University of Lethbridge
Department of
MATHEMATICS & COMPUTER SCIENCE

Speaker: **Hua Li**

Title: **A CAM Based Associative Processor Array for Parallel Implementation of AES**

Room: **A 580**

Date: **Friday, March 26, 2004**

Time: **10:00 - 11:00**

Abstract:

In this talk, a parallel implementation of Advanced Encryption Standard (AES) based on Content Addressable Memory (CAM) is proposed. The architecture and algorithm of CAM based %using CAM based associative processor array %to achieve fast and parallel AES is presented. is proposed to fast implement AES. It can process n (n>= 256) message blocks simultaneously. Moreover, the characteristics of CAM are applied to perform AddRoundKey transformation without additional XOR gates. The throughput of the proposed implementation can achieve 1.210Gbits/s.