20VL026 - HARDWARE SECURITY

Unit-1: Introduction to Physical Unclonable Functions (PUFs):
Introduction, Trust and Security in a Modern World, Information Security and Cryptology, Physical Security and Roots of Trust, The PUF Concept, On PUFs and Fingerprints, PUF Class, PUF Instance, PUF Evaluation, Shorthand Notation, Details of a PUF Experiment, PUF Response Intra-distance, Inter-distance Statistics.

Unit-2: Classification
Non-electronic, Electronic and Silicon PUFs, Intrinsic and Non-intrinsic PUFs, Weak and Strong PUFs, Intrinsic PUF Constructions: SRAM PUF, Latch, Flip-Flop, Butterfly, Buskeeper PUFs, Bistable Ring PUF.

Unit-3: Physically Unclonable Functions: Properties
Introduction, Constructability and Evaluability, Reproducibility, Uniqueness and Identifiability, Unpredictability, Mathematics and True Unclonability, One-Wayness, Tamper Evidence, Unpredictability of a Physical Function System.

Unit-4: Implementation and Experimental Analysis of Intrinsic PUFs
Introduction, Test Chip Design, Top-Level Architecture, PUF Block: Arbiter PUF, Power Domains, Implementation Details, Experimental Uniqueness and Reproducibility Results.

Unit-5: Modeling Attacks and Applications
Modeling Attacks on Arbiter PUFs, Modeling with Machine Learning Techniques, Modeling Entropy Bound, Assessing Entropy Adversary Models and Basic Entropy Bounds, Completely Ignorant Adversary, Adversary Knows Global Bias, Adversary Knows Inter-Bit Dependencies

Text book:
[1]. Physically Unclonable Functions Construction, Properties and Applications: Role Maes, springer, DOI 10.1007/978-3-642-41395-7

References:
[1] O. Kommerling and M. G. Kuhn, ―Design principles for tamper-resistant smartcard processors,‖ in Proc. USENIX Workshop Smartcard Technology,1999, pp. 9–20.
[2] R. Anderson and M. Kuhn, ―Tamper resistance—A cautionary note,‖ in Proc. 2nd USENIX Workshop Electronic Commerce, Nov. 1996, pp. 1–11.
[3] O. Goldreich, S. Goldwasser, and S. Micali, ―On the cryptographic applications of random functions,‖ Proc. Crypto Advanceds in Cryptology, pp. 276–288, 1985.
[4] P. S. Ravikanth, ―Physical one-way functions,‖ Ph.D. dissertation, Dept.