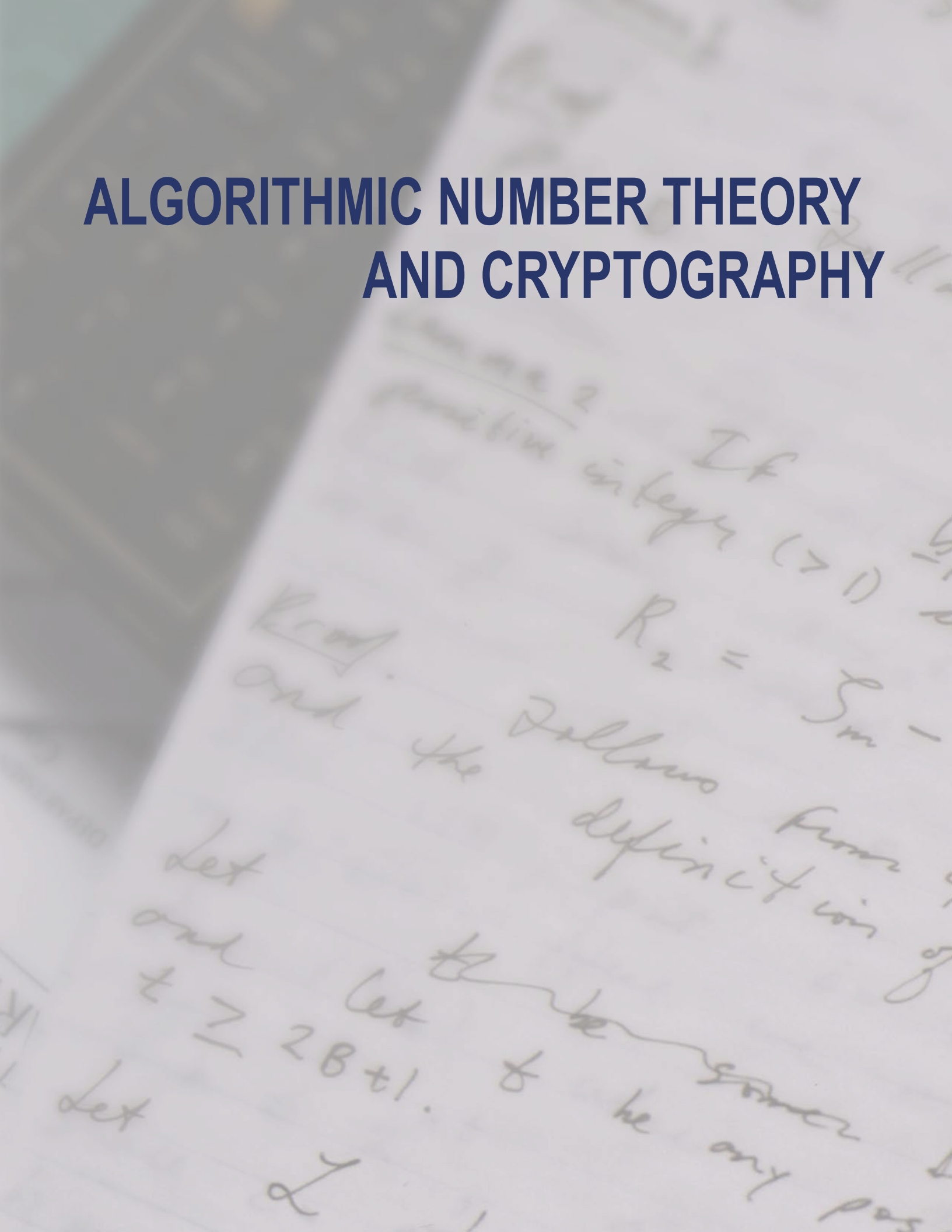
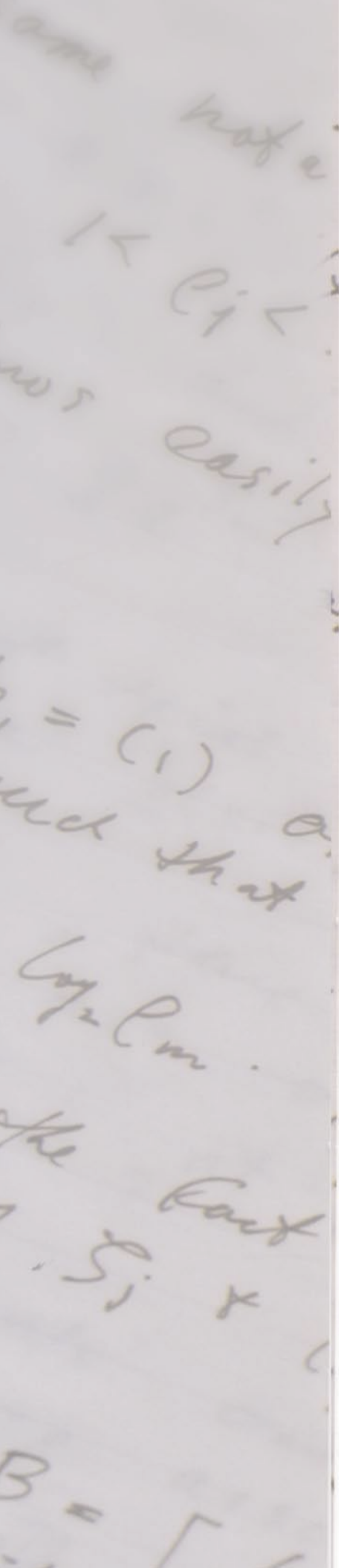
ALGORITHMIC NUMBER THEORY AND CRYPTOGRAPHY





HUGH WILLIAMS

iCORE Chair
Mathematics and Statistics, University of Calgary
http://www.cisac.math.ucalgary.ca/

In the three years since iCORE created ICANTC, we have focused on establishing the program and reaching some early goals. One of our most significant accomplishments has been getting CISaC established as an interdisciplinary centre dedicated to research in cryptography and information security. The goal of the centre is to conduct research into the testing and establishment of protocols to ensure secure communications, with a particular emphasis on studying, improving and implementing mathematically based cryptosystems. This includes everything from abstract theory to fabricating special cryptographic and computing devices.

EXECUTIVE SUMMARY

A highlight of the past year was the official launch of the Centre for Information Security and Cryptography (CISaC), which took place October 10, 2003. New courses on cryptography have been added to the math and computer science curricula. New facilities like the Advanced Cryptography Laboratory have been added, which attract even more students. The best news is that CISaC is a cross-disciplinary initiative, one that brings together researchers in mathematics, electrical and computer engineering and computer science. This kind of collaboration has tremendous potential.

Now that the centre is officially launched and our membership continues to grow, we are confident we will see more partnerships develop between academia and the private sector. As these partnerships mature, we believe we will see results in terms of intellectual property and commercial results.

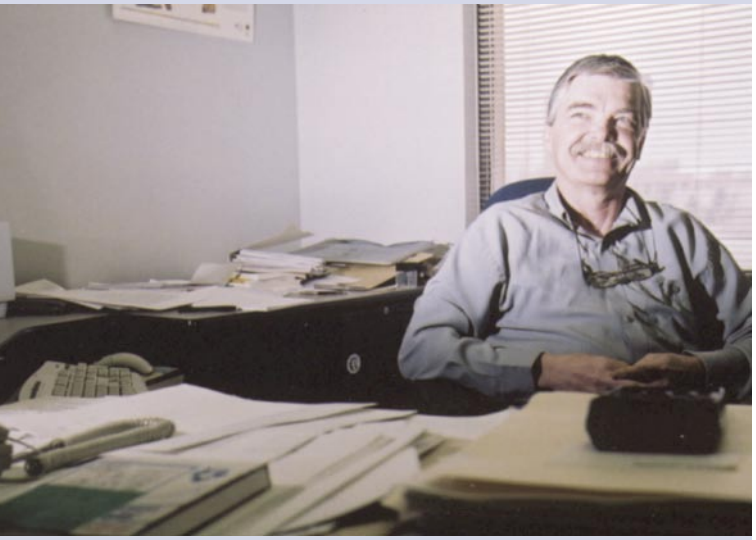
RESEARCH PROJECTS

Work within the new Centre for Information Security and Cryptography (CISaC) include:

- Further development of the Diffie-Hellman key exchange protocol in which for the first time the underlying mathematical structure is not a group. It is based on the discrete logarithm problem in a real quadratic field, but this meant that it was difficult to implement. Michael Jacobson, Renate Scheidler and Hugh Williams have devised a faster method of performing all the ideal reductions required by this system and we decreased

the bandwidth. The overall effect was a more than doubling of the speed of the previous implementation of this technique.

- The design and construction of machines that will perform the numerical sieving operation very rapidly. In a collaborative effort involving MSc student Kjell Wooding and Williams, a first phase has been completed with the development of a very fast software-sieving environment (CASSIE) that is capable of canvassing numbers at the rate of over 10^{15} numbers per second, an increase of over 1000 times faster than our previous device.
- One of the most important aspects of on-line privacy systems is the ability of communicants to authenticate their identity. This is usually achieved by means of digital signatures. These are bit strings that are easy for the sender to compute, but it is computationally infeasible for anyone else to forge. Furthermore, and this is often very important, it should be very easy for anyone to authenticate the identity of the sender by performing simple operations on this bit string. This can be a very important consideration for complicated banking transactions. What this means is that we can now use the one-time calculation mentioned above to determine a lower bound on the pseudosquares, which can next be utilized in tests that can very quickly prove that prime numbers of 100 bits are prime. Dan Bernstein has shown that such prime numbers can therefore be very quickly generated, are beyond the ability of anyone to predict, and can be used for extremely fast verification of Rabin-Williams signatures. These signatures are provably as difficult to forge as it is to factor a large integer.
- At the request of a local Calgary company, Non-Elephant Encryption Systems (NE2), Hugh Williams and Graham Jullien have been looking at the possibility of putting a very interesting cryptosystem developed by NE2 on a chip.
- We were recently able for the first time to compute unconditionally the regulator for a number field with a sixty-digit discriminant. Michael Jacobson and Hugh Williams are making use of an as yet unrefined version of our algorithm implemented on the 139 dual processor cluster mentioned earlier. Thus, when the new algorithm is completely developed and implemented on the cluster, it should be possible to compute regulators for fields of perhaps 65 or even 70 digit discriminants.
- One of the fundamental issues in cryptography is determining the computational complexity of the underlying mathematical problems that modern public-key cryptosystems are based on. Mark Bauer is looking at the question of how difficult is the elliptic curve discrete logarithm and whether there any other problems that we could show of the same complexity. Safuat Hamdy and Bauer proved some limited results on the connection between elliptic curve discrete logarithms and the analogous problem in number fields.
- Mark Bauer and Renate Scheidler are continuing their work on examining general cubic function fields, developing the foundations for the arithmetic in the Jacobian of certain curves that correspond to cubic function fields of a special form. The end goal of this project is to develop algorithms that are suitable for arbitrary cubic function fields.



Hugh Williams

RESEARCH TEAM MEMBERS AND CONTRIBUTIONS

Team Leader

Dr Hugh Williams, Team Leader	Professor, Department of Mathematics and Statistics
iCORE Chair in Algorithmic Number Theory and Cryptography	
Member of the Board of Directors of the Pacific Institute for the Mathematical Sciences	
Recognized by NSERC for "contributions to the sum total of human knowledge over the 25 years of NSERC's existence"	
Member of the Board of Directors for the Canadian Mathematical Society on July 1, 2003	
Member of the NSERC Leadership Support Initiative Grant Selection Committee August 22-23, 2003	

Faculty Team Members

NAME AND POSITION	ROLE/TOPIC
Dr Michael J. Jacobson, Jr.	Assistant Professor, Department of Computer Science
	Member, CISaC Management Board
Dr Renate Scheidler	Associate Professor, Department of Mathematics and Statistics and the Department of Computer Science
	iCORE Research Associate
	Member, CISaC Management Board
Dr Mark Bauer	Assistant Professor, Department of Mathematics and Statistics

Hugh Williams and some research team members at the 2004 Banff Informatics Summit

Affiliated Faculty

NAME	ROLE/TOPIC
Dr Vassil Dimitrov	Associate Professor, Department of Electrical and Computer Engineering, University of Calgary
Sid Tolchinsky	Security and Controls Specialist, ExxonMobil and Chairperson of Calgary Security Professionals Information Exchange (SPIE)
Dr John Aycock	Assistant Professor, Department of Computer Science, University of Calgary
Dr Mark L. Bauer	Assistant Professor, Department of Mathematics and Statistics, University of Calgary
Gerry Bliss	President, Bliss Informatics
Dr Richard Cleve	Professor, Department of Computer Science, University of Calgary
Dr Clifton Cunningham	Assistant Professor, Department of Mathematics and Statistics, University of Calgary
Dr. Behrouz Homayoun Far	Associate Professor, Department of Electrical and Computer Engineering, University of Calgary
Kenneth Fung	Program Director, Faculty of Continuing Education, University of Calgary
Dr Peter Høyer	Assistant Professor, Department of Computer Science, University of Calgary
Dr Graham Jullien	Professor, Department of Electrical and Computer Engineering, University of Calgary
Zak Karbalai	Director eSecurity and BCP, Care Factor Computer Services Inc.
Shalin Kashyap	Information Security Advisor, Security Operations, Shell Canada Limited
Dr Thomas Keenan	Adjunct Professor, Department of Computer Science, University of Calgary, and Director, e-Security Innovation Centre
Kathy Macdonald	Constable, Calgary Police Service
Dr Richard Mollin	Professor, Department of Mathematics and Statistics, University of Calgary
Dr Barry Sanders	iCORE Professor, Department of Physics and Astronomy, University of Calgary
Dr John Watrous	Associate Professor, Department of Computer Science and Canada Research Chair, University of Calgary
Dr Carey Williamson	iCORE Professor, Department of Computer Science, University of Calgary

Postdoctoral Fellows

NAME	ROLE/TOPIC AND AWARDS
Dr Filip Saidak	Research Focus: Analytic and probabilistic number theory Postdoctoral fellow Filip Saidak is now at the University of Missouri (Columbia). His research focus is analytic and probabilistic number theory.
Dr Safuat Hamdy	Research Focus: Number field cryptography Postdoctoral fellow Safuat Hamdy accepted a faculty position at the University of the United Emirates in Dubai (UAE). He will begin in August 2004.
Dr Siguna Mueller	Research Focus: Public-key cryptography and primality testing APART (Austrian Programme for Advanced Research and Technology) Scholarship

NAME	ROLE/TOPIC AND AWARDS
Dr Lassina Dembélé	Research Focus: Computations concerning the arithmetic of Hilbert modular forms Began November 2003
Dr Stéphane Lemieux	Currently at the University of Alberta Scheduled to begin May 1, 2004
Dr Roger Patterson	Currently at Macquarie University in Sydney, Australia Scheduled to begin May 1, 2004

PhD Students

NAME AND POSITION	ROLE/TOPIC
Kell Cheng	Topic: Simple Continued Fraction Expansions of Quadratics PhD student Kell Cheng successfully completed all his degree requirements in September 2003. His thesis is entitled: "Some Results Concerning Periodic Continued Fractions."

MSc Students

NAME	TOPIC	AWARDS
Richard Cannings	On the Security of the BB84 Quantum Key Distribution Protocol	
Chris Foster	The Solution of Catalan's Problem	
Brendan Oseen	Isogenies of Elliptic Curves	
Reginald Sawilla	Algorithims in Quadratic Fields	NSERC Postgraduate Scholarship, Alberta Ingenuity Ph.D. Studentship, iCORE Graduate Student Scholarship
Kjell Wooding	Development of a High-speed Numerical Sieving Device	NSERC Postgraduate Scholarship, Alberta Ingenuity Ph.D. Studentship, iCORE Graduate Student Scholarship
Andreas Hirt	A Practical Buses Protocol for Anonymous Network Communication	NSERC Canada Research Scholoarship, iCORE Graduate Student Scholarship
Guarav Jain	Intrusion Prevention Systems Based on Mobile Agents	

Other Team Members

SUPPORT STAFF

NAME AND POSITION	ROLE
Susan Schuck	Administrative Support
Marc Wrubleski	Computer Technician
STUDENT VISITORS	
Daniel Weimer	Technical University of Darmstadt
Robbert de Haan	University of Amsterdam
Roger Patterson	Macquarie University

SUMMER STUDENTS

NAME AND POSITION	ROLE
Kris Luttmer	NSERC scholar, working with Michael Jacobson
Leonard Nooy	Working with Michael Jacobson, funded by Jacobson's NSERC grant and the iCORE grant
Mark Velichka	NSERC scholar, working with Michael Jacobson and Renate Scheidler
Josiah Xiong	Working with Michael Jacobson, funding by Jacobson's NSERC grant and the iCORE grant
Rick Zhang	Working with Michael Jacobson, funding by Jacobson's NSERC grant and the iCORE grant
Bill Hutchinson	NSERC scholar, working with Renate Scheidler
Anguo Dong	Working with Renate Scheidler, supported by NSERC grant

Visitors: April 1, 2003 to March 31, 2004

Andreas Stein from the University of Illinois at Urbana Champaign
Andy Klapper from the University of Kentucky
Jeff Lagarias from Information Sciences Research, ATandT Labs (USA)
Igor Shparlinski from Macquarie University, Sydney, Australia,
Sam Wagstaff from Purdue University, West Lafayette, Indiana
Maurizio Laporta from the University of Naples (Italy)
Oliver Schirokauer from Oberlin College, Ohio
Jonathan Sorenson from Butler University, Indiana
Pedro Berrizbeitia from the Universidad Simon Bolivar in Caracas, Venezuela
Filip Saidak from the University of Missouri
Laurent Imbert from the Montpellier Laboratory of Computer Science, Robotics, and Microelectronics (LIRMM). This is a cross-faculty research entity of the University of Montpellier II (UMII) and the National Center for Scientific Research (CNRS)
Peter Borwein from Simon Fraser University, British Columbia

COLLABORATIONS AND AWARDS

INSTITUTION	NATURE OF COLLABORATION
PROVINCIAL	
Dr 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
NATIONAL	
Centre for Applied Cryptographic Research at the University of Waterloo	Formalized a partnership in 2003
INTERNATIONAL	
Illinois Center for Cryptography and Information Protection (ICCIP), University of Illinois at Urbana-Champaign and the Centre for Information Security and Cryptography at the University of Calgary	Negotiations formally completed June 30, 2003
Professor Hans Dobbertin of Ruhr- Universität Bochum, Germany	Pursuing a partnership with his cryptographic group
Technical University of Darmstadt	Pursuing a partnership with their cryptographic group
University of Salerno (Italy)	Pursuing a partnership with their cryptographic group
INDUSTRIAL	
BigBangWith, an Edmonton-based company	Developing an application to Western Economic Diversification for the establishment of a fast backup/ restore (RETSBAR) laboratory as part of CISaC. This $2.275M project's purpose is to provide industrial participants and researchers high-bandwidth access to remote storage to enable secure and encrypted real-time backup and restore of sensitive computing applications.
General Dynamics, Calgary	Currently negotiating to develop a cooperative think tank. This should result in a means by which ICANTC can effect technology transfer.
Fields Institute	Currently working on the development of an application for support of a six-month program devoted to cryptography with a budget of $325,000. Specific areas of concentration • Quantum computing and quantum cryptography • Algebraic curves and cryptography • Cryptographic protocols • Applied aspects of cryptography

FUNDING

Hugh Williams and team receive funding from many sources including AIF ($260K), CFI ($320K), MITACS ($360K), NSERC and the University of Calgary for a total of over $1.2M in addition to his iCORE funding.

PUBLICATIONS

REFEREED JOURNAL CONTRIBUTIONS

D. Hühnlein, M.J. Jacobson, Jr., and D. Weber, "Towards Practical Non-interactive Public-key Cryptosystems Using Non-maximal Imaginary Quadratic Orders", *Designs Codes and Cryptography* 30 (2003), no. 3, 281-299.

H. te Riele and H.C. Williams, "New Computations Concerning the Cohen-Lenstra Heuristics," *Experimental Mathematics*, 12 (2003), 99-113.

M.J. Jacobson, Jr., A.J. Menezes, and A. Stein, "Hyperelliptic Curves and Cryptography", *High Primes and Misdemeanors -- Conference in Number Theory in Honour of Professor Hugh Williams,* 2003, to appear.

M.J. Jacobson, Jr., Á. Pinter, and P.G. Walsh, "A Computational Approach for Solving $y^2 = 1^k + 2^k + \ldots + x^k$", *Math. Comp.* 72 (2003), no. 244, 2099-2110.

R.A. Mollin, "Construction of Families of Long Continued Fractions Revisited", to appear: *Acta Math. Acad. Paedagozicae Nyiregyhaziensis* (new series).

R.A. Mollin, "A Continued Fraction Approach to the Diophantine Equation ax^2-by^2=+-1", *Journal of Algebra, Number Theory and Applications*, 4 (2004, 159-207.

R.A. Mollin, "When the Central Norm is 2 in the Simple Continued Fraction Expansion of, √D", to appear in *Math. Rep. Acad. Sci. Canada*.

R.A. Mollin, "A Description of Continued Fraction Expansions of Quadratic Surds Represented by Polynomials", to appear in the *Journal of Number Theory*.

R.A. Mollin, "Infinitely Many Diophantine Equations Solvable Everywhere Locally but Nowhere Globally", to appear: *JPANTA*.

S. Mueller, "On the Computation of Cube Roots Modulo p", *High Primes and Misdemeanours – Conference in Number Theory in Honour of Professor Hugh Williams*, 2003, to appear.

Y. Lee, R. Scheidler and C. Yarrish, "Computation of the Fundamental Units and the Regulator of a Cyclic Cubic Function Field," *Experimental Mathematics* 12 (2003), 211-225.

REFEREED CONFERENCE PROCEEDINGS

M.J. Jacobson, Jr., "The Security of Cryptosystems Based on Class Semigroups of Imaginary Quadratic Non-maximal Orders", to appear in *ACISP* 2004.

M. Jacobson, H. C. Williams, K. Wooding, "Imaginary Cyclic Quartic Fields with Large Minus Class Numbers", to appear: *Proceedings of Algorithmic Number Theory, Sixth International Symposium*, ANTS-6. Accepted Feb. 6, 2004.

P. Berrizbeitia, S. Mueller and H.C. Williams, "Pseudocubes and Primality Testing", to appear: *Proceedings of Algorithmic Number Theory, Sixth International Symposium*, ANTS-6. Accepted February 6, 2004.

R. Scheidler, "An Algorithmic Perspective of Cubic Function Fields", to appear: *Proceedings of Algorithmic Number Theory, Sixth International Symposium*, ANTS-6. Accepted February 6, 2004.

S. Hamdy and M. Bauer, "On Class Group Computations Using the Number Field Sieve," *Proceedings of Asiacrypt 2002, appeared in Springer-Verlag. Advances in Cryptology-ASIACRYPT 2003*, Springer LNCS 2894, 2003, pp. 311-325.

PRESENTATIONS AND INVITED TALKS

H.C. Williams, Some Results Concerning Periodic Continued Fractions. AMS Special Session on Cryptography and Computational and Algorithmic Number Theory, Bloomington, Indiana, April 4-6, 2003.

H.C. Williams, Some Results Concerning Periodic Continued Fractions. A. Schinzel's Number Theory Seminar, Mathematical Institute of the Polish Academy of Sciences, Warsaw, May 9, 2003.

H.C. Williams, Some Contributions of Cryptography to Number Theory. Workshop in Honour of the 60th Birthday of H.C. Williams, Mathematical Institute of the Polish Academy of Sciences, Warsaw, May 13, 2003.

H.C. Williams, Some Contributions of Cryptography to Number Theory. AARMS Combinatorics Workshop, Memorial University of Newfoundland, July 15, 2003.

H.C. Williams, Cryptography, Pseudosquares and Number Sieves. Invited talk, PIMS Lunchbox Lecture Series, Calgary, Alberta, October 6, 2003.

H.C. Williams, What's Behind the Standards that Keep our Secrets Safe? Invited talk presented to SPIE (Calgary Security Professionals Information Exchange), Calgary, October 30, 2003.

H.C. Williams, Number Theory Inspired by Cryptography. Invited talk, MPKC 2003, Mathematics of Public-Key Cryptography, Chicago, Illinois (USA), November 8, 2003.

H.C. Williams, Periodic Continued Fractions with Short Periods. Invited special session speaker, CMS Winter meeting, Vancouver, BC, December 8, 2003.

H.C. Williams, Cryptography and Number Theory. Invited talk, Short course on Cryptography, CMS Winter Meeting, Vancouver, BC, December 6, 2003.

H. C. Williams, Cryptography, Pseudosquares and Number Sieves. Invited talk, UNBC Mathematics and Physics Symposium, Vancouver, BC, January 16, 2004.

K. Wooding, Recent Results on Pseudosquares. West Coast Number Theory Conference, Monterey, CA (USA), December 17-21, 2003.

M. Bauer, Point Counting on Picard Curves. West Coast Number Theory Conference, Pacific Grove, California (USA), December 17-21, 2003.

M. Bauer, Integer Factorization and the Discrete Logarithm Problem. Computer Security and Cryptography Seminar, University of Wisconsin, Madison (USA), February 16, 2004.

M. Bauer, Point Counting on Picard Curves. Elliptic Curve Cryptography Seminar, University of Wisconsin, Madison (USA), February 17, 2004.

M.J. Jacobson, Jr., NUCOMP II - Implementation and Applications. AMS Special Session on Cryptography and Computational and Algorithmic Number Theory, Bloomington, Indiana, April 4-6, 2003.

M.J. Jacobson, Jr., New Results on Dan Shanks' NUCOMP Algorithm. Conference in Number Theory in Honour of Professor Hugh Williams, Banff, Alberta, May 2003.

M.J. Jacobson, Jr., Cryptography lecture at CMS Math Camp, July 2003.

M.J. Jacobson, Jr., New Results on Dan Shank's NUCOMP Algorithm. Università degli Studi di Salerno, July 2003.

M.J. Jacobson, Jr., Cryptography and Information Security. Invited talk, Computer Science Calgary/Lethbridge Liaison Meeting, Calgary, Alberta, October 16, 2003.

M.J. Jacobson, Jr., Applications of NUCOMP. Invited talk, Mathematics of Public-Key Cryptography 2003, University of Illinois at Chicago, November 9, 2003.

M.J. Jacobson, Jr., Minus Class Numbers of Imaginary Cyclic Quartic Fields. Computational Number Theory Seminar, University of Illinois at Urbana-Champaign (USA), November 11, 2003.

M.J. Jacobson, Jr., Cryptography in Non-maximal Quadratic Orders, Invited talk, Information Protection Seminar, University of Illinois at Urbana-Champaign (USA), November 12, 2003.

M.J. Jacobson, Jr., Minus Class Numbers of Imaginary Cyclic Quartic Fields. Western Coast Number Theory Conference, Asilomar Conference Grounds, Pacific Grove, California, December 2003.

R. Mollin, The Many Vistas of Continued Fractions. American Mathematical Society Annual Meeting, Phoenix, Arizona (USA), January 9, 2004.

R. Sawilla, Fast Ideal Arithmetic in Real Quadratic Fields. West Coast Number Theory Conference, Pacific Grove, California (USA), December 20, 2003.

R. Scheidler, NUCOMP I – Idea and Algorithm. AMS Special Session on Cryptography and Computational and Algorithmic Number Theory, Bloomington, Indiana, April 4-6, 2003.

R. Scheidler, How to Exchange a Secret – Communication of Cryptographic Keys. University of Salerno (Italy), July 2003.

R. Scheidler, The Signature of a Cubic Function Field. Western Number Theory Conference, Pacific Grove, California (USA), December 17-21, 2003.

S. Hamdy, On Class Group Computations Using the Number Field Sieve. AMS Special Session on Cryptography and Computational and Algorithmic Number Theory, Bloomington, Indiana, April 4-6, 2003.

S. Hamdy, The IQ-MPQS with Two Large Primes. Conference in Number Theory in honour of Professor Hugh Williams, Banff, Alberta, May 24-30, 2003.

S. Hamdy, Public-Key Cryptography in Practice. MITACS Theme Meeting on Information Technology, Banff, Alberta, October 19-20, 2003.

S. Hamdy, Number Fields in Cryptography. AMSI Workshop on The Mathematics of Communications Security, Melbourne, Australia, November 18-21, 2003.

S. Hamdy, On Class Group Computations Using the Number Field Sieve. Asiacrypt 2003, Taipei, Taiwan, November 30 to December 4, 2003.

S. Mueller, On the Computation of Cube Roots Modulo p. AMS Special Session on Cryptography and Computational and Algorithmic Number Theory, Bloomington, Indiana, April 4-6, 2003.

S. Mueller, On a Cubic Generalization of the Lucas Functions and the Computation of Cube Roots Modulo p. XXIIIrd Journées Arithmétiques, Graz, Austria, July 6–12, 2003.

S. Mueller, Faster Methods of Generating Certain Cryptographic Keys. Invited talk, MITACS NCE 5th IT Theme Meeting, Banff, Alberta, October 19-20, 2003.

S. Mueller, On Pseudocubes and Primality Testing. MPKC 2003, University of Illinois at Chicago (USA) November 7 to 9, 2003.

S. Mueller, On Pseudocubes and Primality Proving. Invited talk, Kempner Colloquium, University of Colorado at Boulder (USA), November 17, 2003.

S. Mueller, Pseudopowers and Cryptography. Invited Talk, Institute for Information Security and Cryptography, Bochum, Germany, January 29, 2004.

S. Mueller, Pseudocubes and Applications to Primality Proving. Discrete Mathematics Seminar, University of Calgary, Alberta, February 27, 2004.