SAC 2013 Program

All talks take place in the IRMACS Presentation Studio, room 10900 in the Applied Sciences Building at Simon Fraser University, Burnaby, BC, Canada. Registration, reception and coffee breaks take place in the IRMACS Centre in the proximity of the lecture room.

Breakfasts take place in the Dining Hall. Lunches take place in MacKenzie Café. Conference dinner takes place at the Diamond Alumni Centre on campus.

For maps please visit the SAC 2013 website, and click the link Participation > Conference Venues.

Wednesday August 14, 2013

13:00–18:30	*Registration*
13:50–14:00	*Conference opening* Dr. Norbert Haunerland, Associate Vice-President, Research, Simon Fraser University
14:00–15:30	**Invited lecture:** Paulo S. M. L. Barreto, University of São Paulo, Brazil *The Realm of the Pairings* (Session Chair: Tanja Lange)
15:30–16:00	*Coffee break*
16:00–17:00	**Lattices (part I)** (Session Chair: Michael Naehrig)
16:00–16:20	Feng Zhang, Yanbin Pan and Gengran Hu, *A Three-Level Sieve Algorithm for the Shortest Vector Problem*
16:20–16:40	Rachid El Bansarkhani and Johannes Buchmann, *Improvement and Efficient Implementation of a Lattice-based Signature Scheme*
16:40–17:00	Thomas Pöppelmann and Tim Güneysu, *Towards Practical Lattice-Based Public-Key Encryption on Reconfigurable Hardware*
17:00–18:30	**Invited lecture:** Douglas R. Stinson, University of Waterloo, Canada *Key Distribution in Wireless Sensor Networks* (Session Chair: Carlisle Adams)
18:30	*Reception (IRMACS Centre)*

Thursday August 15, 2013

07:00–	*Breakfast (Dining Hall)*
08:30–09:00	*Registration*
09:00–10:00	**Invited lecture:** Antoine Joux, CryptoExperts and Université de Versailles Saint-Quentin-en-Yvelines, France *Revisiting Discrete Logarithms in Small/Medium Characteristic Finite Fields* (Session Chair: Kristin Lauter)

10:00–10:40 **Discrete logarithms** (Session Chair: Craig Costello)
10:00–10:20 Jung Hee Cheon, Taechan Kim and Yong Soo Song, *A Group Action on $\mathbf{Z}_p^\times$ and the Generalized DLP with Auxiliary Inputs*
10:20–10:40 Faruk Göloğlu, Robert Granger, Gary McGuire and Jens Zumbrägel, *Solving a* 6120*-bit DLP on a Desktop Computer*

10:40–11:10 *Coffee break*

11:10–12:10 **Stream ciphers and authenticated encryption** (Session Chair: Guang Gong)
11:10–11:30 Toshihiro Ohigashi, Takanori Isobe, Yuhei Watanabe and Masakatu Morii, *How to Recover Any Byte of Plaintext on RC4*
11:30–11:50 Dmitry Khovratovich and Christian Rechberger, *The LOCAL attack: Cryptanalysis of the authenticated encryption scheme ALE*
11:50–12:10 Hongjun Wu and Bart Preneel, *AEGIS: A Fast Authenticated Encryption Algorithm*

12:10–13:50 *Lunch (MacKenzie Café)*

13:50–14:30 **Post-quantum cryptography (hash-based and system solving)** (Session Chair: Christiane Peters)
13:50–14:10 Charles Bouillaguet, Chen-Mou Cheng, Tung Chou, Ruben Niederhagen and Bo-Yin Yang, *Fast Exhaustive Search for Quadratic Systems in $\mathbf{F}_2$ on FPGAs*
14:10–14:30 Thomas Eisenbarth, Ingo von Maurich and Xin Ye, *Faster Hash-based Signatures with Bounded Leakage*

14:30–15:10 **White-box cryptography** (Session Chair: Bart Preneel)
14:30–14:50 Cécile Delerablée, Tancrède Lepoint, Pascal Paillier and Matthieu Rivain, *White-Box Security Notions for Symmetric Encryption Schemes*
14:50–15:10 Tancrède Lepoint, Matthieu Rivain, Yoni De Mulder, Peter Roelse and Bart Preneel, *Two Attacks on a White-Box AES Implementation*

15:10–15:50 *Coffee break*

15:50–16:50 **Block ciphers** (Session Chair: Yu Sasaki)
15:50–16:10 Thierry P. Berger, Marine Minier and Gaël Thomas, *Extended Generalized Feistel Networks using Matrix Representation*
16:10–16:30 Ryad Benadjila, Jian Guo, Victor Lomné and Thomas Peyrin, *Implementing Lightweight Block Ciphers on* x86 *Architectures*
16:30–16:50 Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen and Baudoin Collard, *Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA*

16:50–17:50 **Invited lecture:** Hugh C. Williams, Director, The Tutte Institute for Mathematics and Computing, Ottawa, Canada
The Tutte Institute for Mathematics and Computing
(Session Chair: Michael Jacobson, Jr.)

19:00 *Conference dinner (Diamond Alumni Centre)*

Friday August 16, 2013

07:00–	*Breakfast (Dining Hall)*
08:30–09:00	*Registration*
09:00–10:00	**Stafford Tavares Lecture:** Anne Canteaut, INRIA Paris-Rocquencourt, France *Similarities between Encryption and Decryption: How far can we go?* (Session Chair: Petr Lisonek)
10:00–10:40	**Lattices (part II)** (Session Chair: Joppe Bos)
10:00–10:20	Sujoy Sinha Roy, Frederik Vercauteren and Ingrid Verbauwhede, *High Precision Discrete Gaussian Sampling on FPGAs*
10:20–10:40	Johannes Buchmann, Daniel Cabarcas, Florian Göpfert, Andreas Hülsing and Patrick Weiden, *Discrete Ziggurat: A Time-Memory Trade-off for Sampling from a Gaussian Distribution over the Integers*
10:40–11:10	*Coffee break*
11:10–12:30	**Elliptic curves, Pairings and RSA** (Session Chair: Damien Robert)
11:10–11:30	Yuan Ma, Zongbin Liu, Wuqiong Pan and Jiwu Jing, *A high-speed elliptic curve cryptographic processor for generic curves over GF*(p)
11:30–11:50	Joppe W. Bos, Craig Costello and Michael Naehrig, *Exponentiating in Pairing Groups*
11:50–12:10	Christophe Doche, Daniel Sutantyo, *Faster Repeated Doublings on Binary Elliptic Curves*
12:10–12:30	Joppe W. Bos, Peter L. Montgomery, Daniel Shumow and Greg Zaverucha, *Montgomery Multiplication Using Vector Instructions*
12:30–14:00	*Lunch (MacKenzie Café)*
14:00–15:00	**Hash functions and MACs** (Session Chair: Jooyoung Lee)
14:00–14:20	Yu Sasaki and Lei Wang, *Improved Single-Key Distinguisher on HMAC-MD5 and Key Recovery Attacks on Sandwich-MAC-MD5*
14:20–14:40	Charles Bouillaguet and Bastien Vayssière, *Provable Second Preimage Resistance Revisited*
14:40–15:00	Jérémy Jean, María Naya-Plasencia and Thomas Peyrin, *Multiple Limited-Birthday Distinguishers and Applications*
15:00–15:40	**Side-channel attacks** (Session Chair: Daniel J. Bernstein)
15:00–15:20	Aurélie Bauer, Eliane Jaulmes, Emmanuel Prouff and Justine Wild, *Horizontal Collision Correlation Attack on Elliptic Curves*
15:20–15:40	David Oswald, Daehyun Strobel, Falk Schellenberg, Timo Kasper and Christof Paar, *When Reverse-Engineering Meets Side-Channel Analysis–Digital Lockpicking in Practice*
15:40–16:10	*Coffee break*