MARK BAUER
University of Calgary

Relating the ECDLP to other curves

A sub-exponential algorithm for the discrete logarithm problem (DLP) on hyperelliptic curves of high genus has been know for quite some time now. Perhaps somewhat surprising, new classes of curves have been found recently which admit a sub-exponential algorithm for the DLP which have running times similar to that of the number field sieve. In this talk, we will describe how one could try to use these alorithms to develop a sub-exponential algorithm for the elliptic curve discrete logarithm problem (ECDLP). In particular, we will attempt to prove that in most cases the ECDLP can be embedded into the Jacobian of one of these curves with a fast sub-exponential algorithm. Of course, these techniques are guaranteed to fail, but there are (arguably) interesting insights to be drawn from this technique. My hope is to point out some of these problems and stimulate discussion on the possible conclussions. (This is very much a work in progress)

NILS BRUIN
Simon Fraser University

Deciding the existence of rational points on curves

While it is known that Hilbert's 10th problem - deciding whether a polynomial equation has integral solutions - has no automatic solution, one can still hope that for subclasses of polynomial equations and for rational solutions, such an algorithm might exist. Recently, experiments and theoretical work inspired by these experiments have provided some quite convincing evidence that for rational points on projective curves, such an algorithm does indeed exist and that we in fact already know the algorithm. I will outline this algorithm and indicate the heuristics that indicate it is correct.

JOHANNES BUCHMANN
Technische Universitat Darmstad

CMSS - Digital signatures without number theory?

The security of all digital signature schemes that are used in practice is based on the intractability of computational problems in number theory. However, already in 1978 Ralph Merkle invented a signature scheme based whose security is only based on the collision resistance of the hash function that is used in the scheme. For efficiency reasons the Merkle signature scheme (MSS) was never used in practice. But a very interesting property of MSS is that any new cryptographic hash function gives rise to a new instance of MSS. Therefore, MSS is a very good post-quantum candidate. In this talk we present CMSS, an improvement of MSS which incorporates many optimizations to MSS that have

been invented in the past. We report about implementations of CMSS that show that CMSS is a competitive signature scheme. This raises the question of whether number theory needed in digital signature schemes at all.

ALINA CARMEN COJOCARU
University of Illinois at Chicago

Effective versions of Serre's Theorem for elliptic curves

Let E be an elliptic curve over the field of rational numbers, without complex multiplication. In 1972, Serre proved that there exists a constant C=C(E) such that for any prime p ¿ C, the mod p Galois representation associated to E is surjective. He also asked if this constant could be made effective in E, or, even, more, if it could be made uniform in E. I will discuss ways of answering the first question, and ways of answering the second question if the base field of E is a function field. This last result is based on joint work with Chris Hall.

JINTAI DING
Technical University of Darmstadt

Multivariate Public Key Cryptography

Public key cryptography is an indispensable part of our modern communication systems. However, quantum computers can break the most commonly-used public key cryptosystems like RSA, which are based on "hard" number theory problems. Recently a great effort has been put into the search for alternative public key cryptosystems. Multivariate public key cryptosystems (MKPC), whose public key is a set of multivariate polynomials over a finite field, provide one such promising alternative. The theoretical security assumption comes from the fact that solving a system of polynomial equations over a finite field is in general NP-complete and quantum computers are not yet effective in solving this problem. Furthermore, computations in a finite field can be more efficient, therefore MPKCs also have the potential in application for devices with limited computing power. In this talk, we will first present an systematic introduction of the recent development in this new area, the focus will be on the Matsumoto-Imai cryptosystems , the Sflash cryptosystems, the HFE cryptosystems, the Oil-Vinegar cryptosystems, the HFEv cryptosystems, the TTM cryptosystems, the cryptosystems of internal perturbation and the Rainbow cryptosystems, and we will also present the main challenges we are currently facing.

STEVEN GALBRAITH
Royal Holloway University of London

Some open problems in elliptic curve cryptography

This talk will survey some computational problems arising from elliptic and hyperelliptic curve cryptography. In particular, I will discuss some new results on pairing implementation and will examine the possibility of multivariate attacks on the pairing inversion problem.

PIERRICK GAUDRY
Ecole Polytechnique

Variants of the Montgomery form based on Theta functions

The Montgomery form for elliptic curves is a particular form of the equation that allow a fast scalar multiplication using a Lucas chain. This is used in the ECM factoring algorithm and to obtain very fast public key cryptosystems. Starting from ideas by Chudnovsky and Chudnovsky, we have used Theta functions to design formulae with similar properties for genus 2 curves. In this talk we will explain this construction. We will also discuss about an analogous construction for genus 1 that is not exactly the same as the original Montgomery form. Finally, we will show that at least in genus 1, our formulae can be adapted to characteristic 2, thus recovering the best known formulae.

MARK GIESBRECHT AND ARNE STORJOHANN
University of Waterloo

Speedy new algorithms for solving integer linear systems

While there have been methods known for solving linear systems of integer equations for at least two millennia, the past few years have seen improvements in both the practical and asymptotic efficienies of algorithms for this problem. We will discuss algorithms which narrow and even eliminate the gap between the algebraic and "bit" complexity of linear algebra for dense and sparse matrices. In particular, the algorithms require a sub-cubic number of machine operations, even when accounting for coefficient growth. Linear system solving serves as the lynch-pin for most other linear algebra problems, including linear Diophantine problems, so these techniques have wide application. Both the asymptotic analysis and implementation in Linbox and IML will be discussed.

This is joint work with Zhuliang Chen, Wayne Eberly, Pascal Giorgi, and Gilles Villard.

ELISA GORLA
University of Zurich

Computational challenges arising in torus-based cryptography

We will discuss different aspects of torus-based cryptography, with an eye on the computational side and on the open problems that arise in this context. In particular, we will discuss the discrete logarithm problem in the algebraic tori.

FLORIAN HESS
Technische Universitt Berlin

The Ate pairing - computational aspects of pairings in cryptography

We survey some computational aspects of pairings in cryptography regarding existence, efficient evaluation and security, and present a new fast pairing, the "Ate" pairing.

DAVID JAO
University of Waterloo

The discrete logarithm problem on algebraic curves

In this talk we explore the mathematical foundations underlying the conjectured difficulty of the discrete logarithm problem in Jacobians of algebraic curves. We review current state-of-the-art algorithms for computing discrete logarithms, and present relationships between discrete logarithm problems in various contexts, both within a single family of curves (e.g. elliptic curves) and across curve families. Recent developments and open problems in the case of elliptic and hyperelliptic curves are also discussed.

MICHAEL JACOBSON
University of Calgary

Computing Class Groups of Quadratic Fields

Class groups of quadratic fields have been studied since the time of Gauss, and in modern times have been used in applications such as integer factorization and public-key cryptography. The class group and its order, the class number, play a crucial role in these applications. In this talk, we describe state-of-the-art methods for computing the class number and the class group structure (decomposition into prime order subgroups) of quadratic fields. We also discuss our recent efforts to extend existing, unconditionally correct tables of class groups. The data is used to provide valuable numerical evidence in support of a number of unproven heuristics and conjectures related to class groups.

KIRAN KEDLAYA
Massachusetts Institute of Technology

Recent results on p-adic computation of zeta functions

We survey several recent extensions of the speaker's application of p-adic cohomology to the efficient computation of zeta functions of varieties over fields of small characteristic. These include a generalization of Castryck-Denef-Vercauteren from hyperelliptic curves to nondegenerate curves on toric surfaces, a method of Hubrechts to perform low-memory computations for hyperelliptic curves, and an extension to smooth projective surfaces given by Abbott-Kedlaya-Roe.

ERICH KALTOFEN
North Carolina State University

Finding Small Degree Factors of Multivariate Supersparse (Lacunary) Polynomials Over Algebraic Number Fields

We present algorithms that compute all irreducible factors of degreef $\leq d$ of supersparse (lacunary) multivariate polynomials in n variables over an algebraic number field in deterministic polynomial-time in $(L + d)^n$, where L is the size of the input polynomial. In supersparse polynomials, the term degrees enter logarithmically as their numbers of binary digits into the size measure L. The factors are again represented as supersparse polynomials. Our approach follows that by H. W. Lenstra, Jr., on computing factors of univariate supersparse polynomials over algebraic number fields. Our generalization appeals to recent lower bounds on the height of algebraic numbers and to a special case of the former Lang conjecture.

This is joint work with Pascal Koiran, ENSL.

YOONJIN LEE
Simon Fraser University

Construction of Cubic Function Fields from Quadratic Infrastructure

We present an efficient method for generating non-conjugate cubic function fields of a given squarefree discriminant, using the infrastructure of the dual real function field assisociated with the hyperelliptic field of the same discriminant. This method was first proposed by Shanks for number fields in an unpublished manuscript from the 1970s.

THE FIELDS INSTITUTE
FOR RESEARCH IN MATHEMATICAL SCIENCES

ABSTRACTS 1.2

ALFRED MENEZES
University of Waterloo

Another Look at Provable Security

The search for mathematically rigorous proofs of security for public-key cryptographic systems has been an important theme of researchers over the past twenty years. We raise some technical points about the interpretation of security proofs and argue that their relevance to real-world security is uncertain and often requires subjective judgements.

DANIELE MICCIANCIO
University of California San Diego

Ideal lattices: cryptographic applications and open problems

Cyclic codes are among the most useful and widely used error correcting codes in coding theory and communication applications. We consider a similarly defined class of "cyclic lattices" (and generalizations), and discuss cryptographic applications, connections with other problems in algebraic number theory, and open problems concerning their computational complexity.

VICTOR S. MILLER
Center for Communications Research

The Weil Pairing, and its efficient calculation

With the advent of the use of Elliptic Curves in Cryptography, the pure mathematical field of Algebraic Geometry has become relevant to the field of Cryptology. The Weil pairing, first introduced by Andr'e Weil in 1940, plays an important role in the theoretical study of the arithmetic of Elliptic Curves and Abelian Varieties. It has also, recently become extremely useful in cryptologic constructions related to those objects. In this paper, I'll give the definition of the Weil pairing, describe efficient algorithms to calculate it, give two applications and describe the motivation to considering it.

FRANCOIS MORAIN
Ecole Polytechnique, LIX

Recent improvements to the SEA algorithm in genus 1

The Schoof-Elkies-Atkin (SEA) algorithm aims at computing the cardinality of elliptic curves over finite fields. It is the only one that can be used in the case where the characteristic p is large. The basic idea is to compute the characteristic polynomial of the restriction of the Frobenius on the curve modulo small primes ℓ. To speed up the process, isogenies of degree ℓ can be used in some cases, and this step uses modular equations as a key ingredient. We will describe the state of the art in computing these equations, as well as new techniques for computing the eigenvalue of the Frobenius in the last stage of the so-called Elkies case. This will include Mihailescu's recent approach using elliptic Gauss sums.

ROGER OYONO
University of Waterloo

Computation of non-hyperelliptic modular Jacobians of dimension 3

We present a method to solve in an efficient way the problem of constructing the curves given by Torelli's theorem in dimension 3 over the complex numbers: For an undecomposable principally polarized abelian threefold A over $\mathbb{C}$ given by its period matrix Ω, compute a model of the curve of genus three (unique up to isomorphism) whose Jacobian, equipped with its canonical polarization, is isomorphic to A as a principally polarized abelian variety. We use this method to describe the non-hyperelliptic modular Jacobians of dimension 3. We also present another method in finding $\mathbb{Q}$-rational equations of non-hyperelliptic modular curves of genus 3. We investigate all the non-hyperelliptic new modular curves C_f of genus 3 with $\mathrm{Jac}(C_f) \sim_{\mathbb{Q}} A_f$, where $f \in S_2^{\mathrm{new}}(X_0(N))$, $N \leq 4000$.

ALLISON M. PACELLI
Williams College

Constructing Number Fields and Function Fields with Prescribed Class Group Properties

Constructing families of fields with a prescribed class group or class number is a difficult problem. Even when simplifying the question to that of class number divisibility, many proofs are not constructive. We will give a survey of some results on constructing number fields and function fields whose class groups satisfy certain properties.

RACHEL PRIES
Colorado State University

Computing the invariants of p-torsion of Jacobians in characteristic p

An elliptic curve in characteristic p can be either ordinary or supersingular. This distinction has a big impact on the cryptosystems that rely on these elliptic curves. To generalize this concept for a curve of higher genus, it is necessary to look at the p-torsion of its Jacobian. I will explain invariants, such as the p-rank and a-number, that arise for the p-torsion of Jacobians of curves in characteristic p. I will explain methods to compute these invariants. I will end with some results about the invariants for the p-torsion of Jacobians of curves with automorphisms.

TAKAKAZU SATOH
Tokyo Institute of Technology

On Euclid prime sequences (joint work with Nobushige Kurokawa)

A proof by Euclid that there exists infinitely many prime numbers is very well known. Our problem is whether we can obtain ALL the primes by this algorithm. Among some earlier papers, D. Shanks gave a heuristic argument which suggests that the answer is affirmative. Despite of recent advances of computational number theory, numerical examples do not seem to make this conjecture convincing. We reformulate the problem to polynomial rings over finite fields and prove that in some explicitly characterized cases Shanks' argument does NOT hold. On the other hand, numerical computations are performed, which suggests that except for the above cases, Shanks' conjecture is TRUE.

PETER STEVENHAGEN
Universiteit Leiden

Computational challenges arising in complex multiplication

we discuss computational challenges arising in classical 'genus 1 complex multiplication', and solutions that have been found to cope with them, before moving on to challenges arising for genus 2.