Curriculum Vitae
Allison Bishop

Email Address: allibishop@gmail.com

Education and Experience

2019 - present		President and co-founder of Proof Trading
2021 - present		Visiting assistant professor, Computer Science Department, City College, CUNY
2018 - 2019		Adjunct assistant professor, Computer Science Department, Columbia University
2015 - 2018		Quantitative researcher at IEX
2013 - 2018		Assistant professor, Computer Science Department, Columbia University
2012 - 2013		Postdoctoral researcher, Microsoft Research New England
2012	Ph.D.	Computer Science, The University of Texas at Austin (advisor: Brent Waters)
2011	Intern	Microsoft Research New England (mentor: Yael Tauman Kalai)
2007	CASM	Certificate of Advanced Study in Mathematics, The University of Cambridge (with distinction)
2006	A.B.	Mathematics, Princeton University (summa cum laude)

Awards and Honors

2023	Distinguished lecture in the computer science department at the University of Michigan
2022	Distinguished lecture in the computer science department at Columbia University
2022	NYC Fintech Women's Inspiring Fintech Females
2016	Invited speaker at Theory of Cryptography Conference, TCC 2016-b
2016	Invited speaker at TEDx New York
2016	NSF Career Award
2014	Forbes 30 under 30 in Science and Healthcare
2011	Microsoft Research PhD Fellow
2008	National Defense Science and Engineering Graduate Fellow
2006	Marshall Scholar

Consulting

- Entrepreneur in Residence at Green Visor Capital
- Advisor to Evertas
- Advisor to Axelar Network
- former technical advisor to Omidyar Network
- short-term cybersecurity consulting work: Soros Economic Development Fund, Gaiascope, Inc.

Media and Performance

- host for "Jokes and Jabs" stand-up comedy show at Women's World of Boxing (recurring)
- guest appearance on Boxes and Lines Podcast, Ep. 71: Launching a New Institutional Equities Broker, October 31, 2022
- fourth place in the "Funniest Person in Finance" stand-up comedy competition at Gotham Comedy Club, April 18, 2022

- creator and co-host of "Extreme Makeover: Wall Street Edition": a live comedy show at Caveat, October 6, 2021
- Math Encounters: "Vulnerable in Digital Life: How Graph Theory Can Help Us Understand and Protect Our Digital Selves," MoMath, April 1, 2020
- "A Regular Person's Guide to Cybersecurity," an event as part of the Taste Of Science Festival, April 23, 2019
- key contributor to Proof Trading's blog: https://medium.com/prooftrading
- Wall Street Journal Op-Ed: *Calculus Is So Last Century* by Tianhui Michael Li and Allison Bishop, March 4, 2016

Teaching, Research Advising, and Community Leadership

Courses taught

- *Adversarial AI* and *Privacy for Data Scientists* at City College, CUNY
- *Introduction to Cryptography*, *Analysis of Algorithms I*, *Computer Science Theory*, and *Advanced Cryptography* at Columbia University

Former Postdoctoral Advisees

- Valerio Pastro

Former Doctoral Advisees

- Kevin Shi (Phd Dec. 2019)
- Ghada Almashaqbeh (Phd May 2019)
- Lucas Kowalczyk (Phd November 2018)

Former Undergraduate and Masters Advisees

- Victor Lecomte, Garrison Grogan, Eli Goldin, Alex Bienstock, Justin Whitehouse, Lalita Devadas, Harish Karthikeyan, Anindya Bhandari, Jonathan Sun, Ellen Vitercik

Former Highschool Advisees

- Nora Koe, Yoggi Koppol, Michael Paucillo

Service and Community Leadership

- Founder and general chair of CFAIL: the first conference for failed approaches and insightful losses in cryptology. CFAIL is an annual conference devoted to improving transparency, accountability, and collaboration in cryptology research by publishing efforts that fail to yield the kinds of positive results rewarded by typical conferences.
- Vice President of the board of the International Association for Cryptologic Research (IACR), 2023-2025
- General Chair of CRYPTO 2022 and appointed member of the board of the IACR for 2021-2022
- program committee member for: Pairing 2012, TCC 2013, PKC 2013, ASIACRYPT 2013, PKC 2014, CCS 2014, TCC 2015, CRYPTO 2015, STOC 2016, CRYPTO 2023

Publications

Preprints, Articles, and Books

1. A. Bishop. *Rejecting the Black Box: An inside look at the design of Proof Trading's New Algorithm.* Preprint, available at prooftrading.com/research
2. A. Bishop. *A Volume-Weighted Average Paper.* Preprint, available at prooftrading.com/research
3. A. Bishop and M. Schoenbauer. *Refining Proxy Symbol Selection for Distilled Impact.* Preprint, available at prooftrading.com/research
4. A. Bishop. *Distilled Impact.* Preprint, available at prooftrading.com/research
5. A. Bishop. *Pretrade Analysis: A Delicate Exercise in Hubris and Humility.* Preprint, available at prooftrading.com/research
6. A. Bishop. *A Framework for Historical Simulation of Trading Behavior.* Preprint, available at prooftrading.com/research
7. A. Bishop. *The Evolution of the Crumbling Quote Signal.* Automated Trader Magazine, 2017.
8. E. Wah, S. Feldman, F. Chung, A. Bishop, and D. Aisen. *A Comparison of Execution Quality across U.S. Stock Exchanges.* Global Algorithmic Capital Markets: High Frequency Trading, Dark Pools, and Regulatory Challenges, edited by Walter Mattli and published by Oxford University Press.
9. A.O. Fradkin and A. B. Bishop. *Funville Adventures.* Children's math-inspired fantasy adventure book, published by Natural Math.

Peer-reviewed journal articles and conference papers

*Note: some published under my former name, Allison Bishop Lewko

1. A. Bienstock, A. Bishop, E. Goldin, G. Grogan, and V. Lecomte. *From discrete-log to lattices: maybe the real lessons were our broken schemes along the way?.* CFAIL 2020
2. G. Almashaqbeh, A. Bishop, and J. Cappos. *MicroCash: Practical Concurrent Processing of Micropayments.* Financial Cryptography, 2020.
3. A. Bishop, L. Kowalczyk, T. Malkin, V. Pastro, M. Raykova, and K. Shi. *In Pursuit of Clarity in Obfuscation.* CFAIL, 2019.
4. K. Shi, D. Hsu, and A. Bishop. *A cryptographic approach to black box adversarial machine learning.* Security and Privacy of Machine Learning Workshop, ICML 2019.
5. G. Almashaqbeh, K. Kelley, A. Bishop, and J. Cappos. *CAPnet: A Defense Against Cache Accounting Attacks on Content Distribution Networks.* IEEE CNS, 2019.

6. G. Almashaqbeh, A. Bishop, and J. Cappos. *ABC: A Cryptocurrency-Focused Threat Modeling Framework.* IEEE INFOCOM Workshop - CryBlock, 2019.
7. A. Bishop, L. Kowalczyk, T. Malkin, V. Pastro, M. Raykova, and K. Shi. *A Simple Obfuscation Scheme for Pattern-Matching with Wildcards.* CRYPTO, 2018.
8. A. Bishop, V. Pastro, R. Rajaraman, and D. Wichs. *Essentially Optimal Robust Secret Sharing with Maximal Corruptions.* EUROCRYPT, 2016.
9. A. Bishop and V. Pastro. *Robust Secret Sharing Schemes Against Local Adversaries.* PKC, 2016.
10. A. Bishop and Y. Dodis. *Interactive Coding for Interactive Proofs.* TCC, 2016.
11. A. Bishop, S. Hohenberger, and B. Waters. *New Circular Security Counterexamples from Decision Linear and Learning with Errors.* ASIACRYPT, 2015.
12. A. Bishop, A. Jain, and L. Kowalczyk. *Function-Hiding Inner Product Encryption.* ASIACRYPT, 2015.
13. C. Gentry, A. Lewko, A. Sahai, and B. Waters. *Indistinguishability Obfuscation from the Multilinear Subgroup Elimination Assumption.* FOCS, 2015.
14. L. Kowalczyk and A. Lewko. *Bilinear Entropy Expansion from the Decisional Linear Assumption.* CRYPTO, 2015.
15. V. Koppula, A. Lewko, and B. Waters. *Indistinguishability Obfuscation for Turing Machines with Unbounded Memory.* STOC, 2015.
16. A. Lewko and S. Meiklejohn. *A Profitable Sub-Prime Loan: Obtaining the Advantages of Composite Order in Prime-Order Bilinear Groups.* PKC, 2015.
17. A. Jain, Y. T. Kalai, and A. Lewko. *Interactive Coding for Multiparty Protocols.* ITCS, 2015.
18. C. Gentry, A. Lewko, and B. Waters. *Witness Encryption from Instance Independent Assumptions.* CRYPTO, 2014.
19. A. Lewko and M. Lewko. *An Exact Asymptotic for the Square Variation of Partial Sum Processes.* Annales de l'Institut Henri Poincaré (to appear).
20. A. Lewko and M. Lewko. *The Square Variation of Rearranged Fourier Series.* Amer. J. Math. (to appear).
21. A. Lewko and B. Waters. *Why Proving HIBE Systems Secure is Difficult.* EUROCRYPT, 2014.
22. A. Lewko and M. Lewko. *On the Complexity of Asynchronous Agreement Against Powerful Adversaries.* PODC, 2013.
23. A. Lewko and M. Lewko. *Orthonormal Systems in Linear Spans.* Analysis & PDE (to appear).
24. A. Lewko and M. Lewko. *Maximal Operators Associated to Multiplicative Characters.* Proc. Amer. Math. Soc. (to appear).
25. M. Gerbush, A. Lewko, A. O'Neill, and B. Waters. *Dual Form Signatures: An Approach for Proving Security from Static Assumptions.* ASIACRYPT, 2012.
26. Y. Kalai, A. Lewko, and A. Rao. *Formulas Resilient to Short-Circuit Errors.* FOCS, 2012.
27. A. Lewko and B. Waters. *New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques.* CRYPTO, 2012.
28. A. Lewko and M. Lewko. *A Variational Barban-Davenport-Halberstam Theorem.* Journal of Number Theory 132 (9), 2012.
29. A. Lewko. *Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting.* EUROCRYPT, 2012.

30. S. Hohenberger, A. Lewko, and B. Waters. *Detecting Dangerous Queries: A New Approach for Chosen Ciphertext Security.* EUROCRYPT, 2012.
31. A. Lewko and M. Lewko. *Estimates for the Square Variation of Partial Sums of Fourier Series and their Rearrangements.* Journal of Functional Analysis 262, 2012.
32. S. Goldwasser, A. Lewko, and D. Wilson. *Bounded-Collusion IBE from Key Homomorphism.* TCC, 2012.
33. A. Lewko and M. Lewko. *Endpoint Restriction Estimates for the Paraboloid over Finite Fields.* Proc. Amer. Math. Soc. 140, 2012.
34. Y. Dodis, A. Lewko, B. Waters, and D. Wichs. *Storing Secrets on Continually Leaky Devices.* FOCS, 2011.
35. A. Lewko. *The Contest Between Simplicity and Efficiency in Asynchronous Byzantine Agreement.* DISC, 2011.
36. A. Lewko, M. Lewko, and B. Waters. *How to Leak on Key Updates.* STOC, 2011.
37. A. Lewko and B. Waters. *Decentralizing Attribute-Based Encryption.* EUROCRYPT, 2011.
38. A. Lewko and B. Waters. *Unbounded HIBE and Attribute-Based Encryption.* EUROCRYPT, 2011.
39. A. Lewko and M. Lewko. *On the Structure of Sets of Large Doubling.* European Journal of Combinatorics 32, 2011.
40. A. Lewko and Y. Rouselakis and B. Waters. *Achieving Leakage Resilience Through Dual System Encryption.* TCC, 2011.
41. A. Lewko and B. Waters. *On the Insecurity of Parallel Repetition for Leakage Resilience.* FOCS, 2010.
42. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. *Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption.* EUROCRYPT, 2010.
43. A. Lewko and B. Waters. *New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts.* TCC, 2010.
44. A. Lewko, A. Sahai, and B. Waters. *Revocation Systems with Very Small Private Keys.* IEEE Symposium of Security and Privacy, 2010.
45. A. Lewko and B. Waters. *Efficient Pseudorandom Functions from the Decisional Linear Assumptions and Weaker Variants.* CCS, 2009.