**Advanced Topics on Security- From Theory to Practice**

|  |  |  |
| --- | --- | --- |
| DAY | Topics | Drills |
| 1 | 1. Introduction to Hardware Security, 2. Introduction to Side Channel 3. Introduction to Finite Field 4. Introduction to Field Isomorphism | 1. HDL code of AES S-Box 2. Generating Simulated Power Trace |
| 2 | 1. Compact AES- S-Box using field isomorphism 2. Differential Power Attacks using difference of mean (DoM) | 1. HDL code of AES S-Box using field isomorphism 2. DoM on simulated power traces 3. Dom on actual power traces |
| 3 | 1. Correlation Power Analysis (CPA) 2. Mutual Information (MI) Analysis 3. Template Attacks | 1. CPA on actual power traces 2. MI on actual power traces 3. Template attack on actual power traces |
| 4 | Fault Attacks   1. Different fault attack methodologies 2. Note on countermeasures | 1. Differential fault attacks 2. Differential fault intensity analysis |
| 5 | Micro-Architectural Attacks   1. Cache timing attacks 2. Hardware performance counters, branch prediction attacks | Demo:   1. Cache timing attack 2. Hardware performance counters |

**Schedule**