Computer Algebra Research Group
of Wilfrid Laurier University

and

LAURIER SEMINAR SERIES IN Computational Science and Applied & Statistical Modelling (CSASM)

Website: www.mmcs.wlu.ca/csasm/

CSASM Seminar Series Co-ordinators:
Ilias Kotsireas and Roderick Melnik | Email: csasm@wlu.ca

present

Douglas R. Stinson

In this talk, we discuss the use of combinatorial set systems (combinatorial designs) in the design of key predistribution schemes (KPS) for sensor networks. We show that the performance of a KPS can be improved by carefully choosing a certain class of set systems as "key ring spaces." Especially, we analyze KPS based on a type of combinatorial design known as a transversal design. We employ two types of transversal designs, which are represented by the set of all linear polynomials and the set of quadratic polynomials (over some finite field), respectively. These KPS turn out to have significant efficiency in a shared-key discovery phase without degrading connectivity and resiliency.

PROFESSOR DOUGLAS R. STINSON

David R. Cheriton School of Computer Science, University of Waterloo

A Combinatorial Approach TO Key Predistribution FOR Distributed Sensor Networks

Thursday, April 26, 2007

2:30 P.M. | Room BA 210

(LOCATED IN THE BRICKER ACADEMIC BUILDING)

Wilfrid Laurier University, 75 University Avenue West, Waterloo

This event is hosted by the CARGO lab - www.cargo.wlu.ca
and the CSASM seminar series - http://www.mmcs.wlu.ca/csasm/

Seminar Series Sponsors:

STEP
SCIENCE AND TECHNOLOGY ENDOWMENT PROGRAM

SHARCNET™

LAURIER
Faculty of Science

CSASM.Plt.John.McKay 06.03.07