Submittee: Mark Bauer
Date Submitted: 2009-10-02 11:44
Title: Workshop on Elliptic Curve Cryptography
Event Type: Conference-Workshop

Location:
University of Calgary, Calgary, AB

Dates:
Aug. 19-22, 2009 (Summer School). -- Aug. 24-26, 2009 (Conference).

Topic:
Elliptic Curve Cryptography and related areas.

Methodology:
Summer School - 14 one hour lectures presented over 4 days followed by daily problem sessions, delivered by prominent researchers in the field. Public lecture held the day before the conference, 60 people in attendance. -- Conference - 15 invited lectures and a rump session spread out through 5 sessions.

Objectives Achieved:
The combination of the summer school, public lecture and conference was a resounding success. By holding these events together, we were able to attract members from academia, industry and government, with vastly different backgrounds and levels of development. The environment was exceptionally conducive to learning, dissemination of new ideas and the building of fresh collaborations. -- In the week leading up to the conference, we hosted a summer school. The goal was to bring in two or three top researchers (who are also known for their teaching), and younger faculty members and post-doctoral fellows to give a week long series of lectures geared towards enabling newer graduate students to the field to take as much away from the conference as possible. Our lecturers were Scott Vanstone, co-founder of Certicom and largely responsible for the commercial success of elliptic curve cryptography, Professor Larry Washington, who is the author of arguably the best graduate textbook on elliptic curve cryptography. Local participants included Professor Matthew Greenberg, Professor Mark Bauer, two graduate students, Sarah Chisholm and Matthew Musson. This year, the summer school had almost 40 participants, most of which were graduate students. The students came from 4 continents and many different countries. -- On Sunday, August 23, 2009, we arranged a public lecture to be given by Professor Scott Vanstone. As one of the visionaries in the field and initial proponents of the need to switch to elliptic curve cryptography over traditional public key cryptosystems, he has incredible insight into the development of this field. Professor Vanstone gave an incredibly insightful public lecture aimed at the general public and was able to emphasize the importance that public key cryptography plays in our everyday lives. Since Professor Williams ICANTC chair sponsor an ongoing public lecture series, we were able to tap into the resources we have built up to advertise this talk and make it a resounding success. For a Sunday afternoon, we still had about 60 attendees, which included members for local industry and other individuals who did not attend the conference. -- The

culmination of these events was the conference itself. Since their inception in 1997, the Workshops on Elliptic Curve Cryptography has been the premier international forum for the dissemination of new research in elliptic curve cryptography. We believe the meeting continued to encourage and stimulate further research on the security and implementation of elliptic curve cryptosystems and related areas, while encouraging collaboration between mathematicians, computer scientists and engineers in the academic, industry and government sectors. We succeeded in attracting speakers from 4 continents, ranging from graduate students to senior academic researchers to industrial leaders.

Organizers:
Bauer, Mark, Dept. of Math. & Statistics, University of Calgary. Scheidler, Renate, Dept. of Math. & Statistics, University of Calgary. Jacobson, Michael J, Dept. of Computer Science, University of Calgary. Teske, Edlyn, Dept. Of Combinatorics & Optimization, University of Waterloo. Lange, Tanja, Dept. of Math. & Computer Science, Eindhoven University.

Speakers:
See Attachment (speakers.pdf)

Links:
http://ecc.math.ucalgary.ca/; http://ecc.math.ucalgary.ca/organization/programme; http://ecc.math.ucalgary.ca/organization/public_lecture

---

Comments / Miscellaneous:
We are immeasurably grateful for the funding from the various agencies that we were able to obtain. Without them, we would not have been able to fund nearly as many students for the Summer School, nor would we have been able to have recruit such high quality speakers. We hope these agencies are able to continue their support of these kind of mathematical events in the future.

File Uploads:
Additional Upload 1: http://www.pims.math.ca/files/final_report/speakers.pdf

---