# Preface

Previously called the Workshop on Selected Areas in Cryptography, the Conference on Selected Areas in Cryptography (SAC) series was initiated in 1994, when the first workshop was held at Queen's University in Kingston. The SAC conference has been held annually since 1994 in various Canadian locations, including Calgary, Kingston, Montreal, Ottawa, Sackville, St. John's, Toronto, Waterloo, and Windsor. More information on SAC conferences can be found at the main SAC conferences website at http://sacconference.org/.

SAC 2013 was the 20th conference in this series, and for this special occasion it was extended to a two-and-half day conference, which was attended by 65 participants.

This volume contains revised versions of papers presented at SAC 2013, held during August 14–16, 2013, at Simon Fraser University in Burnaby, Canada. The objective of the conference is to present cutting-edge research in the designated areas of cryptography and to facilitate future research through an informal and friendly conference setting.

The themes for the SAC 2013 conference were:

– 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

There were 105 paper submissions, of which seven were withdrawn prior to the submission deadline, and 98 submissions were refereed. Each submission was reviewed by at least three Program Committee members. Submissions (co-)authored by a Program Committee member were reviewed by at least five Program Committee members. Upon recommendations of the Program Committee, 26 papers were accepted making the acceptance rate $26/98 = 26.5$ %. The program also included four invited lectures, which were given by Paulo Barreto, Anne Canteaut, Antoine Joux, and Douglas Stinson. The speakers were invited to submit papers to the proceedings; these invited papers underwent a thorough reviewing process.

We greatly appreciate the hard work of the SAC 2013 Program Committee. We are also very grateful to the many others who participated in the review process. The reviewing process was run using the iChair software, written by Thomas Baignères from CryptoExperts, France, and Matthieu Finiasz from EPFL, LASEC, Switzerland. We are grateful to them for letting us use their software.

SAC 2013 was generously supported by its sponsors and partners: Microsoft Research, Tutte Institute for Mathematics and Computing, Simon Fraser University, Pacific Institute for the Mathematical Sciences, and Interdisciplinary Research in the

Mathematical and Computational Sciences Centre (IRMACS) at Simon Fraser University. The conference was held in co-operation with the International Association for Cryptologic Research (IACR). Hugh Williams from the Tutte Institute delivered the invited lecture "The Tutte Institute for Mathematics and Computing."

Special thanks go to Carlisle Adams, Huapeng Wu, and Ali Miri for generously sharing their experience in organizing SAC conferences with us. We would also like to thank Springer for publishing the SAC proceedings series since 1998 in the *Lecture Notes in Computer Science* series.

We would like to thank Pam Borghardt, Zena Bruneau, and Kelly Gardiner for their hard and tireless work in taking care of the local arrangements.

November 2013

Tanja Lange
Kristin Lauter
Petr Lisoněk