FIELDS INSTITUTE Research in Mathematical Sciences

FIELDS

www.fields.utoronto.ca

SAC 2010

SELECTED AREAS IN CRYPTOGRAPHY WORKSHOP

August 12–13, 2010 at University of Waterloo

The objective of the workshop is to present cutting edge research in the designated areas of cryptography and to facilitate future research through an informal and friendly workshop setting.

SAC 2010 is held in co-operation with the International Association for Cryptologic Research (IACR), the leading professional organization for cryptographic research.

Four areas will be covered at SAC 2010:

- design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions and MAC algorithms
- efficient implementations of symmetric and public key algorithms
- mathematical and algorithmic aspects of applied cryptology
- applications of coding theory and combinatorics in cryptography

The SAC proceedings are published in the *Lecture Notes in Computer Science* series published by Springer.

ORGANIZING COMMITTEE

Alex Biryukov (Luxembourg) **Guang Gong** (Waterloo) **Douglas Stinson** (Waterloo)

INVITED SPEAKERS

Alexandra Boldyreva (Georgia Tech) **Keith Martin** (Royal Holloway)

FIELDS

UNIVERSITY OF Waterloo

For more information, visit sac2010.uwaterloo.ca

FIELDS INSTITUTE
Research in Mathematical Sciences
222 COLLEGE STREET • TORONTO • ONTARIO • M5T 3J1 • CANADA

Phone: (416) 348-9710
Fax: (416) 348-9759
www.fields.utoronto.ca