Bruce M. Kapron
Department of Computer Science, University of Victoria
Victoria, BC, CANADA V8W 2Y2
(250)-472-5725 (w), (250)-813-3343 (c)
bmkapron@uvic.ca

RESEARCH INTERESTS

Computability, 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

5/22-7/22 Distinguished Professor, Fondation Sciences Mathématiques de Paris

2/22-4/22 Visiting Fellow, Insitute of Advanced Studies, University of Bologna

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.

BOOKS

1. Bruce M. Kapron: *Logic, Automata, and Computational Complexity: The Works of Stephen A. Cook.* ACM Books 43, ACM 2023, ISBN 979-8-4007-0779-7

REFEREED JOURNAL PUBLICATIONS

2. Emmanuel Hainry, Bruce M. Kapron, Jean-Yves Marion, Romain Péchoux: Complete and tractable machine-independent characterizations of second-order polytime. *Log. Methods Comput. Sci.* **21** (1) (2025)
3. Emmanuel Hainry, Bruce M. Kapron, Jean-Yves Marion, Romain Péchoux: A tier-based typed programming language characterizing Feasible Functionals. *Log. Methods Comput. Sci.* **18** (1) (2022)
4. Bruce M. Kapron, Florian Steinberg: Type-two polynomial-time and restricted lookahead. *Theor. Comput. Sci.* **813**: 1-19 (2020)
5. Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan: A generalization of Schönemann's theorem via a graph theoretic method. *Discret. Math.* **342** (11): 3057-3061 (2019)

6. 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)

7. Mohammad Hajiabadi, Bruce M. Kapron: Reproducible Circularly Secure Bit Encryption: Applications and Realizations. *J. Cryptology* **30** (4): 1187-1237 (2017)

8. Khodakhast Bibak, Bruce M Kapron, Venkatesh Srinivasan, Roberto Tauraso, László Tóth: Restricted linear congruences. *Journal of Number Theory* **171**: 128-144 (2017)

9. Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan: On a restricted linear congruence. *International Journal of Number Theory* **12** (8): 2167-2171 (2016)

10. 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)

11. Khodakhast Bibak, Bruce M. Kapron, Venkatesh Srinivasan: MMH* with arbitrary modulus is always almost-universal. *Inf. Process. Lett.* **116** (7): 481-483 (2016)

12. 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)

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

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

15. 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)

16. 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)

17. D. Holtby, B.M. Kapron, V. King: Lower bound for scalable Byzantine Agreement. *Dist. Com.* **21**(4): 239-248 (2008)

18. R. Impagliazzo, B.M. Kapron: Logics for reasoning about cryptographic constructions. *JCSS* **72**(2): 286-320 (2006)

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

20. S.R. Buss, B.M. Kapron: Resource-bounded continuity and sequentiality for type-two functionals. *ACM Trans. Comput. Log.* **3**(3): 402-417 (2002)

21. 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)

22. B.M. Kapron: Feasibly Continuous Type-Two Functionals. *Comp. Compl.* **8**(2): 188-201 (1999)

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

24. 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)

25. 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)

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

27. J.Y. Halpern, B.M. Kapron: Zero-One Laws for Modal Logic. *APAL* **69**(2-3): 157-193 (1994)

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

REFEREED CONFERENCE PUBLICATIONS

29. Bruce M. Kapron, Koosha Samieefar: On The Computational Complexity of Games with Uncertainty. To appear in *CIAC 2025*.

30. Bruce M. Kapron, Koosha Samieefar: The Computational Complexity of Equlibria with Strategic Constraints. *SOFSEM 2025*: 112-127.

31. Emmanuel Hainry, Bruce M. Kapron, Jean-Yves Marion, Romain Péchoux: Declassification Policy for Program Complexity Analysis. *LICS 2024*: 41:1-41:14

32. Ugo Dal Lago, Davide Davoli, Bruce M. Kapron: On Separation Logic, Computational Independence, and Pseudorandomness. *CSF 2024*: 80-95

33. Bruce M. Kapron, Koosha Samieefar: On the Computational Complexity of Quasi-Variational Inequalities and Multi-Leader-Follower Games. *AAMAS 2024*: 2324-2326.

34. Zahra Javar, Bruce M. Kapron: Linicrypt in the Ideal Cipher Model. *ProvSec 2023*: 91-111

35. Zahra Javar, Bruce M. Kapron: Preimage awareness in Linicrypt. *CSF 2023*: 33-42

36. Emmanuel Hainry, Bruce M. Kapron, Jean-Yves Marion, Romain Péchoux: Complete and tractable machine-independent characterizations of second-order polytime. *FoSSaCS 2022*: 368-388 (Winner of the EATCS Award for Best Theory Paper at ETAPS)

37. Emmanuel Hainry, Bruce M. Kapron, Jean-Yves Marion, Romain Péchoux: A tier-based typed programming language characterizing Feasible Functionals. *LICS 2020*: 535-549

38. Bruce M. Kapron, Florian Steinberg: Type-two Iteration with Bounded Query Revision. *DICE-FOPARA@ETAPS 2019*: 61-73

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

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

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

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

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

44. 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.

45. 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.

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

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

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

49. 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*)

50. 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.

51. 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.

52. G. Barthe, M. Daubignard, B.M. Kapron, Y. Lakhnech: Computational indistinguishability logic. *ACM CCS 2010*: 375-386.

53. G. Barthe, M. Daubignard, B.M. Kapron, Y. Lakhnech, V. Laporte: On the Equality of Probabilistic Terms. *LPAR 2010*: 46-63.

54. 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.

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

56. D. Holtby, B.M. Kapron, V. King: Lower bound for scalable Byzantine Agreement. *PODC 2006*: 285-291.

57. R. Impagliazzo, B.M. Kapron: Logics for Reasoning about Cryptographic Constructions. *FOCS 2003*: 372-383.

58. S.R. Buss, B.M. Kapron: Resource-Bounded Continuity and Sequentiality for Type-2 Functionals. *LICS 2000*: 77-83.

59. Bruce M. Kapron, Michael R. Fellows, Rodney G. Downey, Michael T. Hallett, Harold T. Wareham: The Parameterized Complexity of Some Problems in Logic and Linguistics. *LFCS 1994*: 89-100

60. P. Clote, A. Ignjatovic, B.M. Kapron: Parallel computable higher type functionals. *FOCS 1993*: 72-81.

61. J.Y. Halpern, B.M. Kapron: Zero-One Laws for Modal Logic. *LICS 1992*: 369-380.

62. B.M. Kapron, S.A. Cook: A New Characterization of Mehlhorn's Polynomial Time Functionals. *FOCS 1991*: 342-347.

63. 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: $55,000. Years of tenure: 2021-2026. Title: "The Complexity of Computing with Infinite Data".

RECENTLY 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".
- Intel Research Contract. Amount: $70,000. Years of tenure 2015-2016. Title: "Automated Antivirus Evaluation via Malware Mutations".
- Intel Research Gift. Amount: $70,000. Years of tenure 2014-2015. 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

MASTER'S DEGREE

- Zehou Wu, M.Sc., 2025. "Two Views of Cryptography and the Gap In-Between"
- Guy-Warwick Evans, M.Sc., 2017. "Artificial Intelligence: Where We Came From, Where We Are Now, and Where We Are Going"
- Erkan Ersan, M.Sc., 2017. "On the (In)security of Behavioral-based Dynamic Anti-Malware Techniques"
- Ariel Webster, M.Sc., 2016. "Stability of Certainty and Opinion in Influence Networks"
- Wanda Boyer, M.Sc., 2016. "A Decision and Minimization Procedure for Modal Logic"
- Chelsea Foster, M.Sc., 2015. "Finitely iterated rational secret sharing with private information"
- Nicholas Vining, M.Sc., 2011. "Next generation content creation: an investigative approach"
- Mohammad Hajiabadi, M.Sc., 2011. "Coinduction and computational semantics for public-key encryption"
- Warren Schenkenfelder, M.Sc., 2008. "Learning bisimulation"
- Chris Ware, M.Sc., 2008. "Modeling and analysis of quantum cryptographic protocols".
- Gautam Srivastava, M.Sc., 2006. "PRNGs using multiple sources of entropy".

- 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"
- Wai-Han Chiu, M.Sc., 2003. "Modeling and verification of message sequence charts using process algebras and temporal logic model checking."
- Georgi Kostadinov, M.Sc., 2000. "A compositional proof system for model checking with tagging."
- Brent Knight, M.Sc., 1994. "Safe strict evaluation of redundancy-free programs from proofs."

DOCTORAL

- Zahra Javar, Ph.D. 2024. "Formal Algebraic Reasoning About Compression Function Security". Current Position: Applied Cryptographer, gnosis.io.
- Eduard Wisernig, Ph.D. 2020. "Marine Visualization System: an Augmented Reality Approach". Current position: Founder and CEO, Wiser Marine Technologies.
- Khodakhast Bibak, Ph.D. 2017. "Number Theoretic Methods and their Significance in Computer Science, Information Theory, Combinatorics, and Geometry". Current position: Staff Engineer (Post-Quantum Cryptography), Walmart Global Tech
- Mohammad Hajiabadi, Ph.D., 2016. "Encryption Security Against Key-Dependent-Message Attacks: Applications, Realizations and Separations". Current position: Associate Professor, Computer Science Department, University of Waterloo.
- Gautam Srivastava, Ph.D., 2011. "Graph anonymization through edge and vertex addition". Current position: Asociate Professor, Department of Mathematics and Computer Science, Brandon University, Brandon, MB, Canada.
- Lior Malka, Ph.D., 2008, "A study of perfect zero-knowledge proofs". Current position: Senior Security Architect, Intel, Santa Clara, CA.
- Dilian Gurov, Ph.D., 1997. "A modal mu-calculus and a proof system for value passing processes." Current position: Professor, Division of Theoretical Computer Science, KTH, Stockholm.

SELECTED INVITED TALKS

"Fifty Years of NP-Completeness", *Institute for Advanced Studies, University of Bologna*, February 8 2022. (Invited Public Lecture)

"Complexity of Type-3 Sequential Functionals", *Shonan Seminar 151: Higher-order Complexity Theory and its Applications*, October 7–11 2019, Shonan Village Center, Japan (International workshop.) October 7 - 10, 2019

"Type-two Feasibility via Bounded Query Revision", *Sixteenth International Conference on Computability and Complexity in Analysis*, July 8–11, 2019, Zagreb, Croatia (International conference with contributed and invited talks.) (PlenaryTalk)

"Subrecursion, P and NP", *Symposium on 50 Years of Complexity Theory: A Celebration of the Work of Stephen Cook*, May 6–9, 2019, The Fields Institute, Toronto, ON (International workshop.)

"Min-max from a Higher-order Perspective", *PIHOC 2019, Second Workshop on Probabilistic Interactive and Higher-Order Computation*, 6–7 February 2019 (International workshop.)

"Restricted-query Models for Type-two Polynomial Time", *Shonan Seminar 115: Intensional and extensional aspects of computation: From computability and complexity to program analysis and security*, January 22–25, 2018, Shonan Village Center, Japan (International workshop.)

"Gambling, Computational Information, and Encryption Security", *32nd British Colloquium of Theoretical Computer Science (BCTCS 2016)*, March 22–24 2016, Queen's University Belfast (Regional conference with contributed and invited talks.)

"Type-2 Polynomial Time and Composability", *Higher Order Computation: Types, Complexity, Applications*, June 16–18 2014, Institut Henri Poincaré, Paris (International workshop.)

"Implicit Computational Complexity and Computational Soundness", *Shonan Seminar 033: Implicit Computational Complexity and Applications: Resource Control, Security, Real-Number Computation*, November 4–7, 2013, Shonan Village Center, Japan (International workshop.)

"Characterising Computational Entropy", *Workshop on Computed-Aided Security*, January 13 2012, Verimag, Grenoble (Regional workshop.)

"Formal Methods in Security (Tutorial)", *1st Canada-France MITACS Workshop on Foundations & Practice of Security*, May 31–June 2, 2008 Montreal, QC (International workshop.)

"Tutorial: Formal Representations of Polynomial-time Algorithms and Security", *DIMACS Workshop on Security Analysis of Protocols*, June 7–9, 2004, DIMACS Center, Rutgers University, Piscataway, NJ (International workshop.)

"An Induction Principle for Computational Indistinguishability", *A Workshop in Honour of Stephen A. Cook: "Steve Cook at 60"*, April 28–29, 2000, Fields Institute, Toronto, ON (International workshop.)

"Towards a theory of time-bounded type-2 computability", *DIMACS Workshop on Computational Complexity and Programming Languages*, July 25–26, 1996, RUTCOR, Rutgers University, Piscataway, NJ (International workshop.)