ANNEXURE – DETAILED SYLLABUS

(CS) Hardware Security 3-0-0 Credits: 3

Overview of Different Issues of Hardware Security

Preliminaries: Algebra of Finite Fields, Basics of the Mathematical Theory of Public Key Cryptography, Basics of Digital Design on Field-programmable Gate Array (FPGA), Classification using Support Vector Machines (SVMs)

Useful Hardware Security Primitives: Cryptographic Hardware and their Implementation, Optimization of Cryptographic Hardware on FPGA, Physically Unclonable Functions (PUFs), PUF Implementations, PUF Quality Evaluation, Design Techniques to Increase PUF Response Quality

Side-channel Attacks on Cryptographic Hardware: Basic Idea, Current-measurement based Side-channel Attacks (Case Study: Kocher's Attack on DES), Design Techniques to Prevent Side-channel Attacks, Improved Side-channel Attack Algorithms (Template Attack, etc.), Cache Attacks

Testability and Verification of Cryptographic Hardware: Fault-tolerance of Cryptographic Hardware, Fault Attacks, Verification of Finite-field Arithmetic Circuits

Modern IC Design and Manufacturing Practices and Their Implications: Hardware Intellectual Property (IP) Piracy and IC Piracy, Design Techniques to Prevent IP and IC Piracy, Using PUFs to prevent Hardware Piracy, Model Building Attacks on PUFs (Case Study: SVM Modeling of Arbiter PUFs, Genetic Programming based Modeling of Ring Oscillator PUF)

Hardware Trojans: Hardware Trojan Nomenclature and Operating Modes, Countermeasures Such as Design and Manufacturing Techniques to Prevent/Detect Hardware Trojans, Logic Testing and Side-channel Analysis based Techniques for Trojan Detection, Techniques to Increase Testing Sensitivity

Infrastructure Security: Impact of Hardware Security Compromise on Public Infrastructure, Defense Techniques (Case Study: Smart-Grid Security)

Textbooks:

Ahmad-Reza Sadeghi and David Naccache (eds.): Towards Hardware-intrinsic Security: Theory and Practice, Springer (free e-book download through IIT subscription).

Ted Huffmire *et al*: Handbook of FPGA Design Security, (free e-book download through IIT subscription).

Stefan Mangard, Elisabeth Oswald, Thomas Popp: Power analysis attacks - revealing the secrets of smart cards, Springer (free e-book download through IIT subscription).

Mark Joye and Michael Tunstall: Fault Analysis in Cryptography, Springer (free e-book download through IIT subscription).

Reference Books:

D. Mukhopadhyay and R. S. Chakraborty, "Hardware Security: Design, Threats and Safeguards", CRC Press, (forthcoming).

A. Das and C. E. Veni Madhavan, Public-Key Cryptography: Theory and Practice, Pearson Education Asia.

Doug Stinson, Cryptography Theory and Practice, CRC Press.

5. Syllabus of CS60041 CRYPTOGRAPHY AND NETWORK SECURITY

Introduction: Basic objectives of cryptography, secret-key and public-key cryptography, one-way and trapdoor one-way functions, cryptanalysis, attack models, classical cryptography.

Block ciphers: Modes of operation, DES and its variants, RCS, IDEA, SAFER, FEAL, BlowFish, AES, linear and differential cryptanalysis.

Stream ciphers: Stream ciphers based on linear feedback shift registers, SEAL, unconditional security.

Message digest: Properties of hash functions, MD2, MD5 and SHA-1, keyed hash functions, attacks on hash functions.

Public-key parameters: Modular arithmetic, gcd, primality testing, Chinese remainder theorem, modular square roots, finite fields.

Intractable problems: Integer factorization problem, RSA problem, modular square root problem, discrete logarithm problem, Diffie-Hellman problem, known algorithms for solving the intractable problems.

Public-key encryption: RSA, Rabin and EIGamal schemes, side channel attacks.

Key exchange: Diffie-Hellman and MQV.

Digital signatures: RSA, DSA and NR signature schemes, blind and undeniable signatures.

Entity authentication: Passwords, challenge-response algorithms, zero-knowledge protocols.

Standards: IEEE, RSA and ISO standards.

Network security: Certification, public-key infra-structure (PKI), secure socket layer (SSL), Kerberos.

Advanced topics: Elliptic and hyper-elliptic curve cryptography, number field sieve, lattices and their applications in cryptography, hidden monomial cryptosystems, cryptographically secure random number generators.

References

1. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press.
2. William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall of India.
3. Neal Koblitz, A course in number theory and cryptography, Springer.
4. Johannes A. Buchmann, Introduction to Cryptography, Undergraduate Text in Mathematics, Springer.
5. Doug Stinson, Cryptography Theory and Practice, CRC Press.
6. A. Das and C. E. Veni Madhavan, Public-Key Cryptography: Theory and Practice, Pearson Education Asia.