

## NPTEL Video Lecture Topic List - Created by LinuXpert Systems, Chennai

NPTEL Video Course - Computer Science and Engineering - NOC:Hardware Security

Subject Co-ordinator - Dr. Debdeep Mukhopadhyay

Co-ordinating Institute - IIT - Kharagpur

Sub-Titles - Available / Unavailable | MP3 Audio Lectures - Available / Unavailable

Lecture 1 - Introduction to Hardware Security - Part 1  
Lecture 2 - Introduction to Hardware Security - Part 2  
Lecture 3 - Algorithm to Hardware  
Lecture 4 - Finite Field Architectures - 1  
Lecture 5 - Finite Field Architectures - 1 (Continued...)  
Lecture 6 - Hardware Design for Finite Field Inverse  
Lecture 7 - Hardware Architecture for Finite Field Inverse  
Lecture 8 - Background on Cryptography, Cryptanalysis and Advanced Encryption Standard (AES)  
Lecture 9 - Advanced Encryption Standard (AES) and Side Channel Analysis  
Lecture 10 - Field Isomorphisms  
Lecture 11 - Field Isomorphisms (Continued...)  
Lecture 12 - Hardware Implementation of Advanced Encryption  
Lecture 13 - Hardware Implementation of Advanced Encryption  
Lecture 14 - Hardware Implementation of Advanced Encryption (Continued...)  
Lecture 15 - Compact AES-Box  
Lecture 16 - Compact AES S-Box - Part II  
Lecture 17 - Compact AES S-Box in Normal Basis - Part I  
Lecture 18 - Compact AES S-Box in Normal Basis - Part II  
Lecture 19 - Hardware for Elliptic Curve Cryptography - Part I  
Lecture 20 - Hardware for Elliptic Curve Cryptography - Part II  
Lecture 21 - Hardware for Elliptic Curve Cryptography - Part III  
Lecture 22 - Hardware for Elliptic Curve Cryptography - Part IV  
Lecture 23 - Hardware for Elliptic Curve Cryptography - Part V  
Lecture 24 - Introduction to Side Channel Analysis  
Lecture 25 - Power Analysis - Part I  
Lecture 26  
Lecture 27  
Lecture 28  
Lecture 29

---

Get Digi-MAT (Digital Media Access Terminal) For High-Speed Video Streaming of NPTEL and Educational Video Courses in LAN

[www.digimat.in](http://www.digimat.in)

## NPTEL Video Lecture Topic List - Created by LinuXpert Systems, Chennai

Lecture 30  
Lecture 31 - Power Analysis - Part VII  
Lecture 32 - Power Analysis - Part VIII  
Lecture 33 - Power Analysis - Part IX  
Lecture 34 - Power Analysis - Part X  
Lecture 35 - Power Analysis - Part XI  
Lecture 36  
Lecture 37  
Lecture 38  
Lecture 39  
Lecture 40  
Lecture 41 - Power Analysis - Part XVII  
Lecture 42 - Power Analysis - Part XVIII  
Lecture 43 - Power Analysis Countermeasures  
Lecture 44 - Power Analysis Countermeasures (Continued...)  
Lecture 45 - Power Analysis Countermeasures (Continued...)  
Lecture 46 - Fault Analysis of Cryptosystems  
Lecture 47 - Improved DFA of AES  
Lecture 48 - Multi-Byte and key Scheduling Based Fault Analysis of AES  
Lecture 49 - Multi-Byte and key Scheduling Based Fault Analysis of AES (Continued...)  
Lecture 50 - Redundancy Based Fault Intensity  
Lecture 51 - Redundancy Base Fault Countermeasures and Differential Fault Intensity Attacks (Continued...)  
Lecture 52 - Infective Countermeasures for DFA  
Lecture 53 - Infective Countermeasures for DFA (Continued...)  
Lecture 54 - Infective Countermeasures for DFA (Continued...)  
Lecture 55 - Microarchitectural attacks  
Lecture 56 - Microarchitectural attacks  
Lecture 57 - Microarchitectural attacks  
Lecture 58 - Microarchitectural attacks  
Lecture 59 - Microarchitectural attacks  
Lecture 60 - Microarchitectural attacks