Error Control Codes, Information Theory, and Applied Cryptography
Codes de contrôle d'erreurs, théorie de l'information et cryptographie appliquée
(Org: **Tim Alderson** (UNB - Saint John))

AIDEN A. BRUEN, University of Calgary, 2500 University Drive NW, Calgary, Alberta, T2G 1N4
Elliptic curves in cryptography and geometry

This lecture describes joint work with James Hirschfeld and David Wehlau. In the lecture I focus on 2 main topics:

(1) A clarification of the actual definition of an elliptic curve, both historically, and as used in ECC, is presented. From this I then show how the scope of ECC can be significantly widened by adopting a more general approach.

(2) The geometry of elliptic curves. In particular, using classical ideas, I show how to construct new configurations in finite planes having desirable algebraic and combinatorial properties.

This generalizes well-known results of A. Zirilli and P. M. Neumann (relating also to work of Voloch and Alderson–Bruen).

Time permitting I will skirmish with the case of infinite fields.

TREVOR BRUEN, Saint Francis Xavier University
A characterization of certain (0,1) matrices

Let A be a square $(0,1)$ v by v matrix with constant row and column sums. Assume furthermore that A has no $(\lambda, 2)$ isolated zeroes. That is, assume A has no λ by 2 submatrix containing exactly one 0. Under suitable conditions we obtain a lower bound on v and characterize the case of equality.

PETER DUKES, University of Victoria, Victoria, BC
Arrangement Codes

Let $m \leq n$ be positive integers. An m-arrangement from an alphabet X of size n is a permutation of m distinct elements from X. Regarding them as words, the Hamming distance (as usual) measures the number of disagreeing positions between two m-arrangements.

Define an n-ary *arrangement code* of length m and minimum distance d to be a set Γ of m-arrangements from an n-set such that all pairs of different words in Γ have Hamming distance $\geq d$. Note that when $n = m$, one recovers (the more familiar) permutation codes.

This talk will survey my preliminary observations on this topic.

FREDERIC EDOUKOU, Nanyang Technological University, Singapore
The functional codes from non-degenerate Hermitian variety

We study the functional codes of order h defined by G. Lachaud on a non-degenerate Hermitian variety. We exhibit a divisibility condition satisfied by all the weights of this code. In the case this functional code is defined by evaluating quadratic functions on the non-degenerate Hermitian surface, we list the first five weights, we describe the geometric structure of the corresponding quadrics and give a positive answer to a conjecture formulated on this question. We will present two new conjectures. The first is about the divisor (largest integer dividing all the weights) of the functional code. The second is on its minimum distance and the distribution of the codewords of its first $2h + 1$ weights.

This is a joint work with San Ling (NTU, Singapore) and Chaoping Xing (NTU, Singapore).

ANWAR HASAN, University of Waterloo
Resisting Fault Analysis Attacks on ECC via Repeated and Parallel Computations

In cryptographic systems, faults can occur naturally and/or due to some malicious acts of an attacker. In the past, researchers showed how an attacker could exploit computational errors to break some popular crypto-systems. This has made the task of verification of the correctness of cryptographic computations quite important. In some applications, further robustness in term of the ability to continue performing correct computations in presence of certain faults is also sought.

In elliptic curve cryptography, a well-known technique to detect errors in its group operation is to verify whether or not the operation output is a point on the curve. This point verification scheme has however been shown to be insufficient against certain types of fault based attacks. In this talk, error-detecting schemes for elliptic curve scalar multiplication, which is fundamental to elliptic curve crypto-systems, are considered. We present structures based on re-computation and parallel computation along with point verification. These structures use encoding techniques that rely on proprieties of elliptic curves and provide a high probability of error detection.

This is joint work with A. Dominguez-Oviedo.

MICHAEL JACOBSON, University of Calgary, Calgary, Alberta
Security Estimates for Quadratic Field Based Cryptosystems

The security of public-key cryptosystems using quadratic fields is based on two types of discrete logarithm problem. In the imaginary quadratic case, the discrete logarithm problem in the ideal class group is used, whereas in the real quadratic case the principal ideal problem (also known as the infrastructure discrete logarithm problem) is used instead. In this talk, we describe recent improvements to the best known algorithms for solving these two problems. Our numerical results are presented, as well as extrapolations leading to recommendations for parameter sizes providing approximately the same level of security as block ciphers with 80, 112, 128, 192, and 256-bit symmetric keys.

DAVID JAO, University of Waterloo, 200 University Ave. W., Waterloo, ON N2L 3G1
Evaluating isogenies on elliptic curves in subexponential time

An isogeny between elliptic curves is an algebraic morphism which is a group homomorphism. Many applications in cryptography require evaluating large degree isogenies between elliptic curves efficiently. For ordinary curves of the same endomorphism ring, the previous best known algorithm has a worst case running time which is cubic exponential in the length of the input. We show that this problem can be solved in subexponential time under reasonable heuristics, and we present examples of evaluated isogenies which well exceed the previous world record for the evaluation of general prime degree isogenies, including examples of cryptographic size. Time permitting, we will also discuss applications to elliptic curve cryptography and the discrete logarithm problem.

Joint work with Vladimir Soukharev.

PETR LISONEK, Simon Fraser University, Burnaby, BC
Bent functions on finite fields

Bent functions are a class of functions from $\mathrm{GF}(p^n)$ to $\mathrm{GF}(p)$ that are in a precise sense as far as possible from any affine function. This makes them resistant to some well-known cryptographic attacks. There are other features desired in the cryptographic applications, such as a high algebraic degree of the function, and the talk focuses on classes of bent functions that perform well with respect to such additional criteria.

We show how tools from different areas, such as arithmetic geometry (elliptic and hyperelliptic curves), finite fields (character sums) and combinatorics (spreads, relative difference sets, Desarguesian planes) are all used in the study of bent functions. The results are theoretical (characterizations, necessary conditions, constructions) and algorithmic (polynomial time certification of bentness).

MICHELE MOSCA, University of Waterloo/Perimeter Institute, Waterloo
Quantum Key Agreement in a Classical World

Quantum key distribution (QKD) promises secure key agreement by using quantum mechanical systems. Assuming practical and affordable QKD systems become widely available, what role will QKD play in future cryptographic infrastructures?

QKD can provide long-term confidentiality for encrypted information without reliance on computational assumptions. Will anyone really care?

Like classical key establishment protocols, QKD requires authentication to prevent man-in-the-middle attacks. If authentication is achieved using a short shared secret key, one can regard QKD as a form of key expansion. If one is willing to accept some conservative computational assumptions, does QKD still add any value?

I will discuss these and related questions and present situations where QKD can add practical value. I will ask the audience some questions too.

MONICA NEVINS, University of Ottawa, Ottawa, ON, K1N 6N5
NTRU over the Eisenstein Integers

NTRU is a cryptosystem proposed by Hoffstein, Pipher and Silverman in 1996. It is based on polynomials with integer coefficients, where secrecy is obtained by performing operations modulo two different primes in $\mathbb{Z}$. We propose a variant of NTRU, in which $\mathbb{Z}$ is replaced by the Eisenstein integers $\mathbb{Z}[\omega]$. In this talk, we describe this variant, and show how the key property which makes NTRU over $\mathbb{Z}[\omega]$ so efficient and secure is its hexagonal lattice structure in $\mathbb{C}$.

This is joint work with Ali Miri (Ryerson), Camelia Karimianpour (Ottawa) and most recently, Katherine Jarvis (Ottawa).

DANIEL PANARIO, Carleton University
Self-Inverse Permutation Functions over Finite Fields and Interleavers for Turbo Codes

We introduce and study a set of new interleavers for Turbo codes based on permutation functions with known inverses over finite fields. We use monomial, Dickson, Mobius and Redei permutation functions. Our process requires information on the cycle structure of these permutation functions. We use known information on the cycles of monomials, Dickson and Mobius functions. As a byproduct, we provide the cycle structure of Redei functions, as well as an expression for the inverse of any Redei function. Finally, self-inverse permutation functions are used to construct interleavers, that are their own de-interleavers, and are useful for turbo codes.

Joint work with Amin Sakzad and Mohammad-Reza Sadeghi.

PRADEEP SARVEPALLI, University of British Columbia
Quantum Secret Sharing, Matroids and Stabilizer Codes

Quantum secret sharing schemes deal with the distribution of a quantum state among a set of n players, so that only authorized subsets can reconstruct the secret. While the connections between codes, secret sharing schemes and matroids have been subject of extensive investigations, their analogues in the context of quantum secret sharing schemes have not been studied as much, in particular no associations have been made with matroids. In this talk we give the first steps toward establishing the connections between matroids and quantum secret sharing schemes. In addition to providing a new perspective on quantum secret sharing schemes, this characterization has important benefits; they enable us to construct efficient quantum secret sharing schemes for many general access structures. We show that an identically self-dual matroid that is representable over a finite field induces a quantum secret sharing scheme with information rate one. Using the theory of quantum stabilizer codes, we make this association constructive which additionally elaborates on the correspondence between quantum codes and secret sharing schemes.

This is a joint work with Robert Raussendorf (University of British Columbia).

RENATE SCHEIDLER, University of Calgary
Efficient Divisor Reduction on Hyperelliptic Curves

A key ingredient in hyperelliptic curve arithmetic is divisor reduction. Standard reduction methods take as input a non-reduced divisor in Mumford representation and iteratively generate a sequence of divisors until a reduced one is obtained. In this computationally expensive process, the degrees of the intermediate Mumford coefficients gradually decrease down to the genus of the curve. This talk will illustrate how to replace this costly procedure by the computation of just two linear recurrences which allow the recovery of the Mumford polynomials of the reduced target divisor at the end. The two scenarios under consideration are a large input divisor that could have been obtained via an inexpensive tupling procedure for example, and an input divisor that is the sum of two reduced divisors, as encountered in scalar multiplication using non-adjacent form.

ERIC SCHOST, The University of Western Ontario, London, ON
Some applications of multivariate modular composition

In 2008, Kedlaya and Umans introduced the first quasi-linear time algorithm to compute the modular composition of univariate polynomials, namely, $f(g)$ modulo h.

I will describe an extension of this idea to a multivariate setting, and its application to computations with modular polynomials, as seen for instance in the SEA algorithm for elliptic curve point counting.

FRANCESCO SICA, University of Calgary, Dept. of Mathematics and Statistics, 2500 University Drive NW, Calgary, AB T2N 1N4
An Analytic Approach to Subexponential Factoring

I will highlight a polynomial-time reduction to translate the problem of factoring a product N of two primes into the computation of some multiple series with analytic coefficients. In particular, I conjecture that these series can be computed in $O\big(\exp(\log^{\epsilon} N)\big)$ bit operations for any $\epsilon > 0$, therefore providing a similar estimate for the inferred subexponential deterministic factoring algorithm. Unlike previous leading subexponential-time factoring algorithms related to the Quadratic Sieve, this one does not use "Fermat-type" equalities. It rather finds an approximation to the value of a carefully chosen multiplicative function related to the sum of divisors of N (hence its deterministic character). Analytic number theoretic techniques and especially the Riemann zeta function play here an essential role.

BRETT STEVENS, Carleton University
Codes, Capacities and Covering Arrays

Let $\mathcal{B}$ be an alphabet and suppose that there is a set of noisy channels on symbol sets $\mathcal{B}$. We will associate a family of graphs, $\mathcal{G}$ with the channels: if $(x, y) \in E(G)$ for $G \in \mathcal{G}$ then in the channel associated to G, the letters x and y are distinguishable with positive probability. There is a corresponding notion when the graphs are directed. If we are given such a family of noisy channels, what is the best code to use if we do not know which precise channel we will get. The answer is to find a largest possible set of sequences where each pair is distinguishable in any given channel for at least one of their indices. In the directed graph case this code corresponds to a covering array which is an object that generalizes orthogonal arrays and is more typically encountered in software engineering and reliability testing. This talk does not present any new results but surveys this interesting connection.

DMITRI TRUHACHEV, University of Alberta
A Connection between Rateless Coding and Multiple Stream Information Transmission

A construction of a rateless code family for communication over additive white Gaussian noise (AWGN) channels is presented. The proposed code structure is based on transmission of information in the form of multiple redundant data streams. The decoder separates the received multiple layers of data using parallel low complexity detection and then decodes each layer

individually. The impact of the density of design rate points on code performance is examined. It is also demonstrated how the proposed codes can be applied for communication over multiple access and interference channels.

RUIZHONG WEI, Lakehead University, Department of Computer Science, Thunder Bay, ON P7B 5E1
Some Combinatorial Methods for Wireless Sensor Network Scheduling

We consider the node scheduling problem for t-covered and connected sensor networks. Some combinatorial methods are proposed to allocate all nodes in the sensor network into $k(k \geq t)$ different groups $\{0, 1, \ldots, k-1\}$ without requiring location information such that each group will be connected and maintaining the coverage ratio as high as possible. Theoretical analysis and simulation results show that the new scheduling method has better performance than previous randomized scheduling scheme. It can be used to prolong the lifetime of sensor networks effectively.