Jason T. LeGrow

Virginia Tech
Department of Mathematics
470 McBryde Hall
225 Stanger Street
Blacksburg, VA, 24060 USA

jlegrow@vt.edu
https://jasonlegrow.github.io

Research Interests

Isogeny-based cryptography. Particularly, the design of isogeny-based protocols, algorithms for more secure and efficient implementations of isogeny-based protocols, and (quantum) cryptanalysis.

Employment

Assistant Professor, Virginia Tech, Mathematics Department	08/2022 – Present
Research Fellow, University of Auckland, Mathematics Department	09/2020 – 06/2022

Education

PhD in Combinatorics and Optimization—Quantum Information, University of Waterloo	08/2020
MMath in Combinatorics and Optimization, University of Waterloo	04/2016
BSc (Hons) in Pure Mathematics, Memorial University of Newfoundland	04/2014

Publications

Accepted

1. Brown, D. R. L., Koblitz, N., and **LeGrow, J. T.** *Cryptanalysis of 'MAKE'.* Journal of Mathematical Cryptology, vol. 16, no. 1 (2022), pp. 98-102
2. **LeGrow, J. T.** and Hutchinson, A. *(Short Paper) Analysis of a Strong Fault Attack on Static/Ephemeral CSIDH.* Proceedings of The 16th International Workshop on Security—IWSEC 2021.
3. Dobson, S., Galbraith, S. D., **LeGrow, J.**, Ti, Y. B., and Zobernig, L. *An adaptive attack on 2-SIDH.* International Journal of Computer Mathematics: Computer Systems Theory, 5(4), 282–299.
4. Azarderakhsh, R., Jao, D., Koziel, B., **LeGrow, J. T.**, Soukharev, V. and Taraskin, O. *How not to Construct an Isogeny-Based PAKE.* In: Conti M., Zhou J., Casalicchio E., Spognardi A. (eds) Applied Cryptography and Network Security. ACNS 2020. Lecture Notes in Computer Science, vol 12146. Springer, Cham.
5. Hutchinson, A., **LeGrow, J. T.**, Koziel, B., and Azarderakhsh, R. *Further Optimizations of CSIDH: A Systematic Approach to Efficient Strategies, Permutations, and Bound Vectors.* In: Conti M., Zhou J., Casalicchio E., Spognardi A. (eds) Applied Cryptography and Network Security. ACNS 2020. Lecture Notes in Computer Science, vol 12146. Springer, Cham.
6. Taraskin, O., Soukharev, V., Jao, D., and **LeGrow, J. T.** *Towards Isogeny-Based Password-Authenticated Key Establishment.* Journal of Mathematical Cryptology, 15(1), 18–30.
7. Jao, D., **LeGrow, J.**, Leonardi, C., and Ruiz-Lopez, L. A subexponential-time, polynomial quantum space algorithm for inverting the CM group action. Journal of Mathematical Cryptology, 14(1), 129–138.
8. **LeGrow, J. T.**, Pike, D. A., and Poulin, J. *Hamiltonicity and Cycle Extensions in 0-Block-Intersection Graphs of Balanced Incomplete Block Designs.* Designs, Codes, and Cryptography. (2016) 80: 421 – 433.

Preprints and Submitted Articles

1. **LeGrow, J. T.,** Ti, Yan Bo and Zobernig, Lukas. *Supersingular Non-Superspecial Abelian Surfaces in Cryptography.*
2. **LeGrow, J. T.,** Koziel B., and Azarderakhsh, R. *Multiprime Strategies in Serial eSIDH.*
3. Buser, M., Dowsley, R., Esgin, M. F., Gritti, C., Kasra, S. Kermanshahi, Kuchta, V., **LeGrow, J. T.**, Liu, J. K., Phan, R., Sakzad, A., Steinfeld, R., and Yu, J. *A Survey on Exotic Signatures for Post-Quantum Blockchain: Challenges & Research Directions.*
4. **LeGrow, J. T.** *A Faster Method for Fault Attack Resistance in Static/Ephemeral CSIDH.*

Research Talks

Invited

University of Auckland, Algebra and Combinatorics Seminar	05/2022
University of Waterloo, Cryptography Reading Group	12/2021
GITAM Hyderabad, Faculty Development Program	09/2021
University of Auckland, Algebra and Combinatorics Seminar	07/2021
University of Waterloo, Cryptography Reading Group	10/2020
Institute for Quantum Computing, Student Seminar	02/2020
University of Waterloo, Cryptography Reading Group	09/2019

Contributed

International Workshop on Security (IWSEC), Online	09/2021
Mathcrypt, University of California Santa Barbara	08/2019
Mathcrypt, University of California Santa Barbara	08/2018
British Combinatorial Conference, University of Warwick	07/2015
Canadian Undergraduate Mathematics Conference, Carleton University	07/2014
Science Atlantic, University of Prince Edward Island	10/2013

Supervision

University of Auckland

Ling Qin, PhD. Co-supervised with Steven Galbraith and Gabriel Verret	01/2022 – Present
Alexander Sharples, BSc(Hons). Co-supervised with Arkadii Slinko	07/2021 – 04/2022

Teaching

Virginia Tech

Math 4175: Cryptography 1	Fall 2022

University of Auckland

Maths 253: Algebra and Calculus 3	Semester 1, 2022
Maths 714: Number Theory	Semester 2, 2021

University of Waterloo

CO 227: Introduction to Optimization (Non-Specialist Level)	Winter 2020

Teaching Assistance

University of Waterloo

CO 687: Applied Cryptography	Fall 2019
CO 602: Fundamentals of Optimization	Fall 2019
CO 685: Mathematics of Public-Key Cryptography	Fall 2018
CO 687: Applied Cryptography	Winter 2018
MATH 674: Special Topics in Mathematical Connections	Winter 2017
CO 687: Applied Cryptography	Winter 2017
MATH 239: Introduction to Combinatorics	Fall 2016
MATH 239: Introduction to Combinatorics	Winter 2016
CO 685: Mathematics of Public-Key Cryptography	Fall 2015
ECE 103: Discrete Mathematics	Spring 2015
MATH 215: Linear Algebra	Winter 2015
MATH 115: Linear Algebra	Fall 2014

Memorial University of Newfoundland

Math 2130: Technical Writing for Mathematics	Fall 2013
Math 1050: Finite Mathematics I	Fall 2012
Math 1001: Calculus II	Winter 2012

Awards

University of Waterloo

Queen Elizabeth II Graduate Scholarship in Science and Technology	09/2019
NSERC Michael Smith Foreign Study Supplement	01/2019
David Johnston International Experience Award	01/2019
President's Graduate Scholarship	09/2019
NSERC Alexander Graham Bell Canada Graduate Scholarship—Doctoral	09/2016
President's Graduate Scholarship	09/2016
NSERC Alexander Graham Bell Canada Graduate Scholarship—Master's	09/2015
President's Graduate Scholarship	09/2015
Ontario Graduate Scholarship	09/2014
President's Graduate Scholarship	09/2014
Combinatorics and Optimization Entrance Scholarship	09/2014

Memorial University of Newfoundland

Governor-General's Silver Medal for Academic Excellence	06/2014
University Medal for Academic Excellence in Pure Mathematics	06/2014
Lou Visintin Award	04/2014
NSERC Undergraduate Student Research Award	05/2013 – 08/2013
Centenary of Responsible Government Scholarship	02/2013
NSERC Undergraduate Student Research Award	05/2012 – 08/2012
Dr. Arthur Barnes Scholarship	02/2012
Centenary of Responsible Government Scholarship	02/2011
Dr. Warren and Catherine Ball Memorial Entrance Scholarship	09/2010

Service

Professional Service

Program committee for: Indocrypt 2022, ACISP 2022, ICSP 2021
Reviewer or subreviewer for: Australasian Journal of Combinatorics, Journal of Mathematical Cryptology, Theoretical Computer Science, IET Information Security, ANTS XV, PQCrypto 2021, ACISP 2021, AsiaCrypt 2021, AsiaCrypt 2019, IWSEC 2017

Service at Virginia Tech

Colloquium Committee Member	08/2022 – Present
Algebra Seminar Co-organizer	08/2022 – Present

Service at the University of Waterloo

Faculty of Mathematics Faculty Council Adminstrative Committee	09/2018 – 08/2019
Faculty of Mathematics Faculty Council	09/2018 – 08/2019
Combinatorics and Optimization Graduate Student Representative	05/2018 – 08/2020
Faculty of Mathematics Graduate Studies Committee	09/2017 – 08/2019
Mathematics Graduate Student Association—Departmental Director	09/2017 – 08/2020
Combinatorics and Optimization Graduate Student Representative	05/2016 – 04/2017

Service at Memorial University of Newfoundland

Mathematics and Statistics Undergraduate Studies Committee	09/2013 – 04/2014
Faculty of Science Undergraduate Student Society—Treasurer	09/2013 – 04/2014
Mathematics and Statistics Student Society—Communications Director	05/2013 – 04/2014