1086-14-1803 **Craig Costello***, Microsoft Research, One Microsoft Way, Redmond, WA 98052. *Efficient arithmetic on Jacobians of genus 2 curves.* Preliminary report.

This talk will survey the fastest methods of arithmetic on Jacobians of genus 2 curves. In particular, an especially attractive Kummer surface associated to such Jacobians was shown by Gaudry (in 2007) to facilitate much faster arithmetic than on the Jacobian itself. The transformation of the genus 2 curve to this Kummer surface is usually achieved via the Rosenhain invariants. Using these invariants imposes some restrictions on the type of curve one can use, namely that the two torsion must be defined over the ground field. Through the use of analytic theory, we bypass the use of the Rosenhain invariants to (in certain cases) ease this restriction, which allows a wider range of curves to take advantage of the state-of-the-art in fast genus 2 arithmetic. (Received September 24, 2012)