MICHAEL JACOBSON, University of Calgary, 2500 University Drive NW, Calgary, AB, T2N 1N4
Computing Discrete Logarithms on High Genus Hyperelliptic Curves

High genus hyperelliptic curves are of cryptographic interest in the context of the Weil descent method for solving the elliptic curve discrete logarithm problem (ECDLP). Weil descent allows one to reduce the ECDLP on some elliptic curves defined over a characteristic 2 finite field of composite degree to an instance of the hyperelliptic curve discrete logarithm problem (HCDLP) defined over a smaller field. Under certain circumstances, the resulting instance of the HCDLP can be solved in subexponential time using index calculus algorithms. In this talk, we describe recent improvements to an algorithm for solving the usual HCDLP on an imaginary hyperelliptic curve, and the infrastructure discrete logarithm problem on a high genus real hyperelliptic curve. In the imaginary case, we obtain a significant improvement in practice, allowing us to solve an instance of the ECDLP on an elliptic curve defined over $\mathbb{F}_{2^{155}}$ via Weil descent. In the real case, we obtain an algorithm with improved asymptotic complexity, as well as numerical results from the first implementation of any index calculus algorithm for solving the infrastructure discrete logarithm problem.