Cryptography and Coding Theory
Cryptographie et théorie des codes
(Org: **Isabelle Déchène**, **Ariane Masuda** and/et **Monica Nevins** (Ottawa))

TIM L. ALDERSON, University of New Brunswick Saint John, 100 Tucker Park Rd., Box 5050, Saint John, NB, E2L 4L5
Constructions of 2-dimensional codes for OCDMA

We present some new families of $(\Lambda \times T, w, \lambda)$ (2-D) wavelength/time optical orthogonal codes (2D-OOCs) with $\lambda = 1, 2$. Such codes are used in optical code-division multiple access (OCDMA) systems for supporting many simultaneous users. All families presented are either optimal with respect to the Johnson bound (J-optimal) or are asymptotically optimal. The constructions are based on certain pointsets in finite projective spaces of dimension k over $GF(q)$ denoted $PG(k, q)$. Exploiting this framework we establish that all 2D-OOCs constructed are in fact maximal (in that no new codeword may be added to the original whereby code cardinality is increased).

ROBERT BAILEY, Carleton University, School of Mathematics and Statistics, 1125 Colonel By Drive, Ottawa, ON, K1S 5B6
Distance enumerators of permutation groups

The *distance enumerator* of an error-correcting code is a polynomial which "counts" the number of codewords from a fixed word w. (For linear codes, this is often called the *weight enumerator*.) We consider the situation where the code is a group of permutations (where the codewords are permutations written in list form, and with the usual Hamming distance), in which case the distance enumerator is related to a more well-known polynomial, the cycle index.

This is joint work with J. P. Dixon (London/Sydney).

MARK BAUER, University of Calgary, 2500 University Dr. NW, Calgary, AB, T2N 1N4
Cubic Function Fields in Characteristic 3

Much of our knowledge and insight into function field (from a computational perspective) comes from extending what has been learned in the number field case to this new setting. While this can work in positive characteristic, things tend to go awry when the characteristic of the field divides the degree of the extension. The simplest example of this is elliptic and hyperelliptic function fields in characteristic two. In this situation, while many things become more complicated, they are still manageable enough because they are relatively well behaved. By doing something as innocuous as looking at cubic function fields in characteristic three, even calculating the most mundane invariant becomes problematic.

In this talk, we highlight some of the challenges in this area and some successes. We also highlight a class of curves that could be (in some sense) considered an analogue of hyperelliptic curves in characteristic two.

This is joint work with Jonathan Webster.

LUCA DE FEO, École Polytechnique de Paris

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.

DAVID JAO, University of Waterloo
Boneh–Boyen signatures and the Strong Diffie–Hellman problem

The recent advent of non-standard discrete logarithm based assumptions has led to a proliferation of cryptographic protocols for which no proof of equivalence between the security of the protocol and the underlying hard problem is known. One of the prototypical examples of this phenomenon is the Boneh–Boyen short signature scheme, whose security to date has not been proven to be equivalent to the Strong Diffie–Hellman (SDH) problem upon which it is based. The results which we present here provide for the first time a proof that the Boneh–Boyen signature scheme is equivalent to the SDH problem. Using Cheon's algorithm for solving the SDH problem, we obtain an algorithm that in most cases recovers the private key in the Boneh–Boyen signature scheme in less time than it takes to solve the discrete logarithm problem, given sufficiently many message-signature pairs.

ATEFEH MASHATAN, University of Waterloo, Waterloo, Ontario
Message Recognition Protocols for Ad Hoc Networks

We look at message recognition protocols (MRPs) and prove that there is a one-to-one correspondence between non-interactive MRPs and digital signature schemes with message recovery. Further, we look at an existing recognition protocol and point out its inability to recover in case of a specific adversarial disruption. We improve this protocol by suggesting a variant which is equipped with a resynchronization process. Moreover, another variant of the protocol is proposed which self-recovers in case of an intrusion. Finally, we propose a new design for message recognition in ad hoc networks which does not make use of hash chains. This new design uses random passwords that are being refreshed in each session, as opposed to precomputed elements of a hash chain.

KUMAR MURTY, Department of Mathematics, University of Toronto, 40 St. George Street, Toronto, Ontario, M5S 2E4
The ERINDALE hash function

We shall discuss a fast stream-based hash function developed with Nikolajs Volkovs.

TERASAN NIYOMSATAYA, University of Ottawa
Space-Time Hamiltonian Constellations From Group Codes

Space-time coding has been developed for use in multiple antenna wireless communications to achieve high rate and reliable data transmission. In this talk, we will present a new design of space-time Hamiltonian constellations from group codes. These group codes include cyclic groups, permutation codes variant II and finite reflection groups.

This is joint work with Ali Miri and Monica Nevins (University of Ottawa).

DANIEL PANARIO, Carleton University, 1125 Colonel By Dr., Ottawa
The distribution of the number of encryptions in revocation schemes for stateless receivers

We consider the problem of a center broadcasting an encrypted message to a group of users such that some subset is considered revoked and should not be able to obtain the content of the broadcasted message even if all revoked users collaborate. Various encryption schemes have been proposed to solve this problem which arises, for example, with pay-TV and satellite communications.

In one class of proposed schemes the center distributes a unique combination of keys to each user who decrypts the message individually. If keys cannot be updated once distributed the receivers are called stateless. Several key distribution schemes use a balanced binary tree structure. Some examples that we consider are the complete subtree scheme (CST), introduced independently by Wallner, Harder and Agee (1998), and Wong, Gouda and Lam (1998), the subset-difference scheme (SD), introduced by Naor, Naor and Lotspiech (2003), and the layered subset-difference scheme (LSD) by Halevy and Shamir (2002).

Park and Blake (2006) give generating functions that entail the exact mean number of encryptions for the above key distribution schemes. We extend their results by showing that the distribution of the number of encryptions is asymptotically normal.

This is joint work with C. Eagle, Z. Gao, M. Omar, and B. Richmond.

MOHAMMAD SADEGHI, Amirkabir University of Technology, 474 Hafez Ave., Tehran, Iran
Capacity achieving low-density parity-check lattices

In 2000, Forney (IEEE Trans. Inform. Theory **46**, 830–850) defined the concept of capacity achieving of lattices on AWGN channels. By introducing coset-codes, he proved the existence of such lattices and called them "sphere bound achieving".

Low-density parity-check (LDPC) codes (Gallager, 1963) have a very good performance under iterative decoding algorithm. In 2006, Sadeghi et. al. (IEEE Trans. Inform. Theory **52**, 4481–4495) introduced LDPC Lattices. Construction D' (Bos and Convey, Mathematika **29**(1982), 171–180) converts a set of parity checks defined by a family of nested code into congruences for a lattice. This type of construction is applied to LDPC codes to generate LDPC lattices.

In this talk we show that this type of lattices are capable of sphere bound achieving, that is, for AWGN channel with noise variance per dimension σ^2, there exists a lattice with volume V of large enough dimension n such that the error probability is small whenever $\sigma^2 < \frac{V^{\frac{2}{n}}}{2\pi e}$.

SAEED SAMET, University of Ottawa, SITE, 800 King Edward Avenue Ottawa, Ontario, K1N 6N5, Canada
Privacy-Preserving Data Mining

Although, data is very valuable in every organization, it must be processed in order to be useful. Data mining is a collection of techniques which find patterns and associations in raw data, classify or cluster the items according to their attributes. Nowadays, related data is normally distributed among two or more parties in different configurations, and mining can be done in an accurate and useful way for all parties involved, on all data collections. However, privacy is often crucial in different scenarios, and organizations involved do not want to disclose their own private information to each other. Therefore, standard algorithms of data mining must be modified, or new protocols have to be designed to preserve the privacy of the parties. In the last decade, Privacy-Preserving Data Mining has received increase attention from researchers in computer science, and many protocols and techniques have been presented for different data mining methods, each of which has a level of security, efficiency and accuracy. However, there are still many open problems in this field of study in terms of security and efficiency such as developing privacy-preserving protocols for public channels and incremental algorithms, preventing sensitivity and collusion attack, reducing intermediate outputs, and balancing the distribution of the final results. In this talk we shortly review the background, present some solutions, and discuss possible future directions in this area.

RENATE SCHEIDLER, University of Calgary, Department of Mathematics & Statistics, 2500 University Drive NW, Calgary, Alberta, T2N 3Z4
Cryptography on Real Hyperelliptic Curves

Algebraic geometers and cryptographers are very familiar with what we like to call the "imaginary" model of a hyperelliptic curve. Another less familiar description of such a curve is the so-called "real" model; the terminology stems from the analogy

to real and imaginary quadratic number fields. Structurally and arithmetically, the real model behaves quite differently from its imaginary counterpart. While divisor addition with subsequent reduction ("giant steps") is still essentially the same, the real model no longer allows for efficiently computable unique representation of elements in the Jacobian via reduced representatives. However, the real model exhibits a so-called infrastructure, with an additional much faster operation ("baby steps"). We present the real model of a hyperelliptic curve and its two-fold baby step giant step divisor arithmetic. We also indicate how to use these algorithms for potential cryptographic and number theoretic applications.

FRANCESCO SICA, Mount Allison University–AceCrypt, 67 York Street, Sackville, NB, E4L 1E6
Exploring a New Factoring Algorithm

I would like to highlight the principal features of a new factoring algorithm still in preparation. In particular, I believe that this algorithm runs in subexponential time. However, unlike previous leading subexponential-time factoring algorithms related to the Quadratic Sieve, this one does not use "Fermat-type" equalities.

Rather, to factor x, it finds a nontrivial relation between $O(x^\epsilon)$ values of a carefully chosen multiplicative function related to $\sigma(n) = \sum_{d|n} d$. L-functions come to the rescue in finding this relation and the functional equation plays a crucial role.

DAVID THOMSON, Carleton University, Ottawa, ON
Efficient p-th root computations in finite fields of characteristic p

We present a method for computing p-th roots using a polynomial basis over finite fields $\mathbb{F}_q$ of odd characteristic p, $p \geq 5$, by taking advantage of a binomial reduction polynomial. For a finite field extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ our method requires $p-1$ scalar multiplications of elements in $\mathbb{F}_{q^m}$ by elements in $\mathbb{F}_q$. In addition, our method requires at most $(p-1)\lceil m/p \rceil$ additions in the extension field. In certain cases, these additions are not required. If z is a root of the irreducible reduction polynomial, then the number of terms in the polynomial basis expansion of $z^{1/p}$, defined as the Hamming weight of $z^{1/p}$ or $\mathrm{wt}(z^{1/p})$, is directly related to the computational cost of the p-th root computation. We find that $\mathrm{wt}(z^{1/p}) = 1$ in all cases using binomials. We also give conditions on which degrees m admit an irreducible binomial over $\mathbb{F}_q$.