Brent Waters

Computer Science Department
353 Serra Mall, Gates 4B
MC: 9045
Stanford University
Stanford, CA 94305-9045
Phone: 650-269-9282
Email: bwaters@cs.stanford.edu
Web: http://crypto.stanford.edu/~bwaters/

RESEARCH INTERESTS

My research interests fall broadly in the categories of network security and cryptography. I am particularly interested in designing novel cryptographic algorithms for the purpose of building secure systems. I have done recent research in the topics of denial-of-service resistance, broadcast encryption, identity-based encryption, biometrics, and anonymity.

EDUCATION

Ph.D. Computer Science, Princeton University, 2004
M.A. Computer Science, Princeton University, 2002
Adviser: Edward Felten
B.S. Computer Science, UCLA, 2000, Summa Cum Laude

PROFESSIONAL SERVICE

Program Committees

- Network and Distributed System Security Symposium (NDSS), 2005
- European Symposium on Research in Computer Security (ESORICS), 2005
- Workshop on Privacy in the Electronic Society (WPES), 2005
- Security, Privacy and Ethics track of the 15th World Wide Web Conference (WWW2006)

Reviewer, *Handbook of Information Security*, H. Bigdoli, ed., John Wiley & Sons, 2004.

RECENT WORK EXPERIENCE

Postdoc, Stanford University 2004–2005
Postdoc research in network security and cryptography with Dan Boneh. Lectured for introduction to cryptography course in Winter 2005.

Summer Intern, Palo Alto Research Center (PARC) 2003
Summer internship with Dirk Balfanz and Jessica Staddon. Developed a secure audit-trail mechanism and designed algorithms for secure conjunctive keyword search on encrypted data.

Research Assistant, Princeton University 2000–2004
Graduate researcher in Computer Science Department at Princeton University. Research with adviser Ed Felten in the fields of network security and cryptography.

Teaching Assistant, Princeton University 2001
Taught two discussion sections a week for an introduction to programming systems course. Graded programming projects and wrote exams.

PUBLICATIONS

Papers available at `http://crypto.stanford.edu/~bwaters/`.

- Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys. Dan Boneh and Brent Waters. *To Appear in Crypto 2005.*
- Fuzzy Identity Based Encryption. Amit Sahai and Brent Waters. *Proceedings of Eurocrypt 2005*, pages 114–127, Lecture Notes in Computer Science.
- Efficient Identity-Based Encryption without Random Oracles. Brent Waters. *Proceedings of Eurocrypt 2005*, pages 440–456, Lecture Notes in Computer Science.
- A Convenient Method for Securely Managing Passwords. J. Alex Halderman, Brent Waters, and Edward W. Felten. *Proceedings of the 14th International World Wide Web Conference*, 471–479, ACM Press.
- New Client Puzzle Outsourcing Techniques for DoS Resistance. Brent Waters, Ari Juels, J. Alex Halderman, and Edward W. Felten. *The 11th ACM Conference on Computer and Communications Security (CCS 2004)*, pages 246–256. ACM Press, 2004.
- Privacy Management for Portable Recording Devices. J. Alex Halderman, Brent Waters, and Edward W. Felten. *The 3rd Workshop on Privacy in Electronic Society (WPES 2004)*, pages 16–24. ACM Press 2004.
- Secure Conjunctive Keyword Search over Encrypted Data. Philippe Golle, Jessica Staddon, and Brent Waters. *Applied Cryptography and Network Security (ACNS 2004).* Lecture Notes in Computer Science 3089, pages 31–45. Springer Verlag, 2004.
- Building an Encrypted and Searchable Audit Log. Brent R. Waters, Dirk Balfanz, Glenn Durfee, and D.K. Smetters. *The 11th Annual Network and Distributed System Security Symposium (NDSS 2004)*, pages 215–224.
- Receiver Anonymity via Incomparable Public Keys. Brent R. Waters, Ed Felten, and Amit Sahai. *The 10th ACM Conference on Computer and Communications Security (CCS 2003)*, pages 112–121. ACM Press, 2003.
- Secure, Private Proofs of Location. Brent R. Waters and Edward W. Felten. *Princeton Computer Science Technical Report 667-03.*

AWARDS

- ACM CCS Award for Travel Grant, 2003

- Award from Princeton University Dean's Fund for Scholarly Travel, 2003
- Outstanding Bachelor of Science Degree Recipient (UCLA), 2000
- Dean's List for School of Engineering and Applied Science (UCLA)
- National Merit Scholar, 1996

REFERENCES

Dr. Dirk Balfanz
balfanz@parc.com
Palo Alto Research Center
3333 Coyote Hill Road
Palo Alto, CA 94305
(650) 812-4816

Professor Dan Boneh
dabo@cs.stanford.edu
Computer Science Department
Gates 475
Stanford, CA 94305-9045
(650) 725-3897

Professor Edward Felten
felten@cs.princeton.edu
Dept. of Computer Science
35 Olden Street
Princeton, NJ 08544
(609) 258-5906

Dr. Ari Juels
ajuels@rsasecurity.com
RSA Laboratories
174 Middlesex Turnpike
Bedford, MA 01730
(781) 515-7069

Professor Amit Sahai
sahai@cs.ucla.edu
Department of Computer Science
Boelter Hall, Room 3731E
Los Angeles, CA 90095
(310) 267-4982