# LOW POWER CRYPTO-CHIP FOR IOT APPLICATIONS

Secure IoT demands ultra-low power cryptography solutions. The PRESENT algorithm offers a lightweight, hardware-friendly block cipher perfect for resource-constrained devices.

PRESENTED BY: MONISHA C

# INTRODUCTION

- Low power crypto chips are specially designed to perform encryption and decryption efficiently with very low energy usage.
- These chips use lightweight cryptographic algorithms that are optimized for speed and energy efficiency.
- They enable secure communication in IoT devices across various fields like smart homes, healthcare, agriculture, and industrial systems.
- Such chips help achieve real-time security while maintaining long battery life in IoT nodes.

# PROJECT OBJECTIVES

## Design Implementation

Create hardware-optimized PRESENT cipher implementation for IoT applications.

## Power Optimization

Achieve sub-10µW power consumption during active encryption operations

## **Performance Testing**

Measure throughput, latency, and energy consumption on target hardware

## Security Validation

Verify resistance against side-channel and cryptanalytic attacks.

# PROBLEM STATEMENT

IoT devices face unique challenges that conventional cryptographic solutions fail to address.

## Power Constraints

Battery-powered devices need years of operation without replacement.

## Area Limitations

Minimal silicon area available for security functions.

## Security Needs

Must resist sophisticated attacks despite limited resources.

# KEY FEATURES OF PRESENT ALGORITHM

## Lightweight Design

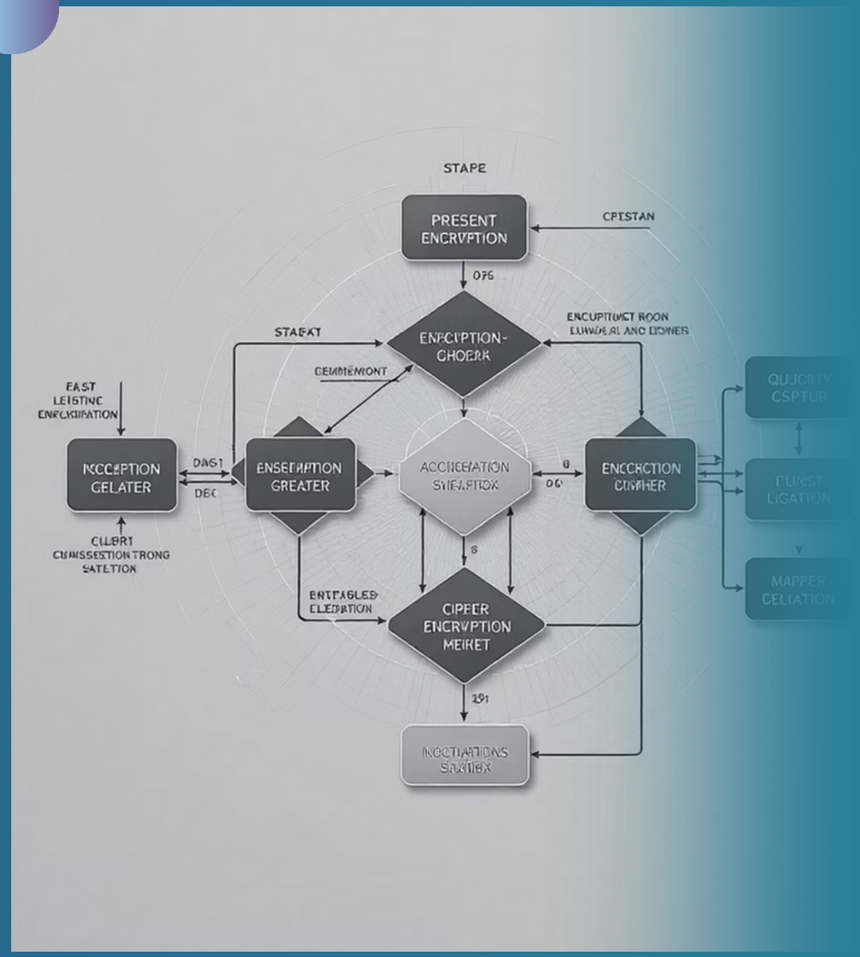
64-bit block size with 80/128-bit key options. Requires just 1570 gate equivalents

## Energy Efficiency

Optimized for hardware implementation with minimal power consumption per operation

## Security Strength

31 rounds provide adequate security margin against known attacks for IoT applications.



# Overview: PRESENT Algorithm

## Key Features

### Structure

- Lightweight block cipher with ISO/IEC standardization
- 64-bit block size with 80/128-bit key options
- Optimized for hardware-constrained environments
- 31 rounds of substitution-permutation network

## Algorithm

### Key Addition

XOR operation with round key

### S-Box Layer

Non-linear substitution with 4-bit S-boxes

### Permutation Layer

Bit permutation for diffusion

# Challenges in IoT Security


## Resource Limitations

Traditional crypto demands too much power and memory.

## Upgrade Difficulties

Long-lived devices need cryptosystem refreshes.

## Quantum Threats

Emerging quantum computing poses additional security risks.

# Performance & Results: Measured Metrics

## Throughput

Up to 200 Mbps @ 100 MHz on FPGA implementation

## Security Level

Resistant to differential cryptanalysis attacks up to 16 rounds


## Energy Efficiency

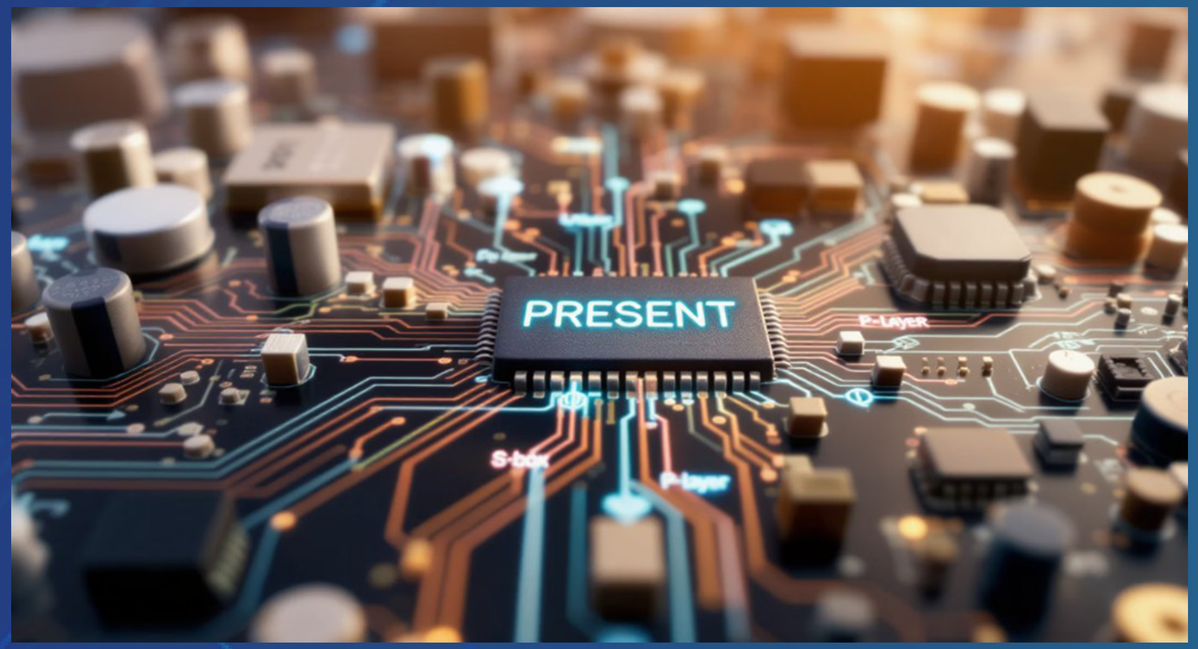
50-200 pJ per bit on measured hardware chips

## Area Efficiency

1.5K-2.5K gate equivalents depending on optimization

# Sample PRESENT Algorithm Implementation (Verilog)

This hardware implementation illustrates the core PRESENT algorithm components

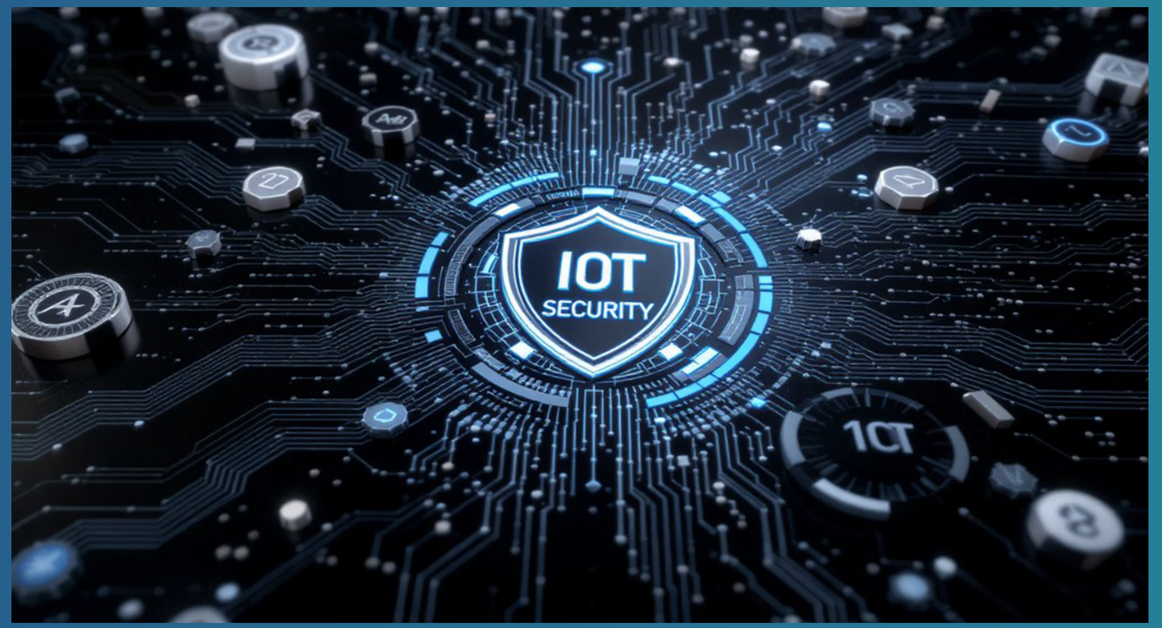



```
module present_round ( input [63:0]
  state_in,
  input [79:0] key,
  output [63:0] state_out
);
  wire [63:0] after_keyadd;
  wire [63:0] after_sbox;

  // Key addition
  assign after_keyadd = state_in ^
  key[79:16];

  // S-box layer present_sbox sbox_inst (
    .data_in(after_keyadd),
    .data_out(after_sbox)
  );

  // Permutation layer present_perm
  perm_inst (
    .data_in(after_sbox),
    .data_out(state_out)
  );
endmodule
```

# Conclusion & Future

PRESENT algorithm offers a proven solution for low-power, secure IoT hardware implementations.

Hardware crypto-chips significantly extend battery life while simplifying software integration.




## Future Directions

Post-quantum cryptography adaptations for IoT security

## Emerging Technologies

Reconfigurable and AI-accelerated cryptographic workflows

# THANK YOU