Curriculum Vitae
Allison Bishop

Office Address: Department of Computer Science
Columbia University
410 Mudd
1214 Amsterdam Avenue MC 0401
New York, NY 10027
Email Address: allison@cs.columbia.edu

Research interests

cryptography, distributed computing, complexity theory, combinatorics, and harmonic analysis

Education and Experience

2013 - present		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

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

Publications

Peer-reviewed journal articles and conference papers

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

1. A. Bishop, V. Pastro, R. Rajaraman, and D. Wichs. *Essentially Optimal Robust Secret Sharing with Maximal Corruptions.* EUROCRYPT, 2016.
2. A. Bishop and V. Pastro. *Robust Secret Sharing Schemes Against Local Adversaries.* PKC, 2016.
3. A. Bishop and Y. Dodis. *Interactive Coding for Interactive Proofs.* TCC, 2016.
4. A. Bishop, S. Hohenberger, and B. Waters. *New Circular Security Counterexamples from Decision Linear and Learning with Errors.* ASIACRYPT, 2015.
5. A. Bishop, A. Jain, and L. Kowalczyk. *Function-Hiding Inner Product Encryption.* ASIACRYPT, 2015.
6. C. Gentry, A. Lewko, A. Sahai, and B. Waters. *Indistinguishability Obfuscation from the Multilinear Subgroup Elimination Assumption.* FOCS, 2015.
7. L. Kowalczyk and A. Lewko. *Bilinear Entropy Expansion from the Decisional Linear Assumption.* CRYPTO, 2015.
8. V. Koppula, A. Lewko, and B. Waters. *Indistinguishability Obfuscation for Turing Machines with Unbounded Memory.* STOC, 2015.

9. A. Lewko and S. Meiklejohn. *A Profitable Sub-Prime Loan: Obtaining the Advantages of Composite Order in Prime-Order Bilinear Groups.* PKC, 2015.
10. A. Jain, Y. T. Kalai, and A. Lewko. *Interactive Coding for Multiparty Protocols.* ITCS, 2015.
11. C. Gentry, A. Lewko, and B. Waters. *Witness Encryption from Instance Independent Assumptions.* CRYPTO, 2014.
12. A. Lewko and M. Lewko. *An Exact Asymptotic for the Square Variation of Partial Sum Processes.* Annales de l'Institut Henri Poincaré (to appear).
13. A. Lewko and M. Lewko. *The Square Variation of Rearranged Fourier Series.* Amer. J. Math. (to appear).
14. A. Lewko and B. Waters. *Why Proving HIBE Systems Secure is Difficult.* EUROCRYPT, 2014.
15. A. Lewko and M. Lewko. *On the Complexity of Asynchronous Agreement Against Powerful Adversaries.* PODC, 2013.
16. A. Lewko and M. Lewko. *Orthonormal Systems in Linear Spans.* Analysis & PDE (to appear).
17. A. Lewko and M. Lewko. *Maximal Operators Associated to Multiplicative Characters.* Proc. Amer. Math. Soc. (to appear).
18. M. Gerbush, A. Lewko, A. O'Neill, and B. Waters. *Dual Form Signatures: An Approach for Proving Security from Static Assumptions.* ASIACRYPT, 2012.
19. Y. Kalai, A. Lewko, and A. Rao. *Formulas Resilient to Short-Circuit Errors.* FOCS, 2012.
20. A. Lewko and B. Waters. *New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques.* CRYPTO, 2012.
21. A. Lewko and M. Lewko. *A Variational Barban-Davenport-Halberstam Theorem.* Journal of Number Theory 132 (9), 2012.
22. A. Lewko. *Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting.* EUROCRYPT, 2012.
23. S. Hohenberger, A. Lewko, and B. Waters. *Detecting Dangerous Queries: A New Approach for Chosen Ciphertext Security.* EUROCRYPT, 2012.
24. 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.
25. S. Goldwasser, A. Lewko, and D. Wilson. *Bounded-Collusion IBE from Key Homomorphism.* TCC, 2012.
26. A. Lewko and M. Lewko. *Endpoint Restriction Estimates for the Paraboloid over Finite Fields.* Proc. Amer. Math. Soc. 140, 2012.
27. Y. Dodis, A. Lewko, B. Waters, and D. Wichs. *Storing Secrets on Continually Leaky Devices.* FOCS, 2011.
28. A. Lewko. *The Contest Between Simplicity and Efficiency in Asynchronous Byzantine Agreement.* DISC, 2011.
29. A. Lewko, M. Lewko, and B. Waters. *How to Leak on Key Updates.* STOC, 2011.
30. A. Lewko and B. Waters. *Decentralizing Attribute-Based Encryption.* EUROCRYPT, 2011.
31. A. Lewko and B. Waters. *Unbounded HIBE and Attribute-Based Encryption.* EUROCRYPT, 2011.
32. A. Lewko and M. Lewko. *On the Structure of Sets of Large Doubling.* European Journal of Combinatorics 32, 2011.

33. A. Lewko and Y. Rouselakis and B. Waters. *Achieving Leakage Resilience Through Dual System Encryption.* TCC, 2011.
34. A. Lewko and B. Waters. *On the Insecurity of Parallel Repetition for Leakage Resilience.* FOCS, 2010.
35. 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.
36. A. Lewko and B. Waters. *New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts.* TCC, 2010.
37. A. Lewko, A. Sahai, and B. Waters. *Revocation Systems with Very Small Private Keys.* IEEE Symposium of Security and Privacy, 2010.
38. A. Lewko and B. Waters. *Efficient Pseudorandom Functions from the Decisional Linear Assumptions and Weaker Variants.* CCS, 2009.

Program Committees

Pairing 2012, TCC 2013, PKC 2013, ASIACRYPT 2013, PKC 2014, CCS 2014, TCC 2015, CRYPTO 2015, STOC 2016