ECE 746 Project Presentations

Friday, May 5th, 2017
4:30 - 7:50 PM
Engineering Building, Room 3507

Session I **CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness**			
4:30	-	4:40	Welcome & Rules of the Contest for the Best Project *Jens-Peter Kaps*
4:40	-	5:00	Hardware Implementation of Lightweight Round 3 CAESAR Candidates *Farnoud Farahmand*
5:00	-	5:20	Implementation of SILC full-width and light-weight (32-bit) versions *Samhita Kanagala*
5:20	-	5:40	Addition of an Hardware Supported AES MCU to the XXBX Cryptographic Benchmarking Platform *Kinnera Chintamaneni and Raghurama Velagala*
5:40	-	6:00	Extending XXBX Support to STM32 Microcontrollers *M. Ryan Carter*
Refreshments			
Session II **Security of Implementations of Cryptographic Algorithms**			
6:20	-	6:40	Investigation on NFC Remote Side-Channel Analysis *Songsong Liu*
6:40	-	7:00	Implementation of Welch's T-Test for Leakage Detection *Abubakr Abdulgadir*
7:00	-	7:20	Area optimized FPGA implementation of the Berlekamp-Massey algorithm for physical unclonable functions *Brian Jarvis*
7:20	-	7:40	No Title *Victor S. Andrei*
7:40	-	7:50	Announcements & Closing Remarks