GUJARAT TECHNOLOGICAL UNIVERSITY

BRANCH: CYBER SECURITY (59)
Subject Code: 2745904
Semester – IV
Subject Name: Hardware Security

Type of course: Master of Engineering (Cyber Security)

Prerequisite: -

Rationale:
This course will focus on the importance of addressing different security threats on modern hardware design, manufacturing, installation, and operating practices. In particular, the threats would be shown to be relevant at scales ranging from a single user to an entire nation's public infrastructure. Through theoretical analyses and relevant practical world case studies, the threats would demonstrate, and then state-of-the-art defense techniques would be described. The course would borrow concepts from diverse fields of study such as cryptography, hardware design, circuit testing, algorithms, and machine learning.

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks						Total Marks
				Theory Marks		Practical Marks				
L	T	P	C	ESE (E)	PA (M)	ESE (V)		PA (I)		
						ESE	OEP	PA	RP	
4	0	2	5	70	30	20	10	10	10	150

Content:

Sr. No.	Content	Total Hrs
1	**Overview of Modern Cryptography** Introduction Cryptography: Some Technical Details Block Ciphers Rijndael in Composite Field Elliptic Curves Scalar Multiplications: LSB First and MSB First Approaches Montgomery's Algorithm for Scalar Multiplication Conclusions	4
2	**Modern Hardware Design Practices** Introduction	4

GUJARAT TECHNOLOGICAL UNIVERSITY

BRANCH: CYBER SECURITY (59)

Subject Code: 2745904

	Mapping an Algorithm to Hardware: Components of a Hardware Architecture Case study: Binary gcd Processor Enhancing the Performance of a Hardware Design Modelling of the Computational Elements of the gcd Processor Experimental Results	
3	**Hardware Design of the Advanced Encryption Standard (AES)** Introduction Algorithmic and Architectural Optimizations for AES Design Circuit for the AES S-Box Implementation of the MixColumns Transformation An Example Reconfigurable Design for the Rijndael Cryptosystem	**5**
4	**Efficient Design of Finite Field Arithmetic on FPGAs** Introduction Finite Field Multiplier Finite Field Multipliers for High Performance Applications Karatsuba Multiplication Karatsuba Multipliers for Elliptic Curves Designing for the FPGA Architecture	**7**
5	**High-Speed Implementation of Elliptic Curve Scalar Multiplication on FPGAs** Introduction The Elliptic Curve Cryptoprocessor Point Arithmetic on the ECCP The Finite State Machine (FSM) Performance Evaluation	**9**
6	**Introduction to Side Channel Analysis** Introduction What Are Side Channels? Kocher's Seminal Works Power Attacks Fault Attacks Cache Attacks Scan Chain Based Attacks Conclusions	**7**
7	**Differential Fault Analysis of Ciphers** Introduction to Differential Fault Analysis DFA and Associated Fault Models Principle of Differential Fault Attacks on AES State-of-the-art DFAs on AES	**6**
8	**Cache Attacks on Ciphers** Memory Hierarchy and Cache Memory Timing Attacks Due to CPU Architecture Trace-Driven Cache Attacks Access-Driven Cache Attacks	**7**

GUJARAT TECHNOLOGICAL UNIVERSITY

BRANCH: CYBER SECURITY (59)
Subject Code: 2745904

Suggested Specification table with Marks (Theory):

Distribution of Theory Marks					
R Level	U Level	A Level	N Level	E Level	C Level
10	**30**	**30**	**20**	**10**	**0**

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Text/Reference Books:

1. Debdeep Mukhopadhyay and Rajat Subhra Chakraborty, "Hardware Security: Design, Threats, and Safeguards", CRC Press
2. Ahmad-Reza Sadeghi and David Naccache (eds.): Towards Hardware-intrinsic Security: Theory and Practice, Springer.
3. Ted Huffmire et al: Handbook of FPGA Design Security, Springer.
4. Stefan Mangard, Elisabeth Oswald, Thomas Popp: Power analysis attacks - revealing the secrets of smart cards. Springer 2007.
5. Doug Stinson, Cryptography Theory and Practice, CRC Press.

Course Outcomes:

Sr. No.	CO statement	Marks % weightage
CO-1	Describe and analyze hardware design and fabrication and their interrelations.	25%
CO-2	Develop solutions for hardware security problems.	25%
CO-3	Characterize and assess hardware attacks and hardware trojans.	25%
CO-4	Use appropriate resources to stay abreast of new hardware attacks and tools and techniques.	25%