

# David Molnar

515 Soda Hall  
University of California, Berkeley  
Berkeley, CA 94720  
(510) 642-5266  
dmolnar@eecs.berkeley.edu  
<http://www.cs.berkeley.edu/~dmolnar>

## EDUCATION ◇ **University of California, Berkeley**

PhD in Computer Science in progress. Advisor: David Wagner.

M.S. in Computer Science, Spring 2006.

Master's report: *Privacy and Security In Two RFID Deployments, With New Methods for Private Authentication and RFID Pseudonyms.*

## ◇ **Harvard University**, Cambridge, MA.

AB in Computer Science, Spring 2003.

Thesis title: *Homomorphic Signature Schemes.*

Thesis advisor: M.O. Rabin.

Concentration advisor: S. Shieber.

## ◇ **Park City Math Institute/IAS**, Princeton, NJ.

Summer 2000 program in Computational Complexity.

## ◇ **Awards**

- Sevin Rosen Funds Award, Berkeley EECS 2008
- National Science Foundation Graduate Fellowship (Award 2004, Hon. Mention 2003)
- Intel Open Collaboration Research Fellowship, Fall 2003
- Harvard Division of Engineering and Applied Sciences Teaching Award, Spring 2003
- Harvard Derek Bok Center Certificate of Teaching Distinction, Fall 2000, Fall 2002
- Clay Mathematics Institute Scholarship, Summer 2000

RESEARCH Cryptography, privacy, and computer security.

## INTERESTS

PUBLICATIONS P. Godefroid, M.Y. Levin, and D. Molnar. Active Property Checking. EMSOFT 2008.

(REFEREED) P. Godefroid, M.Y. Levin, and D. Molnar. "Automated Whitebox Fuzz Testing." Network Distributed Security Symposium (NDSS) 2008.

N. Hopper, D. Molnar, and D. Wagner. "From Weak to Strong Watermarking." Theory of Cryptography Conference (TCC) 2007.

C. Crutchfield, D. Molnar, and D. Turner. "Approximate Measurement of Privacy Loss in an Election With Precinct Reports." NSF/NIST Voting Systems Performance Rating Workshop 2006.

D. Molnar, T. Kohno, N. Sastry, and D. Wagner. "Tamper-Evident, History-Independent, Subliminal-Free Data Structures on PROM Storage -or- How to Store Ballots on a Voting Machine (Extended Abstract)." Short paper in IEEE Symposium on Security and Privacy ("Oakland") 2006.

C. Crutchfield, D. Molnar, D. Turner, and D. Wagner. "Generic On-line/Off-line Threshold Signatures." Public Key Cryptography (PKC) 2006.

- D. Molnar, M. Piotrowski, D. Schultz, and D. Wagner. “The Program Counter Security Model: Automatic Detection and Removal of Control-Flow Side Channel Attacks.” International Conference on Information Security and Cryptography (ICISC) 2005.
- D. Molnar, A. Soppera, and D. Wagner. “RFID Privacy Through Trusted Computing.” (Short Paper). Workshop on Privacy in the Electronic Society (WPES) 2005.
- C. Gentry, D. Molnar, and Z. Ramzan. “Efficient Designated Confirmer Signatures Without Random Oracles or General Zero-Knowledge Proofs.” ASIACRYPT 2005.
- R. Jain, D. Molnar, and Z. Ramzan. “Towards Understanding Algorithmic Factors Affecting Energy Consumption: Switching Complexity, Randomness, and Preliminary Experiments.” DIALM/POMC 2005.
- D. Molnar, A. Soppera, and D. Wagner. “A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags.” Selected Areas in Cryptography (SAC) 2005.
- A. Juels, D. Molnar, and D. Wagner. “Security and Privacy Issues in E-Passports.” IEEE SecureComm 2005.
- S. Draper, P. Ishwar, D. Molnar, V. Prabhakaran, K. Ramchandran, D. Schonberg, and D. Wagner. “An Analysis of PMF Based Tests for Detection of Least Significant Bit Image Steganography.” Information Hiding Workshop (IH) 2005.
- R. Jain, D. Molnar, and Z. Ramzan. “Towards A Model of Energy Complexity for Algorithms.” (Invited talk) in IEEE Wireless Communications and Networking Conference (WCNC) 2005.
- N. Good, J. Han, E. Miles, D. Molnar, D. Mulligan, L. Quilter, J. Urban, and D. Wagner. “Radio Frequency Id and Privacy with Information Goods.” (Short Paper). Workshop on Privacy in the Electronic Society (WPES) 2004.
- D. Molnar and D. Wagner. “Privacy and Security in Library RFID : Issues, Practices, and Architectures.” ACM Computer and Communications Security (CCS) 2004.
- T.Vila, R. Greenstadt, and D. Molnar. “Why We Can’t Be Bothered To Read Privacy Policies: Models of Privacy Economics as a Lemons Market.” Workshop on Economics and Information Security (WEIS) 2003. Also a book chapter in *Economics of Information Security*, L. J. Camp and S. Lewis eds., Springer-Verlag, September 2004.
- R. Johnson, D. Molnar, D. Song, and D. Wagner. “Homomorphic Signature Schemes.” RSA2002 Conference, Cryptographer’s Track. LNCS 2271.
- R. Dingledine, M. Freedman, D. Hopwood, and D. Molnar. “A Reputation Scheme To Increase MIX-net Reliability.” 2001 Information Hiding Workshop (IH 2001). LNCS 2137.
- R. Dingledine, M. Freedman, and D. Molnar. “Free Haven - A Distributed Anonymous Storage System.” Berkeley Workshop on Design Issues in Anonymity and Unobservability. (WDIAU) 2000. LNCS 2009.

PUBLICATIONS (NON-REFEREED) A. Sotirov, M. Stevens, J. Appelbaum, A. Lenstra, D. Molnar, D. A. Osvik, and B. de Weger. “MD5 considered harmful today Creating a rogue CA certificate.” 25th Chaos Communications Congress, Berlin, Germany. December 2008.

D. Molnar and D. Wagner. “Catchconv : Symbolic execution and run-time type inference for integer conversion errors.” UCB EECS Technical Report 2007-23, February 2007.

T. Burbridge, A. Soppera, and D. Molnar. “RFID Security and Privacy – Issues, Standards, and Solutions.” Chapter in *Intelligent Spaces: The Application of Pervasive Information and Communication Technology*, Alan Steventon and Steven Wright, eds. Springer-Verlag Publishers. February 2006.

D. Molnar, R. Stapleton-Gray, and D. Wagner. “Killing, Recoding, and Beyond.” Chapter in *RFID Applications, Security and Privacy*, Simson Garfinkel and Beth Rosenberg eds., Addison/Wesley Publishers. July 2005.

R. Dingledine, M.J. Freedman, and D. Molnar. "Accountability in Peer-to-Peer Systems." Chapter in Peer-to-Peer: Harnessing The Benefits of a Disruptive Technology , Andy Oram ed., O'Reilly Publishers. March 2001.

Technology description for Harvard University Kennedy School of Government workshop on Digital Identity. With R. Dingledine, M. J. Freedman, and D. Parkes.

D. Molnar. "The SETI@Home Problem." ACM Crossroads: The ACM Student Magazine. 2000. (Translated into Russian.)

- WORK       ◇ Intern - Microsoft Research, Redmond, WA (February 2007 - July 2007)
- EXPERIENCE ◇ Research Assistant, UC-Berkeley (Spring 2004 - Present)
- ◇ Intern - NTT DoCoMo Labs USA, San Jose, CA (Summer 2004)
- ◇ Teaching Assistant, UC-Berkeley (Fall 2003)
- ◇ Consultant - Legra Systems, Inc., Burlington, MA (Summer 2003)
- ◇ Research Assistant, Harvard University (Summer 2003)
- ◇ Teaching Fellow, Harvard University (Fall 2002)
- ◇ Security Engineer, ShieldIP, New York, NY (Summer 2001 - Summer 2002)
- ◇ Research Assistant, Harvard University (Summer 2000)
- ◇ Teaching Fellow, Harvard University (Fall 2000)
- ◇ System Software Engineer Intern, Green Hills Software (Summer 1998)
- SERVICE    Program Committee, SecureComm 2009
- Program Committee, Financial Cryptography 2009
- Program Committee, RFIDSec 2008, 2009
- Program Committee, SocialNets 2008
- Program Committee, AfricaCrypt 2008
- Program Committee, ACM Computer and Communications Security (CCS) 2007, 2008, 2009
- Program Committee, ACM Workshop on Privacy in the Electronic Society (WPES) 2006
- Program Committee, ACM Wireless Security (WiSe) 2006
- Program Committee, Privacy Enhancing Technologies Symposium (PETS) 2006, 2007, 2008, 2009
- Program Committee, Workshop on Pervasive Security (PerSec) 2006, 2007
- Program Committee, Trust, Security, and Privacy in Ubiquitous Computing 2007
- Program Committee, CodeCon 2005, 2006
- Reviewer for Computer Security Foundations Workshop, OSDI 2004, CRYPTO 2004, ACM Electronic Commerce 2005, NDSS 2006, Usenix Security 2005, 2006, J. Comp. Security, Workshop Information Security and Applications 2005, Indocrypt 2005, Oakland 2006, Em-Nets 2005, SIGCOMM 2005, SOSP 2005, CCS 2005, NSS-Globecom 2006, Theory of Cryptography 2007, IEEE Trans. Dependable and Secure Computing, Applied Cryptography and Network Security 2008.
- Organizer, Berkeley Security Reading Group, Fall 2003 - Summer 2006
- Organized workshop on applying to fellowships, Fall 2004
- REFERENCES Available on request.