ECE 646 Project Preferences
as of
09/22/2015

Hardware Projects

1. High-speed Implementation of Authenticated Ciphers Competing in the CAESAR Contest
Abubakr Abdulgadir <aabdulga@gmu.edu>

2. Benchmarking of Candidates in Cryptographic Contests Using High-Level Synthesis

3. Experimental Testing of Cryptographic Modules Using High-Speed FPGA and SoC Boards Based on PCI Express Interface

4. Implementation of a PUF (Physical Unclonable Function)
Daniel May <dmay6@gmu.edu>

5. Implementation of a selected Error Correction Code for PUFs

6. Overview and Comparison of Open Source Hardware Cryptographic Cores
Software Projects

1. Software Extensions to CrypTool - Educational Tool for Learning Cryptography and Cryptanalysis (e.g., internal operation of algorithms, codebreaking schemes, etc.)

2. Educational Software for Teaching Cryptography and Computer-Network Security based on the Windows Presentation Foundation (WPF)

3. Optimizing Best Available Software Implementations of Authenticated Ciphers candidates (using coding techniques, special instructions, assembly language, etc.)

4. Porting Selected C Implementations of Authenticated Ciphers to the TI MSP430 microcontroller or Other Microcontroller Available to You

5. Implementing a selected Cryptographic Algorithm in Cryptol - a new Domain Specific Language

6. Cryptographic App for Android or iOS

Anamika Kesharwani <akesharw@gmu.edu> - G1
Deepika Mallappa <dmallapp@gmu.edu> - G1

7. Software Implementation of a Secure Distributed Storage System

8. Special Microprocessor Instructions Supporting AES and Other Cryptographic Algorithms

9. Overview and Comparison of Open Source Cryptographic Libraries

Ravikumar Kota <rkota@gmu.edu>

10. Comparison of Libraries Used to Implement SSL/TLS

Richard Joy <rjoy@gmu.edu>
Analytical Projects

1. Bitcoin
Ravali Chennamneni <rchennam@gmu.edu> - G2
Rajitha Devabhaktuni <rdevabha@gmu.edu> - G2
Preethi Kondaprithviraj <pkondapr@gmu.edu> - G3
Naga Navya Mingu <nmingu@gmu.edu> - G3

2. Security of Voting Machines

3. Security of Metro/Subway Cards


5. Homomorphic Encryption
Uday Kumar Vatti <uvatti@gmu.edu>

6. Secure Distributed Storage

7. Analyzing the Influence of a Computer Platform on Ranking of the SHA-3 Candidates in Terms of Performance in Software

8. Survey of Codebreaking Machines and Projects Based on FPGAs, GPUs, Cell processors, etc.

9. Encryption Schemes for Copy Protection of Digital Media

10. Security of Transactions Performed Using Credit Card Readers for Smartphones and Tablets
Komrabai Kargbo <kkargbo@gmu.edu>
11. Attacks Against SSL and TLS
Ernest Kushevski <ekushevs@gmu.edu>
Gregory Landosky <glandosk@gmu.edu>
Tejas Sontakke <tsontakk@gmu.edu>

12. Quantum Cryptography
Cong Chen <cchen27@gmu.edu> - G4
Yuqi Wang <ywang39@gmu.edu> - G4
Brian Maher <bmaher2@gmu.edu>

13. Quantum Computing

14. Post-Quantum Cryptography
Qing Chen <qchen7@gmu.edu>
Sathya Kanth Vardhanapu <svardhan@gmu.edu>

15. Identity-Based Encryption

Krishna Nikhila Kalinga <kkalinga@gmu.edu>

17. Challenges of Implementing and Managing Public Key Infrastructure for Large Computer Networks

18. FPGA and All Programmable System on Chip Bitstream Security
Amit Singh <asingh28@gmu.edu>

19. Protections Against Counterfeiting of Integrated Circuits
Your own Topics

1. **Security of EMV Credit Card Chips**
   Matthew Carter <mcarte22@gmu.edu>

2. **Securing the CAN bus protocol for vehicle safety**
   Brienne Douglas <bdougl4@gmu.edu>

3. **Pipelining the SCREAM Cipher**
   Sanjay Deshpande <sdeshpan@gmu.edu>

4. **Message level access control encryption for enterprise messaging systems**
   Michael Risher <mrisher@gmu.edu>

5. **Vivado HLS Implementation of SHA-3 candidates**
   Farnoud Farahmand <ffarahma@gmu.edu>

6. **Implementing AES encryption blocks into GNU Radio using open source crypto library**
   Shawn Wilkinson <swilkin9@gmu.edu>