

BRUCE M. KAPRON  
DEPARTMENT OF COMPUTER SCIENCE  
UNIVERSITY OF VICTORIA  
VICTORIA, BC  
CANADA V8W 3P6  
(250)-472-5725 (w)  
(250)-598-2396 (h)  
[www.cs.uvic.ca/~bmkapron](http://www.cs.uvic.ca/~bmkapron)  
[bmkapron@uvic.ca](mailto:bmkapron@uvic.ca)

---

## RESEARCH INTERESTS

Logic and verification, foundations of cryptography and security, economic aspects of information security.

## EDUCATION

- Ph.D., Computer Science, University of Toronto, June 1991. Thesis: “Feasible computation in higher types,” supervised by S.A. Cook.
- M.Sc., Mathematics, Simon Fraser University, Vancouver, B.C., July 1986. Thesis: “Modal sequents and definability,” supervised by S.K. Thomason.

## PROFESSIONAL EXPERIENCE

- Current:* Professor, Computer Science Department, University of Victoria
- 8/06-6/07:* Visiting Professor, Computer Science Department, Stanford University
- 8/01-7/02:* Visiting Associate Professor, Computer Science Department, Stanford University
- 7/97-6/10:* Associate Professor, Department of Computer Science, University of Victoria
- 1/99-6/99:* Visiting Researcher, Computer Science Department, Stanford University
- 7/98-9/98:* Visiting Associate Professor, DIKU, University of Copenhagen
- 9/94-6/96:* Assistant Professor, Department of Computer Science, University of Victoria

*1/93–8/94*: Visiting Assistant Professor, Department of Computer Science, University of Victoria

*7/92–12/92*: Postdoctoral Fellow, Simon Fraser University.

*1/91–6/92*: Visiting Scientist, Carnegie Mellon University.

## **MAJOR RESEARCH GRANTS**

### **Currently Held**

- Natural Sciences and Engineering Research Council (NSERC) of Canada Research Grant. Amount per year: \$38,000. Years of tenure: 2005-2010. Title: “Logic and foundations of cryptography”.

### **Recently Held**

- Natural Sciences and Engineering Research Council (NSERC) of Canada Research Grant. Amount per year: \$33,000. Years of tenure: 2002-2005. Title: “Complexity of higher-order computation”.

### **Past Projects**

- Network of Centres of Excellence MITACS (Mathematics of Information Technology and Complex Systems) Network Grant. Principle Investigator: Bruce Kapron. Title: “Mathematical methods for modeling, verification and testing in information technology.” Academic partners: University of Victoria, UBC, Simon Fraser University, McGill University. Industry Partners: Nortel Networks.
- BC Advance Systems Systems Institute. Principle investigator: Jeffrey Joyce (UBC and Hughes Aircraft of Canada/Raytheon). Title: “FormalWARE”. Academic partners: UBC, University of Victoria. Industry Partners: Raytheon Systems Canada, MacDonald Dettwiler.

## **GRADUATE STUDENTS**

### **Graduated**

- Brent Knight, M.Sc., 1994. Thesis title: “Safe strict evaluation of redundancy-free programs from proofs.”
- Dilian Gurov, Ph.D., 1997. Thesis title: “A modal mu-calculus and a proof system for value passing processes.”
- Georgi Kostadinov, M.Sc., 2000. Thesis title: “A compositional proof system for model checking with tagging.”

- Wai-Han Chiu, M.Sc., 2003. Thesis title: “Modeling and verification of message sequence charts using process algebras and temporal logic model checking.”
- Samuel Leung, M.Sc., 2006. Thesis title: “Pathway representation using finite state automata and comparison using the NCI thesaurus”
- Gautam Srivastava, M.Sc., 2006. Thesis title: “Pseudorandom number generators using multiple sources of entropy”.
- Daniel Hotlby, M.Sc., 2006. Thesis title: “Lower bound for scalable Byzantine agreement”.
- Chris Ware, M.Sc., 2008. Thesis title: “Modeling and analysis of quantum cryptographic protocols”.
- Warren Shenkenfelder, M.Sc., 2008. Thesis title: “Learning bisimulation”.
- Lior Malka, Ph.D., 2008. Thesis title: “A study of perfect zero-knowledge proofs”.

### **In Progress**

- Mohammad Hajiabadi, M.Sc. Expected completion 2010. Research topic: Dynamic epistemic logic and security.
- Gautam Srivastava, Ph.D. Expected completion 2010. Research topic: Anonymization in social networks.
- Nicholas Vining, M.Sc. Expected completion 2010. Research topic: Dynamical systems and Kolmogorov complexity.
- Chris Ware, Ph.D. Expected completion 2011. Research topic: Economic models in information security and cryptography.

### **RECENT PROGRAMME COMMITTEES**

- 2nd Canada-France Workshop on Foundations and Practice of Security, June 2009, Grenoble, France.
- Co-chair, 8th International Workshop on Logic and Computational Complexity, August 2006, Seattle, WA.
- 3rd IFIP International Conference on Theoretical Computer Science, August 2004, Toulouse, France.

- Latin American Theoretical Informatics, April 2004, Buenos Aires
- 5th International Workshop on Implicit Computational Complexity, July 2001, Ottawa
- 3rd International Workshop on Implicit Computational Complexity, July 2001, Aarhus, DK.

## PUBLICATIONS

### Journal Publications

1. Bruce M. Kapron, David Kempe, Valerie King, Jared Saia, and Vishal Sanwalani. Fast asynchronous byzantine agreement and leader election with full information. To appear in *ACM Transactions on Algorithms*.
2. Dan Holtby, Bruce M. Kapron, and Valerie King. Lower bound for scalable Byzantine agreement. *Distributed Computing*, 21(4):239–248, 2008.
3. Russell Impagliazzo and Bruce M. Kapron. Logics for reasoning about cryptographic constructions. *J. Comput. Syst. Sci.*, 72(2):286–320, 2006.
4. Valentin Goranko and Bruce M. Kapron. The modal logic of the countable random frame. *Arch. Math. Log.*, 42(3):221–243, 2003.
5. Samuel R. Buss and Bruce M. Kapron. Resource-bounded continuity and sequentiality for type-two functionals. *ACM Trans. Comput. Log.*, 3(3):402–417, 2002.
6. Robert J. Irwin, James S. Royer, and Bruce M. Kapron. On characterizations of the basic feasible functionals (part I). *J. Funct. Program.*, 11(1):117–153, 2001.
7. Dilian Gurov and Bruce M. Kapron. A note on negative tagging for least fixed-point formulae. *ITA*, 33(4/5):383–392, 1999.
8. Bruce M. Kapron. Feasibly continuous type-two functionals. *Computational Complexity*, 8(2):188–201, 1999.
9. Faith E. Fich, Russell Impagliazzo, Bruce M. Kapron, Valerie King, and Miroslaw Kutylowski. Limits on the power of parallel random access machines with weak forms of write conflict resolution. *J. Comput. Syst. Sci.*, 53(1):104–111, 1996.
10. Dilian Gurov, Sergey Berezin, and Bruce M. Kapron. A modal mu-calculus and a proof system for value passing processes. *Electr. Notes Theor. Comput. Sci.*, 5, 1996.

11. Bruce M. Kapron and Stephen A. Cook. A new characterization of type-2 feasibility. *SIAM J. Comput.*, 25(1):117–132, 1996.
12. Joseph Y. Halpern, Bruce M. Kapron. Zero-One Laws for Modal Logic. *Ann. Pure Appl. Logic*, 69(2-3):157–193, 1994.
13. Bruce M. Kapron. Modal sequents and definability. *J. Symb. Log.*, 52(3):756–762, 1987.

### Refereed Conference Publications

14. Gilles Barthe, Marion Daubignard, Bruce M. Kapron, and Yassine Laknech. Computational indistinguishability logic. To appear in *Proceedings of 17th Annual ACM Conference on Computer and Communications Security, CCS 2010*.
15. Gilles Barthe, Marion Daubignard, Bruce M. Kapron, Yassine Laknech, and Vincent Laporte. On the equality of probabilistic terms. To appear in *Proceedings of the 16th International Conference on Logic for Programming, Artificial Intelligence and Reasoning, LPAR 2010*.
16. Bruce M. Kapron, David Kempe, Valerie King, Jared Saia, and Vishal Sanwalani. Fast asynchronous byzantine agreement and leader election with full information. In *Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2008*, pages 1038–1047.
17. Bruce M. Kapron, Lior Malka, and Srinivasan Venkatesh. A characterization of non-interactive instance-dependent commitment-schemes (NIC). In *Automata, Languages and Programming, 34th International Colloquium, ICALP 2007*, volume 4596 of *Lecture Notes in Computer Science*. Springer, 2007.
18. Dan Holtby, Bruce M. Kapron, and Valerie King. Lower bound for scalable byzantine agreement. In *Proceedings of the Twenty-Fifth Annual ACM Symposium on Principles of Distributed Computing, PODC 2006*, pages 285–291.
19. Russell Impagliazzo and Bruce M. Kapron. Logics for reasoning about cryptographic constructions. In *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2003*, pages 372–383.
20. Samuel R. Buss and Bruce M. Kapron. Resource-bounded continuity and sequentiality for type-two functionals. In *Proceedings of the Fifteenth Annual IEEE Symposium on Logic in Computer Science, LICS 2000*, pages 77–83, 2000.

21. Peter Clote, Aleksandar Ignjatovic and Bruce M. Kapron. Parallel computable higher-type functionals (extended abstract). In *Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science, FOCS 1993*, pages 72-81.
22. Faith E. Fich, Russell Impagliazzo, Bruce M. Kapron, Valerie King, and Mirosław Kutylowski. Limits on the power of parallel random access machines with weak forms of write conflict resolution. In *10th Annual Symposium on Theoretical Aspects of Computer Science, STACS 1993*, pages 386-397.
23. Joseph Y. Halpern and Bruce M. Kapron. Zero-one laws for modal logic. In *Proceedings of the Seventh Annual IEEE Symposium on Logic in Computer Science, LICS 1992*, pages 369–380.
24. Bruce M. Kapron and Stephen A. Cook. A new characterization of mehlhorn's polynomial time functionals (extended abstract). In *Proceedings of the 32nd Annual IEEE Symposium on Foundations of Computer Science, FOCS 1991*, pages 342–347.
25. Stephen A. Cook and Bruce M. Kapron. Characterizations of the basic feasible functionals of finite type (extended abstract). In *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science, FOCS 1989*, pages 154-159.