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
www.cs.uvic.ca/~bmkapron
orcid.org/0000-0002-3295-543X

## 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 Stephen 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. Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan: Unweighted linear congruences with distinct coordinates and the Varshamov-Tenengolts codes. *Des. Codes Cryptography* **86** (9): 1893-1904 (2018)
2. Mohammad Hajiabadi, Bruce M. Kapron: Reproducible Circularly Secure Bit Encryption: Applications and Realizations. *J. Cryptology* **30** (4): 1187-1237 (2017)
3. Khodakhast Bibak, Bruce M Kapron, Venkatesh Srinivasan, Roberto Tauraso, László Tóth: Restricted linear congruences. *Journal of Number Theory* **171**: 128-144 (2017)
4. Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan: On a restricted linear congruence. *International Journal of Number Theory* **12** (8): 2167-2171 (2016)
5. Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan: Counting surface-kernel epimorphisms from a co-compact Fuchsian group to a cyclic group with motivations from string theory and QFT. *Nuclear Physics B* **910**: 712-723 (2016)
6. Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan: MMH with arbitrary modulus is always almost-universal. *Inf. Process. Lett.* **116** (7): 481-483 (2016)

7. Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan: The Cayley Graphs Associated With Some Quasi-Perfect Lee Codes Are Ramanujan Graphs. *IEEE Trans. Information Theory* **62** (11): 6355-6358 (2016)

8. Bruce M. Kapron, Lior Malka, S. Venkatesh: A Characterization of Non-interactive Instance-Dependent Commitment-Schemes (NIC). *Theoretical Computer Science* **593**: 1-15 (2015)

9. Sean Chester, Bruce M. Kapron, Gautam Srivastava, S. Venkatesh: Complexity of social network anonymization. *Social Netw. Analys. Mining* **3** (2): 151-166 (2013)

10. 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)

11. Bruce M. Kapron, David Kempe, Valerie King, Jared Saia, Vishal Sanwalani: Fast asynchronous Byzantine agreement and leader election with full information. *ACM TALG* **6**(4) (2010)

12. Daniel Holtby, Bruce M. Kapron, Valerie King: Lower bound for scalable Byzantine Agreement. *Dist. Com.* **21**(4): 239-248 (2008)

13. Russell Impagliazzo, Bruce M. Kapron: Logics for reasoning about cryptographic constructions. *JCSS* **72**(2): 286-320 (2006) (*Special issue dedicated to selected papers from FOCS 2003*)

14. Valtentine Goranko, Bruce M. Kapron: The modal logic of the countable random frame. *Arch. Math. Log.* **42**(3): 221-243 (2003)

15. Samuel R. Buss, Bruce M. Kapron: Resource-bounded continuity and sequentiality for type-two functionals. *ACM Trans. Comput. Log.* **3**(3): 402-417 (2002) (*Special issue dedicated to selected papers from LICS 2000*)

16. Robert J. Irwin, James S. Royer, Bruce M. Kapron: On characterizations of the basic feasible functionals (Part I). *J. Funct. Program.* **11**(1): 117-153 (2001)

17. Bruce M. Kapron: Feasibly Continuous Type-Two Functionals. *computational complexity* **8**(2): 188-201 (1999)

18. Dilian Gurov, Bruce M. Kapron: A note on negative tagging for least fixed-point formulae. *ITA* **33**(4/5): 383-392 (1999)

19. Dilian Gurov, Sergei Berezin, Bruce M. Kapron: A modal mu-calculus and a proof system for value passing processes. *Electr. Notes Theor. Comput. Sci.* **5**: 47 (1996)

20. Faith E. Fich, Russell Impagliazzo, Bruce M. Kapron, Valerie King, Marek Kutylowski: Limits on the Power of Parallel Random Access Machines with Weak Forms of Write Conflict Resolution. *JCSS* **53**(1): 104-111 (1996)

21. Bruce M. Kapron, Stephen A. Cook: A New Characterization of Type-2 Feasibility. *SIAM J. Comput.* **25**(1): 117-132 (1996)

22. Joseph Y. Halpern, Bruce M. Kapron: Zero-One Laws for Modal Logic. *Annal Pure and Applied Logic* **69** (2-3): 157-193 (1994) (*Special issue dedicated to selected papers from LICS 1992*)

23. Bruce M. Kapron: Modal Sequents and Definability. *J. Symb. Log.* **52**(3): 756-762 (1987)

## REFEREED CONFERENCE PUBLICATIONS

24. Bruce M. Kapron, Florian Steinberg: Type-two polynomial-time and restricted lookahead. *LICS 2018*: 579-588.

25. Mohammad Hajiabadi, Bruce M. Kapron: Toward Fine-Grained Blackbox Separations Between Semantic and Circular-Security Notions. *EUROCRYPT (2) 2017*: 561-591.

26. Ariel Webster, Bruce M. Kapron, Valerie King: Stability of certainty and opinion in influence networks. *ASONAM 2016*: 1309-1320.

27. Erkan Ersan, Lior Malka, Bruce M. Kapron: Semantically Non-preserving Transformations for Antivirus Evaluation. *FPS 2016*: 273-281.

28. Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan, Lszl Tth: On a variant of multilinear modular hashing with applications to authentication and secrecy codes. *ISITA 2016*: 320-324.

29. Mohammad Hajiabadi, Bruce M. Kapron, Venkatesh Srinivasan: On Generic Constructions of Circularly-Secure, Leakage-Resilient Public-Key Encryption Schemes. *Public Key Cryptography (2) 2016*: 129-158.

30. Russell Impagliazzo, Ragesh Jaiswal, Valentine Kabanets, Bruce M. Kapron, Valerie King, Stefano Tessaro: Simultaneous Secrecy and Reliability Amplification for a General Channel Model. *TCC (B1) 2016*: 235-261.

31. Mohammad Hajiabadi, Bruce M. Kapron: Reproducible Circularly-Secure Bit Encryption: Applications and Realizations. *CRYPTO (1) 2015*: 224-243.

32. Mohammad Hajiabadi, Bruce M. Kapron: Gambling, Computational Information and Encryption Security, *International Conference on Information-Theoretic Security (ICITS) 2015*: 141-158.

33. Mohammad Hajiabadi, Bruce M. Kapron: Computational soundness of coinductive symbolic security under active attacks. *Theory of Cryptography Conference (TCC) 2013*: 539-558.

34. Bruce M. Kapron, Valerie King, Benjamin Mountjoy. Dynamic graph connectivity in polylogarithmic worst-case time. *SODA 2013*: 1131-1142. (*Co-recipent of best paper award*)

35. Sean Chester, Bruce M. Kapron, Ganesh Ramesh, Gautam Srivastava, Alex 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.

36. Bruce M. Kapron, Gautam Srivastava, S. Venkatesh: Social Network Anonymization via Edge Addition. *Int. Conf. on Advances in Social Networks Analysis and Mining, (ASONAM) 2011*: 155-162.

37. Gilles Barthe, Marion Daubignard, Bruce M. Kapron, Yassine Lakhnech: Computational indistinguishability logic. *ACM CCS 2010*: 375-386.

38. Gilles Barthe, Marion Daubignard, Bruce M. Kapron, Yassine Lakhnech, Vincent Laporte: On the Equality of Probabilistic Terms. *LPAR 2010*: 46-63.

39. Bruce M. Kapron, David Kempe, Valerie King, Jared Saia, Vishal Sanwalani: Fast asynchronous byzantine agreement and leader election with full information. *SODA 2008*: 1038-1047.

40. Bruce M. Kapron, Lior Malka, S. Venkatesh: A Characterization of Non-interactive Instance-Dependent Commitment-Schemes (NIC). *ICALP 2007*: 328-339.

41. Daniel Holtby, Bruce M. Kapron, Valerie King: Lower bound for scalable Byzantine Agreement. *PODC 2006*: 285-291.

42. Russell Impagliazzo, Bruce M. Kapron: Logics for Reasoning about Cryptographic Constructions. *FOCS 2003*: 372-383.

43. Samuel R. Buss, Bruce M. Kapron: Resource-Bounded Continuity and Sequentiality for Type-2 Functionals. *LICS 2000*: 77-83.

44. Peter Clote, Aleksander Ignjatovic, Bruce M. Kapron: Parallel computable higher type functionals. *FOCS 1993*: 72-81.

45. Joseph Y. Halpern, Bruce M. Kapron: Zero-One Laws for Modal Logic. *LICS 1992*: 369-380.

46. Bruce M. Kapron, Stephen A. Cook: A New Characterization of Mehlhorn's Polynomial Time Functionals. *FOCS 1991*: 342-347.

47. Stephen A. Cook, Bruce 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: $26,000. Years of tenure: 2016-2021. Title: "Securing the foundations of security".

## RECENTLY HELD MAJOR RESEARCH GRANTS

- Intel Research Gift. Amount: $70,000. Years of tenure 2014-2015. Title: "Automated Antivirus Evaluation via Malware Mutations".
- Intel Research Contract. Amount: $70,000. Years of tenure 2015-2016. Title: "Automated Antivirus Evaluation via Malware Mutations".
- 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: $24,000. Years of tenure: 2011-2016. Title: "Foundational studies in privacy and security".
- 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”

- Wanda Boyer, M.Sc., 2016. “A Decision and Minimization Procedure for Modal Logic

- Mohammad Hajiabadi, Ph.D., 2016. “Encryption Security Against Key-Dependent-Message Attacks: Applications, Realizations and Separations”.

- Ariel Webster, M.Sc., 2016. “Stability of Certainty and Opinion in Influence Networks

- Khodakhast Bibak, Ph.D. 2017. “Number Theoretic Methods and their Significance in Computer Science, Information Theory, Combinatorics, and Geometry

- Erkan Ersan, M.Sc., 2017. “On the (In)security of Behavioral-based Dynamic Anti-Malware Techniques