CO 789 Topics in Cryptography: Cryptographic Protocols

Term: Spring 2022

Instructor: Douglas Stebila

This course investigates state-of-the-art cryptographic protocols, including both those in the academic literature and real-world protocols.

Topics include:

- Analysis methodologies: game-based provable security; the random oracle model; formal methods; universal composability
- Authenticated key exchange and password-authenticated key exchange
- Zero-knowledge proofs
- Multi-party computation
- Privacy protocols
- Anonymous credentials
- Electronic voting
- Real-world protocols (e.g., TLS, Signal, MLS, WPA)
- Attacks on real-world protocols

Suggested reading:

- *Cryptography Made Simple*, by Nigel Smart. Available online at https://link.springer.com/book/10.1007/978-3-319-21936-3
- *Introduction to Modern Cryptography*, 3rd edition, by Jonathan Katz and Yehuda Lindell.

Prerequisites: Familiarity with core cryptographic primitives, both symmetric and asymmetric, such as found in CO 487/687. Students who have taken only a "mathematics of public key cryptography" course such as CO 485/685 should familiarize themselves with symmetric primitives (symmetric encryption, message authentication codes, hash functions). For background reading, focus on abstractions (interfaces of cryptographic primitives, security definitions, and generic constructions) rather than details of specific instantiations. The course will begin with a quick refresher of this background material.