Genus two CM curves and their invariants.

Tonghai Yang, University of Wisconsin

Igusa invariants and Rosenhain invariants are known to be important for genus two cryptosystems using CM curves. They are Siegel modular functions of genus 2 (i.e. for $Sp(4)$). Their CM values, although algebraic, have often denominators. For computational purpose, it is desirable to know the denominator (at least a good bound) to recognize these algebra numbers. We will briefly describe how to compute the denominators.

On the other hand, giving a CM curve (whose Jacobian is a CM abelian variety), the associated CM quartic field has a real quadratic field F. One can embed the Hilbert modular surface into the Siegel 3-fold, and pull back the invariants. They should become easier and sometimes only need two invariants instead of three, for example when the Hilbert surface is P^2. We will also describe one such case $F=Q(\sqrt 5)$.