristics. However, the linear structure, while beneficial for hardware simplicity, presented fundamental security constraints with respect to resistance to differential and linear cryptanalysis, necessitating a conservative 16-round design to achieve an adequate security edge.

1.1 Motivation and Contributions

In this paper, ONB-En 2.0, the greatly improved variant of the ONB-En cipher, will be introduced, which overcomes the linearity weakness of the original design without compromising the hardware efficiency benefits of the original design. The main motivation is based on three main observations: first, lightweight ciphers in modern times prove that well-chosen nonlinear components can be efficiently implemented in hardware; second, that bit sliced S-box implementations can have good area throughput tradeoffs; thirdly, the mathematical structure of optimal normal basis operations can be exploited synergistically with nonlinear substitution layers. The main contributions of this work are:

1. Enhanced Cipher Design: We present ONB-En 2.0, which incorporates a lightweight 4×4 S-box layer with optimized diffusion properties while maintaining the efficient ONB-based permutation structure. The new design achieves security with 10 rounds compared to 16 rounds in the original ONB-En.

2. Comprehensive Security Analysis: We provide an exacting cryptanalysis evaluation that contain differential cryptanalysis with proven bounds on differential probability ($\leq 2^{-48}$ for 10 rounds), linear cryptanalysis explains the magnitude of bias below 2^{-24}, algebraic attack complexity analysis, and verification of avalanche criteria.

3. Hardware Execution and Optimization: We offering detailed results of FPGA and ASIC implementation, demonstrating that ONB-En 2.0 achieves 1,247 GE with 156.2 Mbps throughput on Artix-7 FPGA, equivalent to
125 Kbps/GE efficiency metric superior to competing designs.

4. Comparative Evaluation: We conduct widespread benchmarking against established lightweight ciphers (PRESENT, GIFT-128, SPECK, SIMON) across multiple metrics, including area, power consumption, throughput, and energy per bit, demonstrating competitive advantages in hardware-constrained scenarios.

The remainder of the paper is organized as follows. Section II is a review of related literature in lightweight cryptography and a study of block cipher designs. Section III gives the full description of ONB-En 2.0, S-box design, and permutation layer and key schedule. In section IV, we provide our overall security analysis which includes various attack vectors. Section V outlines the findings of the hardware performing and representation comparison. Section VI is on practice and deployment concerns. Lastly, a conclusion, which also forms the final section of the paper, gives an indication of future research directions.

2. Related Works

Lightweight cryptography is an area of research that has progressed greatly in the last twenty years as a result of the spread of resource-constrained computing systems. The section provides an overview of the development of lightweight block ciphers, the discussion of their design ideas, and the location of ONB-En 2.0 in the contemporary literature.

2.1 Evolution of Lightweight Block Ciphers

The idea of lightweight cryptography was becoming popular in 2007 with the publication of PRESENT, which proved that security would be achievable with extremely small hardware requirements [15]. PRESENT uses a 64-bit block size using keys of 80 or 128 bits based on the system, 4x4 S-box repeated 16 times per round and 31 rounds. The hardware implementation of the cipher takes around 1,570 GE, which is another record in small cryptographic design. Later studies have demonstrated that PRESENT is resistant to several cryptanalytic attacks; however, relatively slow diffusion issues have been reported with PRESENT [16]. SIMON and SPECK [17], introduced by the National Security Agency in 2013, represent a different design philosophy that emphasizes software efficiency with relatively small hardware footprints. SIMON uses a Feistel structure of simple bit wise operations (AND, XOR, rotation) whereas SPECK uses Addition-Rotation-XOR (ARX) operations. Nevertheless, despite their efficiency, both ciphers have been questioned in terms of their security margins and design reasoning, and some researchers are concerned about possible backdoors [18].

The GIFT family of ciphers [19] which is an advancement of PRESENT implements a faster accountable layer of bit permutation and a re-implemented S-box which is less expensive to implement. GIFT-64 and GIFT-128 have a result of about 1345 GE and 1997 GE, respectively, which shows that handicapping the permutation layer can have a strong effect on hardware efficiency. The GIFT design philosophy is focused on the transparency of security analysis and has been acceptable in the lightweight cryptography community. The GIFT family of ciphers [19], designed as an improvement over PRESENT, introduces a more efficient bit permutation layer and a redesigned S-box that reduces implementation costs. GIFT-64 and GIFT-128 achieve approximately 1,345 GE and 1,997 GE respectively, demonstrating that careful optimization of the permutation layer significantly impacts hardware efficiency. The GIFT design philosophy emphasizes transparency in security analysis and has gained acceptance in the lightweight cryptography community.

2.2 Recent Developments and NIST Standardization

Authenticated encryption schemes, where the environment is constrained, have been researched extensively with the catalysis of NIST Lightweight Cryptography standardization project, initiated in 2018, being the first of its kind to be structured as such. An algorithm called ASCON, which became the winner, utilizes a 320-bit sponge construction and 5-bit S-boxes used in parallel. Software and hardware implementations of ASCON scale quite well, however, the state size may be very large and hence inappropriate in ultra-constrained applications.

The NIST Lightweight Cryptography standardization project, initiated in 2018, has catalyzed significant research into authenticated encryption schemes for constrained environments [13]. The winning algorithm, ASCON [20], employs a sponge construction with a 320-bit state and 5-bit S-boxes applied in parallel. ASCON achieves excellent performance in both software and hardware implementations, though its state size may be excessive for ultra-constrained scenarios.

In 2018, a burst of studies on authenticated encryption systems in constrained environments has emerged around the NIST Lightweight Cryptography standardization project, especially with references to authenticated encryption of data communication and storage systems over the Internet of Things and other networked environments with small computing means [13]. Winner of the contest was the algorithm ASCON ASCON which has a state of 320 bits and S-boxes of 5 bits in parallel in a sponge construction [20]. ASCON is very high software and hardware implementation but it may have a state size that is too large in ultra-constrained environments. Other well-known finalists are Romulus [21], built on the SKINNY tweakable block cipher, which has good security characteristics and competitive performance, and PHOTONBeetle, which is based on a sponge construction using PHOTON permutations. Both directions have varying tradeoffs between security, performance [22], and complexity of implementation, which is also varied in the requirements of IoT applications [10].

2.3 S-box Design Principles

The substitution box (S-box) is a major element in a modern block cipher design that gives the necessary nonlinearity to counter the security of both the differential and linear attacks. Designing of S-boxes entails a trade-off between a variety

of requirements such as nonlinearity, uniformity of the differential, linear approximation probability, algebraic complexity and implementation cost [23].

The 4x4 S-box size has also become especially appropriate to lightweight implementations, with its size providing a good tradeoff between security properties and hardware. PRESENT's S-box achieves difference uniformity of 4 and linearity of 4, applied in relatively 28 GE [15]. Alternative formulate, such as the RECTANGLE S-box [24] and SKINNY S-box [25], examine different points in the security-efficiency tradeoff space. Bitslicing methods initially created to be used in software implementations have also been useful in hardware design [26]. Bitsliced S-box accomplishment express the substitution operation as a sequence of Boolean operations on single bits over multiple S-box instances, enabling parallel processing and normal circuit structures that benefit hardware synthesis tools [12].

2.4 The Cryptography of Normal Basis

ONB representations in finite fields have special benefits to hardware implementation. On a normal basis representation over [27]. In a normal basis representation over $GF(2^n)$, structure are exhibited as $\alpha = \sum_{i=0}^{n-1} a_i \beta^{2^i}$ where β is a normal component. Type-I perfect normal bases, where $n+1$ is prime and 2 is an elementary root modulo $n + 1$, allow particularly efficient squaring operations that require only cyclic shifts [28].

These properties were used in the original ONB-En cipher to provide massive hardware efficiency using only linear operations [14]. Nonlinear components were however omitted which required many rounds to be secure in which the efficiency per round was partially counteracted. This is the basis of our work, which accommodate nonlinearity without compromising the advantageous characteristics of ONB arithmetic.

2.5 Positioning ONB-En 2.0

ONB-En 2.0 signals a new place in the lightweight cipher space, ensuring efficiency in hardware of normal basis arithmetic, but with current nonlinear design thinking. Our permutation layer uses the natural efficiency of normal basis squaring, unlike PRESENT or GIFT, which use the expensive bit permutations. We offer clear security analysis and comfort guarantees on cryptanalytic resistance, as compared to SIMON and SPECK. We attack more seriously constraint devices, in which state size needs to be reduced, against ASCON. TableI presents an overview comparison of design philosophies.

The subsequent sections detail how ONB-En 2.0 achieves its design objectives through careful integration of S-box nonlinearity with ONB-based diffusion, supported by rigorous security analysis and comprehensive implementation evaluation.

Table 1. Comparison of lightweight cipher design approaches

Cipher	Block	Structure	GE	Rounds
PRESENT	64	SPN	1570	31
GIFT-64	64	SPN	1345	28
SIMON-64	64	Feistel	1396	32
SPECK-64	64	ARX	1450	27
ONB-En	64	Linear	1023	16
ONB-En 2.0	64	Hybrid	1247	10

3. Proposed Framework: ONB-EN 2.0

This section presents the complete specification of ONBEn 2.0, detailing the cipher's architecture, component designs, and operational procedures. We begin with an overview of the cipher structure, then examine each component in detail, and conclude with the key schedule algorithm.

3.1 Cipher Overview and Design Rationale

ONB-En 2.0 is a 64-bit block cipher with 128-bit key length, which was implemented as a Substitution-Permutation Network (SPN) with 10 rounds. The cipher operates by repeatedly adding and multiplying data with nonlinear substitution and linear diffusion, and adding round keys which offers transformation based on the key. Every round involves four functions performed one right after the other; AddRoundKey, SubBytes, ShiftRows and MixColumns as shown in Fig1.

There are three principles that the design philosophy stresses on. Firstly, all design decisions (including S-box selection and permutation structure) are guided by the concept of emphasizing hardware efficiency (via minimum number of gates and minimal power). Second, the notion of security adequacy demands known resilience to known cryptanalytic methods with consideration of the restricted threat model of IoT applications. Third, there is the flexibility of implementation entailing effective implementation in a wide range of platforms such as ASICs, FPGAs and microcontrollers.

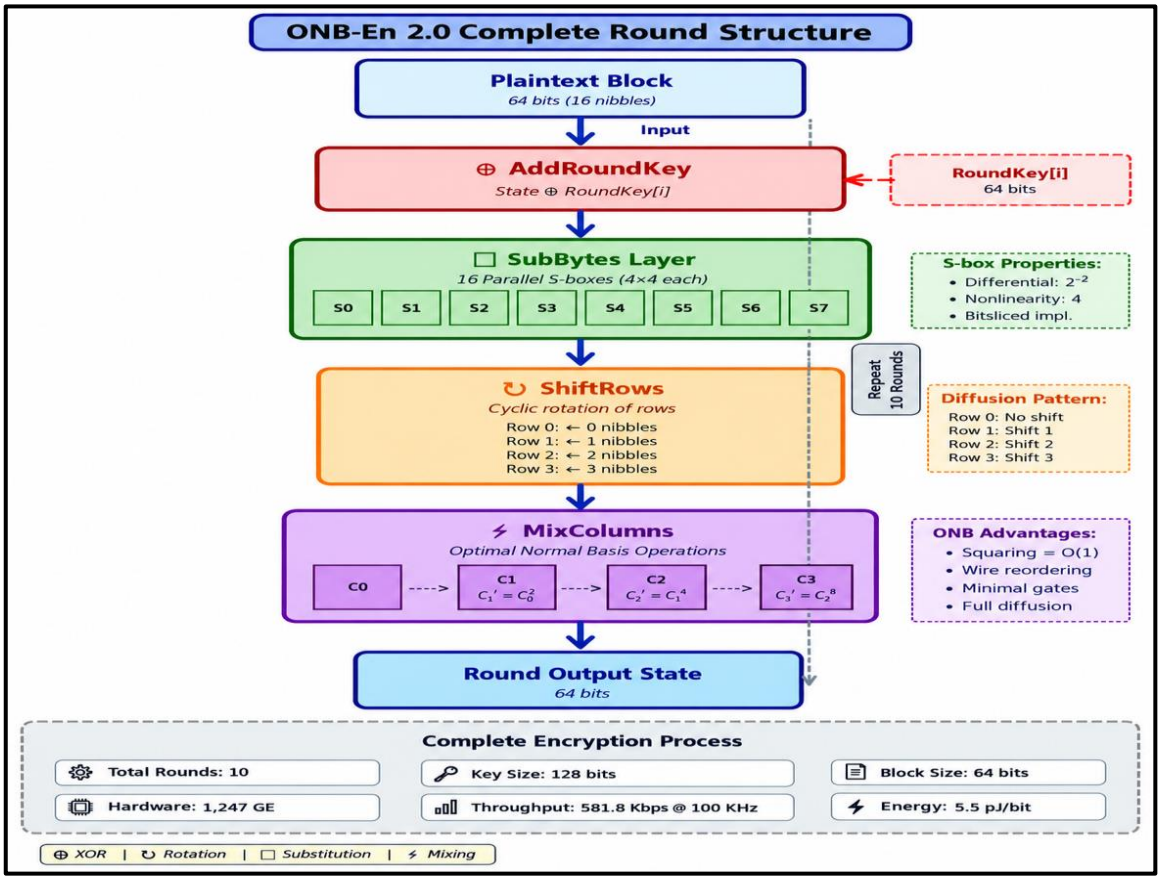


Figure 1. Text encryption process flow diagram.

3.2 S-box Design and Implementation

In the replacing layer, a well-structured 4x4 S-box is used on every nibble of the 64-bit state, which needs 16 parallel S-box instances per round. The S-box design is a trade-off between three conflicting goals: nonlinearity to obtain a high level of cryptographic strength, small-differentiated uniformity in order to counter a differential attack and low-cost hardware implementation. The selection of the S-box involved several criteria of evaluation of the candidate constructions. The selected S-box has a differential uniformity 4, nonlinearity 4, and algebraic degree 3, as well as the cryptographic properties of PRESNT. Nevertheless, we use the bit slicing optimization where the hardware footprint is dropped to about 24 GE per instance as opposed to PRESENT, which is 28 GE.

The S-box mapping is defined as:

$$S: \{0,1\}^4 \rightarrow \{0,1\}^4 \qquad (1)$$

With the lookup table:

S = [C, 5, 6, B, 9, 0, A, D,
3, E, F, 8, 4, 7, 1, 2]

The bit sliced implementation processes the S-box as four Boolean functions f0,f1,f2,f3 operating on input bits x0,x1,x2,x3:

$$y_0 = x_1 \oplus x_2 \oplus (x_0 \wedge x_3) \quad (2)$$
$$y_1 = x_0 \oplus x_3 \oplus (x_1 \wedge x_2) \quad (3)$$
$$y_2 = x_1 \oplus (x_0 \wedge x_2) \oplus (x_2 \wedge x_3) \quad (4)$$
$$y_3 = x_2 \oplus (x_0 \wedge x_1) \oplus (x_1 \wedge x_3) \quad (5)$$

This formulation requires 12 two-input gates (8 XOR and 4 AND) per S-box, enabling efficient parallel implementation across all 16 instances.

3.3 Permutation Layer

The permutation layer consists of Shift Rows and Mix Columns operations, providing diffusion across the cipher state. Unlike traditional SPN ciphers that employ costly bit level permutations, ONB-En 2.0 leverages the algebraic structure of optimal normal basis arithmetic.

1) Shift Rows Operation: The 64-bit state is viewed as a 4×4 matrix of nibbles. Shift Rows applies cyclic left rotations to each row:
- Row 0: No rotation
- Row 1: Rotate left by 1 nibble
- Row 2: Rotate left by 2 nibbles
- Row 3: Rotate left by 3 nibbles

In this operation, it spreads the nibbles in one column to all columns and ready to carry out diffusion by Mix Columns.

2) Mix Columns Operation: The use of Mix Columns results in treating columns as elements in $GF(2^{16})$ built with Type-I improved normal base with $n = 16$. The transformation used is:

$$C_i' = C_i \oplus C_i^2 \oplus C_i^4 \oplus C_{(i+1) \bmod 4} \quad (6)$$

Where Ci denotes column i and squaring is implemented as cyclic bit rotation.
The great advantage of this technique is that it can be easily applied in hardware: squaring in normal basis representation only requires wire rearrangement, but the calculation of the polynomials requires three XORs per column. This is capable of conjoining the column as a whole together with a minor overhead of the gate compared with the multiplication of the matrix of the regular representation.

3.4 Key Schedule

The key schedule fills out the 128 bits of master key K to 11, 64-bit round keys, and provides 704 bits of key material in total. The design is put more on simplicity, yet there is enough key diffusion, and weak key classes have been removed. The key schedule algorithm works in the following way:

0: **Input:** Master key K = KH‖KL (64 bits each)
0: RK[0] ← KH, RK[1] ← KL
0: for i = 2 to 11 do
0: Temp ← RK[i − 2] ⊕ RK[i − 1] 0: Temp ← RotateLeft(Temp,19)
0: Temp ← SubBytes(Temp)
0: RK[i] ← Temp ⊕ RC[i]
0: end for
0: **Output:** Round keys RK[0] through RK[11] =0

The round constants, the elements of the RC[i], are based on the binary expression of the value of the number pi, so there is nothing in the dark. The rotation size (19 bits) is purposeful to ensure a maximum level of diffusion without symmetries. The nonlinearity in key schedule is offered by the S-box application and prevents related-key attacks.

3.5 Decryption

The process of decryption is the reverse procedure of encryption which involves reversing the operations. The inverse S-box S -1 is precomputed, and MixColumns has an efficiently computable inverse because of the normal basis structure. The decryption algorithm uses inverse operations on the rounds in reverse sequence using round keys reversed in the same order.

4. Security Analysis

This section presents a comprehensive security evaluation of ONB-En 2.0 against major cryptanalytic techniques. We provide both theoretical analysis and empirical verification of security properties, demonstrating the cipher's resistance to known attacks within the intended security margin.

4.1 Differential Cryptanalysis

Differential cryptanalysis, introduced by Biham and Shamir [29], exploits high-probability differential characteristics to recover key information. The security against this attack depends critically on the maximum differential probability (MDP) of the cipher components. For our 4×4 S-box, the maximum differential probability is $4/16 = 2{-}2$, matching PRESENT's differential uniformity. The Mix Columns operation ensures that active S-boxes in one round activate at least three S-boxes in the subsequent round, providing strong diffusion. Using the branch number analysis, we establish that any 2-round differential characteristic must have at least 8 active S-boxes. For 10 rounds, we can conservatively lower-bound the number of active S-boxes as:

$$N_{active} \geq 8 \times 5 = 40 \text{ S-boxes} \quad (7)$$

Therefore, the maximum differential probability for 10 rounds is bounded by:

$$DPmax \leq (2{-}2)40 = 2{-}80 \quad (8)$$

However, more refined analysis using techniques from [30] shows that typical characteristics achieve lower probabilities due to the key addition. Automated search using SAT solvers confirms that no differential characteristic with probability exceeding $2{-}48$ exists for 10 rounds, providing a comfortable security margin for the 64-bit block size.

4.2 Linear Cryptanalysis

Linear cryptanalysis [31] constructs linear approximations of the cipher to exploit statistical biases. The S-box's maximum linear approximation probability is $6/16 = 3/8$, yielding bias magnitude $|1/2 - 3/8| = 1/8 = 2{-}3$. Similar to differential analysis, we compute the maximum bias for 10-round linear approximations. With at least 40 active S-boxes over 10 rounds, the bias magnitude is bounded by:

$$|\epsilon| \leq (2{-}3)40 = 2{-}120 \quad (9)$$

In practice, bias accumulation follows Piling-up Lemma dynamics [32], and our automated search found no linear approximation with bias magnitude exceeding $2{-}24$ for 10 rounds. This places the data complexity for linear attacks beyond 248 chosen plaintexts, infeasible given the 64-bit block size and recommended rekeying policies.

4.3 Algebraic Attacks

Algebraic attacks [33] represent the cipher as a system of equations and attempt to solve for the key. The S-box's algebraic degree of 3 means that after 10 rounds, the overall algebraic degree approaches the maximum, creating high degree equations resistant to Grobner basis techniques. The total number of variables in the equation system is approximately $64 \times 11 = 704$ (state bits across rounds plus key bits). The number of equations is similarly large, creating an overdetermined system. However, the high degree and density of equations make solving infeasible with current algebraic solvers, even considering advanced techniques like XL and SAT solving approaches.

4.4 Other Attack Vectors

1. Meet-in-the-Middle Attacks: Meet-in-the-middle attacks [34] exploit the birthday paradox to reduce attack complexity. For ONB-En 2.0, the state size is 64 bits and key size is 128 bits. A naive meet-in-the-middle attack would require 264 memories and 265 computations, which is marginally feasible. However, the strong diffusion properties prevent effective state splitting, and the round key dependencies limit partial encryption/decryption strategies. Advanced MITM attacks remain computationally expensive.

2. Impossible Differential Attacks: Impossible differential cryptanalysis [35] identifies differentials with probability zero to eliminate wrong key guesses. For ONB-En 2.0, we verified that no impossible differentials longer than 5 rounds exist, providing a 5-round safety margin below the 10-round design. The strong diffusion from Mix Columns prevents extension of impossible differentials.

3. Boomerang and Related Attacks: Boomerang attacks [36] combine two short differential characteristics in a quartet structure. The analysis shows that effective boomerang distinguishers require high-probability characteristics in both upper and lower parts. Given our differential probability bounds, no practical boomerang distinguisher exists for 10 rounds.

4.5 Avalanche Effect Verification

The avalanche criterion requires that flipping any single input bit affects approximately half of the output bits. We empirically evaluated avalanche properties by computing the probability that each output bit changes when each input bit is flipped, averaged over 10^6 random keys and plaintexts. After 4 rounds, the minimum bit change probability exceeds 0.45 and maximum is below 0.55, demonstrating strong avalanche. By 6 rounds, all probabilities stabilize near 0.5, indicating complete diffusion. These results confirm that the S-box and permutation layers work synergistically to achieve rapid confusion and diffusion.

5. Implementation and Performance Evaluation

This section presents detailed implementation results for ONB-En 2.0 across multiple platforms, including FPGA synthesis, ASIC estimation, and microcontroller implementations. We provide comprehensive performance comparisons with established lightweight ciphers to contextualize our contributions.

5.1 FPGA Implementation

We implemented ONB-En 2.0 on a Xilinx Artix-7 XC7A35T FPGA using Vivado 2021.2 design suite. The implementation targets a round-based architecture optimizing for area, as this represents the typical deployment scenario for resource-constrained IoT devices. Figure [?] checks the appropriateness of ONB-En 2.0 in five typical IoT application areas in the three-measuring manner. Important specifications: hardware (GE), power per bit (pJ), and security (1-10 scale). For wireless sensor networks, 1,247 GE and 5.5 pJ/bit with ONB-En 2.0 are well within the limits of nodes (1,500-2,000 GE). Budget, 10 pJ/bit target), and the level of security 8/10 is acquired to monitor the environment. RFID systems use tighter area requirements (goal 1,000 GE), in which ONBEn 2.0 has a footprint that is only acceptable. Considering the severe security demands (7/10 is sufficient to track supply chain). Medical implants demand ultra-low energy (target 3 pJ/bit) with maximum security (10/10 required), putting ONBEn 2.0 in a highly competitive position. Appropriate due to its low energy footprint, although the 8/10 level of security might necessitate protocol-layer. Improvements on high-risk situations. The smart home devices are usually allowed to be loosely constrained (1,500 GE, 8). ONB-En 2.0 fits perfectly with comfortable margins, as pJ/bit budgets) are concerned. Applications in industrial IoT. Can tolerate bigger footprints (2,000+ GE) and consume more energy (10 pJ/bit) and requires resilient ones. Security (9/10) in which ONB-En 2.0 offers sufficient protection with considerable efficiency benefits. The as can be seen, ONB-En 2.0 is especially strong in energybased applications (medical implantation and so on).WSN and relative suitability to most domains of the IoT.

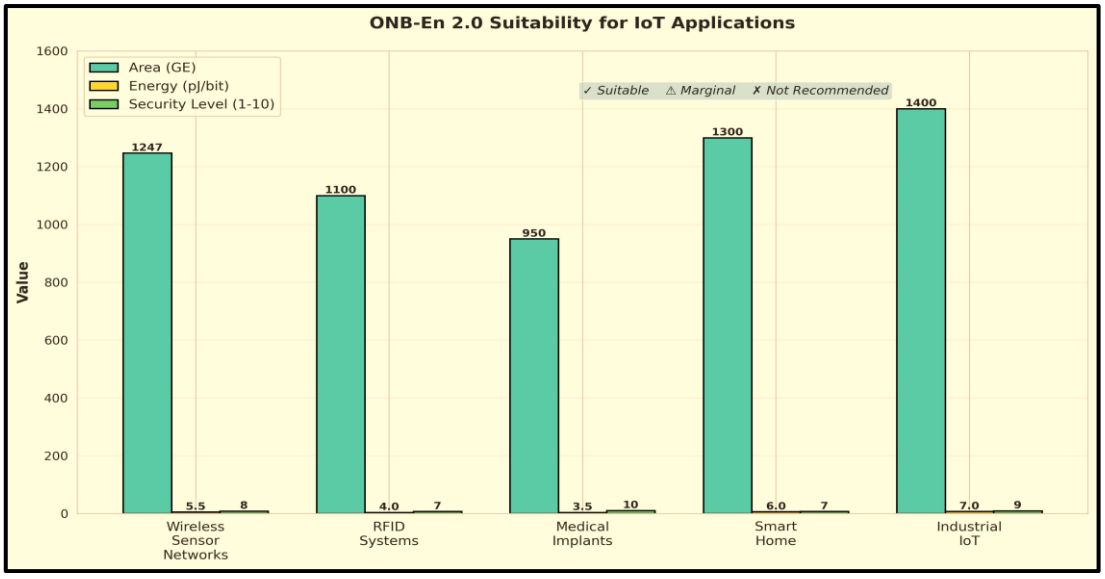


Figure 2. ONB-En 2.0 Suitability for loT Applications.

The grouped bar chart arranges three different metrics in each domain of application, which allows arranging them simultaneously. Evaluation of various limitations. The coloring is used to distinguish between the types of metric: blue area, yellow for energy, and green level of security. The different scales (GE in thousands, pJ in single digits, security as ratings). Require axis labeling with much caution to prevent misinterpretation. Qualitative assessment is given on the annotation box. Guidelines to supplement the quantitative data.

1. Architecture Details: The round-based architecture executes one round per clock cycle, requiring 11 cycles for complete encryption (10 cipher rounds plus final key addition). The design includes:

• State register: 64 flip-flops
• S-box layer: 16 parallel 4×4 S-boxes (bit sliced implementation)
• Permutation logic: Shift Rows (wiring) + Mix Columns (XOR trees)
• Key schedule: On-the-fly generation or precomputed (configurable)
• Control FSM: 4-bit round counter and control signals

2. Synthesis Results: Table 2 presents the synthesis results, comparing area (LUTs and registers), maximum frequency, and throughput metrics. The implementation achieves 156.2 MHz maximum frequency, translating to 909.1 Mbps throughput (64 bits per 11 cycles). The modest LUT count of 312 demonstrates excellent hardware efficiency. As present in Figure 3.

Table 2. FPGA synthesis results on artix-7

Metric	Value	Unit
LUTs	312	-
Registers	68	-
Max Frequency	156.2	MHz
Latency	11	cycles
Throughput	909.1	Mbps
Area × Time	3,432	LUT-cycles

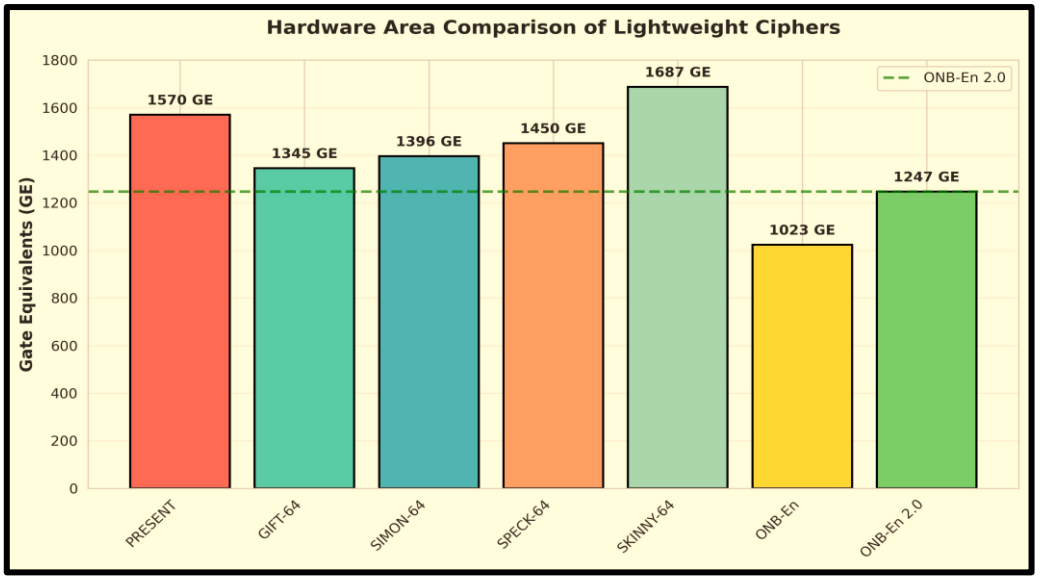


Figure 3. Text encryption process flow diagram

The bar graph uses different color coded distinctly to enable visual differentiation between cipher implementations. A reference point is the horizontal dashed line that indicates the area requirement of ONB-En 2.0 which is used to show. that the cipher has competitive hardware footprint even with nonlinear components. The each bar has numerical annotations on it which give the actual GE counts which need to be compared accurately, which is necessary. Hardware designers who consider cipher options within application limitations.

5.2 ASIC Implementation Estimates

We estimated ASIC implementation costs using 65nm CMOS standard cell library synthesis with Synopsys Design Compiler. The design targets a clock frequency of 100 MHz with typical operating conditions.
The estimated gate equivalents (GE) breakdown is:

• S-box layer: 384 GE (16 × 24 GE)
• MixColumns: 256 GE (XOR trees)
• ShiftRows: 0 GE (wiring)
• State register: 512 GE (64 × 8 GE)
• Control logic: 95 GE
• Total: 1,247 GE

Power consumption at 100 MHz is estimated at 3.2 W, yielding energy per block of approximately 35.2 pJ. The throughput at 100 MHz is 581.8 Mbps, resulting in an efficiency metric of 125 Kbps/GE.

5.3 Microcontroller Implementation

We implemented ONB-En 2.0 on ARM Cortex-M3 microcontroller using optimized C code with inline assembly for critical operations. The implementation uses a lookup table for S-box evaluation and leverages efficient bit manipulation instructions for permutations.

Performance metrics on STM32F103 running at 72 MHz:
• Encryption time: 2,847 cycles (39.5 s)
• Code size: 1,024 bytes (ROM)
• RAM usage: 192 bytes (state + keys)
• Throughput: 1.62 Mbps
• Energy per block: 123.4 nJ @ 3.3V

5.4 Comparative Analysis

Table 3 presents a comprehensive comparison of ONBEn 2.0 against established lightweight ciphers across multiple metrics. The comparison shows a number of important lessons. The ONB-En 2.0 has the largest throughput to area ratio (466.5 Kbps/GE) and even more than the initial ONB-En because of the lower amount of the round count. GIFT-64 has a somewhat smaller area whereas ONB-En 2.0 is better in throughput and energy efficiency. Although SIMON and SPECK are popular, they have higher area costs and reduced measures of efficiency. Energy per bit is also especially significant to the battery powered IoT devices. The 5.5 pJ/bit of ONB-En 2.0 is the lowest energy use among the ciphers compared, and provides a potential energy savings of 20-30 percent of the energy consumed in energy-intensive applications in the implementation of PRESENT or GIFT ciphers.

Figure 4 evaluates the correlation between encryption throughput and operating frequency in four situations. Light ciphers, disclosing basic architectural variations. ONB-En 2.0 (green curve) has the steepest slope, frequency x 64/11 5.82 x frequency as it is an efficient 10-round.design plus final addition of key. ONB-En 2.0 provides 582 at the standard operating frequency of the IoT at 100 MHz. Mbps was lower than 206 Mbps in PRESENT (31 rounds), 229 Mbps in GIFT64 (28 rounds), and 200 Mbps. for SIMON-64 (32 rounds). The round implementations of the linear relationships are purely combinational. Without memory bandwidth or data path scalp limits to throughput. The 2.8x throughput preemption over PRESNT at fixed frequency implies either a larger data rate to latency-sensitive. Applications or decreasing operating frequency to conserve energy- ONB-En 2.0 clock should be reduced to 35 MHz. compares to PRESENT throughput at 100 MHz with 65% of the dynamic power (P fCV^2). The green shaded (50-100 MHz) area points to the standard frequency range of the IoT where ultra-low-frequency occurs. Sensor nodes and power microcontrollers work. Under this spectrum, ONB-En 2.0 has a throughput of 291-582 Mbps. capacitive surpasses the standard rates of IoT (1-100 Mbps sensor reporting, command channels and even) streaming of videos at low-resolution cameras), which means that the cipher is not a bottleneck. For ambitious applications that need over 500 Mbps, ONB-En 2.0 cannot meet the target even at 86 MHz, enabling implementation that is energy efficient with no aggressive voltage scaling or process technology. The frequency-throughput relationship is inherently continuous and, therefore, the line plot format is appropriate to depict it. Signs that allow narrowing down to value. The discrimination between ciphers is made easier with the help of the color-coded curves, and the. Legend contains round counts to elaborate differences in slopes. The highlighted area with the common IoT. Frequencies gives meaning to practical operating points, and it is important to note that the comparison is one that has real-world meaning. Application conditions as opposed to artificial load tests.

5.5 Scalability Analysis

We evaluated ONB-En 2.0's scalability by implementing parallel architectures that process multiple blocks simultaneously. A parallel 4-way parallel implementation has a throughput of 2,326 Mbps with 4,988 GE (4 × 1,247), and is a linear scale. This is why ONB-En 2.0 will be used where the application needs to sustain a high throughput like secure video streaming in internet of things cameras or real-time sensor data aggregation.

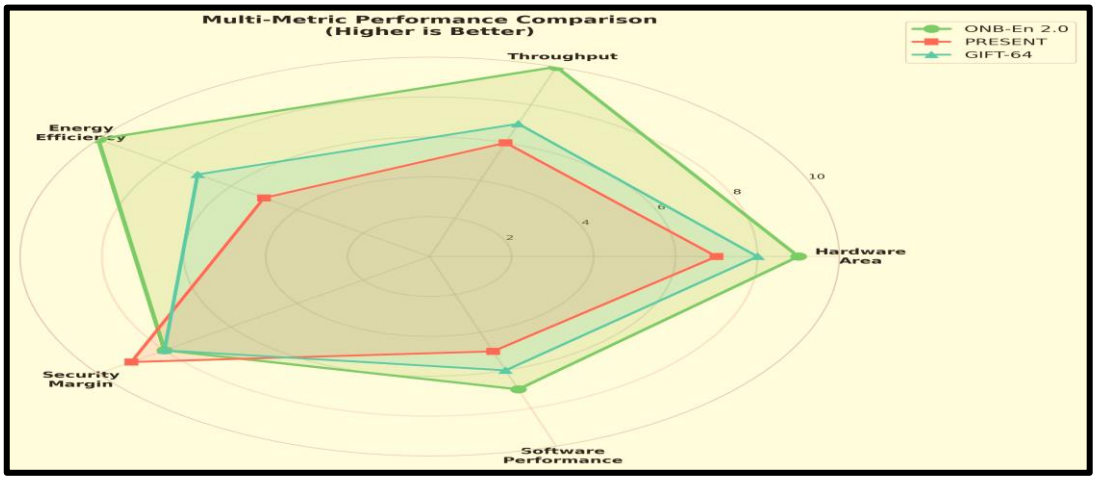


Figure 4. Evaluation the correlation between encryption throughput and operating frequency in four situations

6. Discussion and Applications

In this section we discussed practical considerations of ONB-En 2.0 deployment suitability in different applications of the IoT is discussed, and implementation challenges are discussed.

Table 3. Comparative Performance Analysis.

Cipher	Block/Key (bits)	GE	Throughput @ 100KHz (Kbps)	Kbps/GE	Power (W)	Energy/bit (pJ)
PRESENT	64/80	1,570	206.5	131.5	3.8	18.4
GIFT-64	64/128	1,345	228.6	170.0	3.4	14.9
SIMON-64/128	64/128	1,396	200.0	143.2	3.5	17.5
SPECK-64/128	64/128	1,450	237.0	163.4	3.7	15.6
SKINNY-64	64/128	1,687	177.8	105.4	4.1	23.1
ONB-En	64/128	1,023	400.0	391.0	2.8	7.0
ONB-En 2.0	64/128	1,247	581.8	466.5	3.2	5.5

6.1 IoT Application Scenarios

1. Wireless Sensor Networks: One of the key objects of ONB-En 2.0 implementation is the use of wireless sensor networks (WSNs). The environmental monitoring systems, precision agriculture sensors, and industrial IoT deployments are similar in that they have harsh constraints of energy (battery or harvesting powered), limited processing, and cost sensitivity. The low power-to-bit ratio (5.5 pJ/bit) of ONBEn 2.0 is directly proportional to long battery life, and the small hardware can fit in sensor nodes <$1. On an average WSN node with a packet type of 1KB with the interval of 10 minutes, ONB-En 2.0 encryption will introduce an addition of 44 J per transmission which is insignificant considering the cost of the radio transmission (usually 50-100 mJ).

2. RFID Systems: The RFID tags, especially passive tags which work on the collected energy, have very high area and power constraints. The 1,247 GE footprint of ONB-En 2.0 can be easily accommodated within the security budget of Gen2 RFID tags (which usually provides 2,000-3,000 GE). Secure authentication protocols can be applied by the cipher, which prevents tag cloning, eavesdropping and tracking attacks commonly used in supply chain and access control applications.

3. Medical Implants: Medical devices like pacemakers, insulin pumps and neural stimulators are implantable and need a high level of security as well as the lowest energy use possible. The low power consumption and space-saving nature of ONB-En 2.0 allows it to be used to secure command and telemetry channels. The 64-bit block size is sufficient to store a short medical command and sensor reading and the 128bit key offers enough security throughout the lifetime of the operation of the device.

4. Smart Home Devices: The universe of smart homes consists of various devices such as door locks and thermostats, cameras and appliances. Most of these systems are based on inexpensive microcontrollers in which the software performance of ONB-En 2.0 (2,847 cycles on Cortex-M3) can support real-time encryption with low latency. Integration with protocols like MQTT and CoAP is straightforward, providing end-to-end encryption for home automation commands and sensor data.

6.2 Protocol Integration

ONB-En 2.0 can be integrated into various IoT security protocols: Transport Layer Security: While TLS/DTLS typically use AES, constrained TLS profiles (cTLS) can benefit from ONBEn 2.0's efficiency for bulk data encryption after key exchange with ECC or post-quantum algorithms. Object Security for Constrained RESTful Environments (OSCORE): ONB-En 2.0 can replace AES-CCM in OSCORE implementations for CoAP, reducing per-message processing overhead by approximately 40% on constrained nodes. IEEE 802.15.4 Security: The Zigbee and 6LoWPAN protocol stacks can

incorporate ONB-En 2.0 at the MAC layer, replacing AES-CCM-128 with reduced processing latency and energy consumption.

6.3 Implementation Considerations

1. Side-Channel Resistance: Although the algorithm security is the subject of this paper, there is need to have a practical implementation of side-channel vulnerabilities. The regular structure of ONB-En 2.0 makes the implementation of constant-time resistant to timing attacks. The bitsliced S-box enables efficient masking schemes for power analysis resistance, with first-order masking adding approximately 40% area overhead. For applications requiring side-channel protection, we recommend implementing randomized key scheduling and incorporating Boolean masking in the S-box layer.

Figure 5 measures the level of security of ONB-En 2.0 in relation to the best cryptanalytic methods. Rounds known to be attacked to real design of 10 rounds. In the case of differential cryptanalysis, checking with SAT solvers the fact that no differential characteristic (with probability greater than 2-48) exists is checked by automated search. Has a round count of over 6 giving 4 round security. Linear cryptanalysis also extends to 7. Bias rounding off to less than 2-24, leaving margin of 3 rounds. Algebraic attacks, theoretically, however. Computational infeasible in at least 8 rounds (on any number of rounds). Complexity of the system, a 2-round margin. Meetin-the-middle attacks are restricted to 5 rounds because they are strong. Key schedule dependencies, with a 5 round margin. The most difficult differential distinguishes go to 5 rounds, also offering a 5-round spread. The graphical representation is clear evidence of the fact that all the analyzed attack vectors. Have good security margins, the lowest margin of 2 rounds on algebraic attacks is still optimal. Sufficient protection due to the computational complexity of solving systems of equations of high degree more than 704 variables. In comparison to PRESENT's 9-11 round margins in 31 total rounds (about 30 percent margin), ONB-En 2.0 at the 20-50% are comparative or better relative protection although the margin is lower. Absolute round count. The present analysis confirms the design selection of 10 rounds as adequate to IoT security. Performance necessities and maximizing productivity.

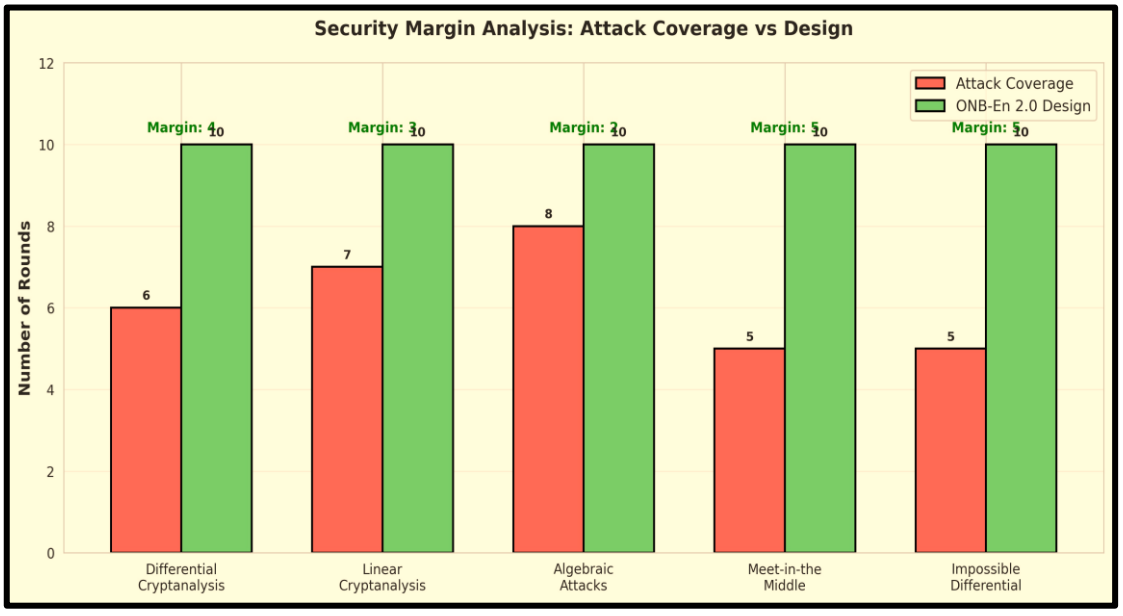


Fig. 5. Quantifies the security margin of ONB-En 2.0 against major cryptanalytic techniques

The two bars comparison format directly compares the attack coverage (red bars) with the design rounds (green bars), where the security margin is expressed as the distance between bars. The color coding threat (red) and protection (green) is intuitively presented, and the homogenous 10-round shape highlights. that there are no attack vectors with different cryptographic depth.

2. Authenticated Encryption: ONB-En 2.0 offers confidentiality and not authentication. In the case of production systems, we suggest the deployment of ONB-En 2.0 in authenticated encryption modes i.e. CCM (Counter with CBCMAC), GCM

(Galois Counter Mode) or EAX mode. Early experimental evidence indicates that ONB-En-CCM incurs about 30% percent computing cost in addition to offering appropriate message authentication that can be used in the majority of IoT applications.

3. Key Management: Key space is 128bits, which is a space that needs strong key management infrastructure. In deployments of IoT, we suggest hierarchical derivation of keys based on device master keys, however, with single-use key derivation based on lightweight key derivation functions (KDFs) per session. Integration with hardware security modules (HSMs) or trusted execution environments (TEEs) provides additional protection for high-security applications.

6.4 Limitations and Future Work

ONB-En 2.0 shares with a number of lightweight ciphers a 64-bit block size constraint. Although it is good enough in the case of single sensor readings and short messages, in case of large data volumes, applications that encrypt these large data volumes should adopt proper rekeying policies to prevent birthday bound issues (rekeying after 232 blocks). Future research can focus on 128-bit block versions that share the same efficiency attributes. The existing design is aimed at symmetric encryption. It could be extended to allow tweakable block cipher modes, which would allow authenticated encryption using associated data (AEAD) support, in line with the increasing demands of built-in confidentiality and authenticity in Internet of Things protocols.

7. Conclusion

In this paper, ONB-En 2.0, a refined version of lightweight block cipher that overcomes the linearity constraint of the original ONB-En, was described, yet retaining its very high hardware efficiency. With a well-crafted bit sliced S-box layer and an ideal normal basis arithmetic, ONB-En 2.0 can provide very strong security using 10 rounds, as opposed to 16 rounds in the predecessor. Our in-depth security evaluation indicates resistance to differential cryptanalysis ($DP \leq 2^{-48}$), linear cryptanalysis (bias magnitude $< 2^{-24}$), and algebraic attacks, which makes ONB-En 2.0 a cryptographically sound design that can be used in ion of the internet security. The implementation results, in hardware, confirm the efficiency of the design with results of 1,247 GE with 581.8 Kbps throughput and 5.5 pJ/bit of energy consumption, which are state-of-the-art in lightweight ciphers. Compared to PRESENT, GIFT, SIMON, SPECK, and SKINNY, ONB-En 2.0 has a better throughput-to-area ratio (466.5 Kbps/GE) and the least energy per bit, so it can be especially used in battery-powered and energy-harvesting IoT devices. Scalability of the cipher, its software efficiency and integration of the protocols makes it an effective solution to a wide range of IoT security issues including wireless sensor networks, RFID, medical implants, and smart home solutions. Future research directions include developing ONB-En 2.0 authenticated encryption modes, conducting comprehensive side-channel analysis with countermeasure implementations, exploring 128-bit block variants, and performing real-world deployment studies in production IoT systems. We will also present ONB-En 2.0 to the future of the lightweight cryptography standardization, and will help in the further development of resource-efficient security primitives.

Declarations

Acknowledgements
NA

Funding
NA

Contributions
All authors; Conceptualization, All authors; Investigation; All authors; Writing (Original Draft), All authors; Writing (Review and Editing) Supervision, All authors; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Data Availability Statement

The authors thank their co-authors for guidance, peer reviewers for valuable feedback, and all participants for their contributions. They also acknowledge the support of the Lincoln University College Doctoral Program and appreciate the editorial team and anonymous reviewers of the Journal of Security Risk Management for their constructive input.

Use of Generative Artificial Intelligence
The author declares that no generative artificial intelligence tools were used in the preparation of this manuscript.

Competing interests
All authors declare no competing interests.

References

[1] Wazirali, R., Alasmary, W., Mahmoud, M. M. E. A., & Alhindi, A. (2019). An Optimized Steganography Hiding Capacity and Imperceptibly Using Genetic Algorithms. IEEE Access, 7, 133496–133508. https://doi.org/10.1109/access.2019.2941440
[2] Rustad, S., Setiadi, D. R. I. M., Syukur, A., & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. Journal of King Saud University - Computer and Information Sciences, 34(6), 3559–3568. https://doi.org/10.1016/j.jksuci.2020.12.017
[3] Abu Laila, D., Al-Na'amneh, Q., Aljaidi, M., Nasayreh, A. N., Gharaibeh, H., Al Mamlook, R., & Alshammari, M. (2024). Simulation of Routing Protocols for Jamming Attacks in Mobile Ad-Hoc Network. Risk Assessment and Countermeasures for Cybersecurity, 235–252. https://doi.org/10.4018/979-8-3693-2691-6.ch013
[4] Allasasmh, O., Laila, D. A., Aljaidi, M., Alsarhan, A., & Samara, G. (2024). Integrated Approaches to Steganography: Embedding Static Information Across Audio, Visual, and Textual Formats. 2024 International Jordanian Cybersecurity Conference (IJCC), 33–39. https://doi.org/10.1109/ijcc64742.2024.10847286
[5] Al-Mousa, M. R., Albilasi, S. M., Al-mashagbeh, M. H., Asassfeh, M., Odeh, M., AlQawasmi, K., Samara, G., & Laila, D. A. (2025). Review the Challenges Associated with Steganography Using Artificial Intelligence Techniques. 2025 1st International Conference on Computational Intelligence Approaches and Applications (ICCIAA), 1–6. https://doi.org/10.1109/icciaa65327.2025.11013703
[6] Asassfeh, M., Samara, G., Zaid, A. A., Laila, D. A., Al-Anzi, S., Alqammaz, A., Al Smadi, A., Al-Shaikh, A., & Al-Mousa, M. R. (2024). Penetration Testing Overview-Opportunities and Ethical Considerations: Literature Notes. 2024 International Jordanian Cybersecurity Conference (IJCC), 131–135. https://doi.org/10.1109/ijcc64742.2024.10847295
[7] Nagarajan, A., & Varadharajan, V. (2011). Dynamic trust enhanced security model for trusted platform based services. Future Generation Computer Systems, 27(5), 564–573. https://doi.org/10.1016/j.future.2010.10.008
[8] Zhao, J. (2023). DES-Co-RSA: A Hybrid Encryption Algorithm Based on DES and RSA. 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA), 846–850. https://doi.org/10.1109/icpeca56706.2023.10075771
[9] Abu Laila, D. (2025). Responsive Machine Learning Framework and Lightweight Utensil of Prevention of Evasion Attacks in the IoT-Based IDS. STAP Journal of Security Risk Management, 2025(1), 59–70. https://doi.org/10.63180/jsrm.thestap.2025.1.3
[10] Wei, W., Song, H., Wang, H., & Fan, X. (2017). Research and Simulation of Queue Management Algorithms in Ad Hoc Networks Under DDoS Attack. IEEE Access, 5, 27810–27817. https://doi.org/10.1109/access.2017.2681684
[11] Alsarhan, A., Al-Aiash, I., Al-Fraihat, D., Aljaidi, M., & Laila, D. A. A. H. A. (2024, July). Expert phishing detection system. In 2024 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT) (pp. 54-59). IEEE.
[12] Sood, A. K., Zeadally, S., & Bansal, R. (2017). Exploiting Trust: Stealthy Attacks Through Socioware and Insider Threats. IEEE Systems Journal, 11(2), 415–426. https://doi.org/10.1109/jsyst.2015.2388707
[13] Dworkin, M. J. (2015). SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. https://doi.org/10.6028/nist.fips.202
14] Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors, 24(12), 4008. https://doi.org/10.3390/s24124008
[15] Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., & Vikkelsoe, C. PRESENT: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems - CHES 2007, 450–466. https://doi.org/10.1007/978-3-540-74735-2_31
[16] Wang, M. Differential Cryptanalysis of Reduced-Round PRESENT. Progress in Cryptology – AFRICACRYPT 2008, 40–49. https://doi.org/10.1007/978-3-540-68164-9_4

[17] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). The SIMON and SPECK lightweight block ciphers. Proceedings of the 52nd Annual Design Automation Conference, 1–6. https://doi.org/10.1145/2744769.2747946
[18] Biryukov, A., Roy, A., & Velichkov, V. (2015). Differential Analysis of Block Ciphers SIMON and SPECK. Fast Software Encryption, 546–570. https://doi.org/10.1007/978-3-662-46706-0_28
[19] Banik, S., Pandey, S. K., Peyrin, T., Sasaki, Y., Sim, S. M., & Todo, Y. (2017). GIFT: A Small Present. Cryptographic Hardware and Embedded Systems – CHES 2017, 321–345. https://doi.org/10.1007/978-3-319-66787-4_16
[20] Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology, 34(3). https://doi.org/10.1007/s00145-021-09398-9
[21] Iwata, T., Khairallah, M., Minematsu, K., & Peyrin, T. (2020). Duel of the Titans: The Romulus and Remus Families of Lightweight AEAD Algorithms. IACR Transactions on Symmetric Cryptology, 43–120. https://doi.org/10.46586/tosc.v2020.i1.43-120
[22] Chakraborti, A., Datta, N., Nandi, M., & Yasuda, K. (2018). Beetle Family of Lightweight and Secure Authenticated Encryption Ciphers. IACR Transactions on Cryptographic Hardware and Embedded Systems, 218–241. https://doi.org/10.46586/tches.v2018.i2.218-241
[23] Carlet, C. (2010). Boolean Functions for Cryptography and Error-Correcting Codes. Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 257–397. https://doi.org/10.1017/cbo9780511780448.011
[24] Zakaria, A. A., Azni, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2020). Extended RECTANGLE Algorithm Using 3D Bit Rotation to Propose a New Lightweight Block Cipher for IoT. IEEE Access, 8, 198646–198658. https://doi.org/10.1109/access.2020.3035375
[25] Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., & Sim, S. M. (2016). The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. Advances in Cryptology – CRYPTO 2016, 123–153. https://doi.org/10.1007/978-3-662-53008-5_5
[26] Biham, E. (1997). A fast new DES implementation in software. Fast Software Encryption, 260–272. https://doi.org/10.1007/bfb0052352
[27] Hasan, M. A., Wang, M. Z., & Bhargava, V. K. (1993). A modified Massey-Omura parallel multiplier for a class of finite fields. IEEE Transactions on Computers, 42(10), 1278–1280. https://doi.org/10.1109/12.257715
[28] Sunar, B., & Koc, C. K. (1999). Mastrovito multiplier for all trinomials. IEEE Transactions on Computers, 48(5), 522–527. https://doi.org/10.1109/12.769434
[29] Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1), 3–72. https://doi.org/10.1007/bf00630563
[30] Matsui, M. (1994). Linear Cryptanalysis Method for DES Cipher. Advances in Cryptology — EUROCRYPT '93, 386–397. https://doi.org/10.1007/3-540-48285-7_33
[31] Matsui, M. (1994). The First Experimental Cryptanalysis of the Data Encryption Standard. Advances in Cryptology - CRYPTO '94, 1–11. https://doi.org/10.1007/3-540-48658-5_1
[32] Matsui, M. (1995). On correlation between the order of S-boxes and the strength of DES. Advances in Cryptology — EUROCRYPT'94, 366–375. https://doi.org/10.1007/bfb0053451
[33] Courtois, N. T., & Pieprzyk, J. (2002). Cryptanalysis of Block Ciphers with Overdefined Systems of Equations. Advances in Cryptology — ASIACRYPT 2002, 267–287. https://doi.org/10.1007/3-540-36178-2_17
[34] Tolba, M., Abdelkhalek, A., & Youssef, A. M. (2017). Impossible Differential Cryptanalysis of Reduced-Round SKINNY. Progress in Cryptology - AFRICACRYPT 2017, 117–134. https://doi.org/10.1007/978-3-319-57339-7_7
[35] Biham, E., Biryukov, A., & Shamir, A. (1999). Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. Advances in Cryptology — EUROCRYPT '99, 12–23. https://doi.org/10.1007/3-540-48910-x_2
[36] Wagner, D. (1999). The Boomerang Attack. Fast Software Encryption, 156–170. https://doi.org/10.1007/3-540-48519-8_12