

ECE 746 Project Presentations

Friday, May 1st, 2015

4:30 - 7:50 PM

Engineering Building, Room 3507

Session I Side Channel Analysis

4:30	-	4:40	Welcome & Rules of the Contest for the Best Project <i>Jens-Peter Kaps</i>
4:40	-	4:55	Rajiv Gautham Champati and Ashritha Rasa <i>Power and EM Analysis Attacks on Contactless Smart-Cards</i>
4:55	-	5:10	Sangamitra Reddy Katamreddy <i>Electromagnetic Analysis</i>
5:10	-	5:25	Jon Erickson <i>Towards a Parallel Analysis in FOBOS Using MapReduce</i>
5:25	-	5:40	Akshay Reddy Veerayyagari <i>Generic Information-Theoretic Distinguisher</i>

Refreshments

Session II Implementations of Cryptographic Algorithms

5:55	-	6:10	Upendarreddy Mamidi <i>Hardware Implementation of Authenticated Cipher SILC</i>
6:10	-	6:25	William Diehl <i>RTL Implementations of Authenticated Ciphers</i>
6:25	-	6:40	Ahmed Ferozpuri <i>Analysis of the BLISS I lattice-based signature scheme on the Zynq-7000 All Programmable SoC</i>

Refreshments

Session III Security Analysis

6:55	-	7:10	Cody Jenkins <i>Secure Distributed Storage Using MongoDB</i>
7:10	-	7:25	Asrat Dea <i>Key Management Protocol on RFID-MIFARE Classic Security</i>
7:25	-	7:40	Victor S. Andrei <i>Secret</i>
7:40	-	7:50	Announcements & Closing Remarks