

Allison Bishop Lewko

Email alewko@cs.utexas.edu

Educational Background

- Currently pursuing a Ph.d. in Computer Science at the University of Texas at Austin (began fall 2007 in the mathematics department, switched to the computer science department for spring 2010)
- Certificate of Advanced Study in Mathematics from the University of Cambridge, 2007 (with distinction)
- A.B. Mathematics degree from Princeton University, 2006 (summa cum laude)

Publications

- “Endpoint Restriction Estimates for the Paraboloid over Finite Fields,” Allison Lewko and Mark Lewko, Proceedings of the AMS
- “Storing Secrets on Continually Leaky Devices,” Yevgeniy Dodis, Allison Lewko, Brent Waters, and Daniel Wichs, FOCS 2011
- “The Contest Between Simplicity and Efficiency in Asynchronous Byzantine Agreement,” Allison Lewko, DISC 2011
- “How to Leak on Key Updates,” Allison Lewko, Mark Lewko, and Brent Waters, STOC 2011
- “Decentralizing Attribute-Based Encryption,” Allison Lewko and Brent Waters, Eurocrypt 2011
- “Unbounded HIBE and Attribute-Based Encryption,” Allison Lewko and Brent Waters, Eurocrypt 2011
- “On the Structure of Sets of Large Doubling,” Allison Lewko and Mark Lewko, European Journal of Combinatorics 32 (2011) 688-708
- “Achieving Leakage Resilience Through Dual System Encryption,” Allison Lewko, Yannis Rouselakis, and Brent Waters, TCC 2011
- “On the Insecurity of Parallel Repetition for Leakage Resilience,” Allison Lewko and Brent Waters, FOCS 2010
- “Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,” Allison Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters, Eurocrypt 2010
- “New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts,” Allison Lewko and Brent Waters, TCC 2010

- “Revocation Systems with Very Small Private Keys,” Allison Lewko, Amit Sahai, and Brent Waters, IEEE Symposium of Security and Privacy, 2010
- “Efficient Pseudorandom Functions from the Decisional Linear Assumption and Weaker Variants,” Allison Lewko and Brent Waters, CCS 2009.

Work Currently Submitted to a Journal

- “An Exact Asymptotic for the Square Variation of Partial Sum Processes,” Allison Lewko and Mark Lewko, available at <http://arxiv.org/abs/1106.0783>
- “Estimates for the Square Variation of Partial Sums of Fourier Series and their Rearrangements,” Allison Lewko and Mark Lewko, available at <http://arxiv.org/abs/1106.0871>

Additional Research and Teaching Experience

- Intern at Microsoft Research New England, summer 2011
- TA for calculus 408L, University of Texas at Austin, fall 2008
- undergraduate mathematics grader, peer advisor, and tutor at Princeton University, 2005-2006
- 2004 Research Experience for Undergraduates Program the University of Nebraska: I researched models in evolutionary game theory along with another undergraduate student (Kevin Loope) and two faculty advisors (Professors Wendy Hines and Jamie Radcliffe).

Invited Talks

- Functional Encryption: Current Systems and Proof Techniques: AWM Anniversary Conference at Brown University, September 2011
- Instantiating the Dual System Encryption Methodology in Bilinear Groups: 15th Workshop on Elliptic Curve Cryptography, September 2011
- Unbounded HIBE and Attribute-Based Encryption: MIT CIS Seminar, April 2011
- How to Leak on Key Updates: New York Area Monthly Crypto Day, March 2011
- Decentralizing Attribute-Based Encryption: Microsoft Research Redmond Cryptography Colloquium, March 2011
- How to Leak on Key Updates: MIT CIS Seminar, December 2010
- The Evolution of Cooperation in Finite, Growing Populations: Nebraska Regional Workshop in Mathematical Sciences, November 2004

Honors/Distinctions

- Microsoft Research PhD Fellowship, 2011
- National Defense Science and Engineering Graduate Fellow, 2008
- Frank Gerth III Graduate Excellence Award, UT-Austin mathematics department, 2008
- University Fellowship recipient at the University of Texas at Austin 2007-2008
- College Award from Churchill College, Cambridge for performance in the Part III of the mathematics tripos, 2007
- 2006 Marshall Scholar
- member of Phi Beta Kappa, 2006
- elected to membership in Sigma Xi, 2006
- Peter Greenberg Prize for excellence in mathematics, Princeton University, 2006
- Runner-up for the 2006 Alice T. Schafer Prize presented by the Association for Women in Mathematics for excellence in mathematics by an undergraduate woman
- undergraduate G.P.A.: 3.93 (out of 4.0)
- 2005 Goldwater Scholar
- Shapiro Award for Academic Excellence, Princeton University, 2003
- Lansing High School Valedictorian and highest G.P.A. in school's history (2002)
- National Merit Scholar 2002
- SAT: 1600 (2001)