Workshop on Curves and Applications — Student Projects

1. **Split Picard curves**, (Jeff Acter, Colorado State University)

   A Picard curve is cyclic triple cover of the projective line. Equivalently, it is a smooth projective curve admitting an affine model of the form $y^3 = f(x)$, where f is a square-free polynomial of degree four.

   In this project, we will initiate the characterization and counting of those Picard curves which cover an elliptic curve.

2. **Divisor class arithmetic on curves in Sage**, (Nils Bruin, Simon Fraser University)

   The main purpose of this project is to implement divisor class arithmetic on general smooth projective curves in Sage. The proposed strategy for accomplishing this is by using divisors that are determined by their global sections (i.e., divisors of sufficiently high degree).

   A promising approach for this is outlined by Kamal Khuri-Makdisi. He reduces all required computations to linear algebra over the base field, provided an integrally closed order in the the function field is given.

   Two relevant articles are:

   - Khuri-Makdisi, Kamal. Linear algebra algorithms for divisors on an algebraic curve. Math. Comp. 73 (2004), no. 245 (see also `http://arxiv.org/abs/math/0105182`)
   - Khuri-Makdisi, Kamal. Asymptotically fast group operations on Jacobians of general curves. Math. Comp. 76 (2007), no. 260, 2213-2239 (see also `http://arxiv.org/abs/math/0409209`)

3. **Arithmetic on high-genus curves**, (Craig Costello, Microsoft Research)

   This will largely be on some follow-up ideas relating to `http://eprint.iacr.org/2011/306.pdf` for arbitrary genus curves (both hyperelliptic and otherwise), which might pursue some of the discussion relating to the first few sections in Gaudry's chapter (VII) in `http://dl.acm.org/citation.cfm?id=1051769`. I am doing some cryptanalytic work over the Summer so we could even look at destructive aspects of high genus curves.

4. **Cryptographic pairings with RELIC**, (David Jao, University of Waterloo)

   This project provides a hands-on tutorial for building, installing, and using Diego Aranha's RELIC cryptographic library to implement pairing-based cryptosystems. Topics covered include the RELIC application programming interface and building for mobile devices.

   In addition to desktop computers provided, devices such as tablets and phones will be made available. Students may also use their own laptops.

   Useful links:

   - relic-toolkit - RELIC is an Efficient LIbrary for Cryptography (http://code.google.com/p/relic-toolkit/)
   - Android SDK (http://developer.android.com/sdk/)
   - Apple Xcode (https://developer.apple.com/xcode/)
   - MinGW - Minimalist GNU for Windows (http://www.mingw.org/)