CSCS 454 - Hardware Design of Cryptographic Algorithms

UNIT I

Hardware Design of the Advanced Encryption Standard (AES) : Algorithmic and Architectural Optimizations for AES Design, Circuit for the AES S-Box, Implementation of the MixColumns Transformation, Reconfigurable Design for the Rijndael Cryptosystem, Single Chip Encryptor/Decryptor. **(12 hours)**

UNIT II

Efficient Design of Finite Field Arithmetic on FPGAs : Finite Field Multiplier, Finite Field Multipliers for High Performance Applications, Karatsuba Multiplication, Karatsuba Multipliers for Elliptic Curves, Designing for the FPGA Architecture, Analyzing Karatsuba Multipliers on FPGA Platforms, High-Performance Finite Field Inversion Architecture for FPGAs, Itoh-Tsujii Inversion Algorithm, The Quad ITA Algorithm, Generalization of the ITA for 2^n Circuit, Hardware Architecture for 2^n Circuit Based ITA, Area and Delay Estimations for the 2^n ITA.

(12 hours)

UNIT III

High-Speed Implementation of Elliptic Curve Scalar Multiplication on FPGAs : The Elliptic Curve Cryptoprocessor, Point Arithmetic on the ECCP, The Finite State Machine (FSM), Acceleration Techniques of the ECC Processor, Pipelining Strategies for the Scalar Multiplier, Scheduling of the Montgomery Algorithm, Finding the Right Pipeline, Detailed Architecture of the ECM. **(12 hours)**

TextBooks:

(1). "Hardware Security Design, Threats, and Safeguards", Debdeep Mukhopadhyay Rajat Subhra Chakraborty, CRC Press, 2015

(2). " Hardware IP Security and Trust " , Prabhat Mishra, Swarup Bhunia, Mark Tehranipoor, Springer, 2017

(3). "Fault Tolerant Architectures for Cryptography and Hardware Security", Sikhar Patranabis Debdeep Mukhopadhyay, Springer, 2018

(4). "Security of Block Ciphers - From Algorithm Design to Hardware Implementation", Kazuo Sakiyama, Yu Sasaki, Yang Li, Wiley, 2015

(5). "Physically Unclonable Functions From Basic Design Principles to Advanced Hardware Security Applications", Basel Halak, Springer, 2018

(6). "Hardware-Based Computer Security Techniques to Defeat Hackers From Biometrics to Quantum Cryptography", Roger Dube, Wiley, 2008