**Submittee:** Michael Jacobson, Jr.
**Date Submitted:** 2014-04-30 11:05
**Title:** Workshop on Curves and Applications
**Event Type:** Conference-Workshop

---

**Location:**
University of Calgary

---

**Dates:**
August 21-23, 2013

---

**Topic:**
The main goal of this project-driven workshop on algebraic curves was to bring together regional and national experts to further current research in the following areas:   - Mathematical aspects of algebraic curves, with emphasis on constructing curves with specific properties;   - Arithmetic infrastructure, with the additional goal of implementation in the computer algebra system SAGE;   - Applications, including cryptography.  The choice of these topics and the hands-on emphasis of the workshop was designed to lead to tangible results for all participants.

---

**Methodology:**
The workshop consisted of six invited lectures (held in the mornings) and four student projects (in the afternoons) on topics related to the lectures. Topics covered theoretical, algorithmic, and applied aspects of curves and applications, giving the participants a broad perspective of on-going research in the area.

---

**Objectives Achieved:**
We had a total of 22 participants, including 6 external invited speakers, 10 external junior participants (all but one of whom were graduate students and junior faculty), and 6 local participants (faculty, postdocs, and graduate students). Except for two participants from partner institutions in France, all participants were from regional (Colorado, Alberta, British Columbia) or national (Toronto, Waterloo) universities. One speaker (Costello) came from Microsoft Research in Redmond, Washington. In summary, the workshop achieved its objectives of initiating collaboration amongst regional and national experts. and seeding a more large-scale funding initiative. We are in the process of applying for a collaborative research grant to help fund further collaborative events on these topics. Our letter of intent was accepted in late 2013, and our full application is due in October 2014.

---

**Scientific Highlights:**
The invited talks were a definite highlight of the workshop.  All of these were of very high quality and well-received by the attendees.  Topics covered theoretical, algorithmic, and applied aspects of curves and applications, giving the participants a broad perspective of on-going research in the area.  The four student workshops were also well-received, providing opportunities to gain hands-on

experience on topics related to the lectures. We are not aware of any papers resulting directly from these projects, but many students obtained valuable training that has aided them in their own research.

**Organizers:**
Bauer, Mark, Mathematics and Statistics, University of Calgary Jacobson, Michael, Computer Science, University of Calgary Scheidler, Renate, Mathematics and Statistics, University of Calgary

**Speakers:**
The six invited speakers were: - Jeff Achter (Colorado State University), Counting Abelian Surfaces; - Nils Bruin (Simon Fraser University), Computing with divisor classes on curves using global sections; - Craig Costello (Microsoft Research), The State-of-the-art in Hyperelliptic Curve Cryptography, - David Jao (University of Waterloo), Isogeny-Based Cryptography on Mobile Platforms; - Kumar Murty (University of Toronto), Splitting of Abelian Varieties; - Ben Smith (INRIA), Explicit isogenies and endomorphisms of low-genus Jacobians: Theory and applications. /// The four student projects were: - Split Picard curves, (Jeff Acter, Colorado State University); - Divisor class arithmetic on curves in Sage, (Nils Bruin, Simon Fraser University); - Arithmetic on high-genus curves, (Craig Costello, Microsoft Research); - Cryptographic pairings with RELIC, (David Jao, University of Waterloo). /// See the attached documents for complete descriptions.

**Links:**
https://www.pims.math.ca/scientific-event/130819-wca

**File Uploads:**
Additional Upload 1:
http://www.pims.math.ca/files/final_report/Workshop_on_Curves_and_Applications__Talks_and_Abstracts.pdf
Additional Upload 2: http://www.pims.math.ca/files/final_report/PIMS-projects.pdf