Submittee: Michael Jacobson, Jr.
Date Submitted: 2009-09-23 11:51
Title: Selected Areas in Cryptography (SAC 2009)
Event Type: Conference-Workshop

Location:
University of Calgary

Dates:
August 13-14, 2009

Topic:
--- 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. --- Privacy enhancing cryptographic systems.

Methodology:
2 invited talks, 28 contributed talks

Objectives Achieved:
We had 86 paper submissions, one of which was withdrawn. The average quality was very high, making the task of selecting a program very challenging. We accepted 28 papers, yielding an acceptance rate of 33% which is on par with previous SACs. We had 10 papers on hash functions, of course because of the NIST competition to replace the current hash function standard. The remaining papers were about block and stream ciphers, public key schemes, implementation, and privacy-enhancing cryptographic systems. --- We had participants from all over the world, the largest group being from Canada. Most of the participants were from the academic sector (many of these were students), but a large portion also came from the industry and government sectors. --- In summary, SAC 2009 has achieved its objective of providing a broad, international forum for the dissemination of high-quality cryptographic research.

Scientific Highlights:
The invited talks were both highlights of our program. Dr. Jan Camenish gave a survey of the state-of-the-art in cryptographic techniques for enhancing privacy, and Dr. Andreas Enge gave a survey of current methods for constructing cryptographically-suitable elliptic curves using complex multiplication. --- Of the contributed sessions, those devoted to hash functions were especially timely and interesting, as the papers presented shed new light on the suitability of several candidates in NIST's on-going competition for the next hash function standard.

Organizers:
Jacobson, Jr., Michael, Computer Science, University of Calgary --- Rijmen, Vincent, K.U.Leuven, Belgium and TU Graz, Austria --- Safavi-Naini, Rei, Computer Science, University of Calgary

---

Speakers:
Please see attached web archive for a list.

Links:
www.sac.ucalgary.ca
