Preface

For the last 22 years, the Conference on Selected Areas in Cryptography (SAC) has been the leading Canadian venue for the presentation and publication of cryptographic research. The conference, which this year was held at Mount Allison University in Sackville, New Brunswick (for the second time; the first was in 2008), offers a relaxed and supportive atmosphere for researchers to present and discuss new results.

SAC has three regular themes:

– Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash functions, MAC algorithms, and authenticated encryption schemes
– Efficient implementations of symmetric and public key algorithms
– Mathematical and algorithmic aspects of applied cryptology

The following special (or focus) theme was added this year:

– Privacy- and anonymity-enhancing technologies and their analysis

A total of 91 submissions were received, out of which the Program Committee selected 29 papers for presentation (three of which were accepted as short papers). It is our pleasure to thank the authors of all the submissions for the high quality of their work. The review process was thorough (each submission received the attention of at least three reviewers, and at least five for submissions involving a Program Committee member).

There were two invited talks. The Stafford Tavares Lecture was given by Paul Syverson, who spoke about "Trust Aware Traffic Security," and the second invited talk was given by Gaëtan Leurent, who spoke on "Generic Attacks Against MAC Algorithms."

Finally, this year we expanded SAC in a new direction by introducing what we hope will become an annual tradition — the SAC Summer School (S3). S3 is intended to be a place where young researchers can increase their knowledge of cryptography through instruction by and interaction with leading researchers. This year, we were fortunate to have Kaisa Nyberg and Christian Rechberger presenting symmetric-key cryptanalysis, and Jan Camenisch and Paul Syverson presenting various aspects of privacy-enhancing technologies. We would like to express our sincere gratitude to these four presenters for dedicating their time and effort to this inaugural event.

Finally, the members of the Program Committee, especially the co-chairs, are extremely grateful to Thomas Baignères and Matthieu Finiasz for the iChair software, which facilitated a smooth and easy submission and review process.

August 2015
Orr Dunkelman
Liam Keliher