ECE 646 Applied Cryptography
Final Project Presentations

Monday, December 6, 2021, 4:00-10:00 PM

Zoom Link:
https://gmu.zoom.us/j/96059425230?pwd=cERXNW9CTmZIRks1MzJOZUFiUkNCZz09

Session I
Public Key Infrastructure

4:00-4:10 PM	**Welcome & Rules of the Contest for the Best Project** by Kris Gaj
4:10-4:25 PM	**Evaluation of X.509 Digital Certificates on Web Browsers** by Rupal Gupta and Venkat Kalyan Reddy Yasa
4:25-4:40 PM	**PKI – Mitigation of Delegation Based Attacks through Distributed CA Models** by Shefali Suri, Abimbola Abel, and John Mihoc
4:40-4:55 PM	**TLS Vulnerabilities and Mitigation Strategies** by Shiva Prasad Mullapudi and Unmesh Lingayat

Session II
Blockchains and Cryptocurrencies

5:10-5:25 PM	**An Analysis of Cryptocurrency Consensus Mechanisms** by Charles "Chip" Beach
5:25-5:40 PM	**Cryptocurrencies – Proof of Work (PoW) vs Proof of Stake (PoS) vs Proof of Burn (PoB)** by Badri Nath Gaur and Rahul Kalsariya
5:40-5:55 PM	**Hash Algorithm Selection for Mining Sustainability of Cryptocurrencies** by Braxon Tawatao

Session III
FPGA Implementations of Cryptographic Algorithms

6:15-6:30 PM	**Hardware Implementation of the NIST Lightweight Cryptography Candidate Grain-128AEAD** by Omar Zabala-Ferrera
6:30-6:45 PM	**Hardware Implementation of the NIST Lightweight Cryptography Candidate HyENA** by Don Hasitha Thalgaswatte
6:45-7:00 PM	**Hardware Implementation of the NIST Lightweight Cryptography Finalist Romulus-N** by Aadam Dirie and Hawa Dirie
7:00-7:15 PM	**RTL Implementations of the Lightweight Cryptography Candidate KNOT** by Alp Onat

Session IV

Developing and Benchmarking Embedded System Implementations of Cryptography

8:00-8:15 PM	**A Flexible Open-Source Framework for Orchestrating Cryptographic Side-channel Analyses, and Application to Protected and Unprotected Microcontroller Implementations** by Jacob Dilles
8:15-8:30 PM	**Implementing Transparent Kernel Encryption via Removable FPGA** by Peter Casey
8:30-8:45 PM	**An Implementation of Edge-Computing-Based Framework for Internet of Things** by Thomas Crowley

Session V

E-mail Encryption and Emerging Cryptographic Schemes

9:00-9:15 PM	**Art of Email Encryption** by Fatimetou Ahmed
9:15-9:30 PM	**Aggregate Signatures: A Systematization of Schemes and Software Tools, with Applications in Blockchains** by Panagiotis Chatzigiannis and Ioanna Karantaidou
9:30-9:45 PM	**Performing Operations on Encrypted Data Using Homomorphic Encryption** by Shamili Tetali
9:45-10:00 PM	**Challenges of Transition to Post-Quantum Cryptography from the Point of View of Major Secure Internet Protocols (TLS, SSH, and IPSec)** Isaac Gibbons, Yaqi He, and Kyle Guthrie