INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student	:	SUSHREE SILA P. GOSWAMI
Roll Number	:	156102025
Programme of Study	:	Ph.D.
Thesis Title: DESIGN OF CRYPTOGRAPHIC PRIMITIVES FOR WIRELESS COMMUNICATION AND BLOCKCHAIN MINING		
Name of Thesis Supervisor(s)	:	Dr. GAURAV TRIVEDI
Thesis Submitted to the Department/ Center	:	EEE
Date of completion of Thesis Viva-Voce Exam	:	31/05/2024
Key words for description of Thesis Work	:	Cryptography, FPGA, Security, Stream cipher, Secret sharing, Blockchain

SHORT ABSTRACT

The rising reliance on the internet across various sectors has heightened the importance of security measures, given the potential threat posed by cyber attackers who could corrupt or misuse data. This thesis explores the implementation of diverse cryptographic algorithms—DES, RSA, AES, ECC, and ECCDH—on FPGA (Field Programmable Gate Array). In secure wireless communications, stream ciphers are preferred for their hardware implementation simplicity. The design of stream ciphers generally involves using a pseudorandom number generator to produce a keystream, which masks the plaintext through a XOR operation, resulting in cipher text. This research presents the realization of these designs using Verilog Hardware Description Language and their implementation on FPGA. Experimental results indicate that a modified SNOW 2.0 architecture is 13% more resource-efficient and 19% more efficient overall compared to the traditional SNOW 2.0, and 104% more efficient than existing architectures. Security is paramount in electronic communication, particularly in wireless networks like LTE, where cryptographic algorithms are vital for protecting sensitive data. While software implementations are straightforward, they often lack the speed required for real-time communication devices, necessitating hardware implementations of cryptographic processors. This thesis introduces a novel SNOW3G crypto processor for 4G LTE security, optimized for area, power, and efficiency. Implemented on the Zynq ZC702 FPGA, this design uses only 0.31% of available area and achieves significant efficiency and low power consumption, making it suitable for mobile devices.

To ensure both confidentiality and reliability, secret sharing methods distribute cryptographic keys among multiple participants. This thesis proposes efficient FPGA implementations of Shamir's linear and Renval-Ding's nonlinear secret sharing schemes, significantly enhancing performance, reducing power consumption, and improving resource utilization compared to software realizations. Furthermore, blockchain security, reliant on computationally intensive algorithms like Bitcoin's proof-of-work, faces challenges due to high energy consumption. This thesis proposes an ASIC implementation for blockchain mining to optimize energy consumption and computational resources, validated through FPGA implementation. This work aims to enhance the efficiency and effectiveness of cryptographic systems in various applications.