

Matthew D. Green

Curriculum Vitae

Contact

3800 N. Charles Street, 209 Maryland Hall, Baltimore, MD 21218
Phone: 410-861-0344 Fax: 928-223-2296
mgreen@cs.jhu.edu
<http://www.spar.isi.jhu.edu/~mgreen>

Education

Ph.D., Computer Science, November 2008
Johns Hopkins University
Baltimore, MD
Thesis: *Cryptography for Secure and Private Databases:
Enabling Practical Data Access without Compromising Privacy*
Advisor: Prof. Susan R. Hohenberger

M.S., Computer Science, December 2005
Johns Hopkins University
Baltimore, MD

B.A., Computer Science, May 1998
Oberlin College
Oberlin, OH

B. Mus., Technology in Music and Related Arts, May 1998
Oberlin Conservatory of Music
Oberlin, OH

Research Interests

Cryptography and computer security.

Employment

9/2010–present	Assistant Research Professor Johns Hopkins University Baltimore, MD
11/2012–present	Research Associate (Adjunct) University of Maryland College Park, MD
2/2005–9/2011	CTO Independent Security Evaluators Baltimore, MD
6/1999–6/2003	Senior Technical Staff Member AT&T Labs/Research Florham Park, NJ

Research Publications

Conference Papers

- Ian Miers, Christina Garman, Matthew Green, and Avi Rubin. Zerocoin: Anonymous Distributed e-Cash from Bitcoin. In *IEEE Symposium on Security and Privacy (Oakland) 2013*, May 2013.
- Joseph A. Akinyele, Matthew Green, Susan Hohenberger, and Matthew W. Pagano. Machine-generated algorithms, proofs and software for the batch verification of digital signature schemes. In *Proceedings of the 2012 ACM conference on Computer and communications security, CCS '12*, pages 474–487, New York, NY, USA, 2012. ACM.
- David Cash, Matthew Green, and Susan Hohenberger. New definitions and separations for circular security. In *Public Key Cryptography (PKC '12)*. Springer, 2012.
- J. A. Akinyele, M. W. Pagano, M. Green, C. Lehmann, Z. Peterson, and A. Rubin. Securing electronic medical records using attribute-based encryption on mobile devices. In *1st ACM CCS-SPSM*, 2011.
- Matthew Green, Susan Hohenberger, and Brent Waters. Outsourcing the decryption of a be cipher-texts. In *Proceedings of the 20th USENIX conference on Security, SEC'11*, pages 34–34, Berkeley, CA, USA, 2011. USENIX Association.
- Matthew D. Green and Aviel D. Rubin. A research roadmap for healthcare IT security inspired by the PCAST health information technology report. In *Proceedings of the 2nd USENIX conference on Health security and privacy, HealthSec '11*, Berkeley, CA, USA, 2011. USENIX Association.
- Matthew Green and Susan Hohenberger. Oblivious transfer from simple assumptions. In *Theory of Cryptography Conference (TCC '11)*. Springer, 2011.
- Matthew Green. Secure blind decryption. In *14th International Conference on Practice and Theory of Public Key Cryptography (PKC '11)*. Springer, 2011.
- Jae Hyun Ahn, Matthew Green, and Susan Hohenberger. Synchronized aggregate signatures. In *ACM Conference on Computer and Communications Security (CCS '10)*. ACM Press, 2010.
- Anna Lisa Ferrara, Matthew Green, Susan Hohenberger, and Michael Østergaard Pedersen. Practical short signature batch verification. In *Proceedings of the The Cryptographers' Track at the RSA Conference 2009: CT-RSA 2009*, volume 5473 of LNCS, pages 309–324. Springer, 2009.
- Scott Coull, Matthew Green, and Susan Hohenberger. Controlling access to an oblivious database using stateful anonymous credentials. In *Proceedings of the 12th International Conference on Practice and Theory in Public Key Cryptography: PKC 2009*, volume 5443 of LNCS, pages 501–520. Springer, 2009.
- Matthew Green and Susan Hohenberger. Universally composable adaptive oblivious transfer. In *Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security: ASIACRYPT '08*, volume 5350 of LNCS. Springer, 2008.
- Matthew Green and Susan Hohenberger. Blind identity-based encryption and simulatable oblivious transfer. In *Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security: ASIACRYPT '07*, volume 4833 of LNCS, pages 265–282. Springer, 2007.
- Matthew Green and Giuseppe Ateniese. Identity-based proxy re-encryption. In *Proceedings of the 5th International Conference on Applied Cryptography and Network Security: ACNS '07*, volume 4521 of LNCS, pages 288–306, 2007.
- Stephen Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel Rubin, and Michael Szydlo. Security analysis of a cryptographically-enabled RFID device. In *Proceedings of USENIX Security '05*. USENIX Association, 2005. **Winner of Best Student Paper Award.**

Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In *The 12th Annual Network and Distributed System Security Symposium: NDSS '05*. The Internet Society, 2005.

Andrea Basso, Charles D. Cranor, Raman Gopalakrishnan, Matthew Green, Charles R. Kalmanek, David Shur, Sandeep Sibal, Cormac J. Sreenan, and Jacobus E. van der Merwe. PRISM, an IP-based architecture for broadband access to TV and other streaming media. In *IEEE International Workshop on Network and Operating System Support for Digital Audio and Video*, 2000.

Journal Papers

Scott Coull, Matthew Green, and Susan Hohenberger. Controlling access to an oblivious database using stateful anonymous credentials. *ACM Transactions on Information and System Security (TISSEC)* — *To appear*, 2011.

Stephen Bono, Aviel Rubin, Adam Stubblefield, and Matthew Green. Security through legality. *Commun. ACM*, 49(6):41–43, 2006.

Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security (TISSEC)*, 9(1), February 2006.

Charles D. Cranor, Matthew Green, Chuck Kalmanek, David Shur, Sandeep Sibal, Jacobus E. Van der Merwe, and Cormac J. Sreenan. Enhanced streaming services in a content distribution network. *IEEE Internet Computing*, 05(4):66–75, 2001.

Patents

- “Method and apparatus for limiting access to sensitive data”, U.S. Patent 7840795 (Issue date Nov 10, 2010).
- “Method for content-aware redirection and content renaming”, U.S. Patent 6954456 (Issue date Oct 11, 2005)

Grants

Co-PI, National Science Foundation award CNS-1010928, “Self Protecting Electronic Medical Records”. Amount: \$1,733,881.

Co-PI, DARPA PROgramming Computation on EncryptEd Data (PROCEED). Amount: \$344,000.

Senior Personnel, Department of Health and Human Services Strategic Healthcare Information Technology Advanced Research Projects on Security (SHARPS), Research Focus Area: Security of Health Information Technology. Amount: \$1,600,399.

Teaching

650.445 (600.454). PRACTICAL CRYPTOGRAPHIC SYSTEMS (Spring 2009, 2010, 2011). In this course I examine the issues surrounding the design and evaluation of industrial cryptographic products, and the ways that these systems fail in practice.

650.445 (600.454). PRACTICAL CRYPTOGRAPHIC SYSTEMS (Spring 2009, 2010, 2011). In this course I examine the issues surrounding the design and evaluation of industrial cryptographic products, and the ways that these systems fail in practice.

Awards

- ‘Award for Outstanding Research in Privacy Enhancing Technologies (PET award), 2007.
- Usenix Security, 2005. Best Student Paper. “Security analysis of a cryptographically-enabled RFID device” (9/15/2005).

Program Committees

Usenix Security 2013. Committee chair: Sam King.

Usenix Security 2012. Committee chair: Tadayoshi Kohno.

Usenix Security 2011. Committee chair: David Wagner.

The Fifth International Conference on Provable Security **ProvSec 2011.**

The 12th International Conference on Information Security and Cryptology **ICISC 2009.**

The Third International Conference on Pairing-based Cryptography **Pairing 2009.**

Electronic Commerce and Web Technologies, Security Track **EC-Web 2009.**

Software Projects

Charm. A Python framework for rapidly prototyping cryptosystems.

The Functional Encryption Library (libfenc). A C implementation of several functional encryption and Attribute-Based Encryption schemes.

The JHU/MIT Proxy Re-cryptography Library (PRL). A prototype C++ implementation of several proxy re-encryption schemes.

Litigation Experience

Experience as a Testifying Expert

Videotron Ltee, Videotron (Regional) Ltee and CF Cable TV inc. vs Bell ExpressVu Limited Partnership (Quebec Superior Court No 500-17-027275-059)

Group TVA inc. vs. Bell ExpressVu Limited Partnership (Quebec Superior Court No. 500-17- 018324-031, 500-17-022586-047, 500-17-027276-057)

Deposition Experience

Keith Dunbar vs Google, Inc. US District Court for the Eastern District of Texas, Civil Action N 5:10CV00194

SmartPhone v. HTC., US District Court for the Eastern District of Texas, Civil Action # 6:10-cv-580

Patent and Source Code Analysis

Symbol Technologies, Inc. Et al. v. Aruba Networks, Inc., Case # 07-519-JJFF

DataSci LLC vs. Medidata Solutions, Inc, Case # 09-cv-01611-MJG

TecSec Inc vs. International Business Machines Corporation, Case # 1:10-CV 115 LMB/TCB

The PACid Group, LLC v. 2Wire, Inc., Brother Industries, Ltd., et al., Case # 6:08-cv-00498

SmartPhone v. HTC., US District Court for the Eastern District of Texas, Civil Action # 6:10-cv-580

SmartPhone v. Apple., US District Court for the Eastern District of Texas, Civil Action # 6:10-cv-00074-LED-JDL

Criminal Cases

US v. Hanjuan Jin 08-CR-192

Press Appearances

John Schwartz. Graduate cryptographers unlock code of ‘thiefproof’ car key. The New York Times (National Edition), January 2005.

Hackers can crack car-key codes. Consumer Reports, July 2007.

Researchers: We cracked car alarm system. USA Today, January 2005.

Samuel Greengard. 6 common IT security mistakes and how to avoid them. Microsoft UK Security Centre.

April 11, 2013