Jason T. LeGrow

Virginia Tech
Department of Mathematics
470 McBryde Hall
225 Stanger Street
Blacksburg, VA, 24061 USA

jlegrow@vt.edu
https://jasonlegrow.github.io
https://scholar.google.com/citations?user=4OMhhMIAAAAJ

Research Interests Post-quantum cryptography. Particularly, design of isogeny-based protocols and alogrithms for their secure and efficient implementation, group action-based cryptography, 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
Thesis: *Design, Analysis, and Optimization of Isogeny-Based Key Establishment Protocols*
Advisors: David Jao and Michele Mosca

MMath in Combinatorics and Optimization, University of Waterloo 04/2016

BSc (Hons) in Pure Mathematics, Memorial University of Newfoundland 04/2014

Publications

Submitted Articles

1. Ryann Cartor, Nathan Daly, Giulia Gaggero, **Jason T. LeGrow**, Andrea Sanguinetti, and Silva Sconza. "Post-Quantum Adaptor Signatures with Strong Security from Cryptographic Group Actions."
2. Veronika Kuchta, Shi Bai, Edoardo Persichetti, and **Jason T. LeGrow**. "The Limits of the Lattice Isomorphism Problem for Advanced Cryptographic Primitives."
3. Veronika Kuchta, **Jason T. LeGrow**, and Edoardo Persichetti. "Post-quantum blind signatures from code equivalence".
4. Sarah Arpin, Ross Bowden, James Clements, Wissam Ghantous, **Jason T. LeGrow**, and Krystal Maughan. "Cycles and Cuts in Supersingular L-Isogeny Graphs".

Accepted

5. **Jason T. LeGrow.** "Duality Lower Bounds for the Cost of Group Action Evaluation in CSIDH." To appear in Transactions on Mathematical Cryptology.
6. Veronika Kuchta, **Jason T. LeGrow**, Hiram Lopez, and Gretchen L. Matthews. "Towards IOPPs from Folded Reed-Solomon Codes." To appear in Transactions on Mathematical Cryptology.

In Print

7. Hailey Egan, **Jason T. LeGrow**, Gretchen L Matthews, and Jeff Suliga. "Influences of some families of error-correcting codes". In: *Involve, a Journal of Mathematics* 18.2 (2025), pp. 329–349
8. **Jason T. LeGrow**, Travis Morrison, Jamie Sikora, and Nic Swanson. "Masking Countermeasures Against Side-Channel Attacks on Quantum Computers". In: *2024 IEEE International Conference on Quantum Computing and Engineering (QCE)*. vol. 01. 2024, pp. 1809–1816
9. Tinghung Chiu, **Jason LeGrow**, and Wenjie Xiong. "Practical Fault Injection Attacks on Constant Time CSIDH and Mitigation Techniques". In: *Proceedings of the 2024 Workshop on Attacks and Solutions in Hardware Security*. 2024, pp. 11–22
10. Shuichi Katsumata, Yi-Fu Lai, **Jason T. LeGrow**, and Ling Qin. "CSI-Otter: Isogeny-based (partially) blind signatures from the class group action with a twist". In: *Des. Codes Cryptogr.* (2024)
11. **Jason T. LeGrow**, Yan Bo Ti, and Lukas Zobernig. "Supersingular non-superspecial abelian surfaces in cryptography". In: *Mathematical Cryptology* 3.2 (2023), pp. 11–23
12. Shuichi Katsumata, Yi-Fu Lai, **Jason T. LeGrow**, and Ling Qin. "CSI-Otter: Isogeny-based (partially) blind signatures from the class group action with a twist". In: *Annual International Cryptology Conference*. Springer Nature Switzerland Cham. 2023, pp. 729–761

13. **Jason T. LeGrow**, Brian Koziel, and Reza Azarderakhsh. "Multiprime strategies for serial evaluation of eSIDH-like isogenies". In: *International Conference on Science of Cyber Security*. Springer Nature Switzerland Cham. 2023, pp. 347–366
14. **Jason T. LeGrow**. "A faster method for fault attack resistance in static/ephemeral CSIDH". in: *Journal of Cryptographic Engineering* (2023), pp. 1–12
15. Maxime Buser, Rafael Dowsley, Muhammed Esgin, Clémentine Gritti, Shabnam Kasra Kermanshahi, Veronika Kuchta, **Jason T. LeGrow**, Joseph Liu, Raphaël Phan, Amin Sakzad, Ron Steinfeld, and Jiangshan Yu. "A survey on exotic signatures for post-quantum blockchain: Challenges and research directions". In: *ACM Computing Surveys* 55.12 (2023), pp. 1–32
16. Daniel RL Brown, Neal Koblitz, and **Jason T. LeGrow**. "Cryptanalysis of 'MAKE"'. in: *Journal of Mathematical Cryptology* 16.1 (2022), pp. 98–102
17. **Jason T. LeGrow** and Aaron Hutchinson. "(Short paper) Analysis of a strong fault attack on static/ephemeral CSIDH". in: *International Workshop on Security*. Springer International Publishing Cham. 2021, pp. 216–226
18. Samuel Dobson, Steven D. Galbraith, **Jason T. LeGrow**, Yan Bo Ti, and Lukas Zobernig. "An adaptive attack on 2-SIDH". in: *International Journal of Computer Mathematics: Computer Systems Theory* 5.4 (2020), pp. 282–299
19. Reza Azarderakhsh, David Jao, Brian Koziel, **Jason T. LeGrow**, Vladimir Soukharev, and Oleg Taraskin. "How not to create an isogeny-based PAKE". in: *Applied Cryptography and Network Security: 18th International Conference, ACNS 2020, Rome, Italy, October 19–22, 2020, Proceedings, Part I 18*. Springer International Publishing. 2020, pp. 169–186
20. Aaron Hutchinson, **Jason T. LeGrow**, Brian Koziel, and Reza Azarderakhsh. "Further optimizations of CSIDH: a systematic approach to efficient strategies, permutations, and bound vectors". In: *Applied Cryptography and Network Security: 18th International Conference, ACNS 2020, Rome, Italy, October 19–22, 2020, Proceedings, Part I 18*. Springer International Publishing. 2020, pp. 481–501
21. Oleg Taraskin, Vladimir Soukharev, David Jao, and **Jason T. LeGrow**. "Towards isogeny-based password-authenticated key establishment". In: *Journal of Mathematical Cryptology* 15.1 (2020), pp. 18–30
22. David Jao, **Jason T. LeGrow**, Christopher Leonardi, and Luis Ruiz-Lopez. "A subexponential-time, polynomial quantum space algorithm for inverting the CM group action". In: *Journal of Mathematical Cryptology* 14.1 (2020), pp. 129–138
23. **Jason T. LeGrow**, David A. Pike, and Jonathan Poulin. "Hamiltonicity and cycle extensions in 0-block-intersection graphs of balanced incomplete block designs". In: *Designs, Codes and Cryptography* 80.3 (2016), pp. 421–433

Talks

Plenaries and Colloquiua

1. **Mathematics of Communication - Cryptography and Coding Theory** 04/2025
   Mathematics - Opportunites in Reseearch and Education (MORE), Virginia Tech
2. **Isogeny-Based Post-Quantum Cryptography** 11/2023
   Mathematics Department Colloquium, Virginia Tech
3. **Optimization of Algorithms for Isogeny-Based Key Establishment** 06/2023
   Mathematics Department Colloquium, University of South Florida
4. **Some Problems in Isogeny-Based Cryptography** 02/2022
   Mathematics Department Colloquium, Virginia Tech

Invited

5. **Preliminary Report: CSI-Dragon - Blind Signatures go HD!** 08/2025
   Workshop on Isogeny Graphs in Cryptography, Banff International Research Station
6. **Practical Fault Injection Attacks on CSIDH and Mitigation Techniques** 07/2025
   Mathematical Congress of the Americas, Special Session on Post-Quantum Cryptography
7. **Practical Fault Injection Attacks on CSIDH and Mitigation Techniques** 07/2025
   SIAM Algebraic Geomtery, Minisymposium on Applications of Isogenies in Cryptography
8. **Duality Lower Bounds on the Cost of CSIDH Group Action Evaluation** 07/2025
   Workshop on Coding Theory and Cryptography, Virginia Tech Steger Center
9. **Duality Lower Bounds on the Cost of CSIDH Group Action Evaluation** 06/2025
   Applied Algebra Days, University of South Florida
10. **Practical Fault Injection Attacks on CSIDH, and Mitigation Techniques** 03/2025
    Special Session on Post-Quantum Cryptography, AMS Southeastern Sectional Meeting
11. **Post-Quantum Blind Signatures from Code Equivalence** 01/2025
    Special Session on Cryptography and Related Fields, Joint Mathematics Meetings
12. **Post-Quantum Blind Signatures from Group Actions** 12/2024
    Mathematical Cryptography Workshop, University of Auckland
13. **Post-Quantum Adaptor Signatures from Non-Abelian Group Actions** 07/2024
    VT-Swiss Coding Theory and Cryptography Summer School, Virginia Tech Steger Center
14. **Post-Quantum Cryptography with Advanced Functionalities** 04/2024
    Workshop on Secure & Trustworthy Data & Technology, Virginia Tech
15. **Matrix Code Equivalence in Cryptography** 04/2024
    Algebraic Coding Theory in Virginia, Virginia Tech
16. **Post-Quantum Blind Signatures from Group Actions** 03/2024
    Crypto Café, Florida Atlantic University
17. **Post-Quantum Cryptography with Advanced Functionalities** 03/2024
    Data Security and Machine Learning Workshop, Clemson University
18. **CSI-Otter: An Isogeny-Based Blind Signature Scheme** 01/2024
    Special Session on Cryptography and Related Fields, AMS Joint Mathematics Meetings
19. **Post-Quantum Cryptography with Advanced Functionalities** 11/2023
    Center for Quantum Information Science and Engineering Symposium, Virginia Tech
20. **Post-Quantum Exotic Signatures from Group Actions** 07/2023
    Workshop in Coding and Cryptography, Virginia Tech Steger Center
21. **CSI-Otter: An Isogeny-Based Blind Signature Scheme** 03/2023
    Minisymposium on Public-Key Cryptography, SIAM SEAS Sectional Meeting
22. **Techniques for Fault Attack-Resistance in Static/Ephemeral CSIDH** 01/2023
    Algebra Seminar, Virginia Tech
23. **Optimization of Algorithms for Isogeny-Based Key Establishment** 10/2022
    Algebra Seminar, Virginia Tech
24. **Some Problems in Isogeny-Based Cryptography** 02/2022
    Cryptography Presentation, Florida Atlantic University
25. **Techniques for Fault Attack-Resistance in Static/Ephemeral CSIDH** 05/2022
    Algebra and Combinatorics Seminar, University of Auckland
26. **CTIDH: Faster Constant-Time CSIDH** 12/2021
    Cryptography Reading Group, University of Waterloo
27. **Isogeny-Based Exotic Signatures in Post-Quantum Blockchain** 09/2021
    Faculty Development Program, GITAM Hyderabad
28. **Optimization of Algorithms for Isogeny-Based Key Establishment** 07/2021
    Algebra and Combinatorics Seminar, University of Auckland

29. **Compact, Efficient, and UC-Secure Isogeny-Based Oblivious Transfer** 10/2020
Cryptography Reading Group, University of Waterloo

Contributed

30. **Towards IOPPs from Folded Reed-Solomon Codes** 08/2025
6th International Workshop on Mathematical Cryptology (MathCrypt), University of California Santa Barbara
31. **Duality Lower Bounds for the Cost of Group Action Evaluation in CSIDH** 08/2025
6th International Workshop on Mathematical Cryptology (MathCrypt), University of California Santa Barbara
32. **Multiprime Strategies for Serial Evaluations of eSIDH-Like Isogenies** 07/2023
International Conference on the Science of Cybersecurity (SciSec), Royal Melbourne Institute of Technology
33. **Analysis of a Strong Fault Attack on Static/Ephemeral CSIDH** 09/2021
International Workshop on Security (IWSEC), Online
34. **Towards Isogeny-Based Password-Authenticated Key Establishment** 08/2019
Mathcrypt, University of California Santa Barbara
35. **A Subexponential-Time, Quantum Polynomial-Space Algorithm for Inverting the CM Group Action** 08/2018
Mathcrypt, University of California Santa Barbara
36. **$\mathbf{A}_1'$ Cyclic Orderings of Balanced Incomplete Block Designs** 07/2015
British Combinatorial Conference, University of Warwick

Current Students

1. Adam Downs, M.S. 08/2024 – Present
2. Andrew Norton, M.S. 08/2024 – Present
3. Nathan Daly, Ph.D. 08/2023 – Present
4. Wendi Gao, Ph.D. 05/2023 – Present

Past Students

Virginia Tech

1. Nathan Daly, M.S. 08/2023 – Present
2. Evan Stosic, M.S. 08/2023 – Present
3. Wendi Gao, M.S. 10/2022 – 05/2023
Optimization of Isogeney Evaluations in CSIDH

University of Auckland

4. Ling Qin, PhD. Co-supervised with Steven Galbraith and Gabriel Verret 12/2021 – 09/2025
Isogeny-Based Cryptographic Protocols with Advanced Functionalities
5. Alexander Sharples, BSc(Hons). Co-supervised with Arkadii Slinko 07/2021 – 04/2022
Authenticated Encrypted Secret Sharing

Teaching

Virginia Tech

1. Math 4176: Cryptography Fall 2025
2. Math 5174: Mathematics of Public-Key Cryptography Spring 2025
3. Math 4175: Cryptography Spring 2025
4. Math 4175: Cryptography Fall 2024
5. Math 4134: Number Theory Spring 2024
6. Math 4124: Introduction to Abstract Algebra Fall 2023
7. Math 4175: Cryptography Spring 2023
8. Math 4175: Cryptography Fall 2022

University of Auckland

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

University of Waterloo

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

Funding **Total Value:** $227 481

1. **CCI Cybersecurity Research (Co-PI)**, $44,096 07/2025 – 06/2026
   Futureproofing Consensus Protocols for Blockchain and More: Constructing Quantum-Resistant Threshold (Ring) Signatures
   PI: Sarah Arpin, Virginia Tech.
2. **MCA 2025 Travel Grant (PI)**, $1 490 06/2025
3. **AMS-Simons Travel Grant (PI)**, $6 000 07/2024
   Design and Analysis of Post-Quantum Cryptographic Protocols
4. **CCI Workforce Program (PI)**, $5 000 05/2024 – 08/2024
   Post-Quantum Mercurial Signatures
5. **College of Science Instructional Grant (PI)**, $13 113 06/2024 – 05/2025
   Automated Evaluation in Cryptography
   Co-PI: Travis Morrison, Virginia Tech
6. **CCI Cybersecurity Research (PI)**, $20 000 06/2023 – 07/2024
   Quantum Algorithms for Ideal Class Group Computations
   Co-PIs: Travis Morrison and Jamie Sikora, Virginia Tech
7. **Academy of Data Science Discovery Fund (PI)**, $25 000 07/2023 – 06/2024
   A Data Science Approach to Data Protection
   Co-PI: Gretchen Matthews, Virginia Tech
8. **CCI Research Engagement Program (PI)**, $20 000 06/2023 – 06/2024
   Enhancements of SQISign
   Co-PI: Travis Morrison, Virginia Tech
9. **Virginia Tech New Faculty Mentoring Grant (PI)**, $1 500 04/2023
10. **CCI Quantum Aspects of Cybersecurity (PI)**, $61 282 01/2023 – 06/2024
    Resurrecting SIKE: Developing and Implementing New Isogeny-Based Post-Quantum Schemes
    Co-PI: Krzysztof Gaj, George Mason University.
11. **Commonwealth Cyber Initiative Faculty Fellowship (PI)**, $30 000 08/2022

Awards **University of Waterloo**

1. **Queen Elizabeth II Graduate Scholarship in Science and Technology**, $15 000 09/2019
   Government of Ontario
2. **NSERC Michael Smith Foreign Study Supplement**, $4 000 01/2019
   Natural Sciences and Engineering Research Council of Canada
3. **David Johnston International Experience Award**, $2 500 01/2019
   University of Waterloo
4. **President's Graduate Scholarship**, $10 000 09/2019
   University of Waterloo
5. **Alexander Graham Bell Canada Graduate Scholarship—Doctoral**, $105 000 09/2016
   Natural Sciences and Engineering Research Council of Canada
6. **President's Graduate Scholarship**, $15 000 09/2016
   University of Waterloo
7. **Alexander Graham Bell Canada Graduate Scholarship—Master's**, $17 500 09/2015
   Natural Sciences and Engineering Research Council of Canada
8. **President's Graduate Scholarship**, $15 000 09/2015
   University of Waterloo
9. **Ontario Graduate Scholarship**, $15 000 09/2014
   Government of Ontario

10. **President's Graduate Scholarship**, $15 000 09/2014
    University of Waterloo
11. **Combinatorics and Optimization Entrance Scholarship**, $3 000 09/2014
    University of Waterloo

Memorial University of Newfoundland

12. **Governor-General's Medal for Academic Excellence** 06/2014
    Canadian Chancellery of Honours
13. **University Medal for Academic Excellence in Pure Mathematics** 06/2014
    Memorial University of Newfoundland
14. **Lou Visintin Award** 04/2014
    Memorial University of Newfoundland
15. **NSERC Undergraduate Student Research Award**, $6 000 05/2013 – 08/2013
    Natural Sciences and Engineering Research Council of Canada
16. **Centenary of Responsible Government Scholarship**, $1 000 02/2013
    Government of Newfoundland and Labrador
17. **NSERC Undergraduate Student Research Award**, $6 000 05/2012 – 08/2012
    Natural Sciences and Engineering Research Council of Canada
18. **Dr. Arthur Barnes Scholarship**, $1 200 02/2012
    Government of Newfoundland and Labrador
19. **Centenary of Responsible Government Scholarship**, $1 000 02/2011
    Government of Newfoundland and Labrador
20. **Dr. Warren and Catherine Ball Memorial Entrance Scholarship**, $30 000 09/2010
    Memorial University of Newfoundland

Service

Conference and Workshop Organization

1. ICERM Graduate Workshop on Linear Algebra over Finite Fields & Applications (LAFFA) 2025
2. Banff International Research Station (BIRS) Workshop on Isogeny Graphs in Cryptography 2025
3. VT-Swiss Coding Theory and Cryptography Workshop 2025
4. Mathematics - Opportunites in Reseearch and Education (MORE) 2025
5. University of Auckland Workshop on Mathematical Cryptography 2024
6. VT-Swiss Coding Theory and Cryptography Summer School 2024
7. AMS Eastern Sectional Meeting 2024 Special Session on Post-Quantum Cryptography
8. Steger Center Coding Theory and Cryptography Workshop 2023
9. SIAM Southeastern Sectional Meeting 2023
10. SIAM Southeastern Sectional Meeting 2023 Special Session on Cryptography and Applications

Program Committee Membership

11. International Conference on Practice and Theory in Public Key Cryptography – PKC 2026
12. International Conference on Cryptology in India – Indocrypt 2025
13. International Workshop on Mathematical Cryptology – MathCrypt 2025 (CRYPTO affiliated event)
14. Australasian Conference on Information Security and Privacy – ACISP 2025
15. International Conference on Security and Privacy – ICSP 2024
16. International Conference on Cryptology in India – Indocrypt 2024
17. Symmetric Key Agreement Workshop – SKAW 2024 (CRYPTO affiliated event)
18. International Conference on Cryptology in India – Indocrypt 2023
19. International Workshop on Mathematical Cryptology – MathCrypt 2023 (CRYPTO affiliated event)
20. International Conference on Cryptology in India – Indocrypt 2022
21. Australasian Conference on Information Security and Privacy – ACISP 2022
22. International Conference on Security and Privacy – ICSP 2021

Manuscript Reviewing

23. Designs, Codes, and Cryptography
24. Journal of Information Security and Applications
25. Australasian Journal of Combinatorics
26. Journal of Mathematical Cryptology
27. Theoretical Computer Science
28. IET Information Security
29. AsiaCrypt 2025
30. International Conference on Practice and Theory in Public Key Cryptography – PKC 2025
31. Algorithmic Number Theory Symposium – ANTS XVI
32. Annual Cryptology Conference – CRYPTO 2023
33. Algorithmic Number Theory Symposium – ANTS XV
34. International Conference on Post-Quantum Cryptography – PQCrypto 2021
35. Australasian Conference on Information Security and Privacy – ACISP 2021
36. AsiaCrypt 2021
37. AsiaCrypt 2019
38. International Workshop on Security – IWSEC 2017

Service at Virginia Tech

39. Option Chair, Applied Discrete Mathematics 08/2025 – Present
40. Senior Fiscal Technician Hiring Committee 08/2025
41. Presidential Postdoctoral Fellows Program Review Committee 03/2025
42. Mathematics Department Preliminary Exam Coordinator 01/2025 – Present
43. Mathematics Department Advising Consultant 11/2024 – Present
44. Teaching Mentor for Leo Herr 08/2024 – 05/2025
45. Educational Technology Committee Member 08/2024 – Present
46. Mathematics Department Graduate Program Committee Member 08/2024 – Present
47. CCI Inclusion and Accessibility in Cybersecurity Research Review Panel 03/2024
48. Presidential Postdoctoral Fellows Program Review Committee 03/2024
49. Lay Nam Chang Dean's Discovery Fund Review Panel 03/2024
50. Post-Quantum Cryptography and Coding Theory Hiring Committee 08/2023 – 12/2023
51. Mathematics Department Colloquium Committee Member 08/2022 – 07/2023
52. Algebra Seminar Co-organizer 08/2022 – 07/2023