Bruce M. Kapron
Department of Computer Science, University of Victoria
Victoria, BC, CANADA V8W 2Y2
(250)-472-5725 (w), (250)-598-2396 (h)
bmkapron@uvic.ca

RESEARCH INTERESTS

Applications of logic, computational complexity, verification, foundations of cryptography and 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

7/10-present Professor, *7/97–6/10* Associate Professor, *1/93–6/96* Assistant Professor, Department of Computer Science, University of Victoria

1/14-4/14 Member, School of Mathematics, Institute for Advanced Study

9/13-12/13 Visiting Scientist, Simons Institute for the Theory of Computing

8/06-6/07 Visiting Professor, *8/01-7/02* Visiting Associate Professor, *1/99-6/99* Visiting Researcher, Computer Science Department, Stanford University

7/98-9/98 Visiting Associate Professor, DIKU, University of Copenhagen

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

REFEREED JOURNAL PUBLICATIONS

1. B.M. Kapron, L. Malka, S. Venkatesh: A Characterization of Non-interactive Instance-Dependent Commitment-Schemes (NIC): to appear in *Theoretical Computer Science*.
2. Sean Chester, Bruce M. Kapron, Gautam Srivastava, S. Venkatesh: Complexity of social network anonymization. *Social Netw. Analys. Mining* **3** (2): 151-166 (2013)
3. Sean Chester, Bruce M. Kapron, Ganesh Ramesh, Gautam Srivastava, Alex Thomo, S. Venkatesh: Why Waldo befriended the dummy? k-Anonymization of social networks with pseudo-nodes. *Social Netw. Analys. Mining* **3** (3): 381-399 (2013)
4. B.M. Kapron, D. Kempe, V. King, J. Saia, V. Sanwalani: Fast asynchronous Byzantine agreement and leader election with full information. *ACM TALG* **6**(4) (2010)
5. D. Holtby, B.M. Kapron, V. King: Lower bound for scalable Byzantine Agreement. *Dist. Com.* **21**(4): 239-248 (2008)
6. R. Impagliazzo, B.M. Kapron: Logics for reasoning about cryptographic constructions. *JCSS* **72**(2): 286-320 (2006)
7. V. Goranko, B.M. Kapron: The modal logic of the countable random frame. *Arch. Math. Log.* **42**(3): 221-243 (2003)
8. S.R. Buss, B.M. Kapron: Resource-bounded continuity and sequentiality for type-two functionals. *ACM Trans. Comput. Log.* **3**(3): 402-417 (2002)
9. R.J. Irwin, J.S. Royer, B.M. Kapron: On characterizations of the basic feasible functionals (Part I). *J. Funct. Program.* **11**(1): 117-153 (2001)
10. B.M. Kapron: Feasibly Continuous Type-Two Functionals. *Comp. Compl.* **8**(2): 188-201 (1999)
11. D. Gurov, B.M. Kapron: A note on negative tagging for least fixed-point formulae. *ITA* **33**(4/5): 383-392 (1999)
12. D. Gurov, S. Berezin, B.M. Kapron: A modal mu-calculus and a proof system for value passing processes. *Electr. Notes Theor. Comput. Sci.* **5**: 47 (1996)
13. F.E. Fich, R. Impagliazzo, B.M. Kapron, V. King, M. Kutylowski: Limits on the Power of Parallel Random Access Machines with Weak Forms of Write Conflict Resolution. *JCSS* **53**(1): 104-111 (1996)
14. B.M. Kapron, S.A. Cook: A New Characterization of Type-2 Feasibility. *SIAM J. Comput.* **25**(1): 117-132 (1996)

15. J.Y. Halpern, B.M. Kapron: Zero-One Laws for Modal Logic. *APAL* **69**(2-3): 157-193 (1994)
16. B.M. Kapron: Modal Sequents and Definability. *J. Symb. Log.* **52**(3): 756-762 (1987)

REFEREED CONFERENCE PUBLICATIONS

14. M. Hajiabadi, B.M. Kapron: Gambling, Computational Information and Encryption Security, *International Conference on Information-Theoretic Security (ICITS) 2015*: 141-158.
15. M. Hajiabadi, B.M. Kapron: Computational soundness of coinductive symbolic security under active attacks. *Theory of Cryptography Conference (TCC) 2013*: 539-558.
16. B.M. Kapron, V. King, B. Mountjoy. Dynamic graph connectivity in polylogarithmic worst-case time. *SODA 2013*: 1131-1142. (*Co-recipent of best paper award*)
17. S. Chester, B.M. Kapron, G. Ramesh, G. Srivastava, A. Thomo, S. Venkatesh: k-Anonymization of Social Networks by Vertex Addition. *Proc. 15th East-European Conf. on Adv. in Databases and Inf. Sys. (ADBIS) 2011*: 107-116.
18. B.M. Kapron, G. Srivastava, S. Venkatesh: Social Network Anonymization via Edge Addition. *Int. Conf. on Advances in Social Networks Analysis and Mining, (ASONAM) 2011*: 155-162.
19. G. Barthe, M. Daubignard, B.M. Kapron, Y. Lakhnech: Computational indistinguishability logic. *ACM CCS 2010*: 375-386.
20. G. Barthe, M. Daubignard, B.M. Kapron, Y. Lakhnech, V. Laporte: On the Equality of Probabilistic Terms. *LPAR 2010*: 46-63.
21. B.M. Kapron, D. Kempe, V. King, J. Saia, V. Sanwalani: Fast asynchronous byzantine agreement and leader election with full information. *SODA 2008*: 1038-1047.
22. B.M. Kapron, L. Malka, S. Venkatesh: A Characterization of Non-interactive Instance-Dependent Commitment-Schemes (NIC). *ICALP 2007*: 328-339.
23. D. Holtby, B.M. Kapron, V. King: Lower bound for scalable Byzantine Agreement. *PODC 2006*: 285-291.
24. R. Impagliazzo, B.M. Kapron: Logics for Reasoning about Cryptographic Constructions. *FOCS 2003*: 372-383.
25. S.R. Buss, B.M. Kapron: Resource-Bounded Continuity and Sequentiality for Type-2 Functionals. *LICS 2000*: 77-83.
26. P. Clote, A. Ignjatovic, B.M. Kapron: Parallel computable higher type functionals. *FOCS 1993*: 72-81.
27. J.Y. Halpern, B.M. Kapron: Zero-One Laws for Modal Logic. *LICS 1992*: 369-380.
28. B.M. Kapron, S.A. Cook: A New Characterization of Mehlhorn's Polynomial Time Functionals. *FOCS 1991*: 342-347.
29. S.A. Cook, B.M. Kapron: Characterizations of the Basic Feasible Functionals of Finite Type. *FOCS 1989*: 154-159

CURRENTLY HELD MAJOR RESEARCH GRANTS

- Natural Sciences and Engineering Research Council (NSERC) of Canada Discovery Grant. Amount per year: $24,000. Years of tenure: 2011-2016. Title: "Foundational studies in privacy and security".
- Intel Research Gift. Amount: $70,000. Years of tenure 2014-2015. Title: "Automated Antivirus Evaluation via Malware Mutations

RECENTLY HELD MAJOR RESEARCH GRANTS

- Natural Sciences and Engineering Research Council (NSERC) of Canada Engage Grant. Amount: $25,000. Years of tenure: 2012. Title: "GPU-based encryption of streaming video".
- Natural Sciences and Engineering Research Council (NSERC) of Canada Discovery Grant. Amount per year: $38,000. Years of tenure: 2005-2010 Title: "Logical foundations of cryptography".

GRADUATE STUDENTS

- Brent Knight, M.Sc., 1994. "Safe strict evaluation of redundancy-free programs from proofs."
- Dilian Gurov, Ph.D., 1997. "A modal mu-calculus and a proof system for value passing processes."
- Georgi Kostadinov, M.Sc., 2000. "A compositional proof system for model checking with tagging."
- Wai-Han Chiu, M.Sc., 2003. "Modeling and verification of message sequence charts using process algebras and temporal logic model checking."
- Daniel Hotlby, M.Sc., 2006. "Lower bound for scalable Byzantine agreement".

- Samuel Leung, M.Sc., 2006. "Pathway representation using FSA and comparison using the NCI thesaurus"
- Gautam Srivastava, M.Sc., 2006. "PRNGs using multiple sources of entropy".
- Lior Malka, Ph.D., 2008, "A study of perfect zero-knowledge proofs".
- Warren Schenkenfelder, M.Sc., 2008. "Learning bisimulation".
- Chris Ware, M.Sc., 2008. "Modeling and analysis of quantum cryptographic protocols".
- Mohammad Hajiabadi, M.Sc., 2011. "Coinduction and computational semantics for public-key encryption".
- Gautam Srivastava, Ph.D., 2011. "Graph anonymization through edge and vertex addition".
- Nicholas Vining, M.Sc., 2011. "Next generation content creation: an investigative approach".
- Chelsea Foster, M.Sc., 2015. "Finitely iterated rational secret sharing with private information"
- Khodakhast Bibak, Ph.D. Expected completion 2016.
- Wanda Boyer, M.Sc. Expected completion 2015.
- Erkan Ersan, M.Sc., Expected completion 2016.
- Mohammad Hajiabadi, Ph.D. Expected completion 2015.
- Ariel Webster, M.Sc., Expected completion 2015.