SELECTED AREAS IN CRYPTOGRAPHY 2013

sac2013.irmacs.sfu.ca

AUGUST 14–16

SIMON FRASER UNIVERSITY
BURNABY, BC, CANADA

CONFERENCE TOPICS

- 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
- Elliptic and hyperelliptic curve cryptography, including theory and applications of pairings

Early registration deadline: July 26, 2013

INVITED SPEAKERS

Paulo S. L. M. Barreto, University of São Paulo, Brazil

Anne Canteaut, INRIA Paris-Rocquencourt, France

Antoine Joux, CryptoExperts and Université de Versailles Saint-Quentin-en-Yvelines, France

Douglas R. Stinson, University of Waterloo, Canada

CONFERENCE CO-CHAIRS

Tanja Lange, Technische Universiteit Eindhoven, The Netherlands

Kristin Lauter, Microsoft Research, USA

Petr Lisonek, Simon Fraser University, Canada

Microsoft Research · Institut Tutte Institute · SFU · pims · The irmacs Centre · Springer · Lecture Notes in Computer Science LNCS LNAI LNBI