Curriculum vitæ

Hovav Shacham

Research Interests

Applied cryptography; systems security.

Publications

Thesis

H. Shacham. *New Paradigms in Signature Schemes.* PhD thesis, Stanford University, Dec. 2005. Nominated by Stanford Department of Computer Science to ACM Doctoral Dissertation Competition.

Journal papers

H. Shacham, D. Boneh, and E. Rescorla. Client side caching for TLS. *ACM Trans. Info. & System Security*, 7(4):553–75, Nov. 2004. Standardized by the IETF as RFC 4507.

D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. *J. Cryptology*, 17(4):297–319, Sept. 2004.

Refereed papers, Security

H. Shacham, M. Page, B. Pfaff, E.-J. Goh, N. Modadugu, and D. Boneh. On the effectiveness of address-space randomization. In B. Pfitzmann and P. Liu, eds., *Proceedings of CCS 2004*, pp. 298–307. ACM Press, Oct. 2004.

E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh. SiRiUS: Securing remote untrusted storage. In M. Tripunitara, ed., *Proceedings of NDSS 2003*, pp. 131–45. Internet Society (ISOC), Feb. 2003.

H. Shacham and D. Boneh. Fast-track session establishment for TLS. In M. Tripunitara, ed., *Proceedings of NDSS 2002*, pp. 195–202. Internet Society (ISOC), Feb. 2002. Extended abstract of journal paper above.

H. Shacham and D. Boneh. Improving SSL handshake performance via batching. In D. Naccache, ed., *Proceedings of CT-RSA 2001*, vol. 2020 of *LNCS*, pp. 28–43. Springer-Verlag, Apr. 2001.

Refereed papers, Cryptography

H. Shacham and B. Waters. Efficient ring signatures without random oracles. In T. Okamoto and X. Wang, eds., *Proceedings of PKC 2007*, LNCS. Springer-Verlag, Apr. 2007. To appear.

X. Boyen, H. Shacham, E. Shen, and B. Waters. Forward secure signatures with untrusted update. In R. Wright, ed., *Proceedings of CCS 2006*, pp. 191–200. ACM Press, Oct. 2006.

S. Lu, R. Ostrovsky, A. Sahai, H. Shacham, and B. Waters. Sequential aggregate signatures and multisignatures without random oracles. In S. Vaudenay, ed.,

Proceedings of Eurocrypt 2006, vol. 4004 of *LNCS*, pp. 465–85. Springer-Verlag, May 2006.

D. Boneh and H. Shacham. Group signatures with verifier-local revocation. In B. Pfitzmann and P. Liu, eds., *Proceedings of CCS 2004*, pp. 168–77. ACM Press, Oct. 2004.

D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In M. Franklin, ed., *Proceedings of Crypto 2004*, vol. 3152 of *LNCS*, pp. 41–55. Springer-Verlag, Aug. 2004.

A. Lysyanskaya, S. Micali, L. Reyzin, and H. Shacham. Sequential aggregate signatures from trapdoor permutations. In C. Cachin and J. Camenisch, eds., *Proceedings of Eurocrypt 2004*, vol. 3027 of *LNCS*, pp. 74–90. Springer-Verlag, May 2004.

D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In E. Biham, ed., *Proceedings of Eurocrypt 2003*, vol. 2656 of *LNCS*, pp. 416–32. Springer-Verlag, May 2003.

D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In C. Boyd, ed., *Proceedings of Asiacrypt 2001*, vol. 2248 of *LNCS*, pp. 514–32. Springer-Verlag, Dec. 2001. Extended abstract of journal paper above.

In Submission

H. Shacham. The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86), 2006. Submitted.

H. Shacham. A Cramer-Shoup encryption scheme from the Linear assumption, 2006. Submitted.

Survey papers

D. Boneh, C. Gentry, B. Lynn, and H. Shacham. A survey of two signature aggregation techniques. *RSA Cryptobytes*, 6(2):1–9, Summer 2003.

D. Boneh and H. Shacham. Fast variants of RSA. *RSA Cryptobytes*, 5(1):1–9, Winter/Spring 2002.

Professional Activities

Invited Talks

Pairings in Cryptography Workshop 2005: "Implementing Pairing-Based Signature Schemes."
ECC 2004: "A New Life for Group Signatures," joint work with Dan Boneh and Xavier Boyen.

Journal Board

AIMS Advances in Mathematics of Communications.

PC Member

Eurocrypt 2008; ICDCS 2007 (Security area); ISPEC 2007; PKC 2007; Asiacrypt 2006; Crypto 2006; ACIS 2006; ACM AsiaCCS 2006; Asiacrypt 2005; WISA 2005; ISC 2004.

Education

10/2005–Present	Weizmann Institute of Science, Faculty of Mathematics and Computer Science. Postdoctoral fellow, supported by a Koshland Scholars Program fellowship. Host: Moni Naor.
9/2000–10/2005	Stanford University, Department of Computer Science. Ph. D. in applied cryptography and systems security. Advisor: Dan Boneh. Thesis: *New Paradigms in Signature Schemes*, nominated by Stanford Department of Computer Science to ACM Doctoral Dissertation Competition
1/1999–6/1999	Stanford Program in Oxford. Tutorials in Shakespeare and textual criticism.
9/1996–6/2000	Stanford University. B. S. in computer science, with distinction and departmental honors; A. B. in English, with distinction. Honors thesis: "Accelerating SSL Performance in Software."

Teaching

Spring 2006	Lecturer, Pairings in Cryptography, Weizmann Institute of Science. Designed and taught semester-long graduate two-hour-per-week course at the Weizmann on the mathematics of pairings and the cryptographic systems based on them. Topics included: mathematical background through Weil Reciprocity and Miller's algorithm; identity-based encryption (IBE); constructions based on IBE and hierarchical IBE, with a focus on CCA-secure encryption schemes; digital signatures and their variants; and the composite-order setting. Course website: `http://crypto.stanford.edu/~hovav/pic/`.
Spring 2003, Spring 2002	Teaching Assistant, CS 155: Computer and Network Security, Stanford. Assisted Profs. Boneh and Mitchell in designing an advanced-undergraduate course on computer and network security. Designed and implemented programming assignments now used at Stanford, UT Austin, Toronto, and Northwestern.

Awards

10/2006	Runner up, Arthur L. Samuel Thesis Award, Stanford Department of Computer Science.
8/2006	Ph. D. thesis nominated by Stanford Department of Computer Science to ACM Doctoral Dissertation Competition.
4/2006	Koshland Scholars Program postdoctoral fellowship, Weizmann Institute.
5/2000	Frederick E. Terman Award for Scholastic Achievement in Engineering, Stanford University School of Engineering.
10/1997	President's Award for Academic Excellence in the Freshman Year, Stanford University.