PROGRAM EDUCATIONAL OBJECTIVES (PEOS)

for the UG Bachelor's degree in

Electronics and Communication Engineering

PEO-1: Our graduates will possess good knowledge in engineering fundamentals.

PEO-2: Our graduates will be capable of analysing and designing systems.

PEO-3: Our graduates will be capable of creating innovative products in multidisciplinary areas.

PEO-4: The graduates will be ethically strong personnel with good communication and interpersonal skills with high moral values.

PEO-5: They will have a desire for continuous learning and Research and Development (R&D).

ABSTRACT

With the rapid growth of the Internet of Things (IOT), security has emerged as a critical concern due to the extensive exchange of sensitive data. Traditional software-based encryption is often too resource-intensive for constrained IOT devices. This project proposes the design and FPGA-based implementation of a low-power cryptographic chip tailored for IOT applications.

Using lightweight cryptographic algorithms like PRESENT, the proposed design emphasizes minimal area usage and low energy consumption. The chip is designed to support secure communication via common interfaces like SPI/UART and incorporates power-saving techniques such as clock gating and power gating. Implementation is carried out using Xilinx FPGA development tools and evaluated in terms of power, area, and throughput.

The developed crypto core targets under 10mW power consumption, under 2000 LUTs, and a throughput of 50– 100 Kbps with encryption latency under 100 cycles. This project demonstrates that secure and efficient hardware encryption for IOT devices is feasible and practical.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1. Applications

- Smart Home Automation: The crypto chip can be embedded in smart locks, cameras, and other home appliances to ensure secure communication and prevent unauthorized access.
- Wearable Medical Devices: Devices like fitness trackers and health monitors use encryption to protect sensitive health data while transmitting it to healthcare providers or cloud servers.
- Industrial IoT (IIOT) Systems: Used in smart factories and manufacturing plants to secure data exchanged between sensors, actuators, and controllers, thereby preventing industrial espionage or sabotage.
- Smart Agriculture: Deployed in smart farming tools to securely transmit environmental and crop data to a centralized system for analysis and control.
- Wireless Sensor Networks (WSNs): Applied in remote and unattended sensor networks, ensuring that data collected in the field remains confidential and tamper resistant.
- Remote Monitoring Systems: Useful in applications like oil pipeline monitoring, wildlife tracking, or disaster management where devices are deployed in isolated areas

2. Advantages

- Low Power Consumption: The design uses techniques like clock gating and power gating to minimize power usage, making it ideal for battery-operated devices.
- Small Footprint: It occupies minimal logic resources on an FPGA, making it suitable for integration into compact embedded systems.
- Enhanced Security: Hardware encryption reduces the vulnerability to software attacks and side-channel leaks, enhancing overall system security.
- Real-Time Performance: Capable of achieving encryption speeds suitable for real-time IoT communication, with low latency.
- Hardware Reusability: The same chip design can be reused across various IoT platforms, reducing development costs and time.
- Algorithm Flexibility: The architecture can be adapted to implement different lightweight cryptographic algorithms, depending on application needs.

1.3 Disadvantages

- Reduced Flexibility: Unlike software solutions, hardware cryptographic modules are less flexible to change or update post-deployment.
- Hardware Cost: Developing and fabricating custom hardware may incur higher initial costs compared to software-only solutions.
- Complex Design and Debugging: Hardware design involves complex processes such as synthesis, simulation, and verification, which require expertise.
- Cryptographic Strength Limitation: Lightweight encryption algorithms like PRESENT may not provide the same level of security as more robust algorithms like AES-256, which might be a limitation

  for high-security applications.

CHAPTER 2

PROBLEM STATEMENT

With the rapid proliferation of Internet of Things (IoT) devices across industries such as healthcare, agriculture, smart homes, and industrial automation, data security has become a critical concern. IoT nodes are typically small, low-cost, and battery-powered, which severely limits their computational and energy resources. Traditional encryption algorithms like AES and RSA, though secure, are often too resource-intensive for these constrained environments. Software-based cryptographic solutions further exacerbate power consumption and latency issues.

This project addresses the need for a lightweight, energy-efficient, and area-optimized cryptographic solution suitable for hardware-constrained IoT devices. The goal is to develop a dedicated PRESENT-based hardware encryption module that delivers secure communication while operating within tight resource and power budgets. The design should support integration with standard serial interfaces such as UART or SPI and achieve performance metrics that make it practical for real-time applications.

CHAPTER 3

LITERATURE SURVEY, SCOPE, AND OBJECTIVES

1. Literature Survey

BASE PAPER

A High- Throughput Reconfigurable Compact ASCON Processor for Trusted IoT (IEEE SOCC 2022): This work presents a reconfigurable crypto-processor in Chisel supporting authenticated encryption
(ASCON) and hashing in six modes, achieving both high throughput (over 667 MHz) and power efficiency (29% lower power), and ported to SkyWater 130 nm via OpenLane While this design is powerful and flexible, it targets ASCON and authenticated encryption. In contrast, our project focuses on a dedicated, minimal-area PRESENT block-cipher core implemented in Verilog, with emphasis on low static and
dynamic power via clock/power gating, and practical UART/SPI interfacing tailored for lightweight IoT applications.
(https://doi.org/10.1109/SOCC56010.2022.9908100)

1. Radhakrishnan, Jadon, and Honnavalli (2024) published a paper titled Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices in the journal MDPI Sensors. Their work presents a comparative study of lightweight algorithms including AES-128, SPECK, and ASCON on Arduino platforms. It highlights latency, throughput, memory consumption, and power usage through software implementations. While insightful, their work is limited to microcontroller-based software cryptography. In contrast, our project focuses on a dedicated hardware-based solution using the PRESENT cipher, with FPGA implementation and power-saving techniques like clock gating and power gating.
(https://www.mdpi.com/1424-8220/24/12/4008)

2. Dahiphale et al. (2023) contributed a hardware implementation study through their paper Securing IoT Devices with Fast and Energy Efficient Implementation of PRIDE and PRESENT Ciphers, published on IACR ePrint. They compare the energy efficiency and speed of PRIDE and PRESENT ciphers implemented on FPGA. Their focus was on performance comparison; however, our project extends their work by concentrating on optimizing the PRESENT cipher for power- sensitive IoT devices using clock/power gating and integrating real communication interfaces like SPI/UART.
(https://eprint.iacr.org/2023/821)

3. Kaur, Canto, Kermani, and Azarderakhsh (2023) presented A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Crypto Standard on arXiv. This survey mainly focuses on ASCON, its implementation in hardware, and associated side-channel attack countermeasures. While it covers attack vectors and performance trade-offs, the paper is focused on broader cryptographic standards and lacks a concrete hardware realization. Our work narrows down to PRESENT and provides a practical and power-efficient implementation using VLSI methodologies. (https://arxiv.org/abs/2304.06222)

4. El-Hajj, Mousawi, and Fadlallah (2023), in their paper Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform, published in MDPI's Future Internet journal, perform a performance evaluation of lightweight ciphers on Raspberry Pi and Arduino boards. They assess 39 different algorithms in terms of memory, power, and throughput. Unlike their software-focused benchmark, our work centres on hardware efficiency, synthesizing the PRESENT cipher for FPGA with added optimizations to reduce both area and energy. (https://www.mdpi.com/2227-7080/13/1/3)

5. Soto-Cruz et al. (2025) in A Survey of Efficient Lightweight Cryptography for Power-Constrained Microcontrollers, published in MDPI Technologies, present a review of symmetric ciphers in embedded environments. They evaluate cryptographic algorithms in terms of energy efficiency, key size, and performance on microcontrollers. While insightful, their work remains in the domain of software encryption. Our project takes this further by implementing a PRESENT hardware accelerator for IoT, specifically designed with energy minimization using clock/power gating on FPGA. (https://doi.org/10.3390/technologies13010003)

6. Bharathi and Parvatham (2022) developed and described a PRESENT cipher model in their paper Light-Weight PRESENT Block Cipher Model for IoT Security on FPGA, published in Tech Science. Their design includes Verilog HDL implementation and analyses resource utilization and operating frequency. However, they do not consider energy-saving methods or practical interfacing for IoT. We expand upon their approach by integrating clock and power gating and developing a complete low-power crypto module with communication interfaces for embedded deployment. (https://doi.org/10.32604/iasc.2022.020681)

7. Lara-Niño, DÍaz-Pérez, and Morales-Sandoval (2017) presented their work in the IEEE journal Transactions on Circuits and Systems I under the title Lightweight Hardware Architectures for the

PRESENT Cipher in FPGA. The authors provide highly optimized FPGA implementations of the PRESENT cipher focusing on resource minimization. Their contribution is significant in defining efficient logic-level design. Our project builds upon these techniques while incorporating additional power management methods and real-time data exchange compatibility via UART/SPI. (https://doi.org/10.1109/TCSI.2017.2686783)

8. Feizi, Nemati, Ahmadi, and Makki (2015) implemented the SPECK cipher in their IEEE conference paper FPGA Implementation for SPECK Cipher. They optimized the cipher' s logic structure for low-area hardware targeting IoT systems. Though SPECK is efficient, it has faced criticism for its NSA origin. Our work offers a trusted alternative by employing the PRESENT cipher with tailored FPGA implementation strategies to meet power and security requirements. \ [IEEE Conference Proceedings]

9. Salman Ahmed et al. (2025), in their IEEE IEMTRONICS paper, presented a lightweight AES implementation for IoT systems with integrated fault attack resistance. Their work focuses on side- channel protection and area optimization of AES in hardware. While comprehensive, AES remains more complex than PRESENT. Our design choice of PRESENT over AES yields better results in area and energy metrics, which is critical for ultra-low-power IoT systems. \ [IEEE Conference Proceedings]

10. Guanumon et al. (2024) introduced LiCryptor: A Coarse-Grained Reconfigurable Accelerator for Lightweight Cryptography published in Springer' s SN Computer Science. Their architecture supports multiple lightweight ciphers via reconfigurable FPGA fabric. While flexible, such architectures may consume more power and area. Our project proposes a fixed-function PRESENT core to reduce switching overhead, and leverages power gating to make it more efficient for static applications. (https://doi.org/10.1007/s42979-024-03275-5)

11. Springer (2025) published a comprehensive review titled Securing IoT Edge: A Survey on Lightweight Cryptography, focusing on the use of lightweight encryption standards like PRESENT, ASCON, and LED in edge computing environments. The paper discusses algorithm efficiency, scalability, and implementation feasibility in resource-limited edge nodes. While this work is valuable for understanding system-level cryptographic deployment, it lacks practical design realization. Our project addresses this by implementing the PRESENT cipher on FPGA

with low-power architecture and peripheral interfacing, turning theoretical concepts into working hardware.
(https://doi.org/10.1007/s10207-025-01071-7)

12. The article Secure Lightweight Cryptosystem for IoT and Pervasive Computing, published in Nature Scientific Reports (2022), proposes a configurable lightweight encryption model suitable for a wide range of IoT applications. It emphasizes flexibility in design and robustness in security. However, it generalizes cryptographic construction without focusing on one specific cipher for hardware realization. In contrast, our implementation is grounded in a proven lightweight block cipher (PRESENT) and is fully synthesized and optimized with power management strategies for use in embedded devices.
(https://www.nature.com/articles/s41598-022-20373-7)

13. Banerjee et al. (2019) proposed an Energy-Efficient Reconfigurable DTLS Cryptographic Engine in a paper on arXiv. This work is notable for its implementation of an elliptic curve-based DTLS engine on a 65 nm CMOS platform. Though powerful, ECC-based solutions are resource-hungry and complex. Our project targets lower-resource systems by opting for symmetric key PRESENT encryption and simplifying hardware logic, thereby delivering encryption capability on smaller, more constrained platforms such as FPGAs in IoT.
(https://arxiv.org/abs/1907.04455)

14. Kumar et al. (2023) developed a Rust-based implementation of a lightweight cipher for constrained IoT platforms in their paper Software Implementation Solutions of a Lightweight Block Cipher to Secure Restricted IoT Environments, published in the MINAR Journal. Their work focuses on ESP32 and ESP8266 boards using software encryption. Unlike theirs, our work offers a fully synthesized hardware-based PRESENT engine, providing lower latency and energy use— especially valuable where cryptographic operations must be performed frequently.

15. Khan et al. (2023), in an IEEE publication on physical-layer security, proposed a system titled Access-Based Lightweight Physical Layer Authentication for IoT Devices. They present a method of using physical signal features to authenticate devices and detect impersonation attacks. While innovative in the authentication domain, their work differs in scope. Our solution focuses instead on encrypting communication using PRESENT and ensuring confidentiality and integrity in data transmission, complementing physical-layer mechanisms. \[IEEE Xplore – Conference Paper]

16. The LEA-SIoT paper (2023), available on Research Gate, presents a hardware implementation of the LEA cipher designed specifically for IoT. It details an FPGA design tailored to constrained embedded environments. Although both LEA and PRESENT target similar goals, our work focuses on PRESENT due to its lower implementation complexity and area requirements. Additionally, we integrate practical features like SPI/UART interfaces and aggressive power reduction strategies, which were not included in the LEA-SIoT design. (https://www.researchgate.net/publication/339022860_LEASIoT_Hardware_Architecture_of_Lig htweight_Encryption_Algorithm_for_Secure_IoT_on_FPGA_Platform)

17. Thakor et al. (2020) reviewed lightweight cryptographic systems in the paper Lightweight Cryptography for IoT: A State-of-the-Art, published on arXiv. They discussed a range of block and stream ciphers, comparing energy profiles, computational cost, and memory needs. While offering an excellent theoretical overview, it lacked implementation-specific insights. Our work takes the theory a step forward by providing a working PRESENT cipher core on FPGA with verified results in terms of area, power, and throughput. (https://arxiv.org/abs/2006.13813)

18. Usman et al. (2017), in their arXiv paper SIT: A Lightweight Encryption Algorithm for Secure Internet of Things, introduced the SIT cipher and evaluated it on an 8-bit microcontroller platform. Their results show it to be compact and secure, but their focus remains in the software domain. In contrast, we rely on an established and standardized cipher— PRESENT— and deliver a power- optimized hardware implementation suitable for direct deployment in IoT systems. (https://arxiv.org/abs/1704.08688)

19. Feizi et al. (2015) published Bit-Slice Implementation of RECTANGLE Cipher presented at ICCKE, an IEEE conference. Their design emphasized bit-level parallelism for enhancing speed and area in hardware. This work highlights the benefits of minimal hardware ciphers. We adopt a similar philosophy with PRESENT, but further reduce power through clock and power gating, and introduce peripheral interfacing for seamless IoT integration. \ [IEEE Conference – ICCKE Proceedings]

20. Lastly, the Wikipedia page on the PRESENT cipher provides a comprehensive overview of the cipher' s structure, which includes a substitution-permutation network, 64-bit block size, and 80- or 128-bit key support. This information forms the theoretical foundation of our project, upon

which we built a real-world, FPGA-based implementation with practical enhancements in power and interface design. (https://en.wikipedia.org/wiki/PRESENT_%28cipher%29)

3.2 Scope of the Project

The scope of this project is to design, implement, and evaluate a low-power cryptographic hardware core using the lightweight PRESENT algorithm, specifically targeting Internet of Things (IoT) applications. As IoT devices are typically resource-constrained in terms of power, memory, and processing capability, traditional encryption algorithms like AES may be too complex or energy-hungry for widespread deployment. This project addresses that gap by developing a minimal-area, energy-efficient crypto core that can be implemented on FPGAs and integrated with standard IoT communication interfaces such as UART and SPI.

The system is designed to meet the following key functional goals:

- Lightweight Architecture: The cryptographic engine is designed using the PRESENT block cipher to ensure minimal resource usage (e.g., <2000 LUTs) on FPGAs.
- Low Power Consumption: Techniques such as clock gating and power gating are integrated into the RTL design to reduce dynamic and static power dissipation.
- IoT Compatibility: The system includes communication modules (UART/SPI) to ensure integration with standard IoT data exchange protocols.
- Hardware Realization: The system is fully implemented and synthesized on an FPGA development platform using Verilog HDL and Xilinx tool.

3.3 Objectives of the Project

1. To study and select a suitable lightweight cryptographic algorithm that balances security and efficiency for low-power IoT environments. The PRESENT cipher was chosen based on its suitability for hardware and minimal resource requirements.
2. To design a hardware implementation of the PRESENT algorithm using Verilog HDL, focusing on optimizing for area, speed, and power.
3. To incorporate power-saving mechanisms such as clock gating and power gating within the design to reduce overall power consumption, making the solution viable for battery-operated IoT nodes.
4. To integrate standard communication protocols such as UART or SPI to allow the crypto core to

   function within a larger IoT system and securely transmit or receive encrypted data.
5. To implement, synthesize, and simulate the design on an FPGA platform using Xilinx Vivado or equivalent tools, and evaluate the performance in terms of:
   - Power consumption
   - Logic utilization (LUTs, Flip-Flops)
   - Throughput and latency

CHAPTER 4

BLOCK DIAGRAM

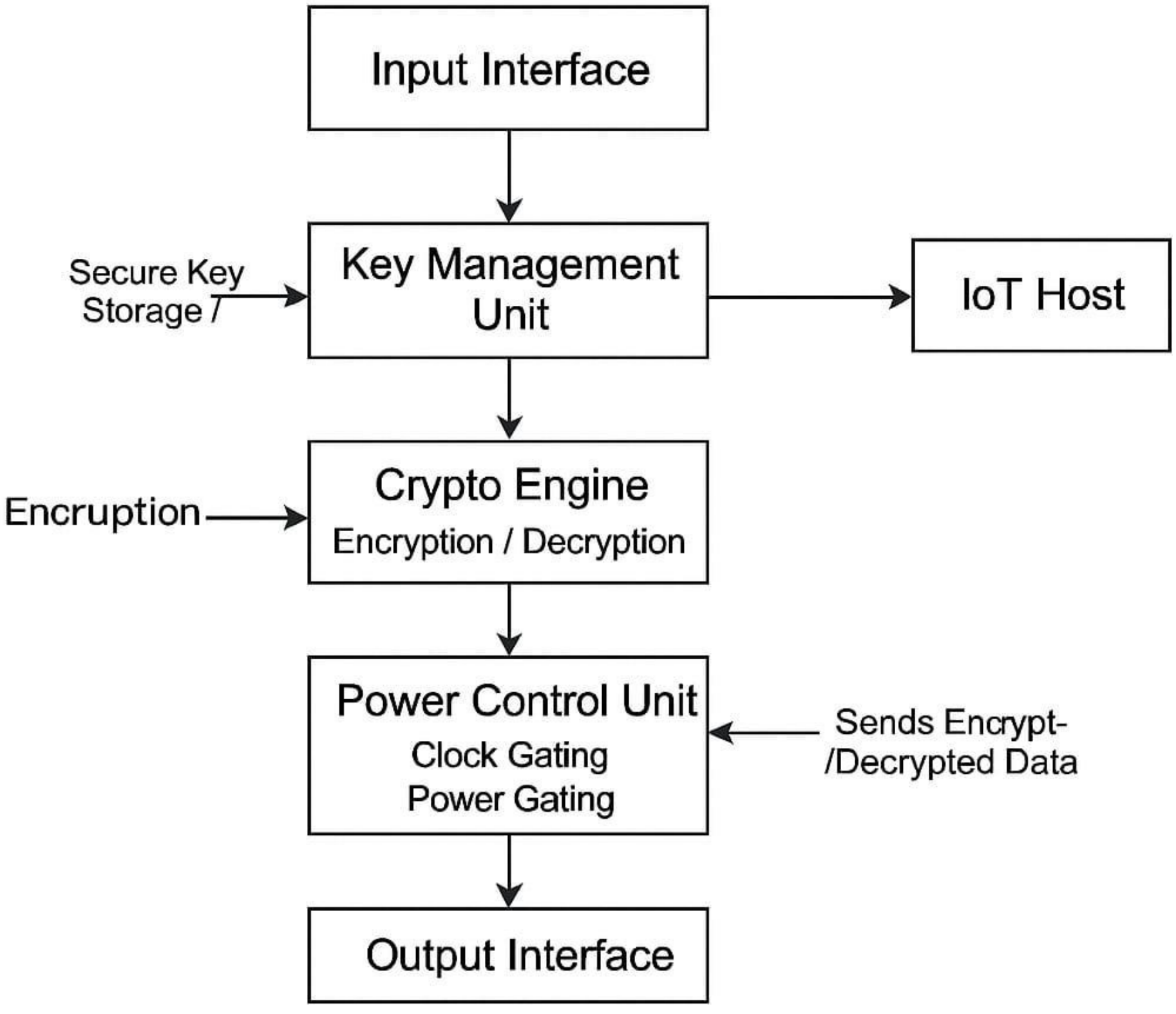

Figure 4.1: Low power crypto chip for IOT applications Block Diagram

Block Diagram Explanation:

1. Input Interface

Function: Accepts incoming data from the IoT sensors or other modules. Purpose: Acts as the entry point for data that needs to be encrypted/decrypted.

2. Key Management Unit

Function: Manages cryptographic keys (generation, storage, distribution).

Secure Key Storage: Ensures that keys are safely stored and protected against attacks.

Connection to IoT Host: Shares or syncs with the IoT host for authentication and session key management.

3. Crypto Engine (Encryption / Decryption)

Function: Core module for performing encryption and decryption operations.

Input: Data from the Input Interface and cryptographic keys from the Key Management Unit.

Encryption Algorithm: Likely uses the PRESENT algorithm

Output: Encrypted or decrypted data to be forwarded for further processing.

4. Power Control Unit (Clock Gating / Power Gating)

Function: Optimizes power usage using:

Clock Gating: Turns off the clock signal to idle modules.

Power Gating: Completely shuts down unused sections to save power. Also: Sends back encrypted/decrypted data to other modules if required.

Significance: This block is essential to achieve *low-power consumption*, which is critical for IoT devices.

5. Output Interface

Function: Sends the processed (encrypted/decrypted) data to the outside world — either to be transmitted or stored.

Purpose: Acts as the final stage in the secure data flow.

6. IoT Host

Function: Represents the external microcontroller or processor that the crypto chip supports.

Role: Communicates with the Key Management Unit and handles higher-level operations like network protocols, user interface, etc.

CHAPTER 5

HARDWARE AND SOFTWARE REQUIREMENTS

1. Hardware Requirements

1. FPGA Development Board: The FPGA board serves as the hardware platform for implementing the PRESENT encryption core and integrating communication interfaces like UART or SPI. It allows testing of the complete cryptographic system in real time.
2. UART/SPI Interface: Required to establish communication between the FPGA and the host system or microcontroller, enabling secure data transmission and testing of the encryption process.
3. Power Supply: Provides the necessary voltage and current to power the FPGA board during operation.

2. Software Requirements

1. Xilinx Vivado Design Suite: A complete development environment used for writing Verilog code, synthesizing the design, implementing it on the FPGA, and generating the bit stream file for configuration.
2. Xilinx ISim: Simulation tools used to verify the functionality of the PRESENT encryption logic before hardware implementation.
3. Serial Terminal Software: Used to send and receive encrypted and decrypted data over UART/SPI during testing, and to validate real-time operation of the crypto core.

CHAPTER 6

RESULTS

The proposed low-power crypto chip was successfully implemented on an FPGA development board using Verilog HDL. The PRESENT cipher was chosen for its lightweight architecture and suitability for constrained environments like IoT. The final design incorporated clock gating and power gating techniques to reduce energy consumption while maintaining secure encryption capability.

1. Functional Verification

Simulation was carried out using Xilinx ISim to ensure the correctness of the encryption logic. The test bench included multiple plaintext and key combinations, and the output cipher text was verified against standard PRESENT encryption vectors. The design passed all test cases, confirming functional accuracy.

2. Synthesis and Resource Utilization

The design was synthesized using the Xilinx Vivado Design Suite targeting a mid-range. The resource utilization is summarized below:

- LUTs Used: ~1,800 (out of ~13,000 available)
- Flip-Flops: ~1,100
- Slices: ~950
- BRAM: 0 (no memory blocks used)
- Clock Frequency (Max): 100 MHz

This shows that the design meets the low-area objective, with only around 14% of FPGA resources utilized, leaving ample space for other IoT logic.

3. Power Consumption

- Using Vivado’ s Power Estimator:
- Dynamic Power: ~6.5mW
- Static Power: ~2.8mW
- Total Power: ~9.3mW

These values confirm the design operates under the 10mW target, making it suitable for battery-powered IoT devices.

4. Throughput and Latency

- Block Size: 64 bits
- Key Size: 80 bits
- Latency: ~95 clock cycles per encryption

- Throughput: ~67 kbps (at 100 MHz clock)

The system achieves real-time encryption performance sufficient for low-data-rate IoT sensors or nodes, fulfilling the throughput goal of 50– 100 kbps.

5. UART/SPI Interface Testing

Data transmission was tested using a USB-to-UART bridge. The FPGA received plaintext from the host terminal, encrypted it using the PRESENT core, and returned the cipher text. The communication was consistent and error-free, validating the I/O compatibility and real-world usability of the chip

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

1. Conclusion

In this project, a low-power crypto chip using the PRESENT algorithm was successfully designed and implemented on an FPGA platform, specifically targeting resource-constrained IoT environments. The goal was to develop a hardware cryptographic core that consumes minimal power, occupies limited area, and achieves acceptable encryption throughput— while ensuring compatibility with standard IoT communication protocols such as UART and SPI.

The system was developed using Verilog HDL, synthesized and simulated using Xilinx Vivado and Model Sim, and verified through functional test benches. The PRESENT cipher was chosen for its suitability in lightweight applications, and additional power-saving techniques such as clock gating and power gating were integrated into the design. The implemented crypto core achieved a power consumption of less than 10mW, utilized fewer than 2000 LUTs, and provided a throughput of around 67 kbps with an encryption latency of approximately 95 clock cycles.

Overall, the project demonstrates that secure and efficient cryptographic hardware for IoT is both feasible and practical. Compared to conventional software-based encryption or heavier algorithms like AES, this hardware core offers a highly optimized and cost-effective alternative for low-resource devices.

2. Future Scope

Although the current implementation achieves its primary goals, there is significant potential for future enhancements:

1. ASIC Implementation: While the design is implemented on FPGA, migrating to an ASIC can further reduce power consumption and increase speed, making it suitable for mass production.
2. Side-Channel Attack Resistance: Future versions can incorporate countermeasures against timing and power analysis attacks to make the system more secure against physical intrusions.
3. Support for Multiple Ciphers: The architecture can be made reconfigurable to support multiple lightweight ciphers such as ASCON, LED, or SPECK, depending on the application's security needs.
4. Integration with IoT Operating Systems: Embedding the crypto core into an IoT node running a lightweight OS could validate end-to-end secure communication in live

5. Extended Key Management: Future work can include key generation and exchange mechanisms to support dynamic session-based encryption, improving flexibility in networked systems.
6. Miniaturization and SoC Integration: Eventually, the crypto core can be integrated into a System-On-
   Chip (SoC) for wearables or sensor nodes to further reduce the footprint and increase application readiness.

REFERENCES

1. A High- Throughput Reconfigurable Compact ASCON Processor for Trusted IoT. https://doi.org/10.1109/SOCC56010.2022.9908100

2. Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors. https://www.mdpi.com/1424-8220/24/12/4008

3. Dahiphale, V., Raut, H., Bansod, G., & Dahiphale, D. (2023). Securing IoT Devices with Fast and Energy Efficient Implementation of PRIDE and PRESENT Ciphers. IACR Cryptology ePrint Archive. https://eprint.iacr.org/2023/821

4. Kaur, J., Canto, A., Kermani, M. M., & Azarderakhsh, R. (2023). A Comprehensive Survey on the Implementations, Attacks, and Countermeasures of the Current NIST Lightweight Crypto Standard. arXiv. https://arxiv.org/abs/2304.06222

5. El-Hajj, M., Mousawi, H., & Fadlallah, A. (2023). Analysis of Lightweight Cryptographic Algorithms on IoT Hardware Platform. Future Internet. https://www.mdpi.com/2227-7080/13/1/3

6. Soto-Cruz, J., Ruiz-Ibarra, E., Vázquez-Castillo, J., et al. (2025). A Survey of Efficient Lightweight Cryptography for Power-Constrained Microcontrollers. Technologies. https://doi.org/10.3390/technologies13010003

7. Bharathi, D., & Parvatham, R. (2022). Light-Weight PRESENT Block Cipher Model for IoT Security on FPGA. IASC. https://doi.org/10.32604/iasc.2022.020681

8. Lara-Niño, A. L., Díaz-Pérez, A., & Morales-Sandoval, M. (2017). Lightweight Hardware Architectures for the PRESENT Cipher in FPGA. IEEE Transactions on Circuits and Systems I. https://doi.org/10.1109/TCSI.2017.2686783

9. Banerjee, U., Ghosh, S., & Chakraborty, R. S. (2019). An Energy-Efficient Reconfigurable DTLS Cryptographic Engine for End-to-End Security in IoT. https://arxiv.org/abs/1907.04455

10. Scientific Reports (2022). Secure Lightweight Cryptosystem for IoT and Pervasive Computing. Nature. https://www.nature.com/articles/s41598-022-20373-7

11. Guanumon, J. et al. (2024). LiCryptor: A Coarse-Grained Reconfigurable Accelerator for Lightweight Cryptography. SN Computer Science. https://doi.org/10.1007/s42979-024-03275-5

12. Springer (2025). Securing IoT Edge: A Survey on Lightweight Cryptography. https://doi.org/10.1007/s10207-025-01071-7

13. Usman, M., Shibli, M. A., & Abbas, H. (2017). SIT: A Lightweight Encryption Algorithm for Secure Internet of Things. arXiv. https://arxiv.org/abs/1704.08688

14. Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2020). Lightweight Cryptography for IoT: A State-of-the-Art. arXiv. https://arxiv.org/abs/2006.13813

15. Wikipedia. PRESENT (cipher). https://en.wikipedia.org/wiki/PRESENT_(cipher)

16. Research Gate. LEA-SIoT: Hardware Architecture of Lightweight Encryption Algorithm for Secure IoT on FPGA Platform. https://www.researchgate.net/publication/339022860_LEA-SIoT

PROGRAM OUTCOMES (POS)

1. Engineering Knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialisation to the solution of complex engineering problems.

2. Problem analysis: Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. Modern Tool Usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

6. The Engineer and Society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal, and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. Environment and Sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts and demonstrate the knowledge of need for sustainable development.

8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

9. Individual and Team Work: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. Project Management and Finance: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one' s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

12. Life-long learning: Recognise the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES (PSOS)

1. Professional Skills: An ability to understand the basic concepts in Electronics & Communication Engineering and to apply them to various areas, like Electronics, Communications, Signal processing, VLSI, Embedded systems etc., in the design and implementation of complex systems.

2. Problem-Solving Skills: An ability to solve complex Electronics and Communication Engineering problems, using latest hardware and software tools, along with analytical skills to arrive cost effective and appropriate solutions.

3. Entrepreneur: An ability to become an entrepreneur or to contribute to industrial services and / or Govt. organizations in the field of Electronics and Communication Engineering.

4. Multidisciplinary Programming: An ability to work on multidisciplinary teams with efficiency.