Cryptography is the topic of the Fall 2006 thematic program at Fields, organized by Ian Blake and Kumar Murty from the University of Toronto, Alfred Menezes from the University of Waterloo and the Centre for Applied Cryptographic Research, Michele Mosca from the University of Waterloo and the Perimeter Institute, Andreas Stein from the University of Wyoming, Renate Scheidler and Hugh Williams from the University of Calgary, and Ramarathnam Venkatesan from Microsoft Research.

Identity theft, bank fraud, malware, wireless communications..... are one’s secrets safe? Financial transactions, credit records, medical information, competitive business intelligence – the integrity and security of information and information systems is often overestimated in the electronic age, with increasingly devastating results. The social and economic costs to individuals and organizations due to the lack of reliable and effective security can be measured in the loss of privacy and information, a loss or lack of confidence in electronic commerce, and economic costs to individuals and organizations due to the lack of reliable and effective security can be measured in the loss of privacy and information, a loss or lack of confidence in electronic commerce, and time, strategic advantage, and billions of dollars in business opportunity, security measures and downtime. How can we be certain of the safety and integrity of the information that is sent to and from us in this information age? There are many parts of this story, but it begins with cryptography, the topic of the fall of 2006 Thematic Program at the Fields Institute.

Cryptography is the study of the design and analysis of mathematical techniques that ensure secure communications in the presence of malicious adversaries.

It is an essential component of any installation in which secure communication is needed.

A sender, Alice, and a receiver, Bob, wish to communicate a message over an insecure channel (mobile phone, internet), and they want to ensure that no other unauthorized party can read their transmission. Both Alice and Bob have access to a very, very large number of different methods of scrambling the message so that it will be unreadable to an eavesdropper (Eve); however, Alice must be able to ensure that Bob will be able to unscramble her message. In order to ensure this, both she and Bob must have communicated earlier – and very securely – a number which they both know refers to the particular scrambling technique that Alice will use. Eve doesn’t know this number, called the key, and therefore

Hyperbolic Geometry

Hyperbolic 3-manifolds figured heavily in the workshop, held May 23-27, 2006, with particular emphasis on improving the quantitative connection between topology and geometry. Jeff Brock (Brown) spoke on the hyperbolic geometry of Heegaard splittings and Juan Souto (Chicago) discussed the relation between the rank of the fundamental group and geometry. David Gabai (Princeton) and Peter Shalen (UIC) outlined quite different programs aimed at relating volume to topological complexity. Classification and deformation of infinite-volume groups were also represented: Ken Bromberg (Utah) and Brian Bowditch (Southampton) presented alternate approaches to the Ending Lamination Conjecture. Dick Canary (Michigan) discussed work on non-bumping points in the boundaries of deformation spaces. Steve Kerckhoff (Stanford) discussed the emerging picture of transitions between the different geometries in dimension 3. Ian Agol (UIUC) discussed subgroup separability in hyperbolic n-manifolds, and presented a striking new construction of closed hyperbolic 4-manifolds with arbitrarily short geodesics, answering a longstanding question. Pete Storm (Stanford) gave a complete generalization of the Besson-Courtois-Gallot volume growth entropy comparison theorems to the (finite volume) non-compact...
case. Francis Bonahon (USC) discussed quantum Teichmüller spaces, and an approach to invariants based on ideas from the geometry of hyperbolic 3-manifolds. Lee Mosher (State Univ. of New Jersey) discussed a notion of axes for irreducible automorphisms of free groups, extending some subtle analogies with the situation of mapping class groups. Mark Sapir (Vanderbilt) described the theory of group actions on tree-graded spaces and its applications, which provides a powerful generalization of the theory of hyperbolic groups. Mario Bonk (Michigan) spoke about fractals in $S^n$, and about quasiconformal equivalence of Sierpinski carpet-like sets.

In addition to the main speakers there were twelve short talks in parallel sessions. Subjects ranged through hyperbolic polyhedra, deformation of hyperbolic 3-manifolds, Teichmüller theory and mapping class groups.

The schedule purposely left open some large blocks of time to encourage conversations among the participants. The blackboards around the Institute were in constant use, and one could see fruitful interactions between the younger and the older participants.

Yair Minsky (Yale) and Bruce Kleiner (Michigan)
The aim of this symposium was to bring together researchers and artists/composers who consider their work to form part of Xenakis’s legacy, either creative or scientific. An important part of the gathering was to hold panel discussions to bring together those from the fields of music, mathematics, and physics. These sessions were organized by Thomas Salisbury (Fields Institute) and Raymond Laflamme (Perimeter Institute).

On June 9, the symposium participants spent the day at the Fields Institute. There were two sessions of presentations: “Xenakis and Mathematics,” and “Applications of Mathematics in Music and Analysis.” Presenters included: Benoît Gibson (Universidade de Evora, Portugal), Paul Steenhuisen (U. Alberta), Ronald Squibbs (U. Conn.), Moreno Andreatta/Carlos Agon (IRCAM, France), Haris Kittos (Royal College of Music, UK), Barry Truax (SFU), and John Rahn (U. Washington).

The Xenakis Legacies Symposium was held in conjunction with the soundaXis Festival (1-11 June, 2006), with a focus on the connections between Architecture, Music, and Acoustics. To underscore the relationship between the symposium and the festival, the day at the Fields Institute closed with a musical performance, held in and around the Institute’s central atrium. Earshot Concerts presented “Reflexions on Xenakis,” a theatrical performance intended to “focus on the war-inspired writings of Xenakis, and … how the war affected not only his art, but his life and soul.”

Funding for the Xenakis Legacies Symposium came from a Conference Grant from the Social Sciences and Humanities Research Council of Canada, and the University of Guelph (Research, College of Arts). In-kind support was also provided by the Fields Institute and Perimeter Institute.

James Harley (Guelph)
The focus of the School was on deterministic models, but there were a substantial number of lectures to demonstrate how and when stochastic and network models should be used, how parameters in the deterministic models are identified and estimated using statistical methods, and how simple deterministic models should be further fine-tuned to deal with disease transmission heterogeneity and spatio-temporal spread patterns.

The Summer School started with background material in mathematics and epidemiology. This was a challenge to the organizers and instructors owing to the background diversity of students. The regular lectures introduced the general principles and frameworks of basic mathematical and statistical techniques in the study of infectious diseases.

An important feature of the Summer School was the series of public lectures. These lectures, covering a wide range of issues and diseases of great interest to public health, illustrated the general framework and abstract mathematical theory in an applied setting. Pauline van den Driessche (Victoria) started this series by providing success stories of how mathematical modeling contributes to the control of infectious diseases. Fred Brauer (UBC) brought the School to a conclusion with a public lecture that introduced the MITACS group’s work on modeling pandemic influenza. There were lectures about the capacity of major cities to resist emerging infectious diseases (D. Earn, McMaster); the challenge and opportunities in modeling wildlife diseases (L. Allen, Texas Tech); the mathematical epidemiological approaches to public security (C. Castillo Chavez, Arizona State); and the integration of epidemic models into cost-effectiveness analysis of universal Hepatitis A vaccination in Canada (C. Bauch, Guelph). The MITACS group and its collaborators also presented their recent work on modeling HIV in India (P. Jha, Toronto); on commercial air traffic as a global conduit for emerging infectious diseases (K. Khan, St. Michael’s Hospital); and how mathematical modeling contributed to the study of West Nile Virus (P. van den Driessche and H. Zhu, York). This series was well liked by the students, and we highly recommend such a component in future programs.

The public lectures were further supplemented by plenary lectures of the CAIMS-MITACS annual meeting, including the CAIMS Research Prize lecture by M. Mackey (McGill) Mathematics, biology, and physics: interactions and interdependence, and the talk by J. Glasse of the US Center for Disease Control about evaluating public health responses to reintroduced smallpox via dynamic, socially structured, and spatially distributed meta-population analysis. To bring the students to the frontiers of the relevant research areas, a number of lectures in the CAIMS-MITACS annual meeting special sessions Nonlinear dynamics in the health sciences, Stochastic models in industrial mathematics and Mathematics outbreaks: epidemics and invasions were also selected as part of the Summer School curriculum.

The pre-assigned student projects were an essential part of the Summer School. Ten projects were identified, thanks to James Watmough (New Brunswick), and announced to the students on Day 1 of the Summer School. Project teams, typically consisting of 6-7 students, were established in consultation with students’ preferences and background on Day 2. Students then worked in these projects in a team environment during the Summer School, and each team chose a particular way to present its work within 30 minutes in the last two days of the Summer School.

This was a great event with an outstanding array of speakers and an excellent mix of wonderful students. The organizers thanked MITACS, The Fields Institute and PIMS for jointly supporting this event that seeded the collaborative spirit for interdisciplinary research in a fascinating field of great importance for public health and for the growth of mathematics.

Jianhong Wu (York)
“COMPLETELY FAIR-MINDED,” “REFLECTIVE,” “insightful, able to see all sides of a question and then to make a thoughtful decision,” “supportive,” “characterized by calm and equanimity, gracious,” “loyal,” “gentle but strong,” “diplomatic”—such are the comments of staff members when they speak of the leadership of Tom Salisbury during his three-year tenure as Deputy Director of the Fields Institute.

On July 1, 2006, Tom began his term as President of the Canadian Mathematics Society, where his role is decidedly different. Yet who can doubt that those qualities will be invaluable in a job where he will be an ambassador and advocate for mathematics across the country?

Sound judgment was needed during Tom’s work at Fields as Deputy Director. For one thing, those years were not years of budget expansion, and, as any financial officer will affirm, making the right decisions during lean times is harder than making the right decisions in times of plenty. With Tom, Fields was able to stretch the dollar both by creatively attracting non-governmental funds and by avoiding spending on ideas and projects that, however nice they might be in the best of all possible worlds, side-tracked funds from the mathematical work of the Institute. He regarded it as a challenge to maintain stakeholders’ enthusiasm for initiating good new projects, while also setting a sustainable budget.

Although as President of the CMS Tom does not carry day-to-day responsibilities similar to those at Fields, he continues to represent Canadian mathematics and mathematicians and their institutes to the wider world. The CMS has set up a liaison committee of all Canadian mathematics institutes to engage in dialogue with NSERC. When asked if this is lobbying, he paused and said that the “CMS has traditionally not lobbied, yet they are seeking new ways to educate government bodies about math.” He gave as an example an Ottawa group called PAGSE that runs a program called Bacon and Eggheads, which holds breakfasts attended by government officials and scientists at which scientists talk about important scientific developments. “People don’t understand about hidden math—cell phones, mutual fund investing, data compression and security, CATSCANs are all mathematics-based, and governments and users need to be reminded of this fact.”

On the importance of mathematics institutes to Canadian mathematics, Tom was emphatic. “Mathematics is increasingly collaborative, and solo work is becoming the exception. Assembling a critical mass of researchers is of vital importance, and institutes do just that. They build a network of researchers sharing ideas, and frequently these networks persist long after a thematic program is over. Senior faculty at conferences become more focused and energized, while the effect upon junior faculty, post-docs, and graduate students is dramatic.”

Fields Director Barbara Keyfitz praises Tom for having “inducted me into my job, and for doing it very well.” When she arrived at Fields, Tom reminded her that his family and hers had an old connection, namely that Tom’s mother, Mary, while serving an internship as a young sociologist in Ottawa, babysat for Barbara and her younger brother. This early family connection merged easily into a congenial working relationship. She also praises Tom for his “willingness to lead and for his willingness to take a subordinate role.” “He is not afraid to make decisions, and he always thinks things through.” Tom, she said was “unflappable … well, nearly always unflappable!”

When asked what he does in his (limited) spare time, Tom spoke of his family, a daughter now doing an internship as an economist with the Brookings Institute in Washington, two sons in university, his wife, Kathy, and their beloved border collie, Pepper. In addition, Tom plays the flute and recorder and reads, especially science fiction. Most recently, he read and enjoyed Susanna Clarke, *Jonathan Strange and Mr Norrell*. What makes science fiction interesting to him is that the plot is “based upon an hypothesis that the author then follows through all the consequences that flow from it.” Sounds mathematical?

Tom and Kathy plan a canoe trip in Algonquin Park in August, where I am sure his almost invariable unflappability, his calm, and good judgment will be as useful as his paddle.

*Elaine Riehm*
The conference was bookended by plenary talks by Richard Hughes of Los Alamos National Laboratories, one of the world leaders in implementing practical quantum-cryptographic systems, and Paul Kwiat of the University of Illinois (the self-styled “last man standing”), a pioneer of engineering entangled-photon sources for applications in quantum optical information processing. Hughes described the “coming of age” of quantum cryptography, 21 years after its introduction by Bennett and Brassard. Kwiat revisited this theme, describing recent experiments in which both quantum mechanics and special relativity are required in order to ensure the security of cryptographic key distribution.

During the course of the week, there were 8 other plenary talks, 8 invited talks, 23 contributed talks, and 32 posters. Speakers included 16 from the U.S., 9 from Europe, 9 from Canada, 5 from Japan, and 2 from Israel. Participants included many of the acknowledged world leaders of most of the subfields of quantum information and quantum control. Topics discussed ranged from the mathematical (what are the limits on the transfer of quantum information in various network topologies?) to the theoretical (should one use Bayesian or maximum-likelihood techniques to best extract a description of a quantum state from experimental data?) to the practical (how can new superconducting architectures be used to build better single-photon detectors which may enable the next generations of quantum information technology?). The three focused-discussion sessions were designed to bring the many different communities together, discussing Applications of quantum control to quantum information, Novel devices for the future of quantum information & control, and Characterization of many-particle states & scalability issues. This culminated in a conference banquet at l’Espresso Bar Mercurio, where the 41 speakers and most of the 50 other attendees started with hors d’oeuvres on the patio and shared a free and enjoyable flow of ... information.

The meeting was supported by the CIAR and MITACS in addition to Fields and the CQIQC, and was followed by a weekend workshop on “Frontiers of Quantum Decoherence” which also attracted many of the world leaders of the field.

Aephraim Steinberg
(Toronto, Director CQIQC)
THE COVERING ARRAY WORKSHOP HELD at Carleton University on May 14-16, 2006, was the first workshop ever to deal specifically with this discrete applied mathematics topic. Covering arrays are combinatorial designs that generalize orthogonal arrays and are important for applications in testing software, networks and circuits.

Brett Steven’s opening talk on Covering arrays and their generalizations, made links between the various aspects of the problem that were going to be explored in the workshop.

The first day focused on fundamental constructions of covering arrays and related objects. Charles Colbourn (Arizona State University) gave a lively plenary lecture on the state of the art of Construction techniques for covering arrays. Contributed talks included constructions of covering arrays and related objects based on extremal set theory (Lucia Moura, Ottawa), probabilistic methods (Anant Godbole, East Tennessee State), finite fields (Daniel Panario, Carleton), and combinatorial design theory (George Sherwood, Testcover.com, and Joe Yucas, Southern Illinois). There was a reception at the end of the day.

The second day focused on applications of covering arrays to software testing, as well as computational methods for the generation of covering arrays. In the plenary talk Covering arrays: mathematical, engineering and scientific perspectives, Alan Hartman (IBM Haifa Research Lab) offered an overview of applications of covering arrays in the area of software testing and proposed many challenges to the community in terms of making covering array research more relevant for this application. This talk prompted some interesting discussions among researchers of 20 in total) that have been identified. In particular, Myra Cohen (DDA tool, University of Nebraska – Lincoln), Yu Lei (IPO tool, University of Texas at Arlington), and George Sherwood (Testcover.com) gave talks on building and applying covering arrays with variable strength, higher strength and mixed alphabets, respectively.

The afternoon of the second day was dedicated to computational methods. Peter Gibbons (University of Auckland), in his tutorial on Computational constructions of combinatorial structures, gave us a deeper insight on selected classical methods for combinatorial design generation and search. He also highlighted applications of simulated annealing and hybrid methods with seeding for constructing covering arrays. A walk to see the tulips at Dow’s Lake followed by dinner at a Mexican restaurant overlooking the lake closed the second day.

The third day had two main themes: Don’t forget your design theory! and Explore theories beyond designs. We started with Doug Stinson’s beautiful presentation of A tutorial on orthogonal arrays: constructions, bounds and links to error-correcting codes. Orthogonal arrays are the classical combinatorial designs most relevant to covering arrays. Covering designs and Mendelsohn designs were presented in the talks by Robert Bailey (Queen Mary, London) in connection with codes and by Frank Bennett (Mount Saint Vincent) in connection with orthogonal arrays, respectively. Discussions prompted by Frank Bennett’s talk revealed connections between Mendelsohn designs and some recent group constructions of covering arrays by Colbourn and by Meagher and Stevens.

The workshop was attended by over 40 participants from Canada and abroad, including around 15 graduate students and postdoctoral fellows from across Canada. Abstracts and slides of the talks can be found at www.site.uottawa.ca/~lucia/CA06/schedule.html

Lucia Moura (Ottawa)
From August 14-18, 2006, over 60 mathematicians, including faculty, postdoctoral fellows and graduate students, came together at the “FMIPW” to dedicate their expertise and energy to six problems presented by several industrial partners. This successful event was sponsored by the Fields Institute and MITACS and was organized by Huaxiong Huang (York), Nilima Nigam (McGill), and Barbara Keyfitz (Fields).

The workshop started on Monday morning with the presentation of the problems by the industry representatives. From Monday afternoon to Friday morning, the academic participants worked on the problems in self-selected groups, often very closely with the industrial participants. They presented their solutions on Friday.

The six workshop problems focused on themes in Finance and Medicine. A problem presented by Helmut Mausser from Algorithmics (Toronto) – a corporate sponsor of the Fields Institute – addressed the question of how multi-objective optimization could best be implemented in a wide range of financial problems which might involve both linear and quadratic objectives, integer variables and soft constraints.

From Manulife (Toronto), Scott Warlow presented a problem that involved issues regarding financial portfolio allocation. Generally, a particular investment strategy is based on estimations of parameters related to expected returns of the various assets. Manulife was interested in how the uncertainty in parameter estimation may affect the optimal investment strategy.

An issue that has recently prompted much concern is the spread of infectious disease across international borders. With the goal of developing strategies to prevent an international pandemic, Kamran Khan from St. Michael’s Hospital (Toronto) asked how commercial airline traffic affects the spread of disease. Data from the spread of SARS was used to validate the models that were developed.

Microarrays generate a very large amount of data that quantify the gene expression levels in a given biological sample. Hidden in the huge data sets is information regarding regulatory networks and biomarkers for disease. Chris Bowman from the National Research Council (Winnipeg) presented the challenging problem of extracting this information from the microarray data by finding relatively low dimensional manifolds from the high dimensional data set.

Another problem came from Mt. Sinai Hospital (Toronto) and addressed the emotional attachment of a mother with her child. The presenters – Bill Lancee, Leslie Atkinson and Jon Hunter – were interested in using mathematical modelling to aid in deciphering which characteristics of a mother’s interaction with her child are most important in determining the behaviour that a child exhibits in a particular experimental situation.

Finally, Richard Gordon from the Manitoba Institute of Child Health presented a problem related to the effects of gravity in the growth of the embryo of a certain salamander found in Mexico. Of particular interest is the cortical rotation that occurs in the eggs just before first cell division. This work has applications to long-range space travel. According to Gordon, this problem, as well as many others in this field, are ones in which mathematicians can make a significant contribution.

The efforts and achievements of the academic participants were much appreciated by the industry presenters, who were very pleased with the results that were obtained. Indeed, almost all expressed interest in coming back to future workshops. Leslie Atkinson, presenter of the Mother/Child attachment problem said that he was “blown away” by the progress that had been made on the problem. Chris Bowman from NRC said that a “highly talented and capable bunch of mathematicians” worked on the problem he presented, and that he was “very pleased, and somewhat surprised, at the new insight into the problem” that they provided. On their part, the academic participants also felt that it was a useful and enjoyable experience.

“Leslie Atkinson… was “blown away” by the progress that had been made on the problem”
On Friday, May 5th, the SNAP Mathematics Foundation, founded by Jim Timourian, launched SNAP Math Fairs in Ontario through a conference at the Fields Institute. Educators from across Canada were inspired by the idea of SNAP Math Fairs, which introduce students to classic old puzzles and problems. The students solve and then build a creative, interactive, hands-on project which includes a model which can help to solve the problem. SNAP math fairs are an opportunity for a school community to gather together to celebrate mathematics!

Tanya Thompson, a teacher from Simcoe County DSB, organized the conference and presented details about the fairs. She described what a math fair is, what SNAP means, how to bring a math fair to a school, and the many benefits to students of participating in a fair. Dr. Ed Barbeau, a professor emeritus of mathematics at the University of Toronto, shared his belief that math fairs provide an excellent opportunity for students to become familiar with some of the main stories, problems and applications of mathematics, as well as to become participants in, rather than observers of, the mathematical enterprise. Suhana Kadoura, a teacher from the Ottawa Carleton Board, talked on the wonderful results she found when her school did a math fair for the first time this year. She also highlighted the necessary links that math fairs have to our Ontario Curriculum Expectations. Tiina Hohn, a professor from Grant MacEwan College in Alberta and a board member of SNAP, presented engaging hands-on puzzles to be used in SNAP Math Fairs. Bill Ritchie, the co-founder and CEO of Thinkfun, the leading manufacturer of mind challenging games, shared some projects in which his company is currently involved. A highlight of the conference was a SNAP Math Fair presented by Nottawa Elementary School. Forty students from Nottawa presented their projects to the participants. The participants had a lot of fun at this fair. The students and their projects were very engaging and the participants could see directly the benefits of doing a math fair. The principal of Nottawa said that the confidence of the students improved immensely from this process and she was duly impressed and appreciative of the fact that her students were enjoying talking about math with the participants for over an hour.

This year’s event, held at McMaster university, was attended by 42 participants. We hosted a lunch each day, and a banquet dinner on the first evening of the event to encourage interaction between seminar attendees.

SOSGSSD 2006 was sponsored by the Department of Mathematics and Statistics and the Department of Clinical Epidemiology and Biostatistics at McMaster University; Fields Institute; SORA; and StatPoint, Inc.

Afisi Ismaila (McMaster)
Workshop on Numerical, Mathematical and Modeling Analysis of Fluid Dynamics in Hydrogen Fuel Cells

Yalchin Efendiev (Texas A&M) presented a rigorous view of mathematical analysis and numerical methods related to multiscale flows and homogenization. It was a nice surprise to “discover” that these techniques (used initially for geophysical applications) may be of interest in fuel cell analysis.

Peter Minev (Alberta) presented a very interesting two-phase flow involving modeling methods, numerical analysis and computations. There was special interest in work related to two-phase flow using averaged models (two-phase flow of bubble column dynamics) and the fictitious domains method.

Keith Promislow (Michigan State) presented an excellent example of how one can tackle extremely difficult modeling problems, using mathematical tools, without compromising mathematical beauty!

He presented transient unit cell models, hysteresis and lateral diffusion and nanophase models.

The workshop fully met its objectives. Problems important to fuel cell dynamics were presented from different viewpoints. An interaction between mathematicians and engineers was established and the student motivation raised!

Arian Novruzi
(University of Ottawa)

“As is always the case, it is not possible in the few pages available to us to report fully on all the Fields activities that have taken place since May. Several of these took place on our PSU campuses. Carleton hosted three such events: The Applied Probability Workshop from June 1 – 3 was organized by Zhicheng Gao, Antal A Járai, Daniel Panario and Yiqiang Zhao; the Ottawa-Carleton Discrete Mathematics Workshop was held May 12 – 13 and organized by Lucia Moura, Brett Stevens and Steven Qiang Wang; a conference on Geometric Methods in Group Theory was organized by Inna Bumagin and Benjamin Steinberg from Aug 16-19. The University of Ottawa hosted a summer school on Valuation Theory and Integral Closures in Commutative Algebra organized by Steven Dale Cutkosky, Sara Faridi, Franz-Viktor Kuhlmann and Irena Swanson. It was also the site of a workshop on Probabilistic Symmetries and Their Applications from May 15-17 2006 organized by Gail Ivanoff and Raluca Balan. George Gadanidis organized an event entitled Digital Mathematical Performance Workshop which took place at Western from June 8 – 11 and addressed the questions: What is a performance mathematician and how might we understand the teaching and learning of mathematics through the lens of performance? The University of Waterloo was the site of the Modeling and Optimization: Theory and Applications conference from July 24-27. The organizing committee was headed by Tony Vannelli and Henry Wolkowicz.”
ACTUARIAL RESEARCH COMMUNITY IN North America has a concentration in Southwestern Ontario and the Midwest US. The University of Western Ontario (UWO) finds itself at the centre of a local cluster of fellow universities with actuarial researchers: the University of Toronto, the University of Waterloo and the University of Michigan. The objective of our one-day event was to discuss the actuarial research being pursued on these campuses. An important aspect of the June 1st gathering at UWO was the fact that many discussants attended from the actuarial community across Canada.

The day’s workshop comprised a spectrum of presentations on timely actuarial topics from risk theory to finance, and their application in insurance and employee benefits. Actuarial researchers from across Canada gathered at this event. The ensuing lively discussions raised important issues, and generated new ideas for further study.

Ragnar Norberg (London School of Economics) gave a keynote address entitled Risk and stochastics. He spoke of “the dazzling beauty and great power” of stochastics that have influenced the development of insurance mathematics over the past century. He provided glimpses of the history, views of the present, and visions of the future.

Kristen Moore (University of Michigan) gave an invited lecture on Optimal strategies for equity-indexed annuity investors. She focused on a free-boundary problem that describes the optimal behavior for an EIA investor who seeks to maximize the expected discounted utility of bequests, describing how the financial parameters, mortality assumptions, and product features affect the optimal strategy.

Sebastian Jaimungal (University of Toronto) gave an invited address Indifference pricing for equity-linked (re)insurance products. Sebastian illustrated how insurance companies are increasingly facing losses that have heavy exposure to capital market risks through the issuance of equity-linked insurance policies. He outlined how the principal of equivalent utility provides insurance premiums within this context. He went on to discuss the related problem of pricing double-trigger reinsurance contracts. Such contracts provide a payoff that is a function of the risky asset and losses providing the insurer with a vehicle to offload unwanted risks.

The next invited lecturer was Jiandong Ren (University of Western Ontario) who spoke on Underwriting cycle and ruin probability. He proposed a model for analyzing the impact of underwriting cycles on an insurer’s surplus. The model allows the insurer to vary its security loading in response to the cycles, with a strategy parameter that indicates the extent to which the insurer follows the loading which prevails in the market. Jiandong presented Lundberg-type upper bounds which are suitable and convenient for comparing ruin probabilities under the different insurer strategies.

Mary Hardy (University of Waterloo) gave the day’s final invited address, entitled The Canadian insured lives longevity project. Longevity improvements have contributed to widespread underfunding of pension plans, and losses in insured annuity portfolios. Mary explored mortality trends apparent in Canadian life insurance data with an adapted Lee-Carter approach, using population data to benchmark the insured lives data.
SYMMETrY AND SPACES:
A Conference on the Occasion of Gerry Schwarz’s 60th Birthday

The conference was organized by Hanspeter Kraft, Loek Helminck, David Wehlau and Eddy Campbell, and took place July 10–14, 2006, at the Fields Institute.

There were 14 speakers: Abraham Broer, Corrado DeConcini, Gene Freudenberg, Peter Heinzner, Friedrich Knop, Bertram Kostant, Hanspeter Kraft, Peter Littelmann, Christine Riedtmann, James Shank, Thierry Vust, Nolan Wallach, David Wehlau, and Jerzy Weyman. The talks at the workshop reflected the depth and breadth of Gerry’s work and the interest it has generated over many years. More than 40 mathematicians attended the meeting, including several graduate students and postdoctoral fellows.

The theme of the workshop was Algebraic Group Actions and Geometry, including Reductive Group Actions, Classical and Modern Invariant Theory, Linearization, G-Invariant Differential Operators and Symmetric Varieties. In addition to the talks there was plenty of time set aside for discussion. Participants expressed their appreciation for this format which allows the ideas that arise during the talks to be pursued at some length during the week.

Gerry Schwarz received his PhD from MIT in 1972 under the supervision of I. Singer. His early work was on properties of \( C^\infty \)-functions and properties of smooth actions of compact groups. His seminal work “Lifting smooth homotopies of orbit space in IHES” marks the beginning of his interest in algebraic groups. He recognized that the solution of the homotopy/isotopy lifting problem required algebraic groups. He continued to work in algebraic groups while expanding his interests in many directions. Today Gerry Schwarz is one of the foremost specialists in invariant theory, algebraic group actions and invariant differential operators.

After a 2-year post-doc at the University of Pennsylvania, Gerry joined the faculty at Brandeis University in 1974, where he was promoted to Full Professor in 1982. In 1975–76 he visited the Institute for Advanced Study. His co-workers and students benefit from his broad knowledge, deep insight, personal warmth and generous nature. He was an Invited Speaker at the ICM in Zürich in 1994. His publications – over 40 in number – appear in such prestigious journals as IHES, Inventiones Mathematicae, Commentarii Mathematici Helvetici, and the Duke Mathematics Journal. He was a Managing Editor of “Transformation Groups” from 1995-2000.

Among his many accomplishments in several areas, Gerry constructed the first counter-example to the linearization problem: in 1989, he used the proofs of Quillen and Suslin of Serre’s conjecture to construct examples of algebraic actions of complex reductive groups on affine space which can not be linearized. Those examples led to many new results in this particularly active area.

Although many speakers were interested in “roasting” Gerry, the embarrassing stories were all about his friends, students and colleagues.

Eddy Campbell (Memorial) and David Wehlau (Queen’s, and RMC)
Workshop on Computational and Combinatorial Commutative Algebra

This summer between July 24 and August 4, 2006, the Fields Institute became a popular destination for researchers working in the “three C’s” of Computation, Combinatorics and Commutative Algebra. The exciting mixture of perspectives from these distinct fields allows for a simultaneous approach to a wide range of mathematical problems. Solutions arising from this combined approach have an impact on nearby fields, such as algebraic geometry, and lead to unexpected insights in areas such as partial differential equations and biological modelling. The mathematics discussed encompassed classical unsolved problems (for example the commuting scheme conjectures) and new prospects in algebraic statistics, biomathematics and image processing.

“The exciting mixture of perspectives from these distinct fields allows for a simultaneous approach to a wide range of mathematical problems.”

The talks highlighted the successful and innovative use of the computer algebra package Macaulay 2, developed by Daniel Grayson (U. Illinois, Urbana-Champaign) and attendee Mike Stillman (Cornell University). Available at www.math.uic.edu/Macaulay2/, this sophisticated research tool unleashes its full power only to those who have a solid understanding of basic homological algebra methods and their applications.

The first week consisted of introductory talks in the mornings and tutorials in the afternoons led by the morning speakers. Most of the 36 participants (19 graduate students, 8 postdocs) were already familiar with some aspects of computer algebra applications from their own research. The hands-on tutorials, executed on laptops in the Institute’s Library, demonstrated the full potential of experimentation and programming in understanding solution varieties of polynomial or exterior systems of equations. Special emphasis was placed on how to prepare and distribute documentation that allows others to access packages and routines for their own research.

The second week focused on current research. The 43 participants, including 20 graduate students and 9 postdocs, came from 29 different departments across Canada and the United States, and reflected the inclusive nature of the field. As noted by several of the participants, four of the eighteen speakers were women. The talks, delivered by graduate students, postdoctoral fellows and senior faculty, included reports on research in hypergeometric systems of differential equations, (hyper-)graph theory, reverse engineering of biological networks, intersection theory on toric varieties, and the classical problem of the structure of secant varieties.

Many of the participants commented on how enjoyable the atmosphere at the conference was both mathematically and socially. In the latter case, the trip to Niagara Falls, including a wine tasting in Niagara-on-the-Lake, should be singled out. Special thanks also goes to Sonja Mapes (Columbia University) and Sonja Petrovic (University of Kentucky) for co-ordinating many outings and activities in the evenings.

We would also thank the Fields Institute and the University of Toronto for providing financial support.

Ragnar Buchweitz (Toronto), Greg Smith (Queen’s), Alexander Yong (Fields/Minnesota)
Call for Proposals, Nominations, and Applications

For detailed information on making proposals or nominations, please see the website: www.fields.utoronto.ca/proposals

General Scientific Activities*

Proposals for short scientific events in the mathematical sciences should be submitted by October 15 or March 15 of each year, with a lead time of at least one year recommended. Proposals will be considered at other times as funds permit. Activities supported include workshops, conferences, seminars, and summer schools. If you are considering a proposal, we recommend that you contact the Director, Barbara Keyfitz (bkeyfitz@fields.utoronto.ca) or Deputy Director, Juris Steprans (deputydirector@fields.utoronto.ca).

Thematic Programs*

Deadlines for letters of intent and proposals for semester or year-long programs at the Fields Institute are March 15 and August 31 each year. Organizers are advised that a lead time of several years is required, and are encouraged to submit a letter of intent prior to preparing a complete proposal. They may consult the directorate about their projects in advance to help structure their proposal.

Postdoctoral Opportunities

Applications are invited for postdoctoral fellowship positions for the 2007-2008 academic year. The thematic program on Operator Algebras will take place at the Institute from July-December 2007, while the thematic program on New Trends in Harmonic Analysis will run from January-June 2008. Qualified candidates who have recently completed a PhD in a related area of the mathematical sciences are encouraged to apply. The fellowships provide for a period of engagement in research and participation in the activities of the Institute. They may be offered in conjunction with partner universities, through which a further period of support may be possible. One recipient will be awarded the Institute’s prestigious Jerrold E. Marsden Postdoctoral Fellowship. Applicants seeking postdoctoral fellowships funded by other agencies (such as NSERC or international fellowships) are encouraged to request the Fields Institute as their proposed location of tenure, and should apply to the address below for a letter of invitation. Additional support is available from NSF to support junior US visitors to this program. Applications are encouraged from all qualified candidates, particularly aboriginal peoples, persons with disabilities, members of visible minorities and women.

The deadline for postdoctoral applications for the 2007-2008 programs is December 7, 2006.

CRM–Fields–PIMS Prize

Nominations are invited for this joint prize in recognition of exceptional achievement in the mathematical sciences. The candidate’s research should have been conducted primarily in Canada or in affiliation with a Canadian university.

Nominations for the CRM-Fields-PIMS Prize should reach PIMS by October 1, 2006.

Submit files to: c/o Alejandro Adem, PIMS Central Office, 200-1933 West Mall, University of British Columbia, Vancouver BC V6T 1Z2 CANADA

Distinguished Lecture Series In Statistical Science (DLSS)

Nominations are being solicited for the seventh Fields Institute Distinguished Lecture Series in Statistical Science, to be given in Spring, 2007. The awardee will be an internationally prominent statistical scientist, who will give two lectures (one general, one specialized) at the Fields Institute.

Nominations for the DLSS should reach the Institute by October 1, 2006.

* A note on diversity. In proposing any activity, applicants are requested to consider the mandate of the Institute to broaden and enlarge the community. Applicants should explain how they plan to include women and members of visible minority groups in the proposed activity. As well, they should ensure that the proposed participant lists include scientists representing a range of career levels, types of institutions and geographical locations in Canada and abroad.

Please send applications, nominations, and proposals to:

The Director, Fields Institute
222 College Street, Toronto, Ontario, M5T 3J1 Canada
CRYPTOGRAPHY*
Organizers: I. Blake, A. Menezes, M. Mosca, K. Murty, A. Stein, R. Scheidler, R. Venkatesan, H. Williams
SEPTEMBER 18-20, 2006
Algebraic Curves in Cryptography: The 10th Workshop on Elliptic Curve Cryptography (ECC 2006)
SEPTEMBER 25-27, 2006
Coxeter Lecture Series: Professor Gerhard Frey (Institut für Experimentelle Mathematik, Universität Duisburg-Essen)
OCTOBER 2-6, 2006
Quantum Cryptography and Computing Workshop
OCTOBER 30-NOVEMBER 3, 2006
Computational Challenges Arising in Algorithmic Number Theory and Cryptography

GEOMETRIC APPLICATIONS OF HOMOTOPY THEORY*
(Starts January 2007)
Organizers: G. Carlsson, D. Christensen, R. Jardine
JANUARY 9-13, 2007
Higher Categories and their Applications

*This program has received support from the National Science Foundation. Post-doctoral students and junior researchers from US universities are encouraged to apply for funding.

General Scientific Activities

FALL 2006
FRSC Day
SEPTEMBER 14-16, 2006
Probability-Statistics Days on Lorenz-Gini Type Asymptotic Methods in Statistics and their Applications held at Carleton University
SEPTEMBER 15-17, 2006
Conference on Nonparametric Statistics and Related Topics held at Carleton University
OCTOBER 21-22, 2006
Workshop on Algebraic Varieties
NOVEMBER 18, 2006
Graduate Students Day
NOVEMBER 20, 2006
2006 CRM-Fields-PIMS Prize Lectures
Nicole Tomczak-Jaegermann
DECEMBER 7-8, 2006
Connecting Women in Mathematics Across Canada
DECEMBER 11-15, 2006
JANUARY 18-21, 2007
Workshop on the Representation Theory of Reductive Algebraic Groups held at the University of Ottawa
IN AUGUST, I HAD THE PRIVILEGE OF joining the Canadian delegation to the General Assembly of the International Mathematical Union (IMU), as a last-minute replacement for Jon Borwein, who was unable to attend. Being part of this unique exercise in governance in the international mathematical community has given me a chance to observe, among other things, some of the ways that Canadian mathematicians are contributing to this process. Christiane Rousseau not only led our delegation, she also chaired the ‘Resolutions Committee’, at the request of the IMU Executive Committee. This task involved rewriting resolutions under pressure of the closing bell. One direction the IMU is taking is to study the need for a fixed headquarters and professional staff; another is to increase its role in capacity-building in mathematics in the developing world; yet a third is reaffirmation of the connections between mathematical research and mathematics education, as represented by the International Commission on Mathematics Education (ICME), a part of the IMU. Canadian mathematicians already play a role in ICME, where Bernard Hodgson is the Secretary General, and there is certainly a role for Canada in capacity-building.

The relationship between Canada and the IMU continued to play out at the International Congress itself, which began on August 22 in Madrid with the much awaited announcement of the Fields Medal winners. Of course, the Fields Medals take their name from John Charles Fields (1863-1932), native of Hamilton, Professor at the University of Toronto, who was responsible for bringing the International Congress to Toronto in 1924, marking the first time this event had been held in Canada. Fields generously endowed the medals, and set the distinguishing criterion: that the awardee be a person with great potential for future achievement, as well as significant recent accomplishments. This year, there was an additional connection with Canada: the prize selection committee, whose identity is secret until the winners are announced, included Don Dawson, director of the Fields Institute from 1996 to 2000. Musing on the task of the committee, Don echoed John Ball, President of the IMU, “There are so many exciting recent developments in mathematics that it is a difficult but important task to pick the most exceptional. We were guided by the three-fold charge to the committee: select at least two and preferably four winners; observe the strict age limit (under 40 on January 1, 2006); and strive to represent the diversity of mathematics. This year’s winners, Andrei Okounkov (mathematical physics, USA), Grigori Perelman (topology, Russia), Terence Tao (analysis, USA) and Wendelin Werner (probability, France) are not only outstanding, but form an outstandingly diverse group. It was an honour to serve on this committee.”

The Fields Institute is sometimes, mistakenly, given credit for the medal itself. When the Institute was formed in 1992, the name Fields was chosen to honour a visionary mathematician who worked hard to raise the sights of the mathematics community in Canada, and to increase communication among mathematicians worldwide. The medal is, and will remain, an international prize awarded by the International Mathematical Union. But along with mathematicians worldwide the Fields Institute joins in celebrating the achievements of the winners. We look forward to welcoming them – or welcoming them back – to Fields.

Canadian representation among the speakers at the 2006 ICM was also particularly strong this year, with six Canadians among about 190 invited speakers. They are Henri Darmon (McGill), François Lalonde (Université de Montréal), Grigory Mikhalkin (Toronto), Michael Shub (Toronto), Godfried Toussaint (McGill) and Vinayak Vatsal (UBC). Our congratulations to this distinguished group, and appreciation for the help many of its members have given to Fields.