INTERNATIONAL CENTRE
OF EXCELLENCE FOR
EDUCATION IN
MATHEMATICS

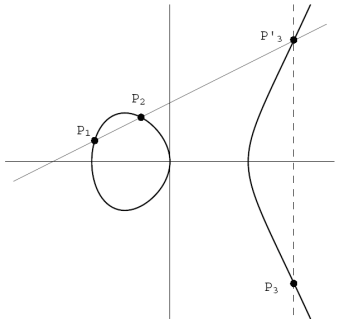
Elliptic curve cryptography

Graeme Pope, School of Mathematics and Statistics, University of Sydney

Over the Christmas break I had the opportunity to complete a project in Elliptic Curves at the University of Sydney. The aim of the project was to look at Elliptic Curve Cryptography (ECC) with the intention of focussing on *Side Channel Attacks, efficient multiplication* and *Hyperelliptic Curves*.

Elliptic Curves are often specified in terms of tuples (x,y) satisfying an equation of the form $y^2 = x^3 + Ax + B$. The set of points (x,y) and a point at infinity, ∞, satisfying this equation from some field $K \times K$ form a group. The group law defines how we "add" two points together.

To add two points, P_1 and P_2, draw the "line" through them. Finding the intersection of the line with the elliptic curve gives a third point P'_3 such that $P_1 + P_2 + P'_3 = \infty$. Reflecting P'_3 in the x-axis gives P_3, such that $P_1 + P_2 = P_3$.



To add to P_1 itself we simply draw the tangent. And if the line does not intersect the curve again, we say that $P_1 + P_2 = \infty$.

Since this set of points form a group we can implement the ElGamal Public Key Algorithm, which forms the basis of many forms of Elliptic Curve Cryptography.

Hyperelliptic curves are given by the set of tuples satisfying a higher order equation, one of the form $y^2 + y\,h(x) = f(x)$ where $f(x)$ has degree $2g+1$ and the degree of $h(x)$ is less than $f(x)$. The curve then has genus g. Elliptic curves have genus 1.

During my project I have looked at a number of ways reducing the information leaked via side-channel attacks, which closely relates to methods of efficient multiplication. As part of this I researched a number of proposals for modified coordinate systems such as modified Jacobian and López-Dahab coordinates and began to implement these in the algebraic-geometry package *SAGE*. I also briefly investigated Hyperelliptic curves and how the group law differs on these from elliptic curves.

I am very grateful to have been given the opportunity to have completed an AMSI summer scholarship and my intention is to use this work as a basis for my thesis in maths honours this year. I would also like to thank both Dr Martine Girard and Dr David Kohel for their time and effort in supervising me.

Graeme received an ICE-EM Vacation Scholarship in December 2005.
See www.ice-em.org.au/students.html#scholarships05