CRG "Explicit Methods for Abelian Varieties" Kick-off Workshop
Talk Titles and Abstracts

Monday, May 25

9:30 **Nils Bruin** (Simon Fraser University), *Relating torsion subgroups of Jacobians to ideal class groups*

The modern approaches for computing n-Selmer groups of Jacobians over global fields use the unit groups and class groups of finite extensions of the base field as the global ingredient in the otherwise local computations involved in determining n-Selmer groups.

There is information available in the other direction too: If C/P^1 is a curve over, say, $\mathbb{Q}$, that is totally ramified over a point p_0 in P^1, and $\mathrm{Jac}(C)$ has particular torsion structure, then this structure is reflected in the class groups of fibers of C near p_0.

There are many cases in the literature where this phenomenon is exploited to prove the existence of certain torsion types in class groups. We will sketch some of these and describe what the common properties are that make these arguments work.

This is a preliminary report inspired by joint work with Victor Flynn and Damiano Testa.

11:00 **Rachel Pries** (Colorado State University), *p-ranks of Prym Varieties*

Tuesday, May 26

9:30 **Kumar Murty** (University of Toronto), *Arithmetic on Abelian Varieties*

We discuss some work with Pramath Sastry in which we try to make explicit the arithmetic on an Abelian variety over a finite field. The methods are inspired by the work of Khuri-Makdisi who considered the case of the Jacobian of a curve.

11:00 **Jeff Achter** (Colorado State University), *Accessible Abelian Varieties*

14:00 **Clifton Cunningham** (University of Calgary), *Lifts of Hilbert modular forms and Abelian varieties*

Thursday, May 28

9:30 **Jan-Steffen Müller** (Carl von Ossietzky Universität Oldenburg), *Computing Integral and Rational Points on Curves Using p-adic Integration*

The method of Chabauty-Coleman, based on p-adic integration, can be used to find all rational points on a curve over the rationals whose Jacobian has Mordell-Weil rank less than the genus. Kim has initiated a program with the goal of extending this approach to more general curves. I will discuss joint work with Balakrishnan and Besser which makes some of Kim's ideas explicit.

11:00 **David Roe** (University of British Columbia), *Positive slope pieces of the eigencurve via interpolation*

Modular symbols are dual to modular forms, and provide a crucial tool for computing with modular forms of weight at least 2. For fixed weight, one can fit each of these vector spaces into larger p-adic Banach spaces known as overconvergent modular symbols/forms. And for

varying weight, one can construct families of modular symbols/forms, including Hida families in the ordinary case.

The eigencurve is a geometric object whose points correspond to these overconvergent modular forms (or to their U_p-eigenvalues). One can interpret Hida families as discs inside the eigencurve, with U_p-eigenvalue a p-adic unit (slope 0). I will describe an algorithm to find positive slope discs inside the eigencurve, using interpolation from calculations at individual weights. This is ongoing work, joint with Ander Steele.

15:30 **Kumar Murty (colloquium)** (University of Toronto), *Symmetry, Periodicity and Information Security*

Two notions that are of central importance in mathematics are symmetry and periodicity. The concept of symmetry is connected to the theory of groups, an important part of algebra, and periodicity is connected with harmonic analysis and special functions, an important part of analysis. The two notions come together in the geometric structure known as an Abelian variety. These varieties, which abound in nature, are now also fundamental to information security. For example, they form the basis of the security of a Blackberry. In this informal talk, we will discuss symmetry and periodicity and illustrate them with examples. We will then introduce the concept of an Abelian variety and explain its connection to information security.

Friday, May 29

9:30 **David Jao** (University of Waterloo), *Quantum algorithms for elliptic curve isogenies*

Most currently deployed protocols for public key cryptography including RSA, DH, and ECC are insecure against quantum computers. A natural response is to develop new cryptosystems based on quantum-resistant assumptions. Schemes based on supersingular elliptic curve isogenies represent a promising candidate for post-quantum cryptography, because they are relatively efficient and involve only one single tunable security parameter. The security analysis for such schemes depends on the difficulty of computing supersingular elliptic curve isogenies. In this work we present a quantum algorithm for computing isogenies between general supersingular elliptic curves, with subexponential complexity over prime fields, and complexity $p^{1/4}$ in the general case. We also discuss the implications of our work for the special case of curves used in supersingular isogeny-based cryptography.

11:00 **Laurent Imbert** (Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier), *Randomizing Scalar Multiplication Using Exact Covering Systems of Congruences*

Exponentiation over a finite group is a central operation for most public key cryptosystems. It is used extensively in the generation/verification of electronic signatures (e.g. using DSA or its elliptic curve variant) and in the encryption/decryption phases of RSA or (EC)DL-based algorithms. In general, data manipulated during these computations should be kept secret, as even a small amount of information may be maliciously exploited by an attacker, for example for forging one's signature or for acquiring some confidential information.

Over the past fifteen years, an extensive variety of constant-time, highly regular exponentiation algorithms have been proposed. Combined together with various randomization techniques, these algorithms offer sound protections against differential, timing and simple side-channel attacks. Unfortunately, the ultimate, all-in-one, protection does not seem to exist.

In order to protect an implementation against all known attacks, several countermeasures should often be carefully stacked together.

In this talk, I will present a novel family of uniformly randomized scalar multiplication algorithms based on covering systems of congruences which offer good performances in terms of both speed and robustness against a wide class of side-channel attacks.