

Curriculum Vitae

ALLISON LEWKO

Office Address: The University of Texas at Austin
Department of Computer Science
1616 Guadalupe, Suite 2.408
Austin, TX 78701

Email Address: alewko@cs.utexas.edu

Research interests

cryptography, distributed computing, combinatorics, and harmonic analysis

Education and Experience

- 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

- 2011 Microsoft Research PhD Fellow
- 2008 National Defense Science and Engineering Graduate Fellow
- 2006 Marshall Scholar

Publications

Peer-reviewed journal articles and conference papers

1. A. Lewko and B. Waters. *New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques*. CRYPTO, 2012.
2. A. Lewko and M. Lewko. *A Variational Barban-Davenport-Halberstam Theorem*. Journal of Number Theory (to appear)
3. A. Lewko. *Tools for Simulating Features of Composite Order Bilinear Groups in the Prime Order Setting*. EUROCRYPT, 2012.
4. S. Hohenberger, A. Lewko, and B. Waters. *Detecting Dangerous Queries: A New Approach for Chosen Ciphertext Security*. EUROCRYPT, 2012.
5. 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.
6. S. Goldwasser, A. Lewko, and D. Wilson. *Bounded-Collusion IBE from Key Homomorphism*. TCC, 2012.
7. A. Lewko and M. Lewko. *Endpoint Restriction Estimates for the Paraboloid over Finite Fields*. Proc. Amer. Math. Soc. 140, 2012.
8. Y. Dodis, A. Lewko, B. Waters, and D. Wichs. *Storing Secrets on Continually Leaky Devices*. FOCS, 2011.
9. A. Lewko. *The Contest Between Simplicity and Efficiency in Asynchronous Byzantine Agreement*. DISC, 2011.
10. A. Lewko, M. Lewko, and B. Waters. *How to Leak on Key Updates*. STOC, 2011.
11. A. Lewko and B. Waters. *Decentralizing Attribute-Based Encryption*. EUROCRYPT, 2011.

12. A. Lewko and B. Waters. *Unbounded HIBE and Attribute-Based Encryption*. EUROCRYPT, 2011.
13. A. Lewko and M. Lewko. *On the Structure of Sets of Large Doubling*. European Journal of Combinatorics 32, 2011.
14. A. Lewko and Y. Rouselakis and B. Waters. *Achieving Leakage Resilience Through Dual System Encryption*. TCC, 2011.
15. A. Lewko and B. Waters. *On the Insecurity of Parallel Repetition for Leakage Resilience*. FOCS, 2010.
16. 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.
17. A. Lewko and B. Waters. *New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts*. TCC, 2010.
18. A. Lewko, A. Sahai, and B. Waters. *Revocation Systems with Very Small Private Keys*. IEEE Symposium of Security and Privacy, 2010.
19. A. Lewko and B. Waters. *Efficient Pseudorandom Functions from the Decisional Linear Assumptions and Weaker Variants*. CCS, 2009.

Submitted journal articles

1. A. Lewko and M. Lewko. *Orthonormal Systems in Linear Spans*. arXiv:math 1205.2420
2. A. Lewko and M. Lewko. *Maximal Operators Associated to Multiplicative Characters*. arXiv:math 1111.6742
3. A. Lewko and M. Lewko. *An Exact Asymptotic for the Square Variation of Partial Sum Processes*. arXiv:math 1106.0783

Program Committees

Pairing 2012, TCC 2013, PKC 2013