

# ECE646 Project Presentations

Wednesday, December 19, 2007

5:00 - 10:00 PM

Student Union II, Room 3 & 4

---

<b>Session I</b>			
<b>Authentication and Digital Rights Management</b>			
5:00	-	5:10	Welcome & Rules of the Contest for the Best Project <i>Jens-Peter Kaps</i>
5:10	-	5:30	<b>AD-1:</b> On Necessity and Sufficiency of Cryptography in Digital Rights Management <i>Srividya Shanmugham</i> [Report] [Specifications]
5:30	-	5:50	<b>AD-2:</b> Zero-Knowledge Proofs as Authentication Method in Wireless Sensor Networks <i>Stephen C. Keith, Sammy Lin</i> [Report] [Specifications]
Refreshments			
<b>Session II</b>			
<b>Random Number Generators</b>			
6:00	-	6:20	<b>RN-1:</b> True Random Number Generators <i>Shashi Prashanth Karanam, Keerat Brar</i> [Report] [Specifications]
6:20	-	6:40	<b>RN-2:</b> Mersenne Twister, a Pseudo-Random Number Generator <i>Duyen Tran, Archana Jagannatam</i> [Report] [Specifications]
Refreshments			
<b>Session III</b>			
<b>Cryptographic Protocols</b>			
6:50	-	7:10	<b>CP-1:</b> Kerberos Using Public Key Cryptography <i>Farhana S. Munnee, Anirudh Jonnavitula</i> [Report] [Specifications]
7:10	-	7:30	<b>CP-2:</b> Analysis of Wireless Network Security Protocols <i>Sanjay Rathi, Vaibhav Vora</i> [Report] [Specifications]
7:30	-	7:50	<b>CP-3:</b> IPSEC <i>Alberto Pena, Daniel Buchholz</i> [Report] [Specifications]
Refreshments			
<b>Session IV</b>			
<b>Hardware Implementations</b>			
8:00	-	8:20	<b>HI-1:</b> AES Finalists and their Performance Comparison using FPGAs <i>Lalitha Chikkam, Bhupathi Karkarlapudi</i> [Report] [Specifications]
8:20	-	8:40	<b>HI-2:</b> Comparisons of Hardware Implementations between Block and Stream Ciphers <i>Chethan Ananth, Marcello Brito</i> [Report] [Specifications]
8:40	-	9:00	<b>HI-3:</b> Efficient Cryptographic Implementations for Smart Cards <i>Swathi Tripuraneni, Trong Nguyen</i> [Report] [Specifications]
Refreshments			
<b>Session V</b>			
<b>Attacks</b>			
9:10	-	9:30	<b>AT-1:</b> Differential Power Analysis Attacks <i>Rajesh Velegalati, Panasayya Yalla</i> [Report] [Specifications]
9:30	-	9:50	<b>AT-2:</b> Enigma <i>Ahmad Salman, Brian Sanders</i> [Report] [Specifications]
9:50	-	10:00	Announcements & Closing Remarks

---