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, the design of isogeny-based protocols, algorithms for more secure and efficient implementations of isogeny-based protocols, 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

Accepted

1. Hailey Egan, **Jason T. LeGrow**, Gretchen L. Matthews, and Jeff Suliga. *Influences of some families of error-correcting codes.* To appear in Involve, a Journal of Mathematics. 2023

In Print

2. **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
3. 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
4. **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
5. **Jason T. LeGrow**. "A faster method for fault attack resistance in static/ephemeral CSIDH". in: *Journal of Cryptographic Engineering* (2023), pp. 1–12
6. 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
7. Daniel RL Brown, Neal Koblitz, and **Jason T. LeGrow**. "Cryptanalysis of 'MAKE"'. in: *Journal of Mathematical Cryptology* 16.1 (2022), pp. 98–102
8. **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
9. 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

10. 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
11. 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
12. 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
13. 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
14. **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

Preprints and Submitted Articles

15. Veronika Kuchta, **Jason T. LeGrow**, and Edoardo Persichetti. "Post-quantum blind signatures from code equivalence".
16. Steven D. Galbraith, **Jason T. LeGrow** and Ling Qin. "Two constructions of ring signatures from SQISign".
17. **Jason T. LeGrow**, Travis Morrison, Jamie Sikora, and Nic Swanson. "Masking countermeasures against side-channel attacks on quantum computers".
18. 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 (full version)".

Research Talks

Invited

1. Virginia Tech, Center for Quantum Information Science and Engineering Symposium 11/2023
   Post-Quantum Cryptography with Advanced Functionalities
2. Virginia Tech, Mathematics Department Colloquium 11/2023
   Isogeny-Based Post-Quantum Cryptography
3. Virginia Tech Steger Centre, Cryptography and Coding Theory Workshop 07/2023
   Post-Quantum Exotic Signatures from Group Actions
4. University of South Florida, Mathematics Department Colloquium 06/2023
   Optimization of Algorithms for Isogeny-Based Key Establishment
5. SIAM Southeastern Sectional Meeting, Minisymposium on Public-Key Cryptography and Applications 03/2023
   CSI-Otter: An Isogeny-Based Blind Signature Scheme
6. Virginia Tech, Algebra Seminar 01/2023
   Techniques for Fault Attack-Resistance in Static/Ephemeral CSIDH
7. Virginia Tech, Algebra Seminar 10/2022
   Optimization of Algorithms for Isogeny-Based Key Establishment
8. University of Auckland, Algebra and Combinatorics Seminar 05/2022
   Techniques for Fault Attack-Resistance in Static/Ephemeral CSIDH

9. University of Waterloo, Cryptography Reading Group 12/2021
CTIDH: Faster Constant-Time CSIDH

10. GITAM Hyderabad, Faculty Development Program 09/2021
Isogeny-Based Exotic Signatures and their Applications to Post-Quantum Blockchain

11. University of Auckland, Algebra and Combinatorics Seminar 07/2021
Optimization of Algorithms for Isogeny-Based Key Establishment

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

Contributed

13. International Conference on the Science of Cybersecurity (SciSec), Royal Melbourne Institute of Technology 07/2023
Multiprime Strategies for Serial Evaluations of eSIDH-Like Isogenies

14. International Workshop on Security (IWSEC), Online 09/2021
Analysis of a Strong Fault Attack on Static/Ephemeral CSIDH

15. Mathcrypt, University of California Santa Barbara 08/2019
Towards Isogeny-Based Password-Authenticated Key Establishment

16. Mathcrypt, University of California Santa Barbara 08/2018
A Subexponential-Time, Quantum Polynomial-Space Algorithm for Inverting the CM Group Action

17. British Combinatorial Conference, University of Warwick 07/2015
A_1' **Cyclic Orderings of Balanced Incomplete Block Designs**

18. Canadian Undergraduate Mathematics Conference, Carleton University 07/2014
Hamiltonicity and Cycle Extensions in 0-Block Intersection Graphs of Balanced Incomplete Block Designs

19. Science Atlantic, University of Prince Edward Island 10/2013
Hamiltonicity and Cycle Extensions in 0-Block Intersection Graphs of Balanced Incomplete Block Designs

Supervision

Virginia Tech

1. TingHung Chin, M.S. (ECE) Committee member 08/2023 – Present
2. Nathan Daly, M.S. Academic advisor 08/2023 – Present
3. Evan Stosic, M.S. Academic advisor 08/2023 – Present
4. Wendi Gao, Ph.D. Committee chair 05/2023 – Present
5. Wendi Gao, M.S. Committee chair 10/2022 – 05/2023
Optimization of Isogeney Evaluations in CSIDH
6. William Maheny, M.S. Committee member 10/2022 – 05/2023
Generalizing Multivariate Goppa Codes
7. Daniel Valvo, Ph.D. Committee member 10/2022 – 05/2023
Linear Exact Repair Schemes for Distributed Storage and Secure Distributed Computation

University of Auckland

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

Teaching

Virginia Tech

1. Math 4134: Number Theory — Spring 2024
2. Math 4124: Introduction to Abstract Algebra — Fall 2023
3. Math 4175: Cryptography — Spring 2023
4. Math 4175: Cryptography — Fall 2022

University of Auckland

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

University of Waterloo

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

Teaching Assistance

University of Waterloo

1. CO 687: Applied Cryptography — Fall 2019
2. CO 602: Fundamentals of Optimization — Fall 2019
3. CO 685: Mathematics of Public-Key Cryptography — Fall 2018
4. CO 687: Applied Cryptography — Winter 2018
5. MATH 674: Special Topics in Mathematical Connections — Winter 2017
6. CO 687: Applied Cryptography — Winter 2017
7. MATH 239: Introduction to Combinatorics — Fall 2016
8. MATH 239: Introduction to Combinatorics — Winter 2016
9. CO 685: Mathematics of Public-Key Cryptography — Fall 2015
10. ECE 103: Discrete Mathematics — Spring 2015
11. MATH 215: Linear Algebra — Winter 2015
12. MATH 115: Linear Algebra — Fall 2014

Memorial University of Newfoundland

13. Math 2130: Technical Writing for Mathematics — Fall 2013
14. Math 1050: Finite Mathematics I — Fall 2012
15. Math 1001: Calculus II — Winter 2012

Sponsored Research

Total Value: $126 282

As Principal Investigator at Virginia Tech

1. CCI Cybersecurity Research, $20 000 — 06/2023 – 07/2024
   Quantum Algorithms for Ideal Class Group Computations
   Co-PIs: Travis Morrison and Jamie Sikora, Virginia Tech
2. Academy of Data Science Discovery Fund, $25 000 — 07/2023 – 06/2024
   A Data Science Approach to Data Protection
   Co-PI: Gretchen Matthews, Virginia Tech
3. CCI Research Engagement Program, $20 000 — 06/2023 – 06/2024
   Enhancements of SQISign
   Co-PI: Travis Morrison, Virginia Tech
4. CCI Quantum Aspects of Cybersecurity, $61 282 — 01/2023 – 06/2024
   Resurrecting SIKE: Developing and Implementing New Isogeny-Based Post-Quantum Schemes
   Co-PI: Krzysztof Gaj, George Mason University. Virginia Tech Portion: $26 283

Awards

Virginia Tech

1. Faculty Fellowship, $30 000 — 08/2022
   Commonwealth Cyber Initiative

University of Waterloo

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

Memorial University of Newfoundland

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

Service

Organizing Committee Membership

1. SIAM Southeastern Sectional Meeting 2023

Event Organization and Administration

2. SIAM Eastern Sectional Meeting 2024 Special Session on Post-Quantum Cryptography
3. Steger Centre Coding Theory and Cryptography Workshop 2023
4. SIAM Southeastern Sectional Meeting 2023 Special Session on Cryptography and Applications

Program Committee Membership

5. Indocrypt 2024
6. Indocrypt 2023
7. MathCrypt 2023
8. Indocrypt 2022
9. ACISP 2022
10. ICSP 2021

Manuscript Reviewing

11. Australasian Journal of Combinatorics
12. Journal of Mathematical Cryptology
13. Theoretical Computer Science
14. IET Information Security
15. Crypto 2023
16. ANTS XV
17. PQCrypto 2021
18. ACISP 2021
19. AsiaCrypt 2021
20. AsiaCrypt 2019
21. IWSEC 2017

Service at Virginia Tech

22. Post-Quantum Cryptography and Coding Theory Hiring Committee 08/2023 – 12/2023
23. Colloquium Committee Member 08/2022 – 07/2023
24. Algebra Seminar Co-organizer 08/2022 – 07/2023

Service at the University of Waterloo

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

Service at Memorial University of Newfoundland

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

Professional Memberships

1. International Association for Cryptologic Research
2. Society for Industrial and Applied Mathematics
3. American Association for the Advancement of Science