INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	**Titu Mary Ignatius**
Roll Number	:	**206102028**
Programme of Study	:	**Ph.D.**

Thesis Title: **Securing RISC-V Micro-architecture cores for High-security Applications in IoT against Power Side-Channel Attacks**

Name of Thesis Supervisor(s)	:	**Prof. Roy Paily Palathinkal**
Thesis Submitted to the Academic Division	:	**Yes**
Date of completion of Thesis Viva-Voce Exam	:	**26/05/2025**
Key words for description of Thesis Work	:	**RISC-V, AES, PAA, MTD, SNR, MI, TVLA**

SHORT ABSTRACT

The rapid growth of IoT edge (IoTe) devices has created a demand for secure, low-power, and area-efficient embedded processors. While the Advanced Encryption Standard (AES) is commonly used to secure these processors, they remain vulnerable to Power Analysis Attacks (PAA). Owing to the resource constraints in IoTe devices, it is essential to design embedded processors with cryptographic capabilities that provide strong security against power attacks while maintaining low resource consumption, area, and power overheads. This thesis proposes secure 32-bit RISC-V micro-architectures tailored for high-security IoTe applications to meet the requirements of reliable and secure embedded processors for modern IoTe devices. The design process begins by optimizing the pipeline stages and techniques to develop a compact low-power RISC-V core. Building on this foundation, two RISC-V crypto-cores are developed, each featuring a dedicated AES hardware unit integrated within the RISC-V pipeline and controlled by custom AES instructions. This integration reduces side-channel leakage, enhancing the intrinsic resilience of these RISC-V crypto-cores. To further improve security by obscuring AES power consumption patterns, a novel Non-Linear Cyclic Variable Clock Feistel Bridge-Inspired Countermeasure (NCVCFB) is designed. Operating in tandem with each AES round, it operates additional random rounds in the first and last AES rounds, disrupting PAA-targeted power samples. Additionally, the thesis explores tightly and loosely coupled AES integration techniques with RISC-V. The tightly coupled approach embeds AES within the RISC-V microarchitecture, extending the ISA for encryption instructions. While this approach offers better security and reduced area, it requires more efforts for integration and requires RISC-V compiler modifications. In contrast, the loosely coupled approach uses an external address enabled AES accelerator IP, offering greater flexibility. Finally, an ultra-low-power Random Clock Self Complementary (RCSC) countermeasure is introduced. It enhances security by introducing variability in both amplitude and time domains through complementary AES operations and inserting random delays in random rounds of AES, resulting in a variable number of clock cycles for each encryption.