ECE 628 - Computer Network Security
Winter 2025

Instructor: Professor G. Gong
Office: E7 5436, x45650, ggong@uwaterloo.ca
https://uwaterloo.ca/scholar/ggong
Office hours: TBA

Course Description

This course focuses on the fundamental principles of computer network security. The topics to be covered include practical symmetric-key and public-key cryptographic schemes, semantic security, network and wireless security, detection of relay attacks, multicast security, trusted platform, tamper resistant hardware, decentralized system security, blockchain and cryptocurrency, zero-knowledge proofs, blockchain privacy, privacy enhanced technologies, secure machine learning, post-quantum cryptography and quantum key distribution.

Background Requirements Students attending this course should have a good working knowledge of probability theory and computer networks.

Resources Lectures: 11:30AM - 2:20PM, Wednesdays, E5 4106.

References There is no textbook for the course, but the following references will be helpful for your reading.

1. M.T. Goodrich and R. Tamassia, *Introduction to Computer Security*, Addison Wesley, 2011 (GT11) (Section 3.3, Chapters 6, Sections 9.1, 9.6-9.7).

2. L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012 (CG12).

3. W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th edition, Pearson, 2017 (Part Five: Chapters 22-24) (SB17).

4. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd edition, Chapman and Hall/CRC, 2014 or 3rd edition 2020 (you may read it if you wish to have a deep crypto knowledge for your future career, but not required from the course).

5. Supplemental materials for the book by Chen-Gong (SM4CG12).

6. ECE 628 Course Notes -Available on UW-LEARN.

7. Selected papers.

Course Outline

1. Basics of Computer Network Security
    - Confidentiality, integrity and authentication
    - Active and passive attacks
    - Basic security protection mechanisms
    - Trust and threat model
2. Cryptographic Fundamentals
    - Practical implementation and analysis of symmetric-key cryptographic schemes, including shift register based pseudorandom generation, AES, SHA, MAC, correlation attacks and time-memory trade-off attacks.
    - Public-key cryptographic schemes, digital signatures, ECC, FHE, fault attacks and side-channel attacks.
    - Semantic security and CPA/CCA for ensuring robust encryption against adaptive adversaries.
3. Network and Wireless Security
    - Network security protocols (IPsec, TLS/SSL, VPN)
    - Wireless system security (5G radio air link protection, flowed WEP, CCMP)
    - Attacks on TLS
    - Detection relay attacks through physical layer.
4. Multicast Security
    - Multicast key distribution
    - Hash chain authentication
    - Merkle tree authentication and commitment.
5. Trusted Platform and Hardware Security
    - Trusted platform
    - Tamper resistant hardware and countermeasures against side-channel and physical attacks
    - Secure storage
    - Remote attestation and anonymous authentication.
6. Decentralized System Security
    - Security in peer-to-peer and decentralized systems

- Practical Byzantine fault tolerance
- Blockchain and cryptocurrency security
- Consensus mechanisms and smart contract vulnerabilities.

7. Zero knowledge proofs and blockchain privacy
   - Zero-knowledge proofs (ZKPs)
   - Polynomial commitment and sum-check protocols
   - Mechanisms for achieving secure, private transactions in decentralized networks.
8. Privacy Enhanced Technologies
   - Differential privacy
   - Secret sharing and multiparty computation
   - Secure machine learning.
9. Post-quantum and Quantum Cryptography
   - Post-quantum cryptography
   - NIST PQC standardization progress
   - Quantum key distribution.

Course Grading

The overall grade is based on a midterm exam (take-home exam), one project (individual or 2-person group) and one final exam (open book exam, but only lecture slides are allowed to bring). For the project, a list of the project problems will be provided. A 5-8 minutes presentation slides and a report of 5-10 pages in an academic research article format are a must to obtain the score for the project. The distribution of the marks are given below.

Tasks	Due Dates	Marks
Midterm Examination	TBA	30
Project (both slides and report)	March 28	30
Final Examination	TBA	40

Note. For each topic, there are assignment questions for helping you to understand the course materials and to prepare for the exams.

Other Resources

- Matthew Green on cryptography engineering, `https://blog.cryptographyengineering.com/useful-cryptography-resources/`
- Schneier on Security, http://www.schneier.com/blog/. A blog covering current computer security and privacy issues.

Academic Integrity, Discipline, Grievances, and Appeals

Academic Integrity: In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility. [Check `www.uwaterloo.ca/academicintegrity/` for more information.]

Grievance: A student who believes that a decision affecting some aspect of his/her university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and Grievances, Section 4, `www.adm.uwaterloo.ca/infosec/Policies/policy70.htm`. When in doubt please be certain to contact the departments administrative assistant who will provide further assistance.

Discipline: A student is expected to know what constitutes academic integrity [check `www.uwaterloo.ca/academicintegrity/`] to avoid committing an academic offence, and to take responsibility for his/her actions. A student who is unsure whether an action constitutes an offence, or who needs help in learning how to avoid offences (e.g., plagiarism, cheating) or about rules for group work/collaboration should seek guidance from the course instructor, academic advisor, or the undergraduate Associate Dean. For information on categories of offences and types of penalties, students should refer to Policy 71, Student Discipline, `www.adm.uwaterloo.ca/infosec/Policies/policy71.htm`. For typical penalties check Guidelines for the Assessment of Penalties, `www.adm.uwaterloo.ca/infosec/guidelines/penaltyguidelines.htm`.

Appeals: A decision made or penalty imposed under Policy 70 (Student Petitions and Grievances) (other than a petition) or Policy 71 (Student Discipline) may be appealed if there is a ground. A student who believes he/she has a ground for an appeal should refer to Policy 72 (Student Appeals) `www.adm.uwaterloo.ca/infosec/Policies/policy72.htm`.

Note for Students with Disabilities: The Office for Persons with Disabilities (OPD), located in Needles Hall, Room 1132, collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with the OPD at the beginning of each academic term [check `http://www.studentservices.uwaterloo.ca/disabilities/`].

Turnitin.com: Text matching software (Turnitin) may be used to screen assignments in this course. Turnitin is used to verify that all materials and sources in assignments are documented. Students' submissions are stored on a U.S. server, therefore students must be given an alternative (e.g., scaffolded assignment or annotated bibliography), if they are concerned about their privacy and/or security. Students will be given due notice, in the first week of the term and/or at the time assignment details are provided, about arrangements and alternatives for the use of Turnitin in this course.