National Institute of Technology Rourkela

Defence Seminar

Seminar Title	: Lightweight Block Cipher Optimizations for Resource Constrained Applications
Speaker	: Ruby Mishra (Rollno : 519ec7013)
Supervisor	: Prof. Manish Okade
Venue	: ECE Seminar Room (2nd Floor)
Date and Time	: 28 Mar 2024 (5:15 pm)

Abstract

: The rise of RFID-based consumer gadgets has led to a thirst for ubiquitous computing. The devices deployed in an IoT environment are constantly involved in handling sensitive data and communicating with each other and end users. As a result, there is a considerable need to protect these data from adversaries. Furthermore, because of their limited size, limited power limitations, and processing capacities, these applications are referred to as resource constrained. The encryption architectures need to be lightweight and satisfy the required performance and sufficient security. As a result, lightweight ciphers, rather than traditional cryptography techniques, are an excellent choice for such applications. The architectural design optimization of these lightweight encryption algorithms is the prime motivation of this work. Considering this, many logic synthesis techniques may be applied to a design before feeding it to the EDA tool for better outcomes. Functional decomposition techniques discussed in the literature are utilized only in benchmark circuits. In this research, we aim for optimized decomposition techniques for improving the design of substitution boxes for lightweight ciphers, with the motivation to realize efficient hardware mapping and performance. Our proposed architectures have less area and high throughput. Besides optimizing lightweight ciphers, side-channel countermeasures must be considered because they pose serious threats to the target applications. Therefore, we have also focused on the side-channel countermeasure for lightweight cipher architectures and have proposed a side-channel countermeasure architecture with low area overheads and improved performance metrics. All the designs are evaluated on FPGA platforms to signify their utility based on the required applications.