

# Dawn Xiaodong Song

387 Soda Hall  
University of California, Berkeley  
Berkeley, CA 94720

Office: 510-642-1266, fax: 510-642-5814  
[dawnsong@cs.berkeley.edu](mailto:dawnsong@cs.berkeley.edu) (Best way to reach me)  
<http://www.cs.berkeley.edu/~dawnsong>

## Research Interests

Security and applied cryptography, including security in systems, networking, databases, and electronic commerce. Applications of program analysis, model checking, and software engineering techniques to computer security.

## Education

- Ph.D., Computer Science, 1999-2002 (expected), University of California, Berkeley  
Thesis Title: *Automatic Tools for Building Secure Systems*  
Advisor: J. D. Tygar
- M.S., Computer Science, 1997-1999, Carnegie Mellon University
- B.S., Physics, 1992-1996, Tsinghua University, China, (Highest Honors)

## Industrial Experience

- Summer 1999, Research Intern, T.J.Watson Research Center, IBM.
- Summer 1998, Research Intern, Computer Science Laboratories, SRI International

## Teaching Experience

- Sprint 2001, Teaching Assistant, Combinatorics and Discrete Probability (Undergraduate), University of California, Berkeley
- Spring 1999, Teaching Assistant, Operating Systems (Undergraduate), Carnegie Mellon University

## Refereed Conference and Journal Papers

1. "Homomorphic Signature Schemes." R. Johnson, D. Molnar, D. Song, and D. Wagner. To appear in *Proceedings of RSA Conference, Cryptographer's track*, February 2002.
2. "SAM: A Flexible and Secure Auction Architecture Using Trusted Hardware." A. Perrig, S. Smith, D. Song, and J. D. Tygar. In *Electronic Journal on E-commerce Tools and Applications*, to appear, 2002.
3. "Practical Forward Secure Group Signature Schemes." D. Song. In *Proceedings of the Eighth ACM Conference on Computer and Communications Security (CCS-8)*, pages 225–234, November 2001.
4. "A Cryptanalysis of the High-bandwidth Digital Content Protection System." S. Crosby, I. Goldberg, R. Johnson, D. Song, and D. Wagner. In *Proceedings of Workshop on Security and Privacy in Digital Rights Management*, November 2001.
5. "Timing Analysis of Keystrokes and SSH Timing Attacks." D. Song, D. Wagner, and X. Tian. In *Proceedings of USENIX Security Symposium*, pages 337–352, August 2001.
6. "Athena, a Novel Approach to Efficient Automatic Security Protocol Analysis." D. Song, S. Berezin, and A. Perrig. In *Journal of Computer Security*, 9(1,2):47–74, 2001.
7. "AGVI — Automatic Generation, Verification, and Implementation of Security Protocols." D. Song, A. Perrig, and D. Phan. In *Proceedings of 13th Conference on Computer Aided Verification CAV 2001*, pages 241–245, July 2001.
8. "ELK, a New Protocol for Efficient Large-Group Key Distribution." A. Perrig, D. Song, and D. Tygar. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 247–262, May 2001.
9. "Advanced and Authenticated Marking Schemes for IP Traceback." D. Song and A. Perrig. In *Proceedings of IEEE Infocomm 2001*, April 2001.
10. "Efficient and Secure Source Authentication for Multicast." A. Perrig, R. Canetti, D. Song, and J. D. Tygar. In *Proceedings of Symposium on Network and Distributed Systems Security (NDSS 2001)*, pages 35–46, February 2001.
11. "Looking for Diamonds in the Desert — Extending Automatic Protocol Generation to Three-Party Authentication and Key Agreement Protocols." A. Perrig and D. Song. In *Proceedings of the 13th IEEE Computer Security Foundations Workshop*, pages 64–76, July 2000.
12. "Efficient Authentication and Signature of Multicast Streams Over Lossy Channels." A. Perrig, R. Canetti, J. D. Tygar, and D. Song. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 56–73, May 2000.

13. "Practical Techniques for Searches on Encrypted Data." D. Song, D. Wagner, and A. Perrig. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 44–55, May 2000.
14. "A First Step towards the Automatic Generation of Security Protocols." A. Perrig and D. Song. In *Proceedings of Symposium on Network and Distributed Systems Security (NDSS '00)*, pages 73–83, February 2000.
15. "Hash Visualization: A New Technique to Improve Real-World Security." A. Perrig and D. Song. In Blum and Lee, editors, *International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99)*, pages 131–138, July 1999.
16. "Athena, an Automatic Checker for Security Protocol Analysis." D. Song. In Proceedings of the IEEE Computer Security Foundation Workshop, pages 192–202, June 1999.

## Papers Submitted for Publication

17. "Expander Graphs for Digital Stream Authentication and Robust Overlay Networks." D. Song, D. Zuckerman, and J. D. Tygar. November 2001.

## IETF Drafts

18. "TESLA: Multicast Source Authentication Transform." A. Perrig, R. Canetti, B. Briscoe, D. Song, and J. D. Tygar. IETF draft, November 2000.

## Patents

19. "Secure Auction Marketplace using a Secure Coprocessor." A. Perrig, S. Smith, and D. Song. U.S. Patent pending, filed in 2000.