Preface

This volume contains revised versions of the papers presented at the 21st conference on Selected Areas in Cryptography (SAC 2014), held during August 14–15, 2014 at Concordia University in Montreal, Canada. The conference Selected Areas in Cryptography (SAC) series was initiated in 1994, when SAC 1994 was held at Queen's University in Kingston, Ontario, Canada. At that time, it was called the Workshop on Selected Areas in Cryptography. Since then, SAC has been held annually in various Canadian cities, including Calgary, Kingston, Montreal, Ottawa, Sackville, St. John's, Toronto, Waterloo, and Windsor. SAC is currently the only cryptography conference series that is held annually in Canada. Information on previous SAC conferences can be found at the main SAC conferences website: http://sacconference.org/.

There are four areas covered at each SAC conference. The three permanent areas are:

- Design and analysis of symmetric key primitives and cryptosystems, including block and stream ciphers, hash function, MAC algorithms, cryptographic permutations, and authenticated encryption schemes.
- Efficient implementations of symmetric and public key algorithms.
- Mathematical and algorithmic aspects of applied cryptology.

This year, the fourth area for SAC 2014 is: Algorithms for cryptography, cryptanalysis, and their complexity analysis.

We greatly appreciate the hard work of the SAC 2014 Program Committee. We are also very grateful to the many others who participated in the review process. This year, we received a total of 103 submissions (co-authored by 260 authors from 30 countries), 22 of them were accepted for presentations at the conference. The 36 Technical Program Committee members were from 13 countries and involved 92 external reviewers. On average, each submitted paper was reviewed by about 3.8 TPC members.

The program also included three invited talks: Nigel Smart, from the University of Bristol, UK, presented a talk entitled "Practical Multi-party Computation." Pierrick Gaudry, from Université de Lorraine, France, presented a talk entitled "NFS: Similarities and Differences Between Integer Factorization and Discrete Logarithm." The Stafford Tavares Lecture was dedicated to the memories of Scott Vanstone and was given by Alfred Menezes from the University of Waterloo. The talk was entitled "Scott Vanstone and the Early Years of Elliptic Curve Cryptography."

SAC 2014 was generously supported by Microsoft Research. We would also like to thank Springer for publishing the SAC proceedings series since 1998 in the Lecture Notes in Computer Science series. Last, but not least, we are very grateful to the staff members at the Concordia Institute for Information Systems Engineering (CIISE) for their tireless work in taking care of the local arrangements.

August 2014

Antoine Joux
Amr Youssef

http://www.springer.com/978-3-319-13050-7

Selected Areas in Cryptography -- SAC 2014
21st International Conference, Montreal, QC, Canada,
August 14-15, 2014, Revised Selected Papers
Joux, A.; Youssef, A. (Eds.)
2014, X, 381 p. 66 illus., Softcover
ISBN: 978-3-319-13050-7