

Preface

The Conference on Selected Areas in Cryptography (SAC) is the leading Canadian venue for the presentation and publication of cryptographic research. The 24th annual SAC was held this year at the University of Ottawa, Ontario (for the second time; the first was in 2007). In keeping with its tradition, SAC 2017 offered a relaxed and collegial 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 for this year was:

- Post-quantum cryptography

A total of 66 submissions were received, out of which the Program Committee selected 23 papers for presentation. 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 Helena Handschuh, who presented “Test Vector Leakage Assessment Methodology: An Update,” and the second invited talk was given by Chris Peikert, who presented “Lattice Cryptography: From Theory to Practice, and Back Again.”

This year, SAC hosted what is now the third iteration of 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 Michele Mosca, Douglas Stebila, and David Jao presenting post-quantum cryptographic algorithms, Tanja Lange and Daniel J. Bernstein presenting public key cryptographic algorithms, and Orr Dunkelman presenting symmetric key cryptographic algorithms. We would like to express our sincere gratitude to these six presenters for dedicating their time and effort to what has become a highly anticipated and highly beneficial event for all participants.

Finally, the members of the Program Committee, especially the co-chairs, would like to thank the additional reviewers, who gave generously of their time to assist with the paper review process. We are also very grateful to our sponsors, Microsoft and Communications Security Establishment, whose enthusiastic support (both financial and otherwise) greatly contributed to the success of SAC this year.

Selected Areas in Cryptography – SAC 2017
24th International Conference, Ottawa, ON, Canada,
August 16–18, 2017, Revised Selected Papers
Adams, C.; Camenisch, J. (Eds.)
2018, XI, 459 p. 70 illus., Softcover
ISBN: 978-3-319-72564-2