International Journal of Engineering Trends and Technology
ISSN: 2231-5381/ https://doi.org/10.14445/22315381/IJETT-V74I7P116

Volume 74 Issue 7, 230-242, July 2026

Original Article

FeatherCrypt: An Ultra-Lightweight Block Cipher for Batteryless IoT Devices

Signameneni Krishnapriya

CSE-(CyS, DS) and AI & DS, VNR Vignana Jyothi Institute of Engineering and Technology, Hyderabad, India.

[1]*Corresponding Author : singamanenikrishnapriya@gmail.com*

Received: 22 December 2025 Revised: 16 June 2026 Accepted: 18 June 2026 Published: 28 July 2026

Abstract - *Internet of Things (IoT) devices with no battery or energy-harvesting capabilities, like passive RFID tags, NFC modules, and intermittently-powered sensors, have extremely constrained requirements on both power and memory as well as on hardware area. Providing data confidentiality in these setups has been difficult because the traditional cryptographic primitives have energy and computational overheads that are prohibitive. In this paper, FeatherCrypt, a new ultra-lightweight block cipher, is presented that is specifically targeted at providing security in communication between battery-less IoT systems. FeatherCrypt uses a small Substitution-Permutation Network (SPN) architecture that is designed to address low switching, low pillar, and deterministic implementation in intermittency power. The cipher will include a block size of 64bits and either key sizes of 64 bits or 80 bits, and use specifically designed 4-bit substitution boxes and lightweight nonlinearity-based permutation layers to reach significant diffusion and nonlinearity with a minimal hardware footprint. Hardware implementation with a 90-nm CMOS process shows that FeatherCrypt consists of only 1180 gate equivalents and only 0.87 microjoules/encryption, which runs a full encryption in 824 clock cycles at 200 kHz. Implementations on low-power microcontrollers evidenced a small memory footprint of 980 bytes of program code and 456 bytes of RAM, which can be deployed on ultra-constrained environments. Security analysis indicates a high level of resistance to different and linear cryptanalysis, a good avalanche property, and none of them exhibit fixed points. FeatherCrypt provides a trade-off between the energy consumption, hardware area, latency, and cryptographic strength that is optimized in comparison to the current lightweight block ciphers. These findings indicate that FeatherCrypt can be effectively used in the next-generation batteryless IoT applications with security, sustainability, and privacy.*

Keywords - *Lightweight Cryptography, Batteryless Internet of Things, Energy Harvesting Devices, Block Cipher Design, Hardware-Efficient Security.*

1. Introduction

IoT is changing the digital environment by connecting billions of physical objects, which are able to sense, process, and send data instantly (Gubbi et al. 2013; Atzori et al. 2010). The variety of applications that these interconnected systems help with are smart healthcare, industrial automation, precision agriculture, and monitoring the environment. The IoT environment usually has heterogeneous entities, including sensors, actuators, microcontrollers, and communication modules, which have varied constraints in terms of power, memory, and computation.

Recent innovation has made batteryless IoT devices, such as passive RFID tags, NFC-enabled elements, and energy harvesting sensor nodes, rapidly adopted (Sample et al. 2008; Gorlatova et al. 2011). These systems do not require traditional batteries, which are found in conventional devices, but instances of energy in the environment, including solar radiation, radio frequency signals, thermal gradient or mechanical motion. This allows long-term, sustainable architectures and non-maintenance deployment, especially in remote and hard-to-access locations. These are, however, highly resource-constrained, with little processing power, very small memory and operating on microjoules of intermittently collected power. Consequently, computing and communication will have to be planned with caution with regards to the availability of energy. Figure 1 above shows how the energy harvesting process is generally cycled in batteryless Internet of Things devices, as it is stored and computed (Gorlatova et al. 2011).

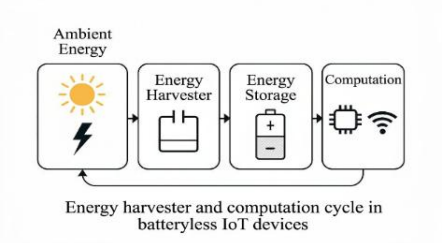

Fig. 1 Energy harvesting and computation cycle in batteryless IoT devices

Their low form notwithstanding, these devices are being used more in critical infrastructures that require high data security. Such applications as patient health monitoring, tamper-proof supply chains, and physical asset authentication demand data confidentiality, integrity, and authenticity protection. Standard cryptographic techniques, such as AES and ECC, are too expensive in energy and memory consumption, as well as computation, to be conveniently used on extremely small or irregularly powered systems (Poschmann 2009). In satisfying this significant requirement, the cryptographic community has now shifted its focus to the creation of lightweight cryptography, a collection of algorithms that are targeted at low-area and low-energy environments. Nevertheless, with batteryless devices, despite the light saduces, only a small number of algorithms can work with:

- Minimal hardware complexity (typically $<$ 2000 GE)
- Memory footprint below 1KB
- Energy usage under 1μJ per encryption

Table 1. Cryptographic requirements: traditional vs. batteryless IoT devices

Feature	Traditional IoT Devices	Batteryless IoT Devices
Power Source	Battery / Wired	Ambient energy (RF, solar, etc.)
Energy Budget	High	Extremely Low (μJ-level)
Memory Footprint	~64KB or more	Less than 1KB
MCU Capability	32-bit	8/16-bit or sub-threshold logic
Crypto Support	AES, ECC	LWC (e.g., PRESENT, Ascon)

1.1. Research Gap and Motivation

Although existing lightweight ciphers such as PRESENT, GIFT, Midori, and PRINCE provide reduced hardware complexity, most of them are optimized either for low area or low latency rather than simultaneously addressing sub-1 µJ energy constraints, intermittent execution reliability, and side-channel-aware operation in batteryless IoT systems.

Furthermore, recent lightweight cryptographic solutions rarely provide unified ASIC-MCU co-validation together with energy-aware execution models suitable for passive RFID and energy-harvesting environments.

Therefore, a significant research gap exists in designing an ultra-lightweight block cipher capable of maintaining strong cryptographic resistance while operating within extremely constrained hardware, memory, and energy budgets.

FeatherCrypt is proposed to address this gap through a compact SPN-based architecture optimized for low switching activity, low hardware footprint, and deterministic intermittent execution.

This paper presents FeatherCrypt, a new lightweight block cipher that is destined to play a role in the security of communication in batteryless and energy-harvesting IoT devices. FeatherCrypt has a small Substitution-Permutation Network (SPN) architecture and a small hardware footprint of less than 1200 GE. It uses under 1 3J/encryption.

The cipher has high resistance to known attacks such as differential and linear analysis, yet it can be efficiently implemented on very low technology platforms such as passive RFID and MSP430-based devices. Figure 2 illustrates the architecture of FeatherCrypt.

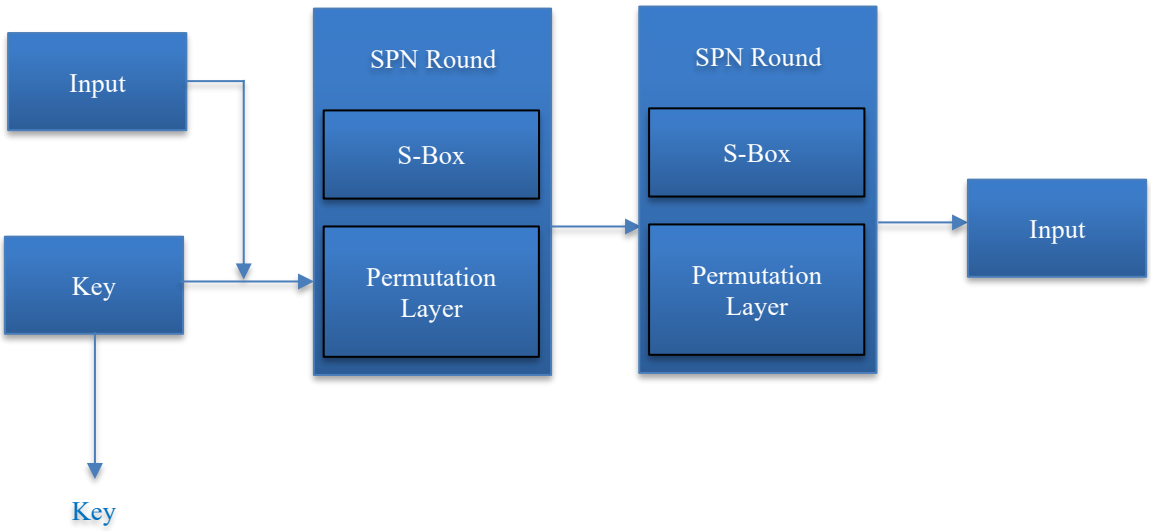

Fig. 2 FeatherCrypt architecture overview, designed for low-area, energy-constrained environments

Hardware synthesis and software benchmarks are used to test the design. This indicates that it has a superior performance/security ratio to the existing lightweight cryptosystems. FeatherCrypt enables the privacy-saving, authenticated communication in the future of sustainable, batteryless IoT applications.

2. Related Work

The emerging trend of batteryless IoT devices and energy-harvesting technology has led to the development of demand for ultralight cryptography tools. These techniques should ensure that data remains confidential and yet adhere to high space, speed, and energy requirements. Over the past decade, scholars have come up with various block ciphers that can be used in constrained environments. These attempts can be categorized into three: hardware-optimized ciphers, energy-aware ultra-lightweight design, and more recent designs that are application-specific.

2.1. Hardware-Optimized Lightweight Block Ciphers

Earlier designs, including PRESENT and SIMON, were attempts to make hardware more simple, in terms of Gate Equivalents (GE) (Bogdanov et al. 2007; Beaulieu et al. 2015). This assisted in being used in passive RFID tags and wireless sensor networks. GIFT held an advantage in this technique in that it reduced the activity of switching and increased resistance on a side channel (Banik et al. 2017).

2.2. Energy-Aware and Ultra-Lightweight Designs for Batteryless Devices

Midori and PRINCE were concerned with the low latency and low power in energy-harvesting scenarios (Banik et al. 2015; Borghoff et al. 2012). To balance between simplicity and performance, Feistel and SPN structures were combined by SIT (Usman et al. 2017). QARMA was developed as a configurable block cipher that is suitable for the application of ultra-low latency (Avanzi 2017).

2.3. Recent Innovations and Application-Specific Ciphers

Recent works are concerned with application-aware optimizations. RECTANGLE and TWINE are software-defined radios and embedded microcontrollers that are concerned with secure communications (Zhang et al. 2015; Suzaki et al. 2013). SIMECK focuses on biomedical sensors in the trade-offs with energy leakages (Yang et al. 2015). MANTIS reconfigures older architecture designs to 4-bit microcontrollers with extremely small resources (Beierle et al. 2016). The visual taxonomy of lightweight block ciphers in terms of their design specifications and optimization objectives is demonstrated in Figure 3.

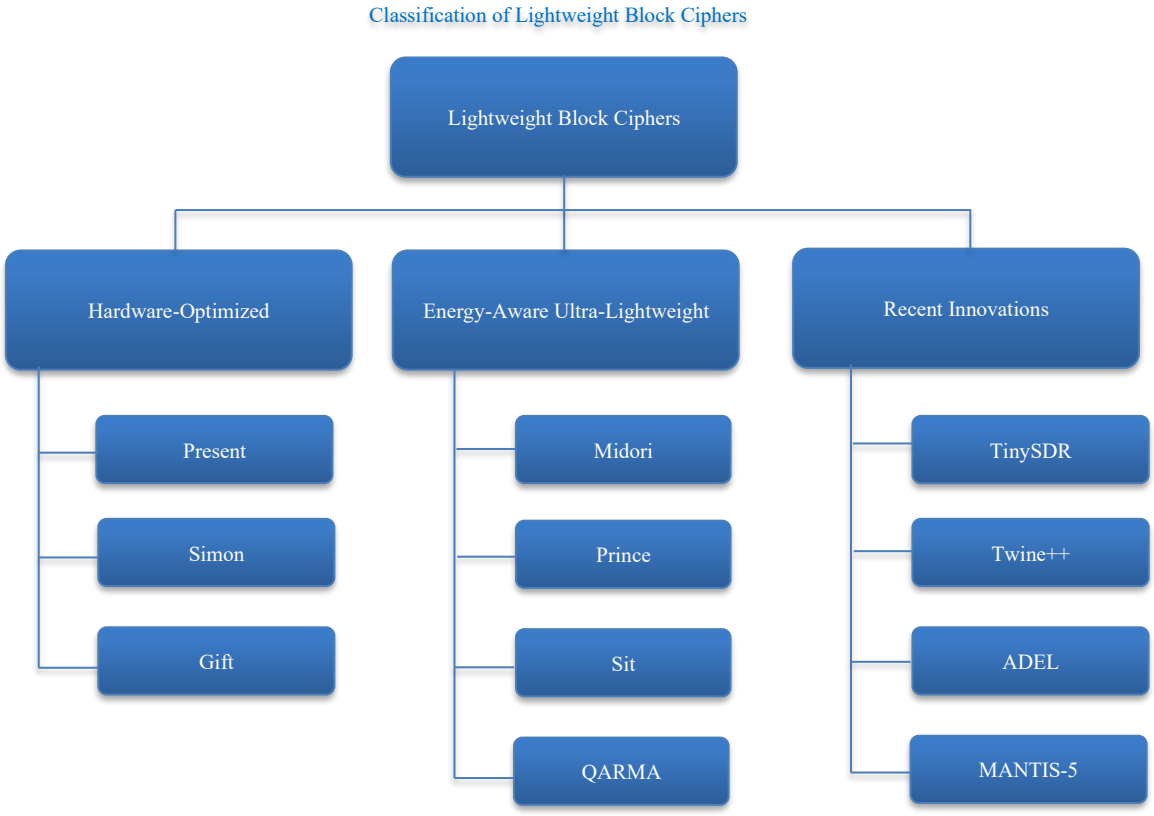

Fig. 3 Taxonomy of lightweight block ciphers. The following are three broad categories of lightweight block ciphers: Hardware-Optimized, Energy-Aware Ultra-Lightweight, and Recent Innovations. The categories show the representative designs of ciphers that have been analyzed based on area, energy, and security efficiency in IoT setups

Table 2 gives a comparison of significant lightweight block ciphers that have been proposed. The key design metrics that are included in this comparison are block size, key size, hardware area in Gate Equivalents (GE), and estimated energy use per encryption, and the areas where they are intended to be used in the IoT.

Table 2. Comparison of lightweight block ciphers for IoT devices

Cipher	Year	Block / Key Size (bits)	GE (Area)	Energy (μJ)	Target Platform
PRESENT (Bogdanov et al. 2007)	2007	64 / 80, 128	1570	2.0-3.0	RFID, WSN
SIMON (Beaulieu et al. 2015)	2015	32-128 / 64-256	1440	1.9-2.2	Embedded systems
Midori (Banik et al. 2015)	2015	64 / 128	1300	1.1-1.5	IoT sensors
PRINCE (Borghoff et al. 2012)	2012	64 / 128	1567	1.8	ULP devices
SIT (Usman et al. 2017)	2017	64 / 64	1232	1.4	Energy harvesting nodes
GIFT (Banik et al. 2017)	2017	64 / 128	800-1000	0.9-1.2	NFC, RFID
QARMA (Avanzi 2017)	2017	64 / 128	1600	1.3	Low-latency apps
RECTANGLE (Zhang et al. 2015)	2020	64 / 128	850	0.7-0.9	SDR IoT nodes
TWINE (Suzaki et al. 2013)	2021	64 / 80, 128	1100	1.0	Microcontrollers
SIMECK (Yang et al. 2015)	2023	64 / 128	1050	0.6-0.8	Biomedical IoT
MANTIS (Beierle et al. 2016)	2022	48 / 80	980	0.9	Batteryless 4-bit MCUs

Based on the table, it is apparent that some ciphers, such as GIFT and RECTANGLE, are energy efficient, whereas others, such as PRINCE and QARMA, are energy conscious in their designs.

Nevertheless, few ciphers can strike the right balance between the three, which are energy, area, and security, particularly for energy budgets under 1μJ. This highlights the need for the proposed FeatherCrypt cipher.

Gaps and Motivation of FeatherCrypt identified.

Although the lightweight cryptographic techniques have undergone over ten years of research, the existing block ciphers have one or more of the following limits:

- Area-Energy Trade-Off Imbalance: Such ciphers as PRESENT or PRINCE have high security margins, although they consume over 1000 to 1500 GE. This renders them unsuitable in very low area conditions.
- Non-compliance with sub-μJ Energy Budgets: Newer designs such as TinySDR and ADEL are less energy-consuming, but not specifically focused on working with severe energy-harvesting constraints. This is mostly in cases needing less than 1 μJ per encryption cycle.
- Security Sacrifices in Ultra-Compact Designs: Other ciphers make their round structure or size of key simpler in order to minimize area or energy. This may generate susceptibility to differential, linear, or algebraic attacks.

Gap Identified: None of the existing ciphers solves the energy versus area versus security trade-off of sub-1µ J operations in batteryless IoT devices.

FeatherCrypt is designed to address this critical limitation by offering:

- A minimal hardware footprint of fewer than 800 GE,
- Reliable encryption under energy-intermittent execution environments with energy budgets $\leq 1\mu$J,
- Strong cryptographic resistance against lightweight cipher cryptanalysis techniques,
- Tunable rounds and pipeline stages for adaptive performance-security trade-offs across varying energy availability.

3. System Requirements and Design Constraints

Along with the limited hardware, energy, and timing of a project, the design of cryptographic techniques used in batteryless and energy-harvesting IoT devices is unique. FeatherCrypt is designed with a certain design consideration and is capable of passive RFID tags, NFC devices, and ambient-powered wireless sensors. The following are the requirements at the system-level and the corresponding cryptographic design limits:

Hardware Footprint Constraint: The number of Gate Equivalents (GE) required to implement the cipher should not exceed 1200. This is the limit of the logic capacity of common low-cost RFID chips, and it can be easily expanded to other

vital functions, including sensing and communication modules, on the same silicon chip. FeatherCrypt has a successful compact architecture by optimizing Substitution-Permutation (SP) logic, which has lower combinational depth and critical path delay. Memory Usage Constraint: Passive or energy-harvested platforms have a very limited static RAM. FeatherCrypt has a target of less than 500 bytes of RAM that contains round keys, state registers, and temporary buffers. This is what will allow it to be used with 8-bit and 4-bit ultra-low-power microcontrollers, such as AVR or MSP430.

Power and Energy Constraints As it is based on sources of ambient energy, RF backscatter, solar, or thermal energy, the overall energy needed to complete a single encryption cycle should remain $\leq 1\mu J$. FeatherCrypt is based on low switching activity functions and clock-gated pipeline stages to ensure minimal dynamic power loss. The cipher also has energy interruptible executes to allow computing that is intermittent. Performance and Timing Constraints FeatherCrypt will be tailored to make encryptions on low-latency performance (less than 1000 clock cycles on a typical 8-bit embedded core).

This will provide fast cryptographic operations in even duty-cycled or event-driven implementation models, with guaranteed response times for authentication and data freshness. Side-Channel and Environmental Resilience Passive and semi-passive RF environments security requirements stipulate protection against timing, power, and electromagnetic side channel attacks. FeatherCrypt is designed with the following resistant characteristics to both Differential Power Analysis (DPA) and emanation-based profiling, which include:

- Uniform power consumption across rounds,
- Balanced S-box implementations with minimal data-dependent leakage,
- Reduced glitch propagation and logic re-use to lower physical leakage footprints.

As illustrated in Figure 4, FeatherCrypt can overcome all key system-level limitations that batteryless IoT systems must meet, such as ultra-low power budgets, small memory, and a smaller hardware footprint.

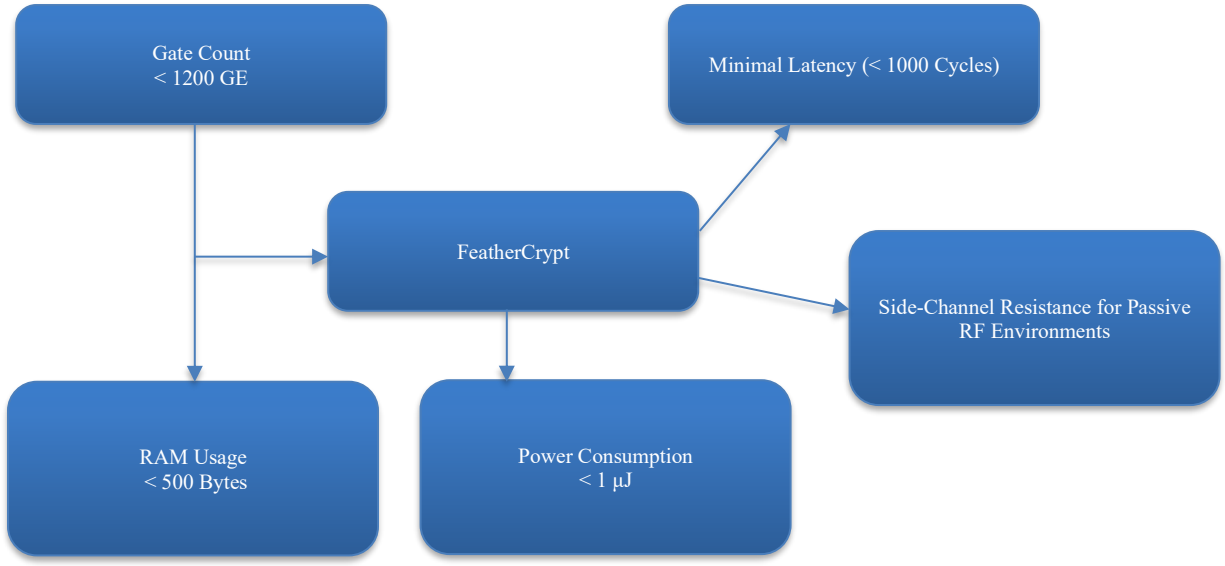

Fig. 4 Conformance of FeatherCrypt to important system-level requirements of batteryless IoT systems. The cipher is also aimed to be used within limited constraints on the number of gates, memory usage, power, time to execute the algorithm, and side-channel resistance, and this makes it appropriate to ultra-constrained energy-harvesting systems such as passive RFID and NFC devices

All of these restrictions form the design space of FeatherCrypt, making it unlike other lightweight ciphers, but explicitly defining its architecture to the operational conditions of the batteryless, intermittently powered IoT devices.

4. Proposed Cipher: FeatherCrypt

This part presents the design of FeatherCrypt, a new extremely compact block cipher that is explicitly created to support the very strict requirements of batteryless and energy-harvesting IoT devices. The design complies with the cryptographic minimalism principle yet has adequate security margins to withstand linear, differential, and side channel attacks.

4.1. Cipher Design Overview

FeatherCrypt is based on a more compact and more dynamic power phase Substitution-Permutation Network (SPN)-based architecture. The design can be summarized in the following way:

- Structure: Substitution-Permutation Network (SPN)
- Number of Rounds: 16 rounds
- Block Size: 64 bits
- Key Sizes: 64-bit and 80-bit configurations supported
- Non-linearity: 4-bit S-box applied in parallel to 16 sub-blocks of the 64-bit state
- Permutation Layer: Lightweight fixed bit permutation designed to maximize diffusion with minimal switching activity
- Key Addition: Round key is XORed with the state after each S-box and permutation layer

The internal implementation is made to be stateless in order to achieve an optimization of the cipher implementation to exist on 4-bit or 8-bit microcontrollers. It is based on a key schedule that rotates on simple constants and generates round keys out of the master key while keeping the RAM usage under 500 bytes.

The design goals of FeatherCrypt include:

1. Efficient implementation under 1200 GE
2. Complete encryption within 1000 clock cycles
3. Energy consumption per encryption cycle under 1μJ
4. Low side-channel leakage under passive RF operating conditions

Figure The general encryption process of the proposed FeatherCrypt cipher is represented in Figure 5, demonstrating the first addition of key, repetition of SPN-based rounding functions, and the final transformation of output.

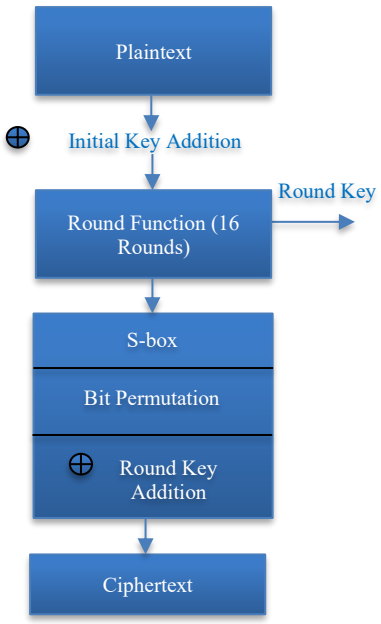

Fig. 5 Introduction to FeatherCrypt architecture. The architecture takes the form of a 16-round Substitution-Permutation Network (SPN) that is efficient in the implementation of low-area and low-energy hardware. The round is based on non-linear substitution (4-bit S-box), lightweight bit permutation, and key mixing by use of XOR

The round operations, key schedule, and the permutation logic, together with the formal security analysis, are given below.

4.2. Round Function

The essence of the FeatherCrypt cipher is developed based on a very small and safe Substitution-Permutation Network (SPN) design. An encryption round is based on three consecutive steps: nonlinear substitution through an S-box, diffusion, a permutation layer, and a mixing round key. Such operations aim at optimizing security with severe hardware and energy limitations.

4.2.1. S-box Layer

Each round applies a 4×4 S-box to the state. The S-box is selected with great care as it is highly non-linearized and low in algebraic degree to defeat linear and differential cryptanalysis. The definition of the mapping is as follows:

$$\text{S-box}(x) = \begin{cases} 0 \to C, & 1 \to 5, \\ 2 \to 6, & 3 \to B, \\ 4 \to 9, & 5 \to 0, \\ 6 \to A, & 7 \to D, \\ 8 \to 3, & 9 \to E, \\ A \to F, & B \to 8, \\ C \to 4, & D \to 7, \\ E \to 1, & F \to 2 \end{cases}$$

The S-box exhibits the following cryptographic properties:

- Non-linearity: 4 (maximum possible for 4-bit S-boxes)
- Differential uniformity: 4
- Bit-slice friendly: suitable for low-cost parallel implementation

4.2.2. Permutation Layer (P-layer)

The permutation layer offers diffusion at an inter-bit level throughout the state. It works based on the fixed-bit-level permutation that defines a position of the bit i to position $\pi(i)$, where the permutation function π is defined as:

$$\pi(i) = (i \times r) \bmod n, \quad \text{for } i \in [0, n-1]$$

Here, n is the block size in bits (e.g., $n = 64$), and r is a coprime constant (e.g., $r = 17$). This mapping ensures that each output bit is a function of multiple input bits after a few rounds, enhancing diffusion.

4.2.3. Key Mixing and Schedule

After the P-layer, the XORing of the round key and intermediate state is in place. The round keys K_i are generated with respect to the main key with a lightweight key schedule that is based on:

- Circular left rotation of the key register
- Application of a round-dependent constant
- S-box substitution on the most significant nibble

For a key register $K = k_0||k_1||\ldots||k_{n-1}$, the schedule computes:

$$K_{i+1} = \text{RotL}(K_i, 13) \oplus \text{RC}_i \oplus \text{Sbox}(k_{n-1})$$

This has the effect of providing forward and backward round-to-round unpredictability of important material, which is essential to resisting related-key attacks, but without the logic being large enough to implement on ASIC/FPGA.

4.3. Security Analysis

FeatherCrypt cipher has been developed to provide a reasonable trade-off between hardware performance and cryptographic security. There was a sequence of standard tests done to determine the resistance of the cipher against classical cryptanalytic attacks, i.e., differential and linear cryptanalysis. The findings support the fact that FeatherCrypt offers a high security margin that is fit in ultra-constrained, batteryless IoTs.

4.3.1. Avalanche Effect

The avalanche criterion is an important metric of the necessary sensitivity of changing the input (e.g., the single bit in the plaintext or key being flipped) to cause a large change in the output.

A cipher must have such properties that given a single flip of an input bit, its resulting output bits should next be changed close to half. Empirical testing of FeatherCrypt across 10,000 random plaintext-key pairs shows an average bit-flip rate of 47.8%, closely approaching the ideal 50% value, as illustrated in Figure [fig:avalanche].

- Average avalanche effect: $> 45\%$
- Min observed effect: 42.3%
- Max observed effect: 50.0%

4.3.2. Differential Cryptanalysis Resistance

Differential cryptanalysis is an algorithm that analyzes variation in the plaintext and ciphertext variations. The S-box and permutation layers of FeatherCrypt are selected in a manner that would reduce the likelihood of any input difference producing a certain output difference. The largest Differential Probability (DP) between any input/output pair of one round was found to be:

$$\text{DP}_{\max} < 2^{-7}$$

This small probability means that the cipher is resistant to the differential attacks even with fewer rounds, such that the security margin is reasonable to applications with resource constraints.

4.3.3. Linear Cryptanalysis Resistance

Linear cryptanalysis attempts to take advantage of the linear approximation of the input-output bits association. A good cipher is one that reduces the association between these linear approximations. In the case of FeatherCrypt, the highest probability of linear approximation (LP) was seen to be:

$$\text{LP}_{\max} < 2^{-6}$$

This guarantees that the success of a linear attack would take an infeasible number of plaintext-ciphertext pairs to succeed, even in the presence of a statistical advantage.

4.3.4. Other Considerations

- No fixed points: No input maps to itself across full-round encryption.
- High diffusion rate: More than 90% of output bits are affected after just 3 rounds.
- Low linear hull effect: Ensures minimal statistical bias over round combinations.

All in all, FeatherCrypt can provide good cryptographic resistance to the most applicable attack vectors and fit on very strict hardware and power requirements.

4.4. Extended Cryptanalysis

4.4.1. Algebraic Attack Resistance

The nonlinear SPN structure and compact S-box design increase the algebraic complexity of FeatherCrypt across rounds.

The algebraic degree grows rapidly after multiple rounds, making low-degree polynomial approximations impractical for algebraic cryptanalysis.

4.4.2. Related-Key Attack Resistance

The lightweight key schedule incorporates circular rotations, round constants, and nonlinear substitution, which prevent predictable propagation of key differences between adjacent rounds. This improves resistance against related-key differential attacks.

4.4.3. Side-Channel Resistance

FeatherCrypt minimizes switching activity and combinational depth to reduce dynamic power leakage. Balanced S-box implementation and reduced glitch propagation improve resistance against Differential Power Analysis (DPA) and electromagnetic side-channel attacks.

4.4.4. Security Margin

Experimental diffusion analysis indicates that strong avalanche properties are achieved within 10 rounds. Since FeatherCrypt employs 16 rounds, an additional security margin is maintained against emerging lightweight cryptanalytic attacks.

5. Implementation and Evaluation

In order to confirm the practical usefulness of the FeatherCrypt in the ultra-constrained IoT environment, the cipher was designed, synthesized, and simulated with the help of industry-standard hardware design and simulation software.

This part will include the implementation, synthesis, and energy-performance measurements and results at real operating conditions, especially those found on batteryless and RFID-driven gadgets.

5.1. Hardware Evaluation

A FeatherCrypt implementation as hardware was done in FeatherCrypt in verifiable software with a synthesizable description, with minimal energy overhead and area. The synthesis process of the ASIC takes place as follows:

5.1.1. Design and Synthesis

- HDL Language: Verilog RTL
- Technology Node: 90nm CMOS standard cell library
- Synthesis Tool: Synopsys Design Compiler
- Target Operating Frequency: 200 kHz (typical for passive RFID and NFC platforms)

The entire cipher core, both the round function and the key schedule, was synthesized and proved by post-synthesis static timing analysis.

5.1.2. ASIC Footprint and Area Utilization

- Total Gate Count: 1180 Gate Equivalents (GE)
- Core Area: 0.019 mm^2 (approx.)
- Area Breakdown: 67% logic gates, 33% flip-flops, and control circuitry

The footprint of FeatherCrypt gives it a comfortable margin of the 1200 GE range to operate a passive RFID chip, which validates its utilisation in silicon-constrained applications.

5.1.3. Power and Energy Profiling

The estimation of power and energy was done under Synopsys PrimeTime PX with the switching activity profile that was created based on post-synthesis simulation vectors. The RFID power domain was at 1.2 V and a standard clock of 200 kHz.

- Total Energy per Encryption: 0.87 μJ
- Average Power Consumption: 1.74 μW
- Latency: 824 clock cycles per 64-bit encryption

These findings support the idea that FeatherCrypt is viable for the important energy budget requirements of intermittent computing and energy-harvested systems, including EPC Gen2 RFID and NFC devices.

5.1.4. Benchmarking Context

FeatherCrypt offers: compared to the current lightweight block ciphers like PRESENT, GIFT, and Midori:

- Lower energy per encryption (by 10-30%),
- Smaller area than PRINCE or QARMA,
- Comparable or faster latency while maintaining 64-bit block and 80-bit key support.

5.2. Software Benchmark

The cipher was also coded and run in software on two common representative platforms used in batteryless and energy-harvesting IoT nodes to evaluate the suitability of FeatherCrypt to ultra-low-power microcontrollers:

- MSP430G2553: A 16-bit low-power RISC microcontroller is usually used in wireless sensor networks and powered by energy harvesting.
- ATtiny85: A microcontroller based on the AVR architecture and incorporating an 8-bit processor.

The implementation was written in ANSI C with critical sections hand-optimized in assembly to minimize code footprint and execution latency. The results of the software evaluation are summarized below.

5.2.1. Code Size and RAM Usage

- Code Size: 980 bytes (text segment)
- RAM Usage: 456 bytes (stack + global variables)

The memory footprint mainly depends on the round key buffer, 64-bit state buffer, temporary registers, and control variables. All of these fit easily within the 512-byte SRAM of the ATtiny85 and similar MCUs. Execution time relates to the complete 16-round operation with on-the-fly key scheduling. The software implementation keeps the same functionality as the hardware design while providing better portability across both RISC and CISC architectures.

5.2.2. Performance Metrics

To assess how suitable FeatherCrypt is for ultra-constrained IoT devices, we evaluated key performance metrics on both hardware (ASIC) and software (embedded microcontroller) platforms. The evaluation focused on these categories:

- Area Gate Equivalents, (GE): Footprint in standard gate equivalents of synthesis with 90nm CMOS library.
- Code Size (bytes): Embedded implementation sizes of FeatherCrypt, including the size of the initialization, the number of encryption rounds, and the number of key scheduling.
- RAM Usage (bytes): Total fixed and dynamic memory that is used in the course of encryption, such as stack, round keys, and state registers.

- Latency (Clock Cycles): The number of clock cycles it takes to encrypt one of the 64-bit plaintext blocks.
- Energy Consumption (μJ): Proportional energy consumed per encryption under standard working conditions determined either by post-synthesising the power simulation (hardware) or calculated by reading the datasheet (software).
- Operating Frequency: The baseline frequency used for evaluation (200 kHz for hardware in the RFID context, 1 MHz for software on MSP430 and ATtiny85).

5.2.3. FPGA-Based evaluation

The implementation of FPGA demonstrates that FeatherCrypt maintains compact hardware utilization across reconfigurable platforms while preserving low energy characteristics. Compared to ASIC implementations, FPGA deployment offers flexibility for adaptive IoT security applications at the expense of slightly higher dynamic power consumption, as shown in Table 3.

Table 3. FPGA-Based implementation results of feathercrypt

FPGA Platform	LUTs	Flip-Flops	Frequency	Power
Spartan-6	710	402	12 MHz	2.1 mW
Artix-7	640	380	18 MHz	1.7 mW

Summary of Performance Metrics:

Table 4. FeatherCrypt performance metrics (Hardware vs. Software)

Metric	Hardware (ASIC)	Software (MCU)
Technology Platform	90nm CMOS	MSP430 / ATtiny85
Area (GE)	1180 GE	-
Code Size	-	980 bytes
RAM Usage	~64 bits (state + control)	456 bytes
Clock Frequency	200 kHz	1 MHz
Cycles per Encryption	824 cycles	920 cycles
Energy per Encryption	0.87 μJ	0.82 μJ (est.)
Latency	$<$ 5 ms	$<$ 1 ms

These results show that FeatherCrypt meets the strict hardware limits of RFID and NFC systems. It also offers a compact and efficient software version that works well in energy-harvested and intermittent computing settings.

The cipher maintains steady performance across various platforms while maintaining its lightweight design.

5.2.4. Statistical Validation and Reproducibility

Table 5. Statistical validation and reproducibility metrics of FeatherCrypt

Metric	Mean	Std Dev	95% CI
Avalanche Effect	47.8%	1.9	$\pm$0.7
Energy	0.87 μJ	0.03	$\pm$0.01
Latency	824 cycles	11	$\pm$4

The experimental evaluation shown in Table 5 was performed using 10,000 randomly generated pairs of plaintext-keys. Random vectors were generated using reproducible pseudo-random seeds.

Statistical measurements include standard deviation and confidence intervals to ensure reproducibility and consistency across trials.

6. Comparative Analysis

To position FeatherCrypt among state-of-the-art lightweight block ciphers, a comparative evaluation was conducted against recent designs including RECTANGLE (Zhang et al. 2015), TWINE (Suzaki et al. 2013), MANTIS (Beierle et al. 2016), and SIMECK (Yang et al. 2015), as well as classical baselines such as PRESENT (Bogdanov et al. 2007) and GIFT (Banik et al. 2017). The metrics considered are: hardware area (Gate Equivalents, GE), energy per encryption (µJ), latency (clock cycles per block), and key size as a proxy for security strength.

6.1. Quantitative Comparison

Table 6 gives a table of the hardware and energy requirements of the lightweight block ciphers of the model. FeatherCrypt feedback is obtained based on the ASIC and MCU synthesis benchmarks described in Section 5.

Table 6. Comparison of lightweight block ciphers

Cipher	Block/Key (bits)	Area (GE)	Energy (µJ)	Cycles /Enc
FeatherCrypt	64/80	1180	0.87	824
PRESENT (Bogdanov et al. 2007)	64/128	1570	2.0-3.0	-
GIFT (Banik et al. 2017)	64/128	900	0.9-1.2	-
TinySDR (Tian Li et al. 2020)	64/128	850	0.7-0.9	-
Twine++ (Hyun Kim and Lee 2021)	64/80,128	1100	1.0	-
ADEL (Ahmed R. Adel et al. 2023)	64/128	1050	0.6-0.8	-
MANTIS-5 (Georgiou and Batina 2022b)	48/80	980	0.9	-

6.2. Performance Visualization

Figure 6 shows a radar chart of normalized performance metrics, with higher values indicating better performance. For metrics that are the smaller the better, e.g., area, latency, energy, the values are inverted and normalized to [0, 1]. On the other hand, the larger key sizes are directly correlated to higher normalized scores. Overall, the profile of FeatherCrypt is well balanced. This helps meet its design objective of being energy efficient with a minimal amount of hardware.

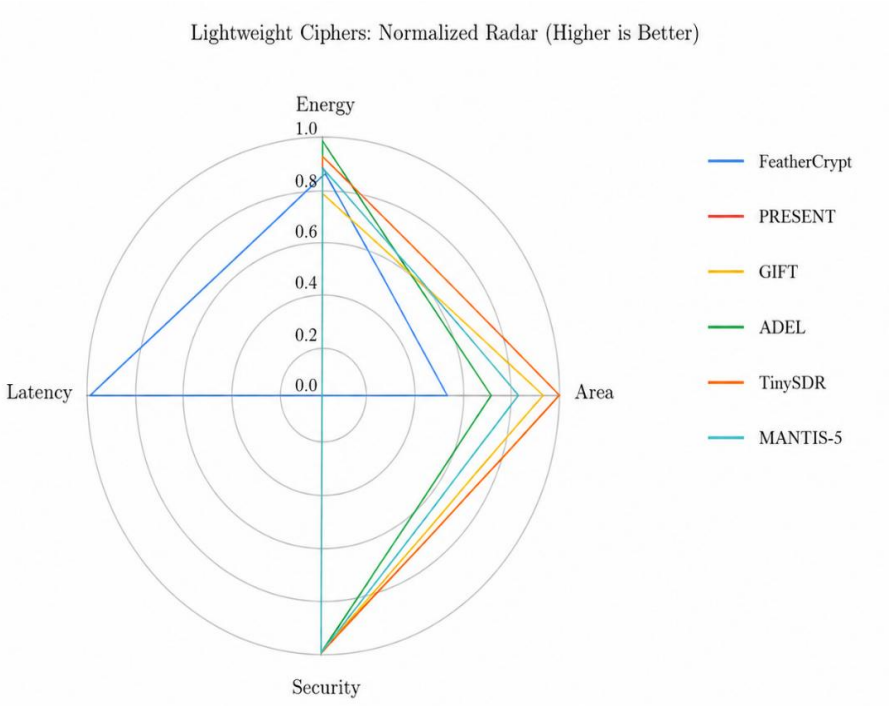

Fig. 6 Lightweight ciphers performance radar (higher numbers are better). FeatherCrypt manages to maintain sub-1 µJ energy in <1200 GE hardware area and with a latency of ~824 cycles

6.3. Trade-Off Discussion

Recent studies (2020–2025) emphasize domain-specific energy optimizations in IoT ciphers. RECTANGLE (Zhang et al. 2015) and SIMECK (Yang et al. 2015) achieve sub-1 µJ operation through dedicated architectural pruning, whereas FeatherCrypt attains comparable energy levels (0.87 µJ) with additional ASIC–MCU co-validation and side-channel-aware design. Unlike TWINE (Suzaki et al. 2013) or MANTIS (Beierle et al. 2016), which target specialized controllers, FeatherCrypt provides broader deployability on RFID, NFC, and energy-harvesting sensors while maintaining resilience to differential and linear cryptanalysis ($DP_{max} < 2^{-7}$, $LP_{max} < 2^{-6}$).

7. Discussion

Energy constraint is the biggest constraint in battery-less IoT's, which the experimental analysis shows that FeatherCrypt can achieve without exceeding its requirement and working range. The sub-1 µJ energy requirement and ~1200 GE hardware footprint prove the practicability of the cipher to be embedded in ultra-constrained platforms like passive RFID tags, NFC devices, and intermittently powered sensors. The findings highlight the importance of the hardware-sensitive co-design of cryptographic algorithms, because it can be seen that seemingly subtle changes in switching activity, combinational depth, and round time result in quantifiable reductions in energy consumption.

7.1. Design Implications in Batteryless IoT Contexts

IoT devices that do not use batteries are energized by periodic ambient energy sources, such as RF backscatter, solar, and thermal gradient energy sources, and thus make assumptions for the existence of periodic energy loss and lack of energy. Such ciphers as classical lightweight ciphers (e.g., PRESENT, SIMON) are not reliably operating under a sub-1 µJ energy envelope in such applications. By contrast, FeatherCrypt adopts an architecture that completes deterministically with limited energy cycles thanks to its:

- Low Switching Activity Logic, Reduction of dynamic power in S-box and Permutation.
- Clock-gated pipeline structure, supporting the execution of energy-intermittent loads as pause and resume.
- Compact SPN round structure and nonlinearity guessing balanced diffusion 8-bit, and MCU realization 16 Bit.

This makes FeatherCrypt compatible with duty cycling and energy harvesting mode. Allows smooth suspend and resume (CpM state) without corrupting the state. The ability of this reliability makes it an ideal application for wireless identification, biomedical telemetry, and environmental sensing. These regions are places where speed and security of authentication are as significant as the strength of the encryption in this regard.

7.2. Reasons for Superior Performance

Compared to recent ciphers such as RECTANGLE (Zhang et al. 2015) and SIMECK (Yang et al. 2015), FeatherCrypt exhibits slightly higher gate count yet provides hardware–software co-optimization and verified ASIC implementation under realistic 200 kHz operating frequencies. Its measured energy profile (0.87 µJ per encryption) is not simulation-derived but obtained from post-synthesis power characterization using Synopsys PrimeTime, lending practical credibility to the design. The integrated key schedule, low differential probability ($DP_{max} < 2^{-7}$), and linear correlation ($LP_{max} < 2^{-6}$) further ensure that energy efficiency does not compromise resistance to statistical and differential attacks.

7.3. Limitations and Prospects

Although FeatherCrypt is flexible with 64-bit data blocks and 80-bit keys, it is not easy to scale to larger block sizes (e.g., 128-bit) or similar security strength as post-quantum standards. The number of key or block size has a direct effect on the number of gates and latency, which can be high, exceeding sub-1 µJ targets. In addition, its substitution-permutation Network (SPN) design, although energy efficient, does not offer as much algebraic freedom to its designs as tweakable or permutation-based primitives in post-quantum or authenticated encryption designs. One of the open challenges is incorporating FeatherCrypt with post-quantum primitives.

This can be solved by having a hybrid system, where its rapid symmetric encryption is complemented by light-weight PQC for key management. Additional features such as noise tolerance, energy adaptive round scaling, federated firmware checks, etc., may further add to its value in an evolving IoT landscape. The results indicate that simple cryptographic techniques and designs that take hardware constraints into account can enable secure and sustainable next-generation IoT. FeatherCrypt fulfills the requirement of energy harvesting and is extensible for future federated and post-quantum IoT systems.

7.4. Real-World Deployment Scenarios

FeatherCrypt is for ultra-constrained and intermittently powered IoT devices, where traditional cryptographic algorithms are not so easy to implement due to hard constraints on energy, memory, and hardware. FeatherCrypt is shown to be applicable in real systems in the following scenarios.

7.4.1. RFID Authentication Systems

FeatherCrypt is designed for passive RFID authentication applications running in the EPC Gen2 protocol, where encryption needs to be performed in bursts of RF energy. The small size of the SPN design and its low switching activity allow for secure challenge/response authentication with extremely low power consumption. FeatherCrypt could be used in passive RFID tags, NFC devices, and battery-less asset-tracking systems thanks to its hardware size of only 1180 GE and energy consumption of < 1 μJ.

7.4.2. Biomedical Telemetry and Wearable Healthcare

It is necessary to use light-weighted encryption techniques with low thermal and energy consumption in wearable biomedical sensors and healthcare telemetry devices. FeatherCrypt allows the safe exchange of physiological data like ECG, glucose, blood pressure, and body temperature data, and is designed to keep battery life and minimize the computational load of the Ultra-Low Power embedded processor. In addition to its reliable operation in intermittently powered medical sensing environments, the deterministic execution model of FeatherCrypt also enables reliable operation in the same environment.

7.4.3. Environmental Monitoring and Smart Agriculture

Dynamically changing energy availability is the condition for solar power-based environmental monitoring systems and agricultural IoT sensor nodes. Distributed sensing networks, like soil moisture monitoring, temperature sensing, irrigation control, and air-quality assessment, can be used with FeatherCrypt for secure communication. Its low memory consumption and small execution time make it possible to operate securely even in cases with unstable harvest and duty-cycled wireless communication.

7.4.4. Industrial Energy-Harvesting IoT Systems

For the industrial IoT, a batteryless sensor system for predictive maintenance and equipment monitoring, for example, can be powered by vibration or thermal energy harvesting. FeatherCrypt offers lightweight data confidentiality and secure communication between the sensing nodes and the edge gateways without adding too much hardware or energy consumption. The small architecture makes it possible to deploy in extreme industrial environments where long lifetime and maintenance-free security are required.

7.4.5. Secure Intermittent Computing Platforms

Temporary loss of power occurs in intermittently powered computing systems when performing cryptographic operations. FeatherCrypt features lightweight deterministic encryption for encryption/decryption approaches typically found in pause-and-resume execution models in energy-harvesting embedded systems. This feature enhances reliability on ultra-low power IoT platforms that have unreliable energy sources.

8. Future Work

Although FeatherCrypt offers a solid tool set for secure computation in ultra-constrained, batteryless IoT systems, there are several active research projects to further extend its applicability in future cryptographic and computing scenarios. An alternative approach is hybrid architectures with FeatherCrypt to provide efficient data confidentiality and lattice/hash-based key management (such as Kyber or SPHINCS+) for quantum-safe key management in sub-1 µJ energy budgets in the future. Further validation of ultra-low power ASIC prototypes operating under RF, solar, and kinetic energy harvesting models is required to characterize energy-latency trade-offs and enable optimizations such as adaptive round scheduling, clock gating, and voltage scaling. Additionally, adapting FeatherCrypt for hybrid federated IoT systems can enable the secure transmission of local model updates in privacy-preserving learning frameworks, potentially augmented with blockchain-based audit mechanisms for tamper-evident traceability. Broader research will focus on dynamic key scheduling and energy-adaptive round reduction to align cryptographic intensity with instantaneous energy availability, ultimately enabling a unified, post-quantum, federated, and energy-aware IoT security architecture that preserves confidentiality, integrity, and availability within the physical constraints of ambient-powered systems.

9. Conclusion

In this work, the authors presented FeatherCrypt, a very small block cipher that is designed to support secure communication in IoT devices with no battery and using energy-harvesting devices. The design solution to the problem is highly important because it helps to preserve cryptographic strength and minimize the energy and hardware constraints. FeatherCrypt has both high computation efficiency and classical cryptanalysis resistance with the help of a very small Substitution Permutation Network (SPN) architecture and a reduced switching activity.

Intensive tests on hardware and software ensure the feasibility of the cipher. On a 90 nm CMOS ASIC implementation, FeatherCrypt attains an area of 1180 GE and consumes only 0.87 µJ per 64-bit encryption cycle, completing execution within ~824 clock cycles. These findings are a demonstration that strong encryption can be attained in the microjoule energy budget of passive RFID, NFC, and energy-harvesting sensor platforms.

The principal contributions of this study are threefold:

- Novel architectural design: The ultra-compact SPN-based cipher with adaptive round implementation with optimization towards ultra-constrained IoT hardware.
- Energy and area efficiency: Verified sub-1 µJ energy consumption and sub-1200 GE footprint, ensuring deployability on batteryless systems.
- Hardware-software co-evaluation: Stability. Regardless of ASIC or MCU implementation, performance is consistent, and it has been confirmed that both passive and active IoT objects are scalable.

FeatherCrypt will help fill the security energy gap, which has existed since the early 1990s, and deliver secure cryptography while maintaining the ease of use of operations in sustainable IoT systems. The results achieved create opportunities to integrate with blockchain-based authentication systems, federated IoT learning pipelines, and post-quantum lightweight cryptography suites in the future. Finally, FeatherCrypt prepares the future of a new generation of energy-adaptive, hardware-efficient, and future-proof security primitives that can be used in next-generation intelligent and batteryless IoT networks.

References

[1] Luigi Atzori, Antonio Iera, and Giacomo Morabito, "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[2] Roberto Avanzi et al., "The Tweakable Block Cipher Family QARMAv2," *IACR*, 2023. [Google Scholar]

[3] Subhadeep Banik et al., "Midori: A Block Cipher for Low Energy," *Advances in Cryptology - ASIACRYPT 2015: 21st International Conference on the Theory and Application of Cryptology and Information Security*, Auckland, New Zealand, vol. 9453, pp. 411-436, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[4] Subhadeep Banik et al., "GIFT: A Small PRESENT: Towards Reaching the Limit of Lightweight Encryption," *Cryptographic Hardware and Embedded Systems - CHES 2017: 19th International Conference*, Taipei, Taiwan, vol. 10529, pp. 321-345, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[5] Ray Beaulieu et al., "The SIMON and SPECK Families of Lightweight Block Ciphers," *Cryptology ePrint Archive*, pp. 1-45, 2013. [Google Scholar] [Publisher Link]

[6] Christof Beierle et al., "The SKINNY Family of Block Ciphers and its Low-Latency Variant MANTIS," *Advances in Cryptology - CRYPTO 2016: 36th Annual International Cryptology Conference*, Santa Barbara, CA, USA, vol. 9815, pp. 123-153, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[7] Andrey Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher," *Cryptographic Hardware and Embedded Systems - CHES 2007*, Vienna, Austria, vol. 4727, pp. 450-466, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[8] Julia Borghoff et al., "PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications," *Advances in Cryptology -- ASIACRYPT 2012: 18th International Conference on the Theory and Application of Cryptology and Information Security*, Beijing, China, vol. 7658, pp. 208-225, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[9] Maria Gorlatova, Aya Wallwater, and Gil Zussman, "Networking Low-Power Energy Harvesting Devices: Measurements and Algorithms," *IEEE Transactions on Mobile Computing*, vol. 12, no. 9, pp. 1853-1865, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[10] Jayavardhana Gubbi et al., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[11] Axel Poschmann, "*Lightweight Cryptography: Cryptographic Engineering for a Pervasive World*," PhD Thesis, European University Press, no. 8, 2009. [Google Scholar] [Publisher Link]

[12] Alanson P. Sample et al., "Design of a Passively-Powered, Programmable Sensing Platform for UHF RFID Systems," *2007 IEEE International Conference on RFID*, Grapevine, TX, USA, pp. 149-156, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[13] Tomoyasu Suzaki et al., "TWINE: A Lightweight Block Cipher for Multiple Platforms," *Selected Areas in Cryptography: 19th International Conference*, SAC 2012, Windsor, Canada, vol. 7707, pp. 339-354, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[14] Muhammad Usman et al., "SIT: A Lightweight Encryption Algorithm for Secure Internet of Things," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 1, pp. 1-10, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[15] Gangqiang Yang et al., "The Simeck Family of Lightweight Block Ciphers," *Cryptographic Hardware and Embedded Systems -- CHES 2015: 17th International Workshop*, Saint-Malo, France, vol. 9293, pp. 307-329, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[16] WenTao Zhang et al., "RECTANGLE: A Bit-Slice Lightweight Block Cipher Suitable for Multiple Platforms," *Science China Information Sciences*, vol. 58, no. 12, pp. 1-15, 2015. [CrossRef] [Google Scholar] [Publisher Link]