CO 687: Project description

Due date: December 12, 2023

Grades for students enrolled in CO 687 include a final project. The project must be completed by **December 12, 2023**, submitted via LEARN. The project can take the form of report (and possibly artifact) documenting a scientific contribution in any area of cryptography of the following form:

1. New research results related to cryptography.
2. Replication of existing results, for example:
   (a) Implementation of an existing cryptographic algorithm and confirming its performance characteristics.
   (b) Implementation of an existing cryptanalytic attack demonstrating its success and performance characteristics.
   (c) Integration of an existing cryptographic algorithm into a new computer system or communications protocol.
3. Survey articles giving an overview of a single topic.

Other project formats may also be acceptable provided that I approve them in advance. Two students may not share substantially similar project topics. *All project topics and formats must be approved in advance, and should be cleared with me by **October 31, 2023**, though you are encouraged to do so earlier.*

Projects that take the form of a written report would typically be in the range of 3500–5000 words (5–8 pages) and should include appropriate references to the literature.

Sample topic areas

Symmetric cryptography

- Argon2
- eSTREAM portfolio
- NIST Lightweight Cryptography competition

Public key cryptography

- Elliptic curve pairings
- Identity-based cryptography

Cryptographic protocols

- Private information retrieval
- Electronic voting
- Password-authenticated key exchange

Implementations

- Side-channel attacks
- FPGA implementations
- Cryptography on embedded devices

Applications

- Messaging Layer Security at the IETF
- Privacy-preserving analytics

Advanced cryptography

- Fully homomorphic encryption
- Garbled circuits
- Secure multi-party computation
- SNARKs

Quantum-resistant cryptography

- Quantum key distribution
- Lattice-based cryptography
- Hash-based signatures
- MPC-in-the-head-based signatures
- Learning with errors / rounding
- Multi-variate polynomial cryptography
- Isogeny-based cryptography

... or another topic of your choice.