1116-11-682 **Craig Costello**, **Alyson Deines*** (aly.deines@gmail.com), **Kristin Lauter** and **Tonghai Yang**. *Constructing Abelian Surfaces via Rosenhain Invariants.*

Algorithms to construct CM genus 2 curves have previously used the well-studied Igusa invariants. In this talk, I present an algorithm to construct CM genus 2 curves using instead the Rosenhain invariants. The Rosenhain invariants typically have much smaller height, so computing them requires less precision. In addition, the Rosenhain model for the curve can be written down directly given the Rosenhain invariants. Similarly, the parameters for a Kummer surface can be expressed directly in terms of rational functions of theta constants. CM-values of these functions are algebraic numbers, and when computed to high enough precision, LLL can recognize their minimal polynomials. Motivated by fast cryptography on Kummer surfaces, we investigate a variant of the CM method for computing cryptographically strong Rosenhain models of curves (as well as their associated Kummer surfaces) and use it to generate several examples of curves at different security levels that are suitable for use in cryptography. (Received September 10, 2015)