Centre for Information Security and Cryptography

Welcome to the University of Calgary's Centre for Information Security and Cryptography (CISaC), an academic research centre housed within the Department of Mathematics & Statistics, and supported and administered by the Faculty of Science.

We are a multidisciplinary centre that focuses on research in cryptography and information security. Together, our team of researchers and students in mathematics, computer science and electrical and computer engineering is collaborating on projects to improve computer security and protect information in every facet of daily life.

Partners and Sponsors

Dr Hugh Williams, iCORE Chair, Information Security anc Cryptography

CISAC MEMBERS

CISaC Management Board
- Dr Hugh Williams

CISaC Management Board
- Dr Vassil Dimitrov
- Dr Michael J. Jacobson, Jr.
- Dr Renate Scheidler

Support Staff
- Susan Schuck
- Betty Teare
- Marc Wrubleski

Graduate Students in Mathematics and Computer Science
- Richard Cannings
- Kell Cheng
- Chris Foster
- Brendan Oseen
- Reg Sawilla
- Kjell Wooding
- Andreas Hirt

Affiliated Faculty
- Dr Richard Cleve
- Dr Clifton Cunningham
- Dr Behrouz Homayoun Far
- Dr Graham Jullien
- Dr Thomas Keenan
- Dr Richard Mollin
- Dr John Watrous

Post-Doctoral Fellows in Mathematics
- Dr Filip Saidak
- Dr Safuat Hamdy
- Dr Siguna Mueller

DR HUGH WILLIAMS

ALGORITHMIC NUMBER THEORY AND CRYPTOGRAPHY

iCORE Chair
Mathematics and Statistics
University of Calgary

Dr Hugh Williams was awarded $600,000 dollars per year for five years to establish the iCORE Chair in Algorithmic Number Theory and Cryptography at the University of Calgary for a total of $3 million in funding.

EXECUTIVE SUMMARY

The iCORE Chair in Algorithmic Number Theory and Cryptography (ICANTC) has the goal of creating a recognized centre of excellence for education, research and industrial cooperation on computer security at the University of Calgary. As the ICANTC team completes its second year of operation, it is well on track to reaching that goal. At the end of March 2003, a number of key milestones have been achieved.

One significant milestone was the establishment of the Centre for Information Security and Cryptography (CISaC), which was inaugurated July 17th, 2002. In the past year, ICANTC has seen CISaC begin to move from a concept to reality. The development and launch of a Web site and a mission statement helped establish an infrastructure for CISaC, two critical elements to building a membership base and attracting private industry participation. An official launch for CISaC is planned in fall 2003.

Other highlights of ICANTC's activities include further progress toward getting the Advanced Cryptography Laboratory up and running, and successfully applying for a Mathematics for Information Technology and Complex Systems (MITACS) grant. ICANTC team members have continued their research, submitting numerous papers and presentations to various journals and publications. They are also actively recruiting graduate and post-doctoral students and faculty. As a result, two new masters' students and one PhD student began in September 2002. They are expecting a new masters' student in September 2003, Paul Sheridan. They also hope to have three more PhD students. Peter Anderson and Kjell Wooding are confirmed, while the third could be confirmed by the end of April.

As a new fiscal year begins, the team will continue to build on achievements in 2002-2003, making steady progress to reaching goals for 2003-2004. Plans include an official launch of CISaC, cultivation of industrial partnerships, the realization of the cryptographic laboratory, and recruiting an additional assistant professor to the team. In addition, the team continues to work with other institutions in Canada, the United States and abroad. The movement and exchange of students with other universities should become even easier as research progresses. As partnerships are forged with business and industry, it is hoped that student internships in the province will follow.

The group is focused on building the program and cultivating partnerships with other universities as well as industry and government. The strength and commitment to these goals demonstrated by the team, along with the support and enthusiasm of iCORE, should make these objectives a reality in 2003-2004.

RESEARCH GOALS AND OBJECTIVES

In the past year, ICANTC has continued to build upon achievements from 2001-2002. Each accomplishment brings the group closer to our goal of making the University of Calgary a recognized centre of excellence for education, research and industrial cooperation on computer security issues in Canada.

The most significant accomplishment is the progress toward establishing a Centre for Information Security and Cryptography (CISaC) at the University of Calgary. CISaC is a multidisciplinary centre that focuses on research in cryptography and information security. Together, CISaC's team of researchers and students in mathematics, computer science and electrical and computer engineering is collaborating on projects to improve computer security and protect information in every facet of daily life.

ONE SIGNIFICANT MILESTONE WAS THE ESTABLISHMENT OF THE CENTRE FOR INFORMATION SECURITY AND CRYPTOGRAPHY (CISAC), WHICH WAS INAUGURATED JULY 17th, 2002.

By employing a broad depth of skills and knowledge, the team members are testing and establishing protocols to ensure secure communications, with a particular focus on mathematically based cryptosystems. This includes all aspects of work from abstract theory to the fabrication of special-purpose cryptographic and computing hardware devices.

The security of almost all commercially available cryptosystems is based on the presumed difficulty of certain mathematical problems. It is important to emphasize that no rigorous mathematical proof of security has ever been given for any of these systems. The difficulty of these problems is usually established anecdotally through frequent and unsuccessful attempts by specialists to solve them.

One particular part of mathematics, the study of quadratic fields, has not been used very much to produce cryptosystems. One major research project is to conduct a full investigation into the development and testing of efficient encryption techniques based on the difficulty of performing certain operations in quadratic fields.

CISaC is creating a foundation that will allow further development of the research. Activities to expand the research team include:

- Maintaining an active Distinguished Visitors' Program to bring top researchers to the University of Calgary;
- Recruiting top students at all levels – undergraduate, masters, PhD and post-doctorate – to be part of the program;
- Offering new undergraduate courses as part of an area of concentration in cryptography;
- Working on a sequence of graduate courses in cryptography that could be accessed by students in mathematics, computer science and engineering;
- Cultivating partnerships with other universities as well as industry and government.

The goal is to broaden CISaC's membership beyond the university, and evolve it into an established centre with links to local businesses and national industry partners.

Other milestones related to CISaC this past year include:

- Building an infrastructure – business cards have been printed and the group is currently developing brochures to promote both academic and business contacts;
- Crafting a mission statement, which captures the centre's goals and objectives;
- Developing a Web site, which provides an information source for students, faculty and other interested parties. See http://cisac.math.ucalgary.ca;
- A management board was appointed to oversee and provide guidance and input on running CISaC's

activities. Currently a director and three members make up the board, but this will expand as the centre grows. The term of office for board members is three years. The management board includes: Renate Scheidler from mathematics and computer science; Michael Jacobson from computer science; and, Vassil Dimitrov from electrical and computer engineering;

- CISaC is also considering setting up a Technical Advisory Panel to provide expertise on specific projects as needed. The initial panel would be comprised of management board members, three researchers from the University of Calgary and three from the industrial sector. The make-up of the panel will be relative to the need that it is required to fulfill.

Other ICANTC accomplishments include:

- Continuing to develop undergraduate and graduate courses in cryptography. Renate Scheidler developed and taught a new fourth year special topics course in cryptography, which was offered in winter 2003. Hugh Williams also developed and taught a graduate course PMAT 603.40: Topics in Computational Number Theory;
- A concentration in cryptography will come on line in September 2003. Renate Scheidler will teach PMAT 329. Richard Mollin will teach PMAT 429 in winter 2003. These courses will run yearly. PMAT 529 will come online in fall 2004 and is the third course in our PMAT 329/429/529 sequence. Teaching assignments have not yet been made for this course;
- Coordinating our graduate and undergraduate courses with Michael Jacobson in computer science. Hugh Williams will teach PMAT 603.38. Michael Jacobson has already taught it under the course descriptor CPSC 699. Michael Jacobson is also developing a follow-up course to PMAT 329 for computer science students that he will offer in winter 2003, at the same time as the math follow-up course PMAT 429 is being offered. This course does not yet have a number, and will focus on computer security. The idea is that math students will take PMAT 329/429/529, while computer science students will take PMAT 329 and Michael Jacobson's new course;
- The Distinguished Visitors' Program, piloted last year by Renate Scheidler, began again in September 2002. The program continues to bring internationally regarded experts to the University of Calgary. Jerzy Urbanowicz from the Polish Academy of Sciences was here August 18th to September 12th; Jonathan Borwein of Simon Fraser University was here on October 18th; and, Stéphane Louboutin, from Institut de Mathématiques de Luminy in Marseilles, France, was here November 15th to December 15th. The team welcomed Roger Patterson in September to October 2002, and Catherine Webster from the University of British Columbia in March 2003;
- ICANTC continued the campaign to recruit graduate students, post-doctoral students and faculty. Three new students began in fall 2002. They are Christopher Foster (MSc), Reginald Sawilla (MSc), and Kell Cheng (PhD). One new masters' student is confirmed for September 2003. Two more PhD students have also been confirmed, with the potential for a third to be confirmed by the end of April. The group is currently developing two new brochures, one targeted at potential students, and the other at potential corporate members; also they have completed a display board for the Faculty of Science that will sit in the case in the corridor outside the Dean's office;
- Alfred Menezes at the University of Waterloo and Hugh Williams have been jointly awarded

$120,000 from MITACS. Dr Williams' half of the funds is already committed to: developing a Web site for the MITACS project, holding a major conference on privacy in Alberta, and funding a post-doctoral fellow who will conduct research in the development of very low power consuming cryptographic protocols for use in wireless medical monitoring systems. These funds should be available toward the end of April 2003. This grant is for one year with the possibility of a second year extension if the year-end report is acceptable;

- ICANTC has received permission to hire an associate professor with a cryptography background. The closing date for applications was March 15th, and the proposed starting date is July 1st, 2003. The interviewing process for this position is complete, and an offer has been made.

The Advanced Cryptography Laboratory is now up and running. Work on the lab began in February 2003. In a short time, a space agreement was drafted, appropriate renovations were done and the necessary equipment was ordered. Preliminary tests began in mid-March, and were completed at the end of the month. This laboratory was made possible through the merging of Hugh Williams' Alberta Ingenuity Fund grant with Michael Jacobson's CFI grant. The Advanced Cryptography Laboratory consists of an extensive, powerful and dedicated system of high-speed computing devices used to test and benchmark cryptographic systems. The hardware in the laboratory is configured on the Beowulf cluster design, where many commodity-grade processors are interconnected using commodity hardware. The head node monitors these many processors and controls what jobs are running on the system. This cluster consists of 129 computers interconnected using Ethernet (100Mbps). Each computer has Dual 2.4 Ghz Pentium 4 processors, 2 GB memory, and a 40 GB hard disk. The head node has a 2.4 Ghz processor, 1.5 GB memory, and 40 GB of usable disk space. This system has a theoretical maximal processing power of 1.2 Teraflops. IBM supplied the innovative Blade Center solution to enable the system to fit in less than half the space of conventional systems. This solution was easier to build, and is easier to maintain than conventional systems. The system is configured to allow us to build and run computer programs utilizing the Message Passing Interface (MPI). MPI is an add-on to programming languages that enable programs to run on many systems at a time and to take advantage of the processing power of the entire system.

Other Advances:

- Together with Lynn Batten of Deakin University in Melbourne, Australia, the group applied to the Australian National University Centre for Mathematics and its Application National Research Symposia Committee to hold a workshop on Polynomial Aspects of Cryptography. The application was successful with the award of AUD$7,500 to help defray some of the costs in holding this meeting, likely in July 2004. The conference will bring together 30 experts across the fields of algebra, cryptography and algorithm implementation in an Oberwolfach-style meeting. Half of the people will be from Australia and the other half from North America and Europe. The results of this workshop will have a major impact on the direction of this area of cryptography for the next five to 10 years.
- The team continues to move forward in building a partnership with the Illinois Center for Cryptography and Information Protection at the University of Illinois at Urbana-Champaign.

As indicated earlier, one of the principle foci of our research is investigating the use of quadratic fields in cryptography. Results from many different areas of mathematics have been applied to the development of cryptographic systems. One reason for this is that it is always sound cryptographic practice to have access to as many different systems as possible. This ensures that the sender has a choice of possible schemes, a very useful feature if one or more of them is compromised.

One area of mathematics that has not received much attention from cryptographers is algebraic number theory. The simplest number fields are the quadratic fields. Performing arithmetic in these structures is relatively efficient and simple compared to doing this in other algebraic number fields. Nevertheless, they still possess many of the complicating features that make them resistant to methods that have proved to be successful in other structures such as finite fields. The group has developed methods of performing certain fundamental cryptographic protocols, but as yet, these are too slow for commercial use.

There are two main long-term objectives for this project. One is to develop a set of efficient, easily applicable and mathematically rigorous techniques for performing arithmetic in quadratic number fields and function fields. The second (and primary) objective is to use these ideas to develop and test cryptosystems whose security is based upon the presumed difficulty of solving certain problems in these structures. The mathematical results of the research are expected to be useful in developing methods for performing arithmetic efficiently in the structures under investigation. Furthermore, the results are expected to add to the growing number of techniques for ensuring secure communication.

Improved Implementation

In the case of our protocol involving real quadratic fields, we developed a new representation for the objects (called ideals) on which we must perform our operations. This has allowed us to lower considerably the numerical precision needed at the expense of increasing the complexity of a second communication round. It turns out that in practice this second round proved to be no real problem as it is rarely needed and executes rapidly in those cases where it is required. We have also succeeded in integrating a particular technique, called NUCOMP, into our protocol. This is significant because we must make frequent use of a particular operation, involving multiplication and reduction of ideals, which takes over 97 percent of the time required to execute the protocol. Implementing NUCOMP has allowed us to cut the amount of time required by the protocol by a factor of more than half. Renate Scheidler recently received a University of Calgary URGC research grant for further work on NUCOMP and related questions, including its extension to hyperelliptic function fields.

Determination of Optimal Discriminants

One advantage to using number fields for cryptographic purposes is that we have some freedom in selecting a certain parameter, the discriminant. However, this parameter needs to be chosen optimally with respect to both security and efficiency of implementation. We have developed a low cost, high-speed special computing device (CASSIE), called a number sieve, to help determine optimal selections. In the case of real quadratic fields, attempts by adversaries to break the corresponding cryptographic scheme can be thwarted by selecting discriminants that are quadratic nonresidues for many of the smallest primes. Previously, we were able to use the fastest number sieve then in existence, constructed in 1995 at the University of Manitoba, to show that finding such discriminants can be done very quickly. We have used more modern field programmable gate array (FPGA) technology to build a faster and more flexible number sieve that can be tailored to a specific sieve problem instance. The project was a collaborative effort involving Hugh Williams, masters' student Kjell Wooding and Dr C. Patterson of Xilinx (Boulder, Colorado). Our new device can sieve at an effective rate of $2 \cdot 10^{15}$ numbers per second. This is 1000 times faster than the 1995 sieve speed.

Benchmarking

There is no rigorous mathematical proof of the security of our (or almost any other) cryptosystem.

The only way to certify security and effectiveness is to test it extensively. We need to conduct very large-scale numerical experiments to acquire the data needed to accurately determine the security of our cryptographic schemes. We have assembled a Beowulf cluster built of IBM components as the hardware configuration for the testing. A Beowulf cluster is a collection of individual stand-alone processors connected together so they can communicate. The cluster, which is scalable, currently consists of 129 2.4GHz Pentium 4 dual processors, each with 2 GB of RAM and 40 GB of hard disk space. The servers are interconnected with standard fast Ethernet connections and provide the required computer power. All software required for the cluster, including the operating system Linux, is free of charge when used for research purposes. The cluster is sufficiently flexible that it can be used to test the effectiveness of many other cryptosystems and can be used well beyond the lifetime of this project. This facility became operable on March 21st, 2003.

Unconditional Determination of the Regulator

One way to test the effectiveness of techniques is to compute a particular object associated with our quadratic field, called the regulator. Unfortunately, the fastest algorithm currently available to determine the regulator is conditional on an unproved hypothesis. It is of great interest to find the regulator unconditionally. The conditional algorithm can at least be used to compute what should be an integral multiple of the regulator, and this is something that can be checked very quickly. Having made this determination, the next problem is to establish that the integral multiplier of the regulator in the conditional regulator is exactly one. There are two phases in doing this. The first is to establish that the regulator must exceed some predetermined bound. The next is to prove that for no integer less than a certain amount can we have the regulator being the conditional one divided by that integer. It is interesting that both of these phases can be parallelized. Furthermore, the technique can, with an appropriate representation of the ideals involved, be completely integral. That is, we do not at any point have to work with any numbers but integers. This means that we do not have to deal with approximations to irrational numbers and the concomitant loss of rigour that often occurs as a result. Michael Jacobson and Hugh Williams are collaborating on this problem and already have some preliminary results. Recently they were able to compute unconditionally a regulator for a quadratic field with a fifty-five-digit discriminant. This was done with only eight processors; thus, when fully parallelized and running on the new Beowulf cluster, the new algorithm should allow us to compute regulators for fields of perhaps 60 or 65 digit discriminants.

Verifying the Cohen-Lenstra Heuristics

The security of certain cryptographic schemes depends upon the number of reduced principal ideals in the quadratic number field (or function field) and the difficulty of solving the discrete logarithm problem in the field. The first of these problems is easily handled using Cohen-Lenstra heuristics on the distribution of the odd part of the class number. However, as the Cohen-Lenstra heuristics are not rigorously established, it is essential that they be thoroughly tested numerically. Recently, in collaborative work between Dr H. te Riele of CWI, Amsterdam, and Hugh Williams, it was possible for the first time to compute all the class numbers for all real quadratic fields of prime discriminant less than 200,000,000,000. The results obtained agreed with what the Cohen-Lenstra heuristics predicted, and a paper describing this work was recently accepted for publication by *Experimental Mathematics*.

Invariants in Function Fields

Renate Scheidler's research focuses primarily on developing and implementing algorithms for computing invariants of cubic function fields as well as exploring these fields for cryptographic applications. Jointly with Dr Yoonjin Lee of the University of Delaware (USA), she has developed an algorithm for computing the fundamental units and the regulator of a purely cubic function field of unit rank two. This research is to appear in the journal *Experimental Mathematics*. It is expected that this summer, one or two research students will continue work on the implementation of this and other algorithms, a project that undergraduate student Eric Nosal began last summer. Work on developing fast arithmetic in arbitrary cubic function fields and on fast algorithms for computing the Jacobian of a purely cubic function field (jointly with Professor A. Stein of the University of Illinois at Urbana-Champaign) is ongoing.

RESEARCH TEAM

TEAM LEADER	TITLE	RESEARCH
Dr Hugh Williams	Professor, Department of Mathematics and Statistics, iCORE Chair in Algorithmic Number Theory and Cryptography, and CISaC Director	Computational number theory, cryptography, and the design and development of special-purpose hardware devices, secure key exchange systems that make use of the properties of quadratic number fields or function fields.
TEAM MEMBERS	**TITLE**	**RESEARCH**
Dr Michael J. Jacobson, Jr.	Assistant Professor, Department of Computer Science and CISaC Management Board Member	Computational number theory and public-key cryptography, invariant computation in quadratic fields, parallel implementations of index-calculus algorithms.
Dr Richard Mollin	Professor, Department of Mathematics & Statistics	Number theory, algebra and computation, including applications to cryptography, continued fraction expansions, Diophantine analysis and cryptographic applications, on the theory of quadratics.
Dr Renate Scheidler	iCORE Research Associate and Associate Professor jointly appointed to the Department of Mathematics and Statistics and the Department of Computer Science; CISaC Management Board Member	Algorithmic number theory and its applications to cryptology, design and analysis of secure communication schemes whose underlying mathematical structure is associated with an algebraic number field or function field.

AFFILIATED FACULTY	TITLE	RESEARCH
Dr Richard Cleve	Professor, Department of Computer Science	Computational complexity theory and cryptography, quantum information processing, quantum algorithms and quantum information theory.
Dr Clifton Cunningham	Assistant Professor, Department of Mathematics and Statistics	Langlands Programme as it relates to the interplay between number theory, analysis and algebraic geometry.
Dr Vassil Dimitrov	Associate Professor, Department of Electrical and Computer Engineering and CISaC Management Board Member	Efficient algorithms and architectures for digital signal processing, information security and image compression applications, applying methods from number theory and algebraic geometry aimed at speeding up the performance of very complex real-time digital signal processing and information security systems.
Dr Behrouz Homayoun Far	Associate Professor, Department of Electrical & Computer Engineering	Engineering of intelligent, distributed and heterogeneous networked systems, specifically in designing and implementing agent-oriented software systems and support tools and techniques for groupware systems.
Dr Graham Jullien	Professor, Department of Electrical and Computer Engineering and iCORE Research Chair in Advanced Technology Information Processing Systems	Integrated circuit design (from architectures to transistors), digital signal processing for real-time (data stream) applications, and microsystem integration of the disparate technologies of ICs, MEMS and microfluidics for bio-medical applications.
Dr Thomas Keenan	Director, e-Security Innovation Centre and Dean, Faculty of Continuing Education	Computer security, cybercrime, society for policing in cyberspace.
Dr John Watrous	Assistant Professor, Department of Computer Science and Canada Research Chair	Quantum computational complexity theory and quantum algorithms, quantum variants of interactive proof systems and quantum algorithms for group-theoretic problems.

POSTDOCTORAL FELLOWS IN MATHEMATICS	TOPIC
Filip Saidak	Analytic and Probabilistic Number Theory
Safuat Hamdy	Number Field Cryptography
Siguna Müller	Public-key Cryptography and Primality Testing

PHD STUDENTS IN MATHEMATICS	TOPIC
Kell Cheng	Simple Continued Fraction Expansions of Quadratics

MCS STUDENTS IN MATHEMATICS	TOPIC	AWARDS
Richard Cannings	Quantum Computation and Cryptography	
Chris Foster	Diophantine Equations	
Brendan Oseen	Isogenies of Elliptic Curves	
Reginald Sawilla	Algorithms in Quadratic Fields	
Kjell Wooding	Development of a High-speed Numerical Sieving Device	Alberta Ingenuity

GRADUATE STUDENTS IN COMPUTER SCIENCE	
Andreas Hirt	Collaborative Caching in Ad hoc Networks

NEW STUDENT VISITORS IN MATHEMATICS	INSTITUTION/PERIOD OF VISIT
Daniel Weimer	Technical University of Darmstadt, June 2nd, 2003 to May 31st, 2004
Robbert de Haan	University of Amsterdam, April 29th to October 31st, 2003
Roger Patterson	Macquarie University, May 13th to July 10th, 2003

COLLABORATIONS

ICANTC's goal is to position Alberta as a centre of excellence in cryptography that attracts established research leaders, young academics beginning their careers, and graduate students seeking the best education opportunities. As well as attracting top talent, we are committed to seeing results emerging from our research. We cannot achieve these results alone, so we are focused on building strong partnerships with other academic institutions, government and industry.

Now that the Centre for Information Security and Cryptography (CISaC) is a reality, our plan is to develop partnerships with other such centres around the world. We are currently completing a formal partnership agreement with the Illinois Center for Cryptography and Information Protection (ICCIP) at the University of Illinois at Urbana-Champaign.

We are also beginning to negotiate with Professor Hans Dobbertin of Ruhr-Universität Bochum for a partnership with his cryptographic group. We also hope to initiate a program of acquiring further partnerships with groups at the University of Waterloo, the Technical University of Darmstadt, Simon Fraser University and several others.

Alfred Menezes of the University of Waterloo and Hugh Williams have been informed that, as co-investigators, they have been jointly awarded $120,000 from MITACS. Hugh Williams' half of the funds is already committed to the development of a Web site for the MITACS project, hosting a major Alberta conference on privacy, and funding a postdoctoral fellow who will be conducting research in the development of very low power consuming cryptographic protocols for use in wireless medical monitoring systems. These funds should be available toward the end of April 2003. This grant is for one year, with the possibility to extend it a second year.

AS WELL AS ATTRACTING TOP TALENT, WE ARE COMMITTED TO SEEING RESULTS EMERGING FROM OUR RESEARCH. WE CANNOT ACHIEVE THESE RESULTS ALONE, SO WE ARE FOCUSED ON BUILDING STRONG PARTNERSHIPS WITH OTHER ACADEMIC INSTITUTIONS, GOVERNMENT AND INDUSTRY.

We had an exchange agreement with Macquarie University in Australia that provided funding for students and faculty exchanges. This agreement ended December 31st, 2002.

We are collaborating with Graham Jullien's group in the University of Calgary's department of electrical and computer engineering to develop a small, wireless device that can be implanted in patients and used to transmit data over very short distances. Such devices will undoubtedly become important over the next few years for the low-cost, widespread monitoring of patients for a variety of medical conditions. The misuse of such data could have disastrous consequences to the individual; therefore, such devices must be equipped with appropriate safeguards capable of encrypting sensitive medical data to protect it from unauthorized access. Such encryption must be performed quickly and reliably, and at the same time consume very low power.

We are currently working with Graham Jullien on putting together an NSERC Strategic Project Grant to help support our work in this regard. In doing this, it will also be necessary to involve some local industries. We have already contacted SiWorks Inc. and found them to be very interested in participating, and will soon be talking to Non-Elephant Encryption Systems, Inc. (NE2) about their participation.

We have also begun consulting work with another local industry: IQ Soft Professionals, Inc. (IQSP).

These collaborations are forming the base from which we will continue to build. Our future plans are to broaden our partnerships to include more government and industry.

A hiring freeze at the University of Calgary has prevented filling an additional academic position that was proposed in the original budget.

FUNDING

The Alberta Government has invested $131,000 in the current year in addition to the iCORE funding of $600,000 per year over five years. University investment totals over the next year are $33,900 cash and $136,300 in-kind. CFI funding for the current year is $58,000; NSERC funding is $95,000. Other government income for the current year is $48,500. Contracts with the US National Security Agency and the US. National Science Foundation are for $17,000 and $3,600 respectively.

INTELLECTUAL PROPERTY

In the two years since iCORE created ICANTC, the team has focused on establishing the program and reaching some early goals. One of the most significant accomplishments has been the establishment of CISaC as an interdisciplinary centre dedicated to research in cryptography and information security.

Now that the centre is established, the team is confident more partnerships will develop between academia and the private sector. There is potential for joint projects with Professors Jullien, Dimitrov, and Far of the University of Calgary's electrical and computer engineering department. As these partnerships mature, there will be advancement in terms of intellectual property and commercial results.

PUBLICATIONS

Refereed Journal Contributions

1. F. Saidak, "An Elementary Proof of a Theorem of Delange," *Comptes Rendus (Canada)*, vol. 6, to appear in December 2002 (or March 2003).
2. F. Lemmermeyer and R. Mollin, "On the Tate-Shafarevich groups of $y^2=x(x^2-k^2)$," to appear *Acta Math. Universitatis Comenianae.*
3. H. te Riele and H.C. Williams, 'New Computations Concerning the Cohen-Lenstra Heuristics," to appear in *Experimental Mathematics.*
4. J.D. Hühnlein, M.J. Jacobson, Jr., and D. Weber, "Towards Practical Non-interactive Public-key Cryptosystems Using Non-maximal Imaginary Quadratic Orders," to appear in *Designs, Codes, and Cryptography*, 2003.
5. M.J. Jacobson, Jr., Á. Pintér, and P.G. Walsh, "A Computational Approach for Solving $y^2 = 1^k + 2^k +...+ x^k$," to appear in *Math. Comp.*, 2003.
6. M.J. Jacobson, Jr. and H.C. Williams, "New Quadratic Polynomials with High Densities of Prime Values," *Math. Comp.*, vol. 72, 2002, pp. 499-519.
7. M.J. Jacobson, Jr. and H.C. Williams, "Modular Arithmetic on Elements of Small Norm in Quadratic Orders," *Designs, Codes and Cryptography*, vol. 27, 2002, pp. 93-110.
8. R.A. Mollin, "Criteria for Simultaneous Solutions of $X^2-DY^2=c$ and $x^2-Dy^2=-c$," *Canadian Math. Bulletin*, vol. 43, 2002, pp. 428-435.
9. R.A. Mollin, "Ideal Criteria for Both $X^2-DY^2 = m_1$ and $X^2-DY^2=m_2$ to have Primitive Solutions for any Integers m_1, m_2 prime to $D>0$," *Serdica Math. Journal*, Bulgarian Academy of Sciences, vol. 28, 2002, pp. 175-188.

10. R.A. Mollin, "A Brief History of Factoring and Primality Testing B.C. (Before Computers)," *Math. Magazine*, February 2002.
11. R.A. Mollin, "The Diophantine Equation AX^2-BY^2=C and Simple Continued Fractions," *International Math. Journal*, vol. 2, 2002, pp. 1-6.
12. R.A. Mollin, K. Cheng, and B. Goddard, "Pellian Polynomials and Period Lengths of Continued Fractions," *JP Journal Alg., Number Theory and Applications*, vol. 2, 2002, pp. 47-60.
13. R.A. Mollin and K. Cheng, "Continued Fraction Beepers and Fibonacci Numbers," *Math. Rep. Acad. Sci. Canada*, vol. 24, 2002, pp. 102-108.
14. R.A. Mollin, "Period Lengths of Continued Fractions Involving Fibonacci Numbers," to appear in *Fibonacci Quarterly*.
15. R.A. Mollin, "Sums of Squares Revisited," to appear *Inter. Math Journal*.
16. R.A. Mollin, "Infinite Families of Pellian Polynomials and Their Continued Fraction Expansions," to appear in *Results in Mathematics*.
17. R.A. Mollin and K. Cheng, "Beepers, Creepers, and Sleepers," *Intern. Math. Journal*, vol. 2, 2002, pp. 951-956.
18. R.A. Mollin, "New Prime-producing Polynomials Related to Class Number One or Two," *New York Journal Math*, vol. 8, 2002, pp. 161-168.
19. R.A. Mollin, B. Goddard, and K. Cheng, "The Diophantine Equation AX^2-BY^2=C Solved Via Continued Fractions," to appear in *Acta Mathematica Universitatis Comenianae*.
20. R.A. Mollin and K. Cheng, "Matrices and Continued Fractions," *Intern. Math. Journal*, vol. 3, 2003, pp. 41-58.
21. R.A. Mollin, "Cryptography - A Brief History," to appear in *CUBO, Journal of Universidad de la Frontera*, Temuco, Chile.
22. S. Müller, "On the Computation of Square Roots in Finite Fields," to appear in *Designs, Codes, and Cryptography* (DESI1165-01).
23. S. Müller, "A Probable Prime Test with Very High Confidence for n=3 mod 4," *Journal Cryptology*, vol. 16, no. 2, 2003, pp. 117-139.
24. S. Müller, "On the Computation of Cube Roots Modulo p," to appear in *Fields Institute Communications Series*.
25. Y. Lee, R. Scheidler and C. Yarrish, "Computation of the Fundamental Units and the Regulator of a Cyclic Cubic Function Field," to appear in *Experimental Mathematics*.

Books and Book Chapters

1. R.A. Mollin, *RSA and Public-Key Cryptography*, Chapman and Hall/CRC Press, Boca Raton, New York, London, Tokyo, 2003. ISBN # 1-58438-338-3

Please join us

for the launch of the
Centre for Information
Security and Cryptography

Are your secrets safe?

- **90% OF COMPANIES HAVE HAD SOME SORT OF INFORMATION PRIVACY INVASION.**
- **MOST PERSONAL COMPUTERS ARE NOT PROTECTED AGAINST INVASION OF PRIVACY.**

The Centre for Information Security and Cryptography is an academic research centre housed within the Department of Mathematics and Statistics, and supported and administered by the Faculty of Science at the University of Calgary. It works on the mathematical building blocks of encryption systems that keep private information private.

The launch of the Centre includes the opening of Canada's premiere Advanced Cryptography Laboratory, located at the University of Calgary.

Friday October 10
10:30 am – 12:30 pm
Rozsa Centre Great Hall
University of Calgary

10:30 - 11:00 am	Launch
11:00 - 11:30 am	Book signing
11:30 - 12:30 pm	Public lecture

CALGARY KICK-OFF EVENT
SCIENCE & TECHNOLOGY
WEEK 2003
OCTOBER 10-19