abstract

COMPUTER SCIENCE AND DISCRETE MATHEMATICS SEMINAR I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In a joint work with Tsuyoshi Ito we have constructed a fingerprinting scheme (i.e., hashing) that leaks significantly less than log(1/epsilon) bits about the preimage, where epsilon is the error ("collision") probability. It is easy to see that classically this is not achievable; our construction is quantum, and it gives a new example of (unconditional) qualitative advantage of quantum computers.

Technically speaking, for any constant c we give a quantum fingerprinting scheme that maps an n-bit string x to O(log n) qubits, guarantees error at most 1/n^c and leaks at most 1/n^c bits of information about x (any classical scheme with such error would leak Omega(log n) bits). We also demonstrate that our scheme is optimal. I will present these results, trying to keep the quantum parts as modular as possible, such that people less familiar with (or less interested in) Quantum Computing would not regret coming.