COMP-649

Quantum Cryptography

Instructor: Prof. Claude Crépeau

Office : Room 110N, McConnell Eng. Building
3480 University Street
phone: (514) 398-4716
email: crepeau@cs.mcgill.ca

Grader: maybe, maybe-not

Office : Room 235, McConnell Eng. Building
3480 University Street
phone: (514) 398-7071 x0699
email: simonpie@cs.mcgill.ca

Office Hours:
Claude : Wednesday 14-17h, McConnell 110N.

Description: (4 credits, 3 hours). Review of the basic notions of cryptography and quantum information theory. Quantum key distribution and its proof of security. Quantum encryption, error-correcting codes and authentication. Quantum bit commitment, zero-knowledge and oblivious transfer. Multiparty quantum computations.

Evaluation: There will be 4~5 homework assignments worth 25~20% of your final grade each.

Honnêteté académique: L'université McGill attache une haute importance à l'honnêteté académique. Il incombe par conséquent à tous les étudiants de comprendre ce que l'on entend par tricherie, plagiat et autres infractions académiques, ainsi que les conséquences que peuvent avoir de telles actions, selon le Code de conduite de l'étudiant et des procédures disciplinaires (pour de plus amples renseignements, veuillez consulter le site www.mcgill.ca/integrity).

Academic integrity: McGill University values academic integrity. Therefore all students must understand the meaning and consequences of cheating, plagiarism and other academic offences under the Code of Student Conduct and Disciplinary Procedures (see www.mcgill.ca/integrity for more information).

Topics

01. Short - number theory / finite field - background : class notes COMP-547
02. Classical error correcting codes : Madhu Sudan
03. Quantum error correcting codes : Gottesman
04. Classical information theory : BBCM
    - Shannon, Renyi and Min-entropies
    - Generalized Privacy Amplification - leftover hash Lemma
05. BB84 QKD
05. Shor-Preskill proof
05. Amount of tolerable errors (a survey)
06. Quantum teleportation, Quantum Vernam Cipher, density matrix / operators
06. Quantum public-key crypto
07. QVC 2 bits/qubit lower bound - MTW00
07. QVC ~1 bit/qubit upper bound - HLSW03
08. Quantum authentication - BCGST
09. Uncloneable encryption - Gottesman
10. Known plaintext attack & Key recycling - DPS04
11. Classical and Quantum Zero-knowledge – Watrous
12. Approximate QECC – Crépeau-Gottesman-Smith.