

About

Message

Research

Activities

Milestones

Ahead

Affiliates



CISaC

Department of Mathematics & Statistics, University of Calgary, 2500 University Drive NW Calgary, Alberta, Canada T2N 1N4
cisac@ucalgary.ca

www.cisac.ucalgary.ca

About CISaC

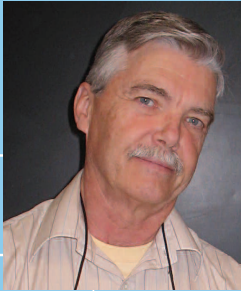
CISaC is a multi-disciplinary research centre at the University of Calgary devoted to research and development that provides security and privacy in information communication systems. CISaC research focuses on the design, evaluation and implementation of cryptographic algorithms and protocols, and the design and development of security architectures and systems for information communication and real-life applications.

Members include researchers in mathematics, computer science, engineering, physics, history and law, and professionals in the information security and law enforcement sectors. The iCORE Chair in Algorithmic Number Theory and Cryptography (ICANTC) and the iCORE Information Security Lab (iCIS) are CISaC's main funders, although the goal is for the Centre to be sustainable beyond ICANTC and iCIS. In 2008-2009, the University of Calgary's Dean of Science gave approval to change CISaC's status from a Centre to an Institute devoted to matters of information security and privacy. The new body will be called the Institute for Security, Privacy and Information Assurance (ISPIA).

CISaC's research includes a broad spectrum of areas ranging from theoretical cryptography and quantum information science to software security, malicious code, network and operating systems security, and technical and legal issues surrounding privacy and digital rights. The work incorporates abstract theory, large-scale hardware and software simulation, prototyping and development of special purpose hardware.

CISaC members coordinate and offer courses in security in the Faculty of Science. In addition, the Centre organizes and conducts outreach activities to build partnerships with industry, government and the local community. The Centre also provides consultancy in the areas of information security and cryptography.

Message from the Directors



Since it was first established, CISaC's goal has been to maintain and grow a strong membership cluster that includes academics in a variety of disciplines as well as professionals from the public and private sectors. As the information security and cryptography field continues to grow and become more important to modern society, we are successfully adapting to meet these changing needs. Our core mandate, however, remains unchanged and includes:

- Building linkages with professional societies, industry and government that result in practical, tangible outcomes such as joint research and collaborative training programs.
- 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 a sequence of courses as part of an area of concentration in cryptography within the undergraduate program in Mathematics as well as offering a concentration in information security within the Computer Science undergraduate program.
- Offering a variety of graduate courses in cryptography and related areas that can be accessed by students in mathematics, computer science and engineering.
- Sponsoring and providing outreach and training activities such as public lectures, special workshops, conferences and summer schools.

Over the past year, CISaC continues to expand as the Centre builds on the public's increasing recognition of the need for better information security technologies and policies. Part of this growth includes developing information security initiatives that can diversify Alberta's economy and create intellectual capital, commercialization and career opportunities within the province.

A key accomplishment in 2008-2009 was receiving approval from the University of Calgary's Dean of Science to change CISaC from a Centre to an Institute devoted to matters of information security and privacy. This body will be called the Institute for Security, Privacy and Information Assurance (ISPIA).

Along with these important changes and initiatives, in the past year the CISaC team published or submitted for publication approximately 60 research articles and gave nearly 40 presentations in Calgary and around the world. CISaC team members were principal investigators on personal research grants and scholarships totalling over \$1,000,000 annually.

In the coming year, as CISaC makes the exciting transition to the new Institute for Security, Privacy and Information Assurance (ISPIA), the team will continue to conduct both planned and opportunity-driven research while remaining relevant, innovative and committed to training highly qualified individuals with the skills to protect the privacy and information security of Albertans and Canadians.

Dr. Rei Safavi-Naini
Dr. Hugh C. Williams
Co-Directors

Research Focus

The research CISaC conducts centers around computational and algorithmic number theory as well as theoretical and applied cryptography. The projects reflect the depth and breadth of research carried out in the group, and build on work done in past years.

The research being conducted is not only of fundamental mathematical interest, but is also central to the development of new and better applications to the growing field of information and network security.

CISaC provides security solutions that rely on in-depth mathematical analysis and provable properties of algorithms, protocols and systems, applicable to different environments and a broad range of real-life problems. Focus areas include:

- **Mathematical Foundations of Cryptographic Algorithms**
 - Number Theoretic Foundations
 - Algorithms and Implementation
- **Modeling and Evaluating Security**
 - Information Theoretic Security
 - Computational Security
 - Quantum Cryptography
- **Wireless and Communication Security**
 - Sensor Security & RFID
 - Spam
- **System and Software Security**
 - Digital Rights Management
 - Privacy Rights Management
 - Biometrics
 - Malicious Software
 - Security Evaluation and Testing

Activities & Accomplishments



A key initiative that continued in 2008-2009 was restructuring CISaC. This restructuring was prompted last year by the arrival of the iCORE Chair in Information Security, Dr. Rei Safavi-Naini, in the Department of Computer Science at the University of Calgary. Dr. Safavi-Naini and Dr. Hugh Williams are co-directors on the CISaC Management Board. CISaC is being restructured to reflect this partnership and the website (www.cisac.ucalgary.ca) was completely revised in 2008.

In November 2008, a prospectus was submitted to the University of Calgary's Dean of Science requesting that CISaC's status be changed from a Centre to an Institute devoted to matters of information security and privacy. This body will be called the Institute for Security, Privacy and Information Assurance (ISPIA). The submission was successful and the new Institute was approved April 16, 2009.

In addition, Professors Safavi-Naini and Williams continue to work with the Global Centre for Securing Cyberspace (GCSC) to assist in establishing this Centre in Calgary. The mission of GCSC is to provide a strategic national approach within a secure environment to address the rapidly increasing social and economic impact of e-crime. The Centre will work collaboratively with a number of agencies within Alberta as well as nationally and internationally to further its objectives through program areas such as academic and applied investigation and research, education and awareness, legislative and regulatory development. The research activities of GCSC will be coordinated through CISaC and its successor Institute, of which Professors Safavi-Naini and Williams will remain co-directors.

Another of CISaC's main goals continues to be to train highly qualified personnel to meet the security demands of today's information-based society. The team continues to recruit students at all levels (undergraduate, masters, PhD and post-doctorate) to join the team.

ICANTC-related Initiatives

Professor Hugh Williams accepted the position of director of the newly created Cryptographic Research Institute. This is to be a worldwide leading research organization with a goal to conduct classified fundamental research in the areas of mathematics and computer science. This Institute operates under the umbrella of the Communications Security Establishment, a branch of the Government of Canada. Dr. Williams' position is a secondment from the University of Calgary and has been approved by the University of Calgary and iCORE.

Another significant initiative completed in mid-2008 was the book Michael Jacobson, Jr. and Hugh Williams co-wrote about the history and theory of the Pell equation. *Solving the Pell Equation* was published by Springer and is now available.

Other activities throughout the past year included organizing a number of major international conferences. *Selected Areas in Cryptography* (SAC 2009) and the 13th workshop on *Elliptic Curve Cryptography* (ECC 2009) will both take place in Calgary in August 2009. ECC is the

Activities & Accomplishments

largest annual meeting on this subject and is held in a different location each year. This is the first time both meetings will be held in Alberta. ECC also includes a summer school for graduate students, which will be held prior to the conference.

Dr. Hugh Williams is also working with John Friedlander (Toronto), Kristen Lauter (Microsoft Research) and Igor Shparlinski (Macquarie University, Australia) to organize a conference devoted to recent developments in mathematical cryptography, which will be held at the Fields Institute in Toronto, Ontario from May 11-15, 2009.

In addition, Professors Safavi-Naini and Williams, together with Dr. Wolfgang Tittel, are program chairs for this year's iCORE Banff Summit.

The theme is *Tools for Information Security and Privacy: Cryptography and Quantum Cryptography*.

iCIS-related Initiatives

Over the last year, members of the iCIS Lab have made significant contributions to world-class security research and education, and successfully worked towards building linkages with industry and the community.

In the past year iCIS successfully recruited a new member for the iCIS Lab. Dr. Philip Fong was appointed an associate professor of the Department of Computer Science in January 2009. Since his appointment, he has been leading development of a Master's degree in Information Security in the Department of Computer Science. This program will provide an opportunity for professionals with a background in information technology to specialize in this area. This initiative is supported by the Department of Computer Science and Faculty of Science and is expected to be presented to the Alberta government for approval in early 2010.

Of particular note is the work iCIS is doing in the area of secure management of electronic health records using the Digital Rights Management (DRM) approach. This initiative is in collaboration with the Faculty of Medicine at the University of Calgary and Cybera, and has attracted the interest of Microsoft Research. Dr. Nicholas Sheppard visited the iCIS Lab for six months to initiate work on the project. The novel aspect of this project is application of the DRM approach for specification and enforcement of privacy and security requirements of electronic health records, and in particular management of patients' consents—ensuring that access to patients' data by health professionals conform to the patients' wishes. The project is a natural continuation of a number of projects on DRM and its application for privacy management that Dr. Safavi-Naini led in Australia, for which Dr. Sheppard was the principle research fellow. The visit resulted in a complete proposal (SEHRI) for secure management of electronic health records in conformance with Canadian context. A related activity is a project for securing access to databases holding patients' information. Partners in this project are HiitTech in the Faculty of Medicine and Cybera, who has provided partial funding for the project. This project is part of MITACS' projects on *Privacy Enhancing Technologies*.

Dr. Pascal Lafourcade visited the Lab as part of the France-Canada collaboration on information security. This initiative is partially funded by MITACS and is between INRIA in France and a number of Canadian universities with a research interest in information security. Dr. Lafourcade's visit resulted in a new collaboration between the iCIS Lab and INRIA.



Milestones

Presentations & Publications

- 33 lectures given by experts from Canada and around the world as part of the *ICANTC Number Theory and Cryptography Seminar Series*, *CISaC Distinguished Lecture Series on Information Security* and the *iCIS Security Seminars*
- 38 presentations and contributed talks given locally and around the world by CISaC researchers and students
- 27 refereed articles published in conference proceedings
- 23 refereed articles accepted or published in academic journals
- 1 book published
- 3 conference proceedings edited

People

- 8 postdoctoral fellows
- 20 PhD students
- 15 M.Sc. students
- 8 successful theses (5 M.Sc. and 3 PhD)
- 20 visitors from universities and companies in Canada, the United States and around the world

Partnerships

- 1 secondment as Dr. Hugh Williams accepted the position of director of the Cryptographic Research Institute in Ottawa, an organization with a vision to a worldwide leading research organization with a goal to conduct classified fundamental research in the areas of mathematics and computer science

Teaching

- 1 new master's degree in information security program being developed for the Computer Science Department
- 1 review and revision of the curriculum of the *Computer Science Undergraduate Concentration in Information Security* and the *Mathematics Undergraduate Concentration in Cryptography*
- 1 review and revision of the graduate curriculum in cryptography offered by the Mathematics & Statistics and Computer Science Departments

Conferences & Meetings

- 10 international and national conferences, workshops and panels organized or co-organized

Grants

- iCORE funding renewal of \$2,250,000 for 2006-2011
- Over \$300,000 annually in personal research grants as principle investigators
- Over \$700,000 as co-investigators on projects
- Ongoing financial support from Alberta Ingenuity, iCORE, Alberta Innovation and Science, MITACS, NSERC, the Canada Foundation for Innovation and the University of Calgary

A Look to the Future



While key research activities and outreach will carry on in the coming year, the addition of new graduate and undergraduate students and collaborators to the CISaC (ISPIA) team will expand the scope of the research program.

The focus in 2009-2010 will be to successfully transition CISaC to the new Institute for Security, Privacy and Information Assurance (ISPIA). This new Institute reflects the growing significance of information and the increasingly important role it is playing in ICANTC and iCIS's work. In addition, work will continue to establish the Global Centre for Securing Cyberspace (GCSC) in Calgary. The research activities of GCSC will be coordinated through the Institute for Information Security and Privacy.

Existing research projects will continue in the next year and new projects are planned. The focus will continue to be the design, analysis, testing, implementation and benchmarking of cryptographic schemes that apply to privacy and ultimately information and network security.

Over the past year, the CISaC group continued to expand information security outreach and raise profile with the public as well as the global academic community through public lectures, conference organization, editorial work, and curriculum development. A highlight of the outreach program is the *CISaC Distinguished Lecture Series on Information Security*, which will resume in autumn 2009 and will continue to bring top researchers and professionals from around the world to the University of Calgary.

In addition, in 2008-2009 CISaC members were involved in organizing and hosting an unprecedented number of workshops and conferences. Team members secured major external funding for these events from PIMS, the Fields Institute, MITACS, and iCORE, as well as contributions from ICANTC, iCIS and the University of Calgary. We will build on these activities in the upcoming year.

Our research will continue in 2009-2010. The focus will continue to be projects that apply to privacy and ultimately enhance information and network security.

Affiliates

CISaC Co-Directors

- Dr. Rei Safavi-Naini, iCORE Chair in Information Security and Cryptography (iCIS) and Professor, Department of Computer Science, University of Calgary
- Dr. Hugh Williams, iCORE Chair in Algorithmic Number Theory and Cryptography (ICANTC) and Professor, Department of Mathematics & Statistics, University of Calgary

CISaC Management Board

- Dr. John Aycock, Assistant Professor, Department of Computer Science, University of Calgary
- Dr. Mark L. Bauer, Assistant Professor, Department of Mathematics & Statistics, University of Calgary
- Dan Chervenka, Security Manager, Axia SuperNet Ltd.
- Abraham Fapojuwo, Associate Professor, Department of Electrical & Computer Engineering, University of Calgary
- Shalin Kashyap, Information Security Advisor – Security Operations, Shell Canada Limited
- Sid Tolchinsky, Security & Controls Specialist, Exxon Mobil and Chairperson of Calgary Security Professionals Information Exchange (SPIE)
- Ian Wilms, IBM Public Safety Executive & Calgary Police Commissioner

CISaC Technical Advisory Panel

- Dr. Daniel J. Bernstein, Department of Mathematics, Statistics, and Computer Science, University of Illinois at Chicago
- Dr. Gilles Brassard, Département d'Informatique et de Recherche Opérationnelle, Université de Montréal
- Dr. Johannes A. Buchmann, Fachbereich Informatik, Technische Universität Darmstadt
- Dr. Matthew Franklin, Department of Computer Science, University of California Davis
- Dr. Ian R. Kerr, Faculty of Law, University of Ottawa
- Dr. Neal Koblitz, Department of Mathematics, University of Washington
- Dr. Evangelos Kranakis, School of Computer Science, Carleton University
- Dr. Alfred J. Menezes, Centre for Applied Cryptographic Research, University of Waterloo
- Dr. Andrew Odlyzko, Digital Technology Center, University of Minnesota
- Dr. Douglas Stinson, School of Computer Science, University of Waterloo
- Dr. Scott Vanstone, Founder and Executive Vice President for Strategic Technology, Certicom
- Dr. Yacov Yacobi, Cryptography and Anti-Piracy Group, Microsoft Research

CISaC

Department of Mathematics & Statistics, University of Calgary, 2500 University Drive NW Calgary, Alberta, Canada T2N 1N4

cisac@ucalgary.ca

www.cisac.ucalgary.ca

