Matthew D. Green

Curriculum Vitae

Contact

3400 N. Charles Street, 313 Malone Hall, Baltimore, MD 21218
Phone: 410-861-0344
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

Applied cryptography and computer security.

Employment

7/2015–present — Assistant Professor
Johns Hopkins University
Baltimore, MD

9/2010–6/2015 — Assistant Research Professor
Johns Hopkins University
Baltimore, MD

9/2009-9/2010 — Assistant Research Scientist
Johns Hopkins University
Baltimore, 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

Alessandro Chiesa, Matthew Green, Jingcheng Liu, Peihan Mao, Ian Miers, and Pratyush Mishra. Decentralized Anonymous Credentials. In *Advances in Cryptology (EUROCRYPT '17), To appear*, 2017.

Matthew Green, Watson B. Ladd, and Ian Miers. A protocol for privately reporting ad impressions at scale. In *ACM Conference on Computer and Communications Security (CCS '16)*, pages 1591–1601, 2016.

Stephen Checkoway, Jacob Maskiewicz, Christina Garman, Josh Fried, Shanaan Cohney, Matthew Green, Nadia Heninger, Ralf-Philip Weinmann, Eric Rescorla, and Hovav Shacham. A systematic analysis of the Juniper Dual EC incident. In *ACM Conference on Computer and Communications Security (CCS '16)*, pages 468–479, 2016. **Winner of Best Paper Award.**

Matthew Green, Jonathan Katz, Alex J. Malozemoff, and Hong-Sheng Zhou. A unified approach to idealized model separations via Indistinguishability Obfuscation. In *Security and Cryptography for Networks (SCN) 2016*, pages 587–603, 2016.

Christina Garman, Matthew Green, Gabriel Kaptchuk, Ian Miers, and Michael Rushanan. Dancing on the lip of the volcano: Chosen ciphertext attacks against Apple iMessage. In *USENIX Security Symposium*, Washington, DC, 2016. Usenix Association. *(Acceptance rate 15.6%)*.

Karthikeyan Bhargavan, Christina Brzuska, Cedric Fournet, Markulf Kohlweiss, Santiago Zanella-Béguelin, and Matthew Green. Downgrade resilience in key exchange protocols. In *IEEE Symposium on Security and Privacy (Oakland) 2016*, pages 506–525, 2016. *(Acceptance rate: 13.3%)*.

Christina Garman, Matthew Green, and Ian Miers. Accountable Privacy for Decentralized Anonymous Payments. In *Financial Cryptography*, 2016.

David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Zanella-Béguelin, and Paul Zimmermann. Imperfect forward secrecy: How Diffie-Hellman fails in practice. In *ACM Conference on Computer and Communications Security (CCS '15)*, pages 5–17. ACM Press, 2015. *(Acceptance rate: 19.8%)* **Winner of Best Paper Award.**

Matthew Green and Ian Miers. Forward Secure Asynchronous Messaging from Puncturable Encryption. In *2015 IEEE Symposium on Security and Privacy, SP 2015*, Oakland '15, pages 305–320, Berkeley, CA, USA, 2015. *(Acceptance rate: 13.5%)*.

Eli Ben-Sasson, Alessandro Chiesa, Matthew Green, Eran Tromer, and Madars Virza. Secure Sampling of Public Parameters for Succinct Zero Knowledge Proofs. In *2015 IEEE Symposium on Security and Privacy, SP 2015*, Oakland '15, pages 287–304, 2015. *(Acceptance rate: 13.5%)*.

Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, and Hovav Shacham. On the Practical Exploitability of Dual EC in TLS Implementations. In *Proceedings of the 23rd USENIX Conference on Security Symposium*, SEC'14, pages 319–335, Berkeley, CA, USA, 2014. USENIX Association. *(Acceptance rate 19%)*.

Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized Anonymous Payments from Bitcoin. In *2014 IEEE Sym-*

posium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014, pages 459–474, 2014. *(Acceptance rate 15.6%)*.

Alex J. Malozemoff, Jonathan Katz, and Matthew D. Green. Automated analysis and synthesis of block-cipher modes of operation. In *In CSF '14.*, volume 2014, pages 140–152, 2014. *(Acceptance rate: 35%)*.

Christina Garman, Matthew Green, Ian Miers, and Aviel D. Rubin. Rational zero: Economic security for Zerocoin with everlasting anonymity. In *BITCOIN '14*, pages 140–155, 2014.

Christina Garman, Matthew Green, and Ian Miers. Decentralized Anonymous Credentials. In *Network and Distributed System Security Symposium: NDSS '14*, 2014. *(Acceptance rate: 18.6%)*.

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*, pages 397–411, May 2013. *(Acceptance rate: 12%)*.

Ayo Akinyele, Matthew Green, and Susan Hohenberger. Using SMT Solvers to Automate Design Tasks for Encryption and Signature Schemes. In *Proceedings of the 2013 ACM conference on Computer and communications security, CCS '13*, pages 399–410, October 2013. *(Acceptance rate: 20%)*.

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. *(Acceptance rate: 18.9%)*.

David Cash, Matthew Green, and Susan Hohenberger. New definitions and separations for circular security. In *Public Key Cryptography (PKC '12)*, pages 540–557. Springer, 2012. *(Acceptance rate 22%)*.

Ian Miers and Matthew Green. Vis-à-vis Cryptography: Private and Trustworthy In-Person Certifications. In *Presented as part of the 3rd USENIX Workshop on Health Security and Privacy*, Berkeley, CA, 2012. USENIX.

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*, pages 75–86, 2011.

Matthew Green, Susan Hohenberger, and Brent Waters. Outsourcing the decryption of ABE ciphertexts. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, pages 34–34, Berkeley, CA, USA, 2011. USENIX Association. *(Acceptance rate: 17%)*.

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, pages 5–10, Berkeley, CA, USA, 2011. USENIX Association.

Matthew Green and Susan Hohenberger. Oblivious transfer from simple assumptions. In *Theory of Cryptography Conference (TCC '11)*, pages 347–362. Springer, 2011. *(Acceptance rate 32%)*.

Matthew Green. Secure blind decryption. In *14th International Conference on Practice and Theory of Public Key Cryptography (PKC '11)*, pages 265–282. Springer, 2011. *(Acceptance rate 27%)*.

Jae Hyun Ahn, Matthew Green, and Susan Hohenberger. Synchronized aggregate signatures. In *ACM Conference on Computer and Communications Security (CCS '10)*, pages 473–484. ACM Press, 2010. *(Acceptance rate: 17.2%)*.

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 12^{th} International Conference on Practice and Theory in Public Key Cryptography: PKC 2009*, volume 5443 of LNCS, pages 501–520. Springer, 2009. *(Acceptance rate 25%)*.

Matthew Green and Susan Hohenberger. Universally composable adaptive oblivious transfer. In *Proceedings of the 14^{th} International Conference on the Theory and Application of Cryptology and Information Security: ASIACRYPT '08*, volume 5350 of LNCS, pages 179–197. Springer, 2008. *(Acceptance rate 17%)*.

Matthew Green and Susan Hohenberger. Blind identity-based encryption and simulatable oblivious transfer. In *Proceedings of the 13^{th} International Conference on the Theory and Application of Cryptology and Information Security: ASIACRYPT '07*, volume 4833 of LNCS, pages 265–282. Springer, 2007. *(Acceptance rate 15%)*.

Matthew Green and Giuseppe Ateniese. Identity-based proxy re-encryption. In *Proceedings of the 5^{th} International Conference on Applied Cryptography and Network Security: ACNS '07*, volume 4521 of LNCS, pages 288–306, 2007. *(Acceptance rate: 12%)*.

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*, pages 1–15. USENIX Association, 2005. *(Acceptance rate: 14.8%)* **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 12^{th} Annual Network and Distributed System Security Symposium: NDSS '05*, pages 1–30. The Internet Society, 2005. *(Acceptance rate: 12.9%)*.

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

Matthew Green and Matthew Smith. Developers Are Not The Enemy! The need for usable security APIs. *IEEE Security & Privacy (To appear)*.

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, and Daniel J. Weitzner. Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 1(1):69–79, 2015.

Ayo Akinyele, Matthew Green, Susan Hohenberger, and Matthew Pagano. Machine-Generated Algorithms, Proofs and Software for the Batch Verification of Digital Signature Schemes. *Journal of Computer Security*, 2014.

Joseph A. Akinyele, Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, and Aviel D. Rubin. Charm: a framework for rapidly prototyping cryptosystems. *J. Cryptographic Engineering*, 3(2):111–128, 2013.

Matthew Green. The Threat in the Cloud. *IEEE Security & Privacy*, 11(1):86–89, January 2013.

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)*, 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.

Technical Reports and Submissions

Ben Adida, Collin Anderson, Annie I. Anton, Matt Blaze, Roger Dingledine, Edward W. Felten, Matthew D. Green, J. Alex Halderman, David R. Jefferson, Cullen Jennings, Susan Landau, Navroop Mitter, Peter G. Neumann, Eric Rescorla, Fred B. Schneider, Bruce Schneier, Hovav Shacham, Micah Sherr, David Wagner, and Philip Zimmermann. CALEA II: Risks of Wiretap Modifications to Endpoints. Public report. Available at `http://www.cs.berkeley.edu/~daw/papers/caleaii.pdf`, May 2013.

Lucas Ballard, Matthew Green, Breno de Medeiros, and Fabian Monrose. Correlation-resistant storage from keyword searchable encryption. Technical Report TR-SP-BGMM-050705, Johns Hopkins University, 2005. Available at `http://eprint.iacr.org/2005/417.pdf`.

Matthew Green. Content Protection for Optical Media. Technical Report. Available at `http://isi.jhu.edu/~mgreen/spdc_aacs_2005.pdf`, 2005.

Other Writing

Matthew Green. Is Apple Picking a Fight With the U.S. Government? In Slate Magazine, Future Tense., September 2014.

Matthew Green. The Daunting Challenge of Secure Email. In The New Yorker, Elements blog, November 2013.

Matthew Green. Which Encryption Apps Are Strong Enough to Help You Take Down a Government? Gizmodo, March 2013.

Invited Talks

Keynote. AppSec USA, October 2016.

Keynote. BSIMM Conference, September 2016.

"Not-so-secure Instant Messaging". Summercon, June 2016.

"Applied cryptography after the prohibition". Boston University Colloquium Talk, April 2016.

"On subverting trust". Keynote, Network and Distributed Systems Security Symposium (NDSS) conference, February 2016.

"Secure protocols in a hostile world". Keynote, Cryptographic Hardware and Embedded Systems (CHES) conference, September 2015.

"From strong mathematics to weak cryptography". Keynote, Applied Cryptography and Network Security (ACNS) conference, June 2015.

"Anonymous Electronic Payments from Bitcoin". Yale University, Colloquium Talk, January 2015.

"Decentralized Anonymous Credentials and Electronic Payments from Bitcoin". Princeton University, Colloquium Talk, November 2014.

"Practical Kleptography" Keynote, Workshop on Offensive Technologies (WOOT), Usenix Security, August 2014.

"Anonymizing Cryptocurrencies: How to make Bitcoin Anonymous". Real World Crypto conference, January 2014.

"Why the NSA is breaking our encryption and why we should care". TEDx MidAtlantic, October 2013.

"What's wrong with cryptographic API design and what we can do to fix it". Usenix Hot Topics on Computer Security (HOTSEC), August 2013.

"Zerocoin: Anonymous Distributed e-Cash from Bitcoin". Microsoft Research, April 2013.

"Zerocash: Decentralized Anonymous Payments from Bitcoin". Rutgers University, January 2013.

"Cryptography is a Systems Problem (or Should we Deploy TLS?)". Dartmouth College, February 2013.

"Charm: A framework for rapidly prototyping cryptosystems". Microsoft Research, July 2011.

"Attacking and Defending RFID Security Systems". National Science Foundation, September 2005.

Patents

- "Unidirectional proxy re-encryption", U.S. Patent 8094810 (Issue date Jan 10, 2012).
- "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

PI, National Science Foundation award EFMA-1441224, "Quantifying Disaster Resilience of Critical Infrastructure-based Societal Systems with Emergent Behavior and Dynamic Interdependencies". Amount $1,452,773. (September 1, 2014 - August 31, 2017)

PI, Google ATAP, "Anonymous Attestation and Identification for a Secure Co-Processor". Amount: $108,000. (August 1, 2014 - August 31, 2015)

PI, Mozilla Research, Scientific analysis of the TLS protocol, $74,000. (September 1, 2014 - August 31, 2015)

PI, Mozilla Research, Analysis of cryptographic protocols, $68,000. (September 1, 2015 - August 31, 2016)

Researcher, Office of Naval Research, "Automating Cryptographic Design Tasks". Amount $623,265. (June 1, 2014 - May 31, 2017)

Co-PI, National Science Foundation award CNS-1010928, "Self Protecting Electronic Medical Records". Amount: $1,733,881. (October 1, 2010 - September 30, 2016)

Co-PI, DARPA PROgramming Computation on EncryptEd Data (PROCEED). Amount: $344,000. (April 2011 - April 2015)

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. (2010 - 2014)

Teaching

600.444. COMPUTER NETWORKS (Spring 2017). Introduction to computer networking for undergraduates and graduate students.

600.443. SECURITY AND PRIVACY IN COMPUTING (Fall 2015). Introduction to computer security and privacy for graduate students and advanced undergraduates.

600.454 (650.445). PRACTICAL CRYPTOGRAPHIC SYSTEMS (Spring 2009-2015 & Fall 2016). 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

- ACM CCS 2016. Best Paper. "A Systematic Analysis of the Juniper Dual EC Incident".
- Electronic Frontier Foundation Pioneer Award, "Keys under Doormats", 2016.
- M3AAWG J.D. Falk Award, "Keys under Doormats", 2015.
- ACM CCS 2015. Best Paper. "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice".
- Pwnie, Most Innovative Research, BlackHat 2015.
- 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".

Program Committees

CRYPTO 2017. Committee chairs: Hovav Shacham, Jonathan Katz.

Financial Cryptography 2017. Committee chair: Aggelos Kiayias.

WWW 2017. Committee chairs: Eugene Agichtein, Evgeniy Gabrilovich.

Usenix Security 2016. Committee chairs: Thorsten Holtz, Stefan Savage.

IEEE Security & Privacy Symposium 2015. Committee chairs: Lujo Bauer, Vitaly Shmatikov.

PKC 2015. Committee chair: Jonathan Katz.

Bitcoin 2015. Committee chairs: Nicolas Christin, Emin Gun Sirer.

Financial Cryptography 2015. Committee chairs: Rainer Boehme, Tatsuaki Okamoto.

ACM CCS 2014. Committee chairs: Moti Yung, Ninghui Li.

Bitcoin 2014. Committee chairs: Rainer Bhme, Tyler Moore.

Financial Cryptography 2014. Committee chair: Nicholas Christin.

Usenix Security 2013. Committee chair: Sam King.

Usenix Security 2012. Committee chair: Tadayoshi Kohno.

Healthsec 2012. Committee chair: Zachary Peterson.

PKC 2012. Committee chair: Marc Fischlin.

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

Usenix Security 2011. Committee chair: David Wagner.

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.**

Ph. D. Student Advising

Christina Garman, JHU (current student, expected graduation May 2017)

Ian Miers, JHU (current student, expected graduation May 2017)

Alishah Chator, JHU (current student)

Ayo Akinyele, JHU (Ph. D. May 2013)

Matthew Pagano, JHU (co-advised, Ph. D. December 2013)

Software Projects

libzerocoin. An implementation of the cryptographic routines for the Zerocoin anonymous currency.

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.

February 10, 2017