David Cash

Updated November 2017

Associate Professor
Department of Computer Science
University of Chicago

email: davidcash@uchicago.edu
phone: 773-702-0805
web: http://david.cash

Education

- PhD, Computer Science, Georgia Institute of Technology, 2009. Advisor: Alexandra Boldyreva.
- MS, Computer Science, Georgia Institute of Technology, 2005.
- BS, Computer Science, Georgia Institute of Technology, 2003.

Research Interests

- Cryptography: Provable security for practice and foundations, searchable encryption, database encryption, lattice-based cryptography, public-key cryptography, symmetric-key cryptography, authentication.
- Computer Security: Database security and privacy, secure information retrieval.

Awards and Honors

- NSF CAREER Award 2015.
- Research Fellow, Simons Institute for Theoretical Computer Science, Summer 2015.
- Publication [9] invited to Journal of Cryptology.
- Best Paper Award at EUROCRYPT 2011 for [18]; Invited to Journal of Cryptology.
- Best Paper Award at EUROCRYPT 2010 for [21]; Invited to Journal of Cryptology. 3 of the 33 papers at EUROCRYPT 2010 were invited.
- Publication [26] invited to Journal of Cryptology. 4 of the 31 papers from EUROCRYPT 2008 were invited.
- Georgia Tech Algorithms & Randomness Center Fellowship, Spring 2009.
- NSF East Asia and Pacific Summer Institutes and Japan Society for the Promotion of Science Fellowship, Summer 2008

Employment History

- *Associate Professor with Tenure*, University of Chicago, January 2018 – present.
- *Assistant Professor*, Rutgers University, August 2012 – December 2017.
- *Postdoc*, IBM T.J. Watson Research Center, 2011 – 2012.
- *Postdoc*, Ruhr University Bochum (Germany) Summer 2011. Advisor: Eike Kiltz.
- *Postdoc*, University of California, San Diego, 2009 – 2011. Advisor: Mihir Bellare.
- *Graduate Research/Teaching Assistant*, Georgia Institute of Technology, 2004 – 2009.

- *Visiting Ph.D. Student*, Ibaraki University (Japan), Summer 2008. Host: Kaoru Kurosawa.
- *Visiting Ph.D. Student*, Center for Mathematics and Computer Science (CWI Amsterdam, Netherlands), Summer 2007.
- *Software Engineering Co-op*, Scientific Research Corporation (Atlanta, GA), May 2001 – June 2003.

Publications

[1] Benedikt Auerbach, David Cash, Manuel Fersch, and Eike Kiltz. Memory-tight reductions. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017, Part I*, volume 10401 of *Lecture Notes in Computer Science*, pages 101–132. Springer, Heidelberg, August 2017.

[2] Liang Wang, Paul Grubbs, Jiahui Lu, Vincent Bindschaedler, David Cash, and Thomas Ristenpart. Side-channel attacks on shared search indexes. In *2017 IEEE Symposium on Security and Privacy*, pages 673–692. IEEE Computer Society Press, May 2017.

[3] F. Betül Durak, Thomas M. DuBuisson, and David Cash. What else is revealed by order-revealing encryption? In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 16: 23rd Conference on Computer and Communications Security*, pages 1155–1166. ACM Press, October 2016.

[4] Zvika Brakerski, David Cash, Rotem Tsabary, and Hoeteck Wee. Targeted homomorphic attribute-based encryption. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B: 14th Theory of Cryptography Conference, Part II, volume 9986 of Lecture Notes in Computer Science*, pages 330–360. Springer Heidelberg, October 2016.

[5] David Cash, Eike Kiltz, and Stefano Tessaro. Two-round man-in-the-middle security from LPN. In Eyal Kushilevitz and Tal Malkin, editors, *TCC 2016-A: 13th Theory of Cryptography Conference, Part I*, volume 9562 of *Lecture Notes in Computer Science*, pages 225–248. Springer, Heidelberg, January 2016.

[6] Cong Zhang, David Cash, Xiuhua Wang, Xiaoqi Yu, and Sherman S. M. Chow. Combiners for chosen-ciphertext security. In Thang N. Dinh and My T. Thai, editors, *Computing and Combinatorics : 22nd International Conference, COCOON 2016, August 2-4, 2016, Proceedings*, pages 257–268. Springer International Publishing, 2016 2016.

[7] David Cash, Paul Grubbs, Jason Perry, and Thomas Ristenpart. Leakage-abuse attacks against searchable encryption. In Indrajit Ray, Ninghui Li, and Christopher Kruegel:, editors, *ACM CCS 15: 22nd Conference on Computer and Communications Security*, pages 668–679. ACM Press, October 2015.

[8] David Cash, Alptekin Küpçü, and Daniel Wichs. Dynamic proofs of retrievability via oblivious RAM. *Journal of Cryptology*. Accepted 2015.

[9] David Cash, Rafael Dowsley, and Eike Kiltz. Digital signatures from strong RSA without prime generation. In Jonathan Katz, editor, *PKC 2015: 18th International Conference on Theory and Practice of Public Key Cryptography*, volume 9020 of *Lecture Notes in Computer Science*, pages 217–235. Springer, Heidelberg, March / April 2015.

[10] David Cash and Stefano Tessaro. The locality of searchable symmetric encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 351–368. Springer, Heidelberg, May 2014.

[11] David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, and Michael Steiner. Dynamic searchable encryption in very-large databases: Data structures and implementation. In *ISOC Network and Distributed System Security Symposium – NDSS 2014*. The Internet Society, February 2014.

[12] David Cash, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, and Michael Steiner. Highly-scalable searchable symmetric encryption with support for Boolean queries. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 353–373. Springer, Heidelberg, August 2013.

[13] David Cash, Alptekin Küpçü, and Daniel Wichs. Dynamic proofs of retrievability via oblivious RAM. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 279–295. Springer, Heidelberg, May 2013.

[14] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of Cryptology*, 25(4):601–639, October 2012.

[15] David Cash, Matthew Green, and Susan Hohenberger. New definitions and separations for circular security. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 540–557. Springer, Heidelberg, May 2012.

[16] Mihir Bellare, David Cash, and Rachel Miller. Cryptography secure against related-key attacks and tampering. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology – ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 486–503. Springer, Heidelberg, December 2011.

[17] Mihir Bellare, David Cash, and Sriram Keelveedhi. Ciphers that securely encipher their own keys. In Yan Chen, George Danezis, and Vitaly Shmatikov, editors, *ACM CCS 11: 18th Conference on Computer and Communications Security*, pages 423–432. ACM Press, October 2011.

[18] Eike Kiltz, Krzysztof Pietrzak, David Cash, Abhishek Jain, and Daniele Venturi. Efficient authentication from hard learning problems. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 7–26. Springer, Heidelberg, May 2011.

[19] Mihir Bellare and David Cash. Pseudorandom functions and permutations provably secure against related-key attacks. In Tal Rabin, editor, *Advances in Cryptology – CRYPTO 2010*, volume 6223 of *Lecture Notes in Computer Science*, pages 666–684. Springer, Heidelberg, August 2010.

[20] Tolga Acar, Mira Belenkiy, Mihir Bellare, and David Cash. Cryptographic agility and its relation to circular encryption. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 403–422. Springer, Heidelberg, May 2010.

[21] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 523–552. Springer, Heidelberg, May 2010.

[22] Alexandra Boldyreva, David Cash, Marc Fischlin, and Bogdan Warinschi. Foundations of non-malleable hash and one-way functions. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 524–541. Springer, Heidelberg, December 2009.

[23] David Cash, Eike Kiltz, and Victor Shoup. The twin Diffie-Hellman problem and applications. *Journal of Cryptology*, 22(4):470–504, October 2009.

[24] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Shai Halevi, editor, *Advances in Cryptology – CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 595–618. Springer, Heidelberg, August 2009.

[25] David Bauer, Douglas M. Blough, and David Cash. Minimal information disclosure with efficiently verifiable credentials. In Elisa Bertino and Kenji Takahashi, editors, *Proceedings of the 4th Workshop on Digital Identity Management*, pages 15–24, October 2008.

[26] David Cash, Eike Kiltz, and Victor Shoup. The twin Diffie-Hellman problem and applications. In Nigel P. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 127–145. Springer, Heidelberg, April 2008.

[27] David Cash, Yan Zong Ding, Yevgeniy Dodis, Wenke Lee, Richard J. Lipton, and Shabsi Walfish. Intrusion-resilient key exchange in the bounded retrieval model. In Salil P. Vadhan, editor, *TCC 2007: 4th Theory of Cryptography Conference*, volume 4392 of *Lecture Notes in Computer Science*, pages 479–498. Springer, Heidelberg, February 2007.

Advising

PhD Students:

- F. Betül Durak (2014-2017, defended thesis September 6, 2017, degree conferral expected October 1, 2017)
- Cong Zhang (2014-current)
- Akshima (2016-current)

Undergraduate and Master's advising:

- Jesse Huang, Undergraduate, Independent Study, Spring 2014. SAS Honors Advisor
- Georgiana Haldeman, MS, Independent Study, Spring 2014
- Prachi Pendse, MS, Independent Study, Spring 2014
- Seth Deneroff, Undergraduate, SAS Honors Advisor
- Alex Ganescu, Undergraduate, SAS Honors Advisor
- Supervised 5 students for CS 395 internships (Summer 2014 and Summer 2015).

Teaching (at Rutgers)

- CS 206 – Introduction to Discrete Structures II (undergraduate). Spring 2013, 2014, 2015, 2016, 2017. Spring 2016 included Honors section.
- CS 671 – Seminar in Cryptography (graduate). Fall 2014.
- CS 596 – Special Topics – Introduction to Cryptography (graduate). Fall 2013.
- CS 442 – Special Topics – Introduction to Cryptography (undergraduate). Fall 2012.

Outreach

- Instructor at Rutgers Young Scholars Program in Discrete Mathematics, Summer 2014 and 2016. One week (20 hour) course on cryptography for high-school age students.
- Speaker at Rutgers First-Year Interest Group Seminar (2014) for Rutgers students interested in computer science.
- Speaker at Rutgers Undergraduate Computer Science Honors Seminar (2014,2015) for Rutgers Honors CS majors to learn about research.
- General audience talks on "Cryptowars 2.0" at Experience Rutgers events in Washington DC, Philadelphia, New York, and Princeton.

Selected Invited Talks (Since joining Rutgers)

- **Side-Channel Attacks on Shared Search Indexes**
  - DIMACS/Northeast Big Data Hub Workshop on Privacy and Security for Big Data, April 2017
- **What else is revealed by order-revealing encryption?**
  - Real World Cryptography Conference, January 2017.
  - Dagstuhl Workshop on Public-Key Cryptography, September 2016.
- **Leakage-Abuse Attacks Against Searchable Encryption**

- U. of California, Santa Barbara, November 2015.
- Yahoo! Inc., July 2015.
- Bertinoro Workshop on Encryption for Search and other Algorithms, June 2015.

- **The Locality of Searchable Symmetric Encryption**
  - Brown U., November 2016.
  - DIMACS/Columbia Data Science Institute Workshop on Cryptography for Big Data, December 2015.
  - DC Area Crypto Day, U. of Maryland, September 2014.
  - New York Area CryptoDay, June 2014.
  - Ecole Normal Superior (France), June 2014.
  - EUROCRYPT 2014, Copenhagen, May 2014.
  - Applied Communication Sciences (Basking Ridge NJ), April 2014.
  - DIMACS Workshop on Secure Cloud Computing, March 2014.
- **Simons Fellow Talk – On Some Open Problems**
  - Simons Institute for Theoretical Computer Science, May 2015.
- **Dynamic Proofs of Retrievability from Oblivious RAM**
  - IBM Research Cryptography Seminar, February 2013.
  - DIMACS Fall Mixer, October 2012.
- **Efficient Authentication from the Learning Parity with Noise Problem**
  - Accenture PLC, June 2013.
  - DIMACS Theory of Computing Seminar (at Rutgers U.), November 2012.
  - New York Area CryptoDay, November 2011.
- **Security Against Related-Key Attacks: Constructions and Applications**
  - NYU Cryptography Seminar, March 2012.
- **Ciphers that Securely Encipher their Own Keys.**
  - DIMACS Fall Mixer, October 2012.
  - ACM CCS, October 2011.

Professional Service

- **Workshop organizer:**
  - DIMACS Workshop on Cryptography and its Interactions: Learning Theory, Coding Theory, and Data Structures (July 2016).
  - DIMACS Workshop on Current Trends in Cryptology (April 2013).
- **Program Committees:**
  - USENIX Security 2017, WAHC 2017, TCC 2016-B, CCS 2016, SCN 2016, EUROCRYPT 2016, 2014, 2012, CCSW 2014, PKC 2014, CRYPTO 2013, ASIACRYPT 2012, AFRICACRYPT 2011, ProvSec 2010.
- **Service at Rutgers:**
  - Undergraduate Curriculum Committee (2013 – present, except sabbatical Fall'15)
  - Tenure-Track Hiring Committee (Fall 2016 – Spring 2017)
  - Non-Tenure-Track Hiring Committee (Fall 2016 – Spring 2017)
  - Rapid Action Taskforce for MS in Data Science Curriculum (Spring 2016)
  - PhD Admissions (Spring 2013)

Funding

- NSF Faculty Early Career Development Program. *CAREER: Cryptography for Secure Outsourcing.* PI: David Cash. June 2015 – May 2020. $566,912.
- Subcontract with Galois Inc. on Brandeis Program grant from DARPA. Rutgers PI: Rebecca Wright. Rutgers coPIs: David Cash, Anand Sarwate. September 2015 – February 2020. $1,013,723.
- NSF. *SaTC: Medium: Collaborative: Cryptographic Data Protection in Modern Systems.* Rutgers PI: David Cash. Cornell PI: Vitaly Shmatikov. Cornell Co-PI: Thomas Ristenpart. September 2017 – August 2021. $400,000 (Rutgers portion).