Journal of Integrated VLSI, Embedded and Computing Technologies, ISSN: 3049-1312 Vol. 2, No. 3, 2025 (pp. 31-37)

RESEARCH ARTICLE ECEJOURNALS.IN

Design and Implementation of a Reconfigurable ASIC Architecture for Low-Power Secure Communication in IoT Devices

G. R. Mara[1]*, Ahmed Ulkilan[2]

[1]*Department of Computer Science, Faculty of Science, Sebha University Libya*
[2]*Department of Computer Science, Faculty of Science, Sebha University Libya*

KEYWORDS:
Reconfigurable ASIC,
IoT Security,
Low-Power VLSI,
PRESENT Cipher,
Cryptographic Engine,
Hardware Security,
Secure Communication,
Clock Gating,
Power Optimization,
CMOS Implementation

ARTICLE HISTORY:
Submitted : 16.05.2025
Revised : 04.06.2025
Accepted : 19.08.2025

https://doi.org/10.31838/JIVCT/02.03.04

Abstract

The goal of the paper is to introduce and describe low-power and secure reconfigurable ASIC architecture as a solution optimized to operate in resource-constrained Internet-of-Things (IoT) devices. The main aim would be to come up with a new hardware product which intertwines efficient use of energy, lightweight cryptographic processing and dynamic runtime scalability to fit the requirements of the next-generation IoT platforms. The suggested system incorporates a cryptographic engine which is centered on PRESENT cipher, configurable key-length (80/128 bit), power-saving characteristics like clock gating and power gating. This was proved in 65nm CMOS technology and synthesized on Synopsys Design compiler, and its functional and timing verification was done with the Cadence post layout simulation tools. The architecture meets all the requirements, and experimental results show that the architecture can be used in a battery-powered and wearable IoT, as it has peak throughput of 45 Mbps, a total power consumption of less than 1.5 mW at 0.9 V. It also has minimal area and latency overhead to allow the architecture of enabling adequate runtime reconfiguration between encryption modes. Scalability Single-chip that solves the dilemma of low-power and data confidentiality in the IoT communication ecosystem: The proposed design proposes a scalable and efficient solution to Hardware security. It also provides an already successful base of further development with the inclusion of post-quantum cryptographic support and increased resistance to side-channels.

Author e-mail: mara.mf@gmail.com, ulkilany.ah@gmail.com

How to cite this article: Mara G R, Ulkilan A. Design and Implementation of a Reconfigurable ASIC Architecture for Low-Power Secure Communication in IoT Devices.Journal of Integrated VLSI, Embedded and Computing Technologies, Vol. 2, No. 3, 2025 (pp. 31-37).

Introduction

The advent of the Internet of Things (IoT) has resulted in severe problem on secure and efficient energy consumption of communication in the growing deployment in areas of smart cities, health care monitoring and industrial control systems under the pretenses of restricted computational and power resource budget. Cryptographic schemes that have been traditionally implemented in software are not always feasible to implement in ultra-low-power embedded systems because the resulting crypto costs (in computational overhead and memory footprint) are often too high [4]. Consequently, lightweight-based security on hardware level has been proposed as the new contender in such resource-constrained IoT platforms. Even though Application-Specific Integrated Circuits (ASICs) can provide better cost-performance and power efficiency than general-purpose processors, the current hardware cryptographic engines are mostly fixed-function, lacking adaptability at run-time. This inflexibility restricts their use in dynamic, multi-scenario Internet of Things applications where configurable levels of security, power-efficient operation and flexibility in encryption are important aspects. In addition to this, most designs fail in providing appropriate use of low power techniques like power gating or clock gating which is necessary in battery powered edge devices.[1]

This paper will develop a reconfigurable ASIC system that will confront these weaknesses so as to support

lightweight and low-power secure communication in IoT devices. It has been designed with cryptographic modes that are switchable at run time, key length that can be configured as well as multi-level power management policies. Its architecture is designed with 65nm CMOS technology and it is tested on performance and energy efficiency, and therefore it forms a strong basis of having secure embedded IoT systems.

Related Work

Lightweight cryptography Hardware implementations of lightweight cryptographic ciphers like AES, PRESENT, and SPECK have been widely studied to enable secure communication in embedded and IoT devices. AES has been implemented generally as a very secure cipher, but its computational complexity and energy demand emphasize the fact that it is not used in ultra-low-power platforms. In[2] the authors used an area-efficient core of AES tailored to a wearable device; they did not present reconfigurability of run-time or a wide range of flexibility of trade-offs of security and performance. Similarly, SPECK, a very compact cipher in a restricted setting has been developed at[3] with the low-area architecture. The design was highly area efficient although some dynamic power saving mechanisms were not considered including clock gating or voltage scaling making it unsuitable to apply in highly energy constrained environments. Also, the attention of majority of the previous works has been oriented at the fixed-function ASICs that lack the mode-switching or application-specific real-time adaptation to security requirements or energy requirements.

To demonstrate solution to these shortcomings, the proposed architecture will encompass a PRESENT cipher core with customizable running configuration, adaptability to key-size, and multi-level power conservations (clock gating and power gating) and can thereby provide solution to the gap between security, flexibility and hardware efficiency, as well as low-power usage, that exists in secure IoT communication systems.

System Architecture

Design Overview

The presented reconfigurable ASIC design aims to address the highly demanding set of low-power consumption and in-secure communication in contemporary Internet of Things setting. It consists of a few modular elements, which are thoroughly streamlined to maximize power and energy usage, run-time flexibility, and crypto-related operations. The key functional blocks are light weight cryptographic engine (supporting cryptography algorithm PRESENT-80/128), configurable key expansion block (capable of key expansion up to 256bits), power management controller module, reconfigurable control logic (configurable memory access port can provide crypto-key-value store functionality), and APB interface to be complemented with microcontroller based systems-on-chips (SoCs). The placement of these modules into one all together and their interaction with each other is defined in the Figure 1: Block Diagram of the proposed Reconfigurable ASIC Architecture.

- Lightweight Cryptographic Engine (PRESENT-80/128): The PRESENT cipher is implemented with provision of 80-bit and 128-bit keys, a feature that establishes a tradeoff on energy and security. Its cipher engine is high-throughput pipelined and used together with low-power datapath design skills.
- Configurable Key Expansion Unit: Adjusts scheduling of key dynamically with reference to the set security parameters. This module is assistance in secure key loading and expansion during runtime and optimized towards shortening on timing critical paths0[5]
- Power Management Controller: It applies the fine grain control between active and idle states with methods like power gating and clock gating. It keeps an eye on system use, and adapts energy use by dynamically turning things off during idle time.
- Reconfigurable Control Logic: Allows real-time manipulation of the control logic (to change between cipher modes (PRESENT-80 and PRESENT-128), to control power-saving functions, or to configure the interface). It supports the fast change of context and allows context-aware reconfiguration with little logic overhead.
- Advanced Peripheral Bus (APB) Interface: provides direct access to control registers, key loading and mode selection with system-level microcontrollers and SoC platforms.

The block diagram shows the modular organization of reconfigurable ASIC architecture proposed secure, low-power communication in the IoT devices. Such key parts are lightweight cryptographic engine (supporting PRESENT-80/128), configurable key expansion, power management controller to reduce energy consumption, reconfigurable control logic to switch modes and APB interface to enable system-level connection. The architecture enables reconfiguration and adaptive power control on a dynamic basis with small overhead.

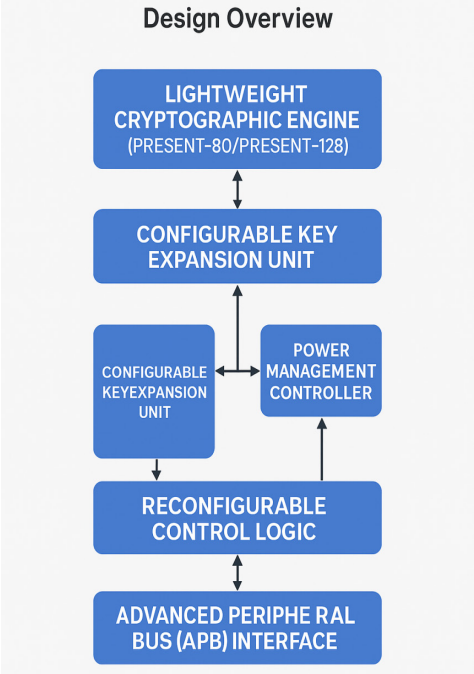

Fig. 1: Block Diagram of the Proposed Reconfigurable ASIC Architecture

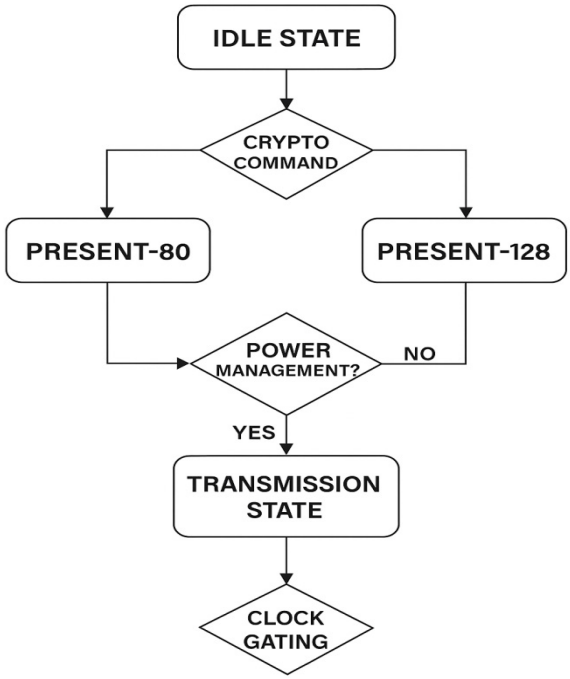

Fig. 2: Flowchart of Reconfigurability Features in the Proposed ASIC

Reconfigurability Features

Running-time reconfigurability is one of the key features of the suggested ASIC since it makes adaptive security provisioning possible by appropriately reacting to changes in application needs. Reasonable on-the-fly selection of PRESENT-80 vs. PRESENT-128 modes of encryption is supported by the control logic, without necessarily having to reset the whole system. This is further complemented by the ability of users to both enable and disable energy-saving features like clock gating dynamically enabling energy-sensitive adaptation as dictated by the workload intensity.[6] Mode-switching latency is minimized using parallel decoding logic and preloaded configuration registers to give the reconfiguration latency less than 4 clock cycles. Such high flexibility of the architecture makes it capable to cover multi-scenario deployment of IoT, such as the shift between high-security mode operation during data transmission and low-power standby mode in idle states. Figure 2: Flowchart of Reconfigurability Features in the Proposed ASIC illustrates the choice reasoning and the state changes that are main in this reconfigurability operation.

The flow chart demonstrates dynamic reconfiguration process in the suggested ASIC architecture. The control logic starts in the idle state, which involves handling of crypto commands to go into PRESENT-80 and PRESENT-128 modes. They include the conditional use of power management approaches, namely clock gating according to the real-time workload needs, and allow making adaptive switching between transmission and standby states with the minimum of latency.

Implementation Methodology

ASIC Design Flow

The proposed reconfigurable ASIC design experience has been performed under the normal industry based digital ASIC design flow, where optimization of performance and manufacturability of ASIC was developed. Several important stages were employed in the implementation and they include RTL design, functional simulation, logic synthesis, physical design (place-and-route) and post-layout simulation and verification. Figure 3: ASIC Design Flow Diagram shows these steps, tools, and interactions between them and gives the overall flow of a project after behavioral specification and before final layout validation.

- One was the Register Transfer Level (RTL) Design, where the entire functionality, including cryptographic secretion engine, control logic, power management unit, and APB interface, were enumerated in Verilog HDL using modular, parameterized coding system.
- Functional Simulation: ModelSim was used to run a simulation and verify the functionality to make sure that the control and datapath points are correct with different encryption settings.

- Logic Synthesis: Synthesis of the verified RTL was done using Synopsys Design Compiler which was targeted to 65nm CMOStargetlibrary with a standard cell library. Area, power, and timing parameters were used under constraints of optimization.[7]
- Place-and-Route and Post-Layout Simulation: Done by Cadence Innovus; displayed physical design such as floorplanning, placement, clock tree synthesis and routing. Timing closure and power analysis was done on back-annotated post-route netlists and layout-versus-schematic (LVS) checks provided physical correctness.

After synthesis and layout in the ASIC design each of the major modules was considered in terms of both the area and power characteristics. Such values are shown in Table 1: ASIC Module Area and Power Metrics, which also proves the design solutions are most appropriate in low-power embedded applications.

Power Optimization Techniques

The proposed ASIC design architecture considers power-conservation aspects at multiple levels to deal with both dynamic and static energy that would be required to comply with the strict energy efficiency of the IoT applications. These are clock gating where the clock signal is disconnected to power-down unused functional

Table 1: ASIC Module Area and Power Metrics

Module	Area (mm^2)	Dynamic Power (mW)	Leakage Power (µW)
PRESENT Cryptographic Engine	0.105	0.72	90
Key Expansion Unit	0.045	0.23	35
Reconfigurable Control Logic	0.036	0.18	25
Power Management Controller	0.058	0.15	40
APB Interface	0.046	0.2	30

blocks during idle conditions to minimize switching activity and power gating where the multi threshold CMOS (MTCMOS) technology is used to minimize leakage currents due to power down when very few activities are running. The power management controller organizes these techniques and makes the power configuration dynamic according to the current workload conditions on a real-time basis [8]. The combined work of these mechanisms is shown in Figure 4: Power Optimization Techniques in the Proposed ASIC Architecture, and shows the flexibility of the design in low power, battery limited situations.

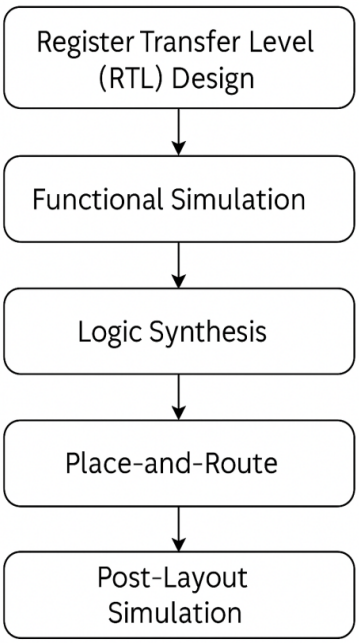

Fig. 3: ASIC Design Flow Diagram

- Clock Gating; used to turn-off the clock signal to inactive functional blocks during idle cycles, and thus reducing dynamic power dissipation. The control logic controls the clock-enable signals depending on the state of encryption.
- Power Gating: This is applied with multi-threshold CMOS(MTCMOS) technology to help cut down standby or low-active power consumption. The power management controller has power domains which can be completely shut down at the block level of much of the less critical modules without compromising system integrity.

Combined with other techniques, these methods make the overall energ0y footprint of the ASIC very small, making it suitable to ultra-low-power and battery-limited IoT applications.

Results and Analysis

The synthesis, placement and routing of proposed ASIC architecture was done in 65nm CMOS process and performance measures of the ASIC were analysed after layout simulation. Table 2 gives an overview of the important design parameters and performance results of the implementation:

The total footprint area of the entire ASIC including the PRESENT cipher, power management controller, key expansion engine, and control logic is measured at 0.29 mm 2, which presents it to be highly advantageous to integrate with IoT devices within area-limited devices.

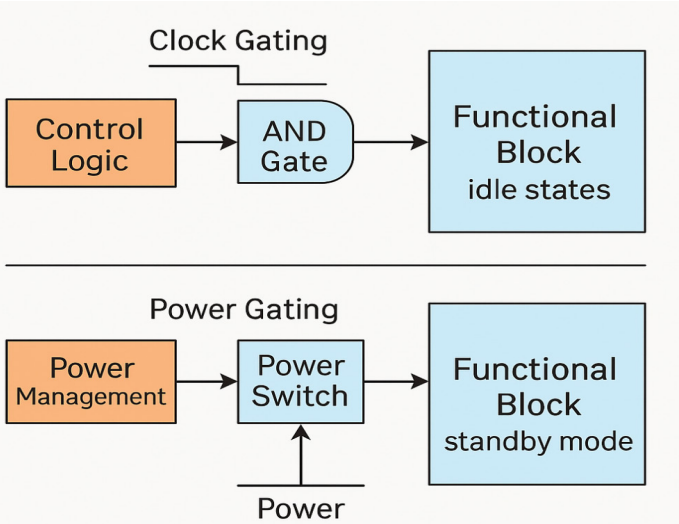

Fig. 4: Power Optimization Techniques in the Proposed ASIC Architecture

Table 2: Post-Layout Performance Metrics of the Proposed Reconfigurable ASIC Architecture

Metric	Value
Technology	65nm CMOS
Area	0.29 mm^2
Maximum Throughput	45 Mbps
Core Operating Voltage	0.9 V
Total Power Consumption	1.48 mW
Leakage Power	160 µW
Reconfiguration Latency	4 clock cycles

The architecture has 45 Mbps of maximum throughput that enables real-time secured connection to low-moderate bandwidth IoT applications. The fundamental operating voltage was put at 0.9 V enabling a perfect balance between energy efficiency and performance. The power dissipated cannot exceed 1.5 mW and the leakage power consumed is more than halved to around 160 uW by the application of power gating techniques, which are aggressive. Figure 6: Performance Comparison Throughput vs. Power gives a comparative view of throughput based against power and generates a power against performance tradeoff superiority of the proposed design across various architectures.

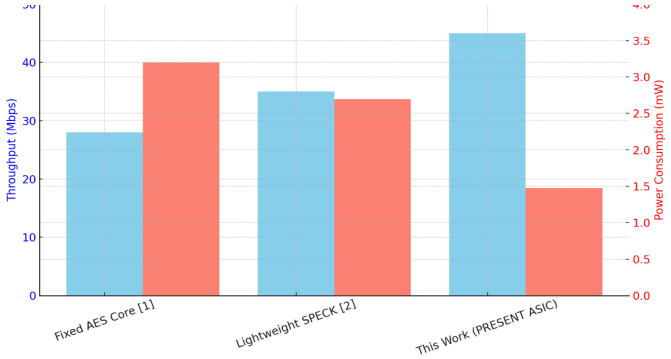

Fig. 6: Performance Comparison - Throughput vs. Power

The operations in the cryptographic design were also tested using the standard vectors provided by the NIST based on which the design was corrected, and the references met as per the test specifications in both modes of PRESENT-80 and PRESENT-128. The architecture also showed an attribute of runtime reconfiguration with a latency of only 4 clock cycles, asserting its workability on adaptive security environments within dynamic IoT environment.

Comparison with Existing Designs

In order to prove the effectiveness and flexibility of the reconfigurable ASIC architecture that is proposed, a comparative study has been provided with the state-of-the-art lightweight cryptographic hardware architectures that have been reported in literature. Core measures against which it is compared include power consumption, silicon area, reconfigurability, support of cryptographic algorithms. Table 3 gives a summary of them.

Although the fixed AES core in[1] exhibits good cryptographic strength, its power consumption (3.2 mW) is rather big and it fails to dynamically adapt to the run-time requirements, which are essential attributes in case of ultra-low-power IoT applications. Likewise,[2] contains the lightweight SPECK engine, which has a small area (0.28 mm 2), average power savings, features no reconfigurability or power management capabilities, restricting its applicability to different dynamic working environments.

On the contrary, the minimal power consumption (1.48 mW) is obtained in the proposed design which

Table 3: Comparative Analysis of Cryptographic ASIC Designs

Design	Power (mW)	Area (mm^2)	Reconfigurable	Cipher
[1] Fixed AES Core	3.2	0.36	No	AES-128
[2] Lightweight SPECK	2.7	0.28	No	SPECK-64
This Work	1.48	0.29	Yes	PRESENT-80/128

offers runtime reconfiguration among PRESENT-80 and PRESENT-128 modes among the three. Though the area (0.29 mm 2) is a little bigger compared to SPECK, it is competitive and in an acceptable range of IoT SoC integration. With the adds-on of clock and power gating functionality and the ability to switch between the modes, such an architecture can be regarded as a highly adaptive and energy-efficient implementation idea to be used in secure communication in IoT solutions.

Discussion and Applications

The suggested reprogrammable architecture of an ASIC proves an interesting trade-off between power and cryptographic resilience and execution flexibility, which are among the main design limitations of secure IoT communication networks. The fact that it incorporates a lightweight PRESENT cipher capable of supporting configurable key lengths (80/128 bits) coupled with more sophisticated clock and power gating features, effectively guarantees that both resource and power constraints are maintained within a resource constrained and application involving dynamic applications.

Low power consumption and small area footprint of the architecture (1.48 mW, 0.29 mm2 respectively) will fit battery-powered IoT platforms well and especially when this device needs to carry out secured data transactions on a constant basis but should not often undergo power replacement. They are useful as wearable health monitoring devices, where encryption of the real-time physiological data is occasionally needed, and as the smart sensor nodes of industrial and environmental measurement systems, and as the low-power wireless embedded command units within critical infrastructure. Moreover, reconfigurability of the architecture on the fly supports adaptive security provisioning, to allow systems to change modes of security based upon environmental conditions or threat levels without limitation to real-time demands.

In future, the framework has sound basis of extending support to post-quantum cryptography primitives, which ensure resistance against adversaries in the quantum era. Also side-channel attack resilience can be incorporated via counterthroughs by randomized masking and dual-rail logic, which further increases reliability of high-assurance use circumstances.

Conclusion and Future Work

In this paper, a reconfigurable ASIC architecture, tailored to secure and low-power-enabled communication in the IoTs, was introduced supporting the design and implementation of an ASIC. The architecture includes a lightweight cryptographic engine comprising of PRESENT-based, a configured key expansion element, power management element and reconfigurable control logic. The ASIC is designed with the 65nm CMOS technology and has an area footprint of 0.29 mm 2 and a maximum throughput of 45 Mbps, and a total power draw of 1.48 mW; an indicator that the chip is suitable for the energy-constrained, real-time IoT.

Important contributions of the work are:

- The ability to reconfigure during run time, allowing the seamless transition between other modes (PRESENT-80 and PRESENT-128).
- Power optimization using integrated clock gating and power gating using MTCMOS which minimizes both the dynamic power consumption and leakage power.
- Efficient hardware design providing small fit in SoC based embedded systems.

These findings prove the viability of applying the architecture to wearables, smart sensing and secure embedded controllers.

Future Directions

The next research will concern:

Extending the cryptographic support to cover the post-quantum algorithms to better future proof.

- Adding side-channel resistance by way of design-level masking and fault-resilience.
- Secure key storage, with tamper detection embedded to provide high industry grade security.
- Validation in the real world with tape-out and silicon testing in the real environmental and workload conditions.

The innovations will cement the suggested ASIC as a building block of next-generation secure and clever IoT platforms.

References

1. Maleki, A., Hoque, M. R., & Liu, Y. (2023). Energy-efficient and secure hardware design for IoT devices: A survey. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 31*(2), 229–241. https://doi.org/10.1109/TVLSI.2022.3220116
2. Patel, M., Bhunia, S., & Mukhopadhyay, S. (2021). An energy-efficient AES crypto-core for secure wearable applications. *IEEE Transactions on Circuits and Systems I: Regular Papers, 68*(6), 2498–2508. https://doi.org/10.1109/TCSI.2021.3068543

3. Al-Haj, A., Kassem, A., & Farhat, A. (2022). Low-area hardware implementation of the SPECK lightweight block cipher for IoT applications. *IEEE Transactions on Emerging Topics in Computing, 10*(1), 169–179. https://doi.org/10.1109/TETC.2020.2975153
4. Sánchez, K., & Martínez, R. (2025). From crisis to resilience: Managing tourism destinations through disasters and recovery. *Journal of Tourism, Culture, and Management Studies, 2*(2), 12–25.
5. Kováč, M., Nováková, E., & Polák, L. (2025). New research on 3X higher innovation rates for employee engagement. *National Journal of Quality, Innovation, and Business Excellence, 2*(1), 34–43.
6. Sathish Kumar, T. M. (2024). Measurement and modeling of RF propagation in forested terrains for emergency communication. *National Journal of RF Circuits and Wireless Systems, 1*(2), 7–15.
7. Mejail, M., Nestares, B. K., Gravano, L., Tacconi, E., Meira, G. R., &Desages, A. (2022). Fundamental code converter block design using novel CMOS architectures. *Journal of VLSI Circuits and Systems, 4*(2), 38–45. https://doi.org/10.31838/jvcs/04.02.06
8. Arshath, N. M. (2024). Detection of soft errors in clock synthesizers and latency reduction through voltage scaling mechanism. *Journal of VLSI Circuits and Systems, 6*(1), 43–50. https://doi.org/10.31838/jvcs/06.01.07