

BRENT WATERS

University of Texas at Austin phone: 512 232 7464
Department of Computer Sciences email: bwaters@cs.utexas.edu
ACES 3.438 web: www.cs.utexas.edu/~bwaters
Austin TX 78712

Research Interests

Cryptography and computer security

Experience

Assistant Professor, University of Texas at Austin, (2008 – Present)
Computer Scientist, SRI International, Computer Science Lab, (9/2005 – 8/2008)
Postdoc, Stanford University, Computer Science Department, (8/2004 – 8/2005)

Education

Ph.D. Computer Science, Princeton University, 2004 (Advisers: Ed Felten, Amit Sahai)
M. A. Computer Science, Princeton University, 2002
B. S. Computer Science, UCLA, 2000 (Graduated Summa Cum Laude)

Honors and Awards

Packard Fellowship (2011)
Microsoft Research Faculty Fellow (2011)
Sloan Research Fellowship (2010)
NSF CAREER Award (2010)
National Academy of Sciences Kavli Fellow (2008)

Conference Publications

- B. Waters. Functional encryption for regular languages. In *CRYPTO*, 2012.
- A. Lewko and B. Waters. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In *CRYPTO*, 2012.
- A. Sahai, H. Seyalioglu, and B. Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In *CRYPTO*, 2012.
- M. Bellare, R. Dowsley, B. Waters, and S. Yilek. Standard security does not imply security against selective-opening. In *EUROCRYPT*, pp. 645–662, 2012.
- M. Bellare, E. Kiltz, C. Peikert, and B. Waters. Identity-based (lossy) trapdoor functions and applications. In *EUROCRYPT*, pp. 228–245, 2012.
- S. Hohenberger, A. B. Lewko, and B. Waters. Detecting dangerous queries: A new approach for chosen ciphertext security. In *EUROCRYPT*, pp. 663–681, 2012.
- J. H. Ahn, D. Boneh, J. Camenisch, S. Hohenberger, A. Shelat, and B. Waters. Computing on authenticated data. In *TCC*, pp. 1–20, 2012.
- D. Boneh, G. Segev, and B. Waters. Targeted malleability: homomorphic encryption for restricted computations. In *ITCS*, pp. 350–366, 2012.
- Y. Dodis, A. B. Lewko, B. Waters, and D. Wichs. Storing secrets on continually leaky devices. In *FOCS*, pp. 688–697, 2011.

- M. Green, S. Hohenberger, and B. Waters. Outsourcing the decryption of abe ciphertexts. In *USENIX Security*, pp. 523–538, 2011.
- A. Dunn, O. Hoffman, B. Waters, and E. Witchel. Cloaking malware with the trusted platform module. In *USENIX Security*, pp. 395–410, 2011.
- A. O’Neill, C. Peikert, and B. Waters. Bi-deniable public-key encryption. In *CRYPTO*, pp. 525–542, 2011.
- A. B. Lewko, M. Lewko, and B. Waters. How to leak on key updates. In *STOC*, pp. 725–734, 2011.
- A. B. Lewko and B. Waters. Decentralizing attribute-based encryption. In *EUROCRYPT*, pp. 568–588, 2011.
- A. B. Lewko and B. Waters. Unbounded hibe and attribute-based encryption. In *EUROCRYPT*, pp. 547–567, 2011.
- M. Bellare, B. Waters, and S. Yilek. Identity-based encryption secure against selective opening attack. In *TCC*, pp. 235–252, 2011.
- D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. In *TCC*, pp. 253–273, 2011.
- A. B. Lewko, Y. Rouselakis, and B. Waters. Achieving leakage resilience through dual system encryption. In *TCC*, pp. 70–88, 2011.
- B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In *Public Key Cryptography*, pp. 53–70, 2011.
- A. B. Lewko and B. Waters. On the insecurity of parallel repetition for leakage resilience. In *FOCS*, pp. 521–530, 2010.
- S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters. Building efficient fully collusion-resilient traitor tracing and revocation schemes. In *ACM Conference on Computer and Communications Security*, pp. 121–130, 2010.
- S. S. M. Chow, Y. Dodis, Y. Rouselakis, and B. Waters. Practical leakage-resilient identity-based encryption from simple assumptions. In *ACM Conference on Computer and Communications Security*, pp. 152–161, 2010.
- A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In *EUROCRYPT*, pp. 62–91, 2010.
- S. Hohenberger and B. Waters. Constructing verifiable random functions with large input spaces. In *EUROCRYPT*, pp. 656–672, 2010.
- X. Boyen and B. Waters. Shrinking the keys of discrete-log-type lossy trapdoor functions. In *ACNS*, pp. 35–52, 2010.
- A. B. Lewko, A. Sahai, and B. Waters. Revocation systems with very small private keys. In *IEEE Symposium on Security and Privacy*, pp. 273–285, 2010.
- S. Wolchok, O. Hofmann, N. Heninger, E. Felten, J. A. Halderman, C. Rossbach, B. Waters, and E. Witchel. Defeating vanish with low-cost sybil attacks against large dhfs. In *NDSS*, 2010.
- A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure hibe with short ciphertexts. In *TCC*, pp. 455–479, 2010.
- A. B. Lewko and B. Waters. Efficient pseudorandom functions from the decisional linear assumption and weaker variants. In *ACM Conference on Computer and Communications Security*, pp. 112–120, 2009.

- S. Hohenberger and B. Waters. Short and stateless signatures from the rsa assumption. In *CRYPTO*, pp. 654–670, 2009.
- B. Waters. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions. In *CRYPTO*, pp. 619–636, 2009.
- S. Hohenberger and B. Waters. Realizing hash-and-sign signatures under standard assumptions. In *EUROCRYPT*, pp. 333–350, 2009.
- C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In *EUROCRYPT*, pp. 171–188, 2009.
- E. Shen, E. Shi, and B. Waters. Predicate privacy in encryption systems. In *TCC*, pp. 457–473, 2009.
- D. Boneh, D. Freeman, J. Katz, and B. Waters. Signing a linear subspace: Signature schemes for network coding. In *Public Key Cryptography*, pp. 68–87, 2009.
- V. Goyal, S. Lu, A. Sahai, and B. Waters. Black-box accountable authority identity-based encryption. In *ACM Conference on Computer and Communications Security*, pp. 427–436, 2008.
- H. Shacham and B. Waters. Compact proofs of retrievability. In *ASIACRYPT*, pp. 90–107, 2008.
- C. Peikert, V. Vaikuntanathan, and B. Waters. A framework for efficient and composable oblivious transfer. In *CRYPTO*, pp. 554–571, 2008.
- J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *EUROCRYPT*, pp. 146–162, 2008. **Invited to Journal of Cryptology, special issue for top four papers of Eurocrypt 2008.**
- D. Boneh, P. Papakonstantinou, C. Rackoff, Y. Vahlis, and B. Waters. On the impossibility of basing identity based encryption on trapdoor permutations. In *FOCS*, pp. 283–292, 2008.
- E. Shi and B. Waters. Delegating capabilities in predicate encryption systems. In *ICALP (2)*, pp. 560–578, 2008.
- C. Peikert and B. Waters. Lossy trapdoor functions and their applications. In *STOC*, pp. 187–196, 2008. **Invited to SIAM Journal of Computing, special issue for top papers of STOC 2008.**
- J. Bethencourt, D. Song, and B. Waters. Analysis-resistant malware. In *Network and Distributed System Security Symposium (NDSS)*, 2008.
- J. A. Halderman and B. Waters. Harvesting verifiable challenges from online sources. In *ACM Conference on Computer and Communications Security*, pp. 330–341, 2007.
- R. Ostrovsky, A. Sahai, and B. Waters. Attribute-based encryption with non-monotonic access structures. In *ACM Conference on Computer and Communications Security*, pp. 195–203, 2007.
- J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pp. 321–334, 2007.
- X. Boyen and B. Waters. Full-domain subgroup hiding and constant-size group signatures. In *Public Key Cryptography*, pp. 1–15, 2007. **Awarded Best Paper.**
- H. Shacham and B. Waters. Efficient ring signatures without random oracles. In *Public Key Cryptography*, pp. 166–180, 2007.
- D. Boneh and B. Waters. Conjunctive, subset, and range queries on encrypted data. In *TCC*, pp. 535–554, 2007.
- J. Bethencourt, D. Boneh, and B. Waters. Cryptographic methods for storing ballots on a voting machine. In *Network and Distributed System Security Symposium (NDSS)*, 2007.

- X. Boyen, H. Shacham, E. Shen, and B. Waters. Forward-secure signatures with untrusted update. In *ACM Conference on Computer and Communications Security*, pp. 191–200, 2006.
- D. Boneh and B. Waters. A fully collusion resistant broadcast, trace, and revoke system. In *ACM Conference on Computer and Communications Security*, pp. 211–220, 2006.
- V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *ACM Conference on Computer and Communications Security*, pp. 89–98, 2006.
- M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. In *ACM Conference on Computer and Communications Security*, pp. 99–112, 2006.
- X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption (without random oracles). In *CRYPTO*, pp. 290–307, 2006.
- X. Boyen and B. Waters. Compact group signatures without random oracles. In *EUROCRYPT*, pp. 427–444, 2006.
- S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters. Sequential aggregate signatures and multisignatures without random oracles. In *EUROCRYPT*, pp. 465–485, 2006.
- D. Boneh, A. Sahai, and B. Waters. Fully collusion resistant traitor tracing with short ciphertexts and private keys. In *EUROCRYPT*, pp. 573–592, 2006.
- A. Barth, D. Boneh, and B. Waters. Privacy in encrypted content distribution using private broadcast encryption. In *Financial Cryptography*, pp. 52–64, 2006.
- D. Boneh, E. Shen, and B. Waters. Strongly unforgeable signatures based on computational diffie-hellman. In *Public Key Cryptography*, pp. 229–240, 2006.
- J. Bethencourt, D. X. Song, and B. Waters. New constructions and practical applications for private stream searching (extended abstract). In *SECP*, pp. 132–139, 2006.
- X. Boyen, Q. Mei, and B. Waters. Direct chosen ciphertext security from identity-based techniques. In *ACM Conference on Computer and Communications Security*, pp. 320–329, 2005.
- D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In *CRYPTO*, pp. 258–275, 2005.
- B. Waters. Efficient identity-based encryption without random oracles. In *EUROCRYPT*, pp. 114–127, 2005.
- A. Sahai and B. Waters. Fuzzy identity-based encryption. In *EUROCRYPT*, pp. 457–473, 2005.
- J. A. Halderman, B. Waters, and E. W. Felten. A convenient method for securely managing passwords. In *WWW*, pp. 471–479, 2005.
- B. Waters, A. Juels, J. A. Halderman, and E. W. Felten. New client puzzle outsourcing techniques for dos resistance. In *ACM Conference on Computer and Communications Security*, pp. 246–256, 2004.
- P. Golle, J. Staddon, and B. R. Waters. Secure conjunctive keyword search over encrypted data. In *ACNS*, pp. 31–45, 2004.
- B. R. Waters, D. Balfanz, G. Durfee, and D. K. Smetters. Building an encrypted and searchable audit log. In *Network and Distributed System Security Symposium (NDSS)*, pp. 16–24, 2004.
- J. A. Halderman, B. R. Waters, and E. W. Felten. Privacy management for portable recording devices. In *WPES*, pp. 16–24, 2004.
- B. R. Waters, E. W. Felten, and A. Sahai. Receiver anonymity via incomparable public keys. In *ACM Conference on Computer and Communications Security*, pp. 112–121, 2003.

Journal Publications

- J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *Journal of Cryptology*, To Appear.
- C. Peikert and B. Waters. Lossy trapdoor functions and their applications. *SIAM J. Comput.*, 40(6):1803–1844, 2011.
- M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure attribute-based systems. *Journal of Computer Security*, 18(5):799–837, 2010.
- J. Bethencourt, D. Song, and B. Waters. New techniques for private stream searching. *ACM Trans. Inf. Syst. Secur.*, 12(3), 2009.

Journal Boards and Program Chair

Associate Editor, International Journal of Applied Cryptography (2006– present)
Program Co-Chair, Pairings (2009)

Program Committee Service

Computer and Communications Security (CCS) 2010,2011
IEEE Symposium on Security and Privacy 2009, 2010,2011
CRYPTO 2008,2010
Africacrypt 2010
Workshop on Public Key Cryptography 2010
PODC 2009
Pairings 2009 (**Program Co-Chair**)
TCC 2009
Electronic Voting Technology (EVT) Workshop 2008
WWW Conference: Security, Privacy, and Ethics Track 2006, 2007, 2008
Eurocrypt 2007, 2008
Asiacrypt 2007
Applied Cryptography and Network Security (ACNS) 2006,2007
RSA Cryptographer’s Track 2007
ACM CCS Industry and Government Track 2006
Workshop on Privacy in the Electronic Society (WPES) 2005
European Symposium on Research in Computer Security (ESORICS) 2005
Network and Distributed System Security Symposium (NDSS) 2005

Volunteer Service

Member of Travis County Elections Study Group (2009)

Teaching

University of Texas at Austin, CS346: Cryptography – Undergraduate (Spring 2012)
University of Texas at Austin, CS388H: Cryptography (Fall 2011)
University of Texas at Austin, CS336H: Analysis of Programs Honors (Spring 2011)
University of Texas at Austin, CS395T: Advanced Cryptography (Fall 2010)
University of Texas at Austin, CS346: Cryptography – Undergraduate (Spring 2010)
University of Texas at Austin, CS388H: Cryptography (Fall 2009)
University of Texas at Austin, CS395T: Advanced Cryptography (Spring 2009)
Stanford University, CS255: Introduction to Cryptography (Fall 2004), Co-Instructor with Dan Boneh

Ph.D. Student Advising

Yannis Rouselakis, UT Austin (2009 – present)

Allison Lewko, UT Austin (2009 – present)