ECE 746 Project Presentations

Tuesday, May 7th, 2013
4:30 - 7:10 PM
Engineering Building, Room 3202

Session I **Physical Unclonable Functions, Factoring and Random Numbers**			
4:30	-	4:40	Welcome & Rules of the Contest for the Best Project *Jens-Peter Kaps*
4:40	-	5:00	Implementation of a Configurable RO-PUF on Spartan6 FPGAs *Yamini Ravishankar*
5:00	-	5:20	Implementation of the General Number Field Sieve (GNFS) algorithm, using Line Sieving, in FPGA Hardware *Robert Lorentz*
5:20	-	5:40	Generation of Truly Random Numbers with Known Factorization *Simrit Kaur Arora*
Refreshments			
Session II **Security of FPGAs, Attacks and Countermeasures**			
6:00	-	6:20	Survey of FPGA security *Shegaw Alemu*
6:20	-	6:40	"DPA in a Box" FOBOS: Flexible Opensource BOard for SideChannel Analysis *Jeremy Barthélemy, Aaron Hunter, AnneMarie Cressin*
6:40	-	7:00	Analysis of Patents Proposing Countermeasures Against Side-Channel Attacks *Anurag Kamat Haldonker*
7:00	-	7:10	Announcements & Closing Remarks