Anna Lysyanskaya
Curriculum Vitae

Computer Science Department, Box 1910
Brown University
Providence, RI 02912
(401) 863-7605
email: anna@cs.brown.edu
http://www.cs.brown.edu/~anna

Research Interests

Cryptography, privacy, computer security, theory of computation.

Education

Massachusetts Institute of Technology Cambridge, MA
Ph.D. in Computer Science, September 2002
Advisor: Ronald L. Rivest, Viterbi Professor of EECS
Thesis title: "Signature Schemes and Applications to Cryptographic Protocol Design"

Massachusetts Institute of Technology Cambridge, MA
S.M. in Computer Science, June 1999

Smith College Northampton, MA
A.B. *magna cum laude*, Highest Honors, Phi Beta Kappa, May 1997

Appointments

Brown University, Providence, RI Fall 2013 - Present
Professor of Computer Science

Brown University, Providence, RI Fall 2008 - Spring 2013
Associate Professor of Computer Science

Brown University, Providence, RI Fall 2002 - Spring 2008
Assistant Professor of Computer Science

UCLA, Los Angeles, CA Fall 2006
Visiting Scientist at the Institute for Pure and Applied Mathematics (IPAM)

Weizmann Institute, Rehovot, Israel Spring 2006
Visiting Scientist

Massachusetts Institute of Technology, Cambridge, MA 1997 – 2002
Graduate student

IBM T. J. Watson Research Laboratory, Hawthorne, NY Summer 2001
Summer Researcher

IBM Zürich Research Laboratory, Rüschlikon, Switzerland Summers 1999, 2000
Summer Researcher

Teaching

Brown University, Providence, RI — Spring 2008, 2011, 2015, 2017, 2019; Fall 2012
Instructor for "CS 259: Advanced Topics in Cryptography," a seminar course for graduate students.

Brown University, Providence, RI — Spring 2012
Instructor for "CS 256: Advanced Complexity Theory," a graduate-level complexity theory course.

Brown University, Providence, RI — Fall 2003,2004,2005,2010,2011 Spring 2007, 2009,2013,2014,2016,2018
Instructor for "CS151: Introduction to Cryptography and Computer Security."

Brown University, Providence, RI — Fall 2016, 2018
Instructor for "CS 101: Theory of Computation," a core course for CS concentrators.

Brown University, Providence, RI — Fall 2007, 2008, 2009, 2014
Instructor for "CS51: Models of Computation," a core course for CS concentrators.

Brown University, Providence, RI — Spring 2004,2005
Instructor for "CS22: Introduction to Discrete Mathematics," a core course for CS concentrators.

Brown University, Providence, RI — Fall 2002
Instructor for "CS195-7: Introduction to Cryptography," an advanced undergraduate/beginning graduate course in Cryptography.

Massachusetts Institute of Technology, Cambridge, MA — Fall 2001
Instructor for "Cryptography and Cryptanalysis," an introductory graduate course in Cryptography.

Advising

- Ph.D. advisor for Brown Ph.D. students Melissa Chase (Ph.D. 2008), Mira Belenkiy (Ph.D. 2008), Alptekin Küpçü (Ph.D. 2010), Feng-Hao Liu (Ph.D. 2013), Foteini Baldimtsi (Ph.D. 2014), Megumi Ando (expected graduation 2019), Apoorvaa Deshpande (expected graduation 2019), Elizabeth Crites (expected graduation 2019), Leah Rosenbloom (expected graduation 2021).
- Ph.D. thesis committee for Nikos Triandopoulos (Brown Ph.D. 2006), Danfeng Yao (Brown Ph.D. 2007), Lucia Draque-Penso (Brown Ph.D. 2008), Jay McCarthy (Brown Ph.D. 2008), Michael Pedersen (Aarhus University Ph.D. 2008), C. Chris Erway (Ph.D. 2011), Babis Papamanthou (Ph.D. 2011), Gert Mikkelsen (Aarhus University Ph.D. 2011), Yuri Malitsky (Brown Ph.D. 2012), Olya Ohrimenko (Ph.D. 2014), Maria Dubovitskaya (ETH Zurich Ph.D. 2014), Marc Bernardeau (Ecole Normale Superieure, Paris, Ph.D. expected 2019), Vikram Saraph (Brown Ph.D. expected 2019).

Awards

Google Faculty Research Award, 2013 ($43K).

Alfred P. Sloan Foundation Fellowship, 2008 ($50K).

IBM Faculty Fellowship, 2008 ($20K).

Women's Forum for the Economy and Society "Rising Talent" 2008.

Technology Review's "35 Innovators under 35" honoree, 2007.

IBM Research best paper award for [LLR06], 2007.

IBM Faculty Award, 2004.

Lucent Technologies Graduate Research Program for Women Fellowship (declined), 1997.

National Science Foundation Graduate Research Fellowship, 1997.

Smith College Alumnae Scholarship, Smith College, September 1997.

Microsoft Women's Technical Scholarship, Smith College, 1995, 1996.

Phi Beta Kappa Honorary Society, Smith College, 1996.

Mendelson Prize in Computer Science, Smith College, 1995, 1997.

Benedict Prize in Mathematics, Smith College, 1995.

Pokora Prize in Mathematics, Smith College, 1997.

Grants

National Science Foundation SaTC Grant, 2014 ($500K).

National Institute of Standards NSTIC (National Strategy for Trusted Identities in Cyberspace) award (sub-award of a $1.8M grant through Internet 2), 2012 ($480K).

National Science Foundation Large Cyber Trust Grant (coPI), 2010 ($1M).

National Science Foundation Medium Cyber Trust Grant (joint with UMass), 2010 ($230K).

National Science Foundation Cyber Trust Grant, 2008 ($300K).

National Science Foundation Cyber Trust Grant, 2006 ($350K).

National Science Foundation CAREER Grant, 2004 ($464K).

Publications

[CL19] Elizabeth Crites and Anna Lysyanskaya. Delegatable Anonymous Credentials from Mercurial Signatures. In RSA Cryptographers' Track (CT-RSA), to appear, 2019.

[ALU18] Megumi Ando, Anna Lysyanskaya and Eli Upfal. Practical and Provably Secure Onion Routing. In International Colloquium on Automata, Languages, and Programming (ICALP), pp. 144:1–144:14, 2018.

[BC+17] Foteini Baldimtsi, Jan Camenisch, Maria Dubovitskaya, Anna Lysyanskaya, Leonid Reyzin, Kai Samelin and Sophia Yakoubov. Accumulators with Applications to Anonymity-Preserving Revocation. In IEEE European Symposium on Security and Privacy (Euro S&P), pages 301–315, IEEE, 2017.

[CLLN14] Jan Camenisch, Anja Lehmann, Anna Lysyanskaya and Gregory Neven. Memento: How to Reconstruct Your Secrets from a Single Password in a Hostile Environment. In Juan Garay and Rosario Gennaro, editors, *Advances in Cryptology — Crypto 2014, Part II*, volume 8617 of *Lecture Notes in Computer Science*, pages 256–275, Springer, 2014.

[DFK+14] Dana Dachman-Soled, Nils Fleischhacker, Jonathan Katz, Anna Lysyanskaya and Dominique Schröder. Feasibility and Infeasibility of Secure Computation with Malicious PUFs. In Juan Garay and Rosario Gennaro, editors, *Advances in Cryptology — Crypto 2014, Part II*, volume 8617 of *Lecture Notes in Computer Science*, pages 405–420, Springer, 2014.

[CKLM14] Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya and Sarah Meiklejohn. Malleable Signatures: Complex Unary Transformations and Delegatable Anonymous Credentials. In 27th Computer Security Foundations Symposium, IEEE, 2014.

[BL13b] Foteini Baldimtsi and Anna Lysyanskaya. On the security of one-witness blind signature schemes. In Kazue Sako and Palash Sarkar, editors, *Proceedings of ASIACRYPT, Part II*, volume 8270 of *Lecture Notes in Computer Science*, pages 82–99. Springer, 2013.

[BL13a] Foteini Baldimtsi and Anna Lysyanskaya. Anonymous Credentials Light. In *ACM Conference on Computer and Communications Security (ACM CCS)*, pages 1987–1098, ACM Press, 2013.

[HZ+13] Gesine Hinterwalder, Christian Zenger, Foteini Baldimtsi, Anna Lysyanskaya, Christof Paar and Wayne Burleson. Efficient E-cash in Practice: NFC-based Payments for Intelligent Transportation Systems. In *Proceedings of the Privacy Enhancing Technologies - 13th International Symposium (PETS)*, volume 7981 of *Lecture Notes in Computer Science*, pages 40–59, Springer, 2013.

[CKLM13a] Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya and Sarah Meiklejohn. Verifiable Elections That Scale for Free. In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Proceedings of 16th International Conference on Practice and Theory in Public-Key Cryptography — PKC 2013*, volume 7778 of *Lecture Notes in Computer Science*, pages 479–496, Springer, 2013.

[CKLM13b] Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya and Sarah Meiklejohn. Succinct Malleable NIZKs and an Application to Compact Shuffles. In Amit Sahai, editor, *Proceedings of 10th Theory of Cryptography Conference — TCC 2013*, volume 7785 of *Lecture Notes in Computer Science*, pages 100–119, Springer, 2013.

[CHLMR13] Melissa Chase, Alexander Healy, Anna Lysyanskaya, Tal Malkin, and Leo Reyzin. Mercurial commitments with applications to zero-knowledge sets. In *Journal of Cryptology*, 26(2), pages 251–279. Springer, 2013. (Journal version of [CHLMR05].)

[CLN12] Jan Camenisch, Anna Lysyanskaya and Gregory Neven. Practical yet universally composable two-server password-authenticated secret sharing. In *ACM Conference on Computer and Communications Security (ACM CCS)*, pages 525–536, ACM Press, 2012.

[LL12] Feng-Hao Liu and Anna Lysyanskaya. Tamper and Leakage Resilience in the Split-State Model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology — Crypto 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 517–532, Springer, 2012.

[BHRLPB12] Foteini Baldimtsi, Gesine Hinterwalder, Andy Rupp, Anna Lysyanskaya, Christof Paar and Wayne P. Burleson. Pay as you go. In *Proceedings of 19th 5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs)*, 2012.

[CKLM12] Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya and Sarah Meiklejohn. Malleable Proof Systems and Applications. In David Pointcheval, editor, *Advances in Cryptology — Eurocrypt 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 281–300, Springer, 2012.

[KL12] Alptekin Küpçü and Anna Lysyanskaya. Usable optimistic fair exchange. In Computer Networks, 56:1, pages 50–63, Elsevier, 2012.

[KL10b] Alptekin Küpçü and Anna Lysyanskaya. Optimistic Fair Exchange with Multiple Arbiters. In *Proceedings of 15th European Symposium on Research in Computer Security (ESORICS)*, volume 6345 of *Lecture Notes in Computer Science*, pages 488–507. Springer, 2010.

[LL10] Feng-Hao Liu and Anna Lysyanskaya. Algorithmic Tamper-Proof Security under Probing Attacks. In *7th International Conference on Security and Cryptography for Networks (SCN)*, volume 6280 of *Lecture Notes in Computer Science*, pages 106–120. Springer, 2010.

[MEKHL10] Sarah Meiklejohn, C. Christopher Erway, Alptekin Küpçü, Theodora Hinkle, Anna Lysyanskaya. ZKPDL: A Language-Based System for Efficient Zero-Knowledge Proofs and Electronic Cash. In *Proceedings of 19th USENIX Security Symposium*, pages 193–206, USENIX Association, 2010.

[KL10a] Alptekin Küpçü and Anna Lysyanskaya. Usable optimistic fair exchange. In Josef Pieprzyk, editor, *Proceedings of the RSA Conference, Cryptographers' Track*, volume 5985 of *Lecture Notes in Computer Science*, pages 252–267. Springer, 2010.

[LTT10] Anna Lysyanskaya, Roberto Tamassia, Nikos Triandopoulos. Authenticated error-correcting codes with applications to multicast authentication. In *ACM Trans. Inf. Syst. Secur. 13(2)*. ACM Press, 2010. (Journal version of [LTT04].)

[BC+09] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable proofs and delegatable anonymous credentials. In *Advances in Cryptology — CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 108–125. Springer, 2009.

[BCKL09] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. Compact e-cash and simulatable vrfs revisited. In *Pairing-Based Cryptography*, volume 5671 of *Lecture Notes in Computer Science*, pages 114–131. Springer, 2009.

[KL09] Alptekin Küpçü and Anna Lysyanskaya. Brief announcement: impossibility results for optimistic fair exchange with multiple autonomous arbiters. In *Proceedings of the 28th Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pages 336–337. ACM, 2009.

[BC+08] Mira Belenkiy, Melissa Chase, C. Christopher Erway, John Jannotti, Alptekin Küpçü, and Anna Lysyanskaya. Incentivizing outsourced computation. In *Proceedings of the ACM SIGCOMM 2008 Workshop on Economics of Networked Systems*, pages 85–90. ACM, 2008.

[BCKL08] Mira Belenkiy, Melissa Chase, Markulf Kohlweiss, and Anna Lysyanskaya. P-signatures and noninteractive anonymous credentials. In Ran Canetti, editor, *Proceedings of the Fifth Theory of Cryptography Conference (TCC)*, volume 4948 of *Lecture Notes in Computer Science*, pages 356–374. Springer, 2008.

[BC+07] Mira Belenkiy, Melissa Chase, Chris Erway, John Jannotti, Alptekin Küpçü, Anna Lysyanskaya and Eric Rachlin. Making P2P accountable without losing privacy. In *Workshop on Privacy in Electronic Society (WPES)*, pages 31–40. ACM Press, 2007.

[CL07] Melissa Chase and Anna Lysyanskaya. Simulatable VRFs with Applications to Multi-theorem NIZK. In Alfred Menezes, editor, *Advances in Cryptology — Crypto 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 303–322. Springer, 2007.

[CLM07] Jan Camenisch, Anna Lysyanskaya and Maria Meyerovich. Endorsed E-cash. In Birgit Pfitzmann and Patrick McDaniel, editors, *2007 IEEE Symposium on Security and Privacy* , pages 101–115. IEEE Computer Society, 2007.

[CL06] Melissa Chase and Anna Lysyanskaya. On signatures of knowledge. In Cynthia Dwork, editor, *Advances in Cryptology — Crypto 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 76–94. Springer, 2006.

[LT06] Anna Lysyanskaya and Nikos Triandopoulos. Rationality and adversarial behavior in multi-party computation. In Cynthia Dwork, editor, *Advances in Cryptology — Crypto 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 177–195. Springer, 2006.

[CHL06] Jan Camenisch, Susan Hohenberger and Anna Lysyanskaya. Balancing accountability and privacy using e-cash. In Moti Yung, editor, *Security and Cryptography for Networks*, volume 4116 of *Lecture Notes in Computer Science*, pages 141–155. Springer, 2006.

[CHKLM06] Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya and Maria Meyerovich. How to win the clone wars: efficient periodic n-times anonymous authentication. In Rebecca Wright, editor, *13th ACM Conference on Computer and Communicatons Security*, pages 201–210. ACM, 2006.

[LM06] Anna Lysyanskaya and Maria Meyerovich. Provably secure steganography with imperfect sampling. In Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, Tal Malkin, editors, *Public Key Cryptography — PKC 2006*, volume 3958 of *Lecture Notes in Computer Science*, pages 123–139. Springer, 2006.

[LLR06] Yehuda Lindell, Anna Lysyanskaya, Tal Rabin. On the composition of authenticated Byzantine agreement. In Journal of the ACM, 52(6), 2006. (Journal version of [LLR02a].)

[CL05] Jan Camenisch and Anna Lysyanskaya. A formal treatment of onion routing. In Victor Shoup, editor, *Advances in Cryptology — Crypto 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 169–187. Springer, 2005.

[CHLMR05] Melissa Chase, Alexander Healy, Anna Lysyanskaya, Tal Malkin, and Leo Reyzin. Mercurial commitments with applications to zero-knowledge sets. In Ronald Cramer, editor, *Advances in Cryptology — Eurocrypt 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 422–439. Springer, 2005.

[CHL05] Jan Camenisch, Susan Hohenberger, and Anna Lysyanskaya. Compact e-cash. In Ronald Cramer, editor, *Advances in Cryptology — Eurocrypt 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 302–321. Springer, 2005.

[HL05] Susan Hohenberger and Anna Lysyanskaya. How to securely outsource cryptographic computations. In Joe Kilian, editor, *Theory of Cryptography, Second Theory of Cryptography Conference (TCC 2005)*, volume 3378 of *Lecture Notes in Computer Science*, pages 264–282. Springer, 2005.

[YFDL04] Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, and Anna Lysyanskaya. ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption. In V. Atluri, B. Pfitzmann and P. McDaniel, editors, *11th ACM Conference on Computer and Communicatons Security*, pages 356–363. ACM, 2004.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In Matthew K. Franklin, editor, *Advances in Cryptology — CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 56–72. Springer, 2004.

[BCL04] Endre Bangerter, Jan Camenisch, Anna Lysyanskaya. A Cryptographic Framework for the Controlled Release of Certified Data. Invited position paper in *Proceedings of 12th International Workshop on Security Protocols, 2004*, volume 3957 of *Lecture Notes in Computer Science*, pages 20–42. Springer, 2006.

[LTT04] Anna Lysyanskaya, Roberto Tamassia, and Nikos Triandopoulos. Multicast authentication in fully adversarial networks. In David Wagner and Michael Waidner, editors, *IEEE Symposium on Security and Privacy*, pages 241–258. IEEE Computer Society, 2004.

[LMRS04] Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Hovav Shacham. Sequential aggregate signatures from trapdoor permutations. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology — EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 74–90. Springer, 2004.

[GLMMR04] Rosario Gennaro, Anna Lysyanskaya, Tal Malkin, Silvio Micali, and Tal Rabin. Algorithmic tamper-proof (ATP) security: Theoretical foundations for security against hardware tampering. In Moni Naor, editor, *First Theory of Cryptography Conference (TCC 2004)*, volume 2951 of *Lecture Notes in Computer Science*, pages 258–277. Springer, 2004.

[CKLS02] Christian Cachin, Klaus Kursawe, Anna Lysyanskaya, Reto Strobl. Asynchronous Verifiable Secret Sharing and Proactive Cryptosystems. In V. Atluri, editor, *Proceedings of the 9th ACM conference on Computer and Communications Security*, pages 88–97. ACM, 2002.

[CL02b] Jan Camenisch and Anna Lysyanskaya. A Signature Scheme for Efficient Protocols. In S. Cimato, C. Galdi and G. Persiano, editors, *Third International Conference on Security in Communication Networks (SCN 2002)*, volume 2576 of *Lecture Notes in Computer Science*, pages 274–295. Springer, 2002.

[Lys02] Anna Lysyanskaya. Unique signatures and verifiable random functions from the DH-DDH separation. In Moti Yung, editor, *Advances in Cryptology — CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 597–612. Springer, August 2002.

[CL02a] Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In Moti Yung, editor, *Advances in Cryptology — CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 61–76. Springer, 2002.

[LLR02b] Yehuda Lindell, Anna Lysyanskaya, and Tal Rabin. Sequential composition of protocols without simultaneous termination. In *Proceedings of 21st ACM Symposium on Principles of Distributed Computation (PODC)*, pages 203–213. ACM, 2002.

[LLR02a] Yehuda Lindell, Anna Lysyanskaya, and Tal Rabin. On the composition of authenticated Byzantine agreement. In *Proceedings of the 34th ACM Symposium on Theory of Computing (STOC)*, pages 514–523. ACM, 2002.

[LLMRS01] Moses Liskov, Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Adam Smith. Mutually independent commitments. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 385–401. Springer, 2001.

[LP01] Anna Lysyanskaya and Chris Peikert. Adaptive security in the threshold setting: From cryptosystems to signature schemes. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 331–350. Springer, 2001.

[CL01b] Jan Camenisch and Anna Lysyanskaya. An identity escrow scheme with appointed verifiers. In Joe Kilian, editor, *Advances in Cryptology — CRYPTO 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 388–407. Springer, 2001.

[CL01a] Jan Camenisch and Anna Lysyanskaya. Efficient non-transferable anonymous multi-show credential system with optional anonymity revocation. In Birgit Pfitzmann, editor, *Advances in Cryptology — EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, 2001.

[JL00] Stanisław Jarecki and Anna Lysyanskaya. Adaptively secure threshold cryptography: introducing concurrency, removing erasures. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 190–206. Springer, 2000.

[LRSW99] Anna Lysyanskaya, Ron Rivest, Amit Sahai, and Stefan Wolf. Pseudonym systems. In Howard Heys and Carlisle Adams, editors, *Selected Areas in Cryptography*, volume 1758 of *Lecture Notes in Computer Science*, pages 184–199. Springer, 1999.

[LR98] Anna Lysyanskaya and Zulfikar Ramzan. Group blind digital signatures: A scalable solution to electronic cash. In Rafael Hirshfeld, editor, *Proceedings of the Second International Conference on Financial Cryptography*, volume 1465 of *Lecture Notes in Computer Science*, pages 184–197. Springer, 1998.

Popular Press

[CSM] Anna Lysyanskaya. Opinion: Why Apple should build iPhones even it can't unlock. *Passcode: Modern Field Guide to Security and Privacy*, Christian Science Monitor, March 11, 2016.

[ProJo] Anna Lysyanskaya. What better data privacy? Demand it. *The Providence Journal*, February 13, 2015.

[EPIC] Anna Lysyanskaya. Cryptography is the Future. *Visions of Privacy Anthology*, Electronic Privacy Information Center, 2014 (upcoming).

[SciAm] Anna Lysyanskaya. How to Keep Secrets Safe. Scientific American, September 2008, pp. 66–73.

[S&P] Anna Lysyanskaya. Authentication without identification. *IEEE Security & Privacy*, 5(3):69–71, 2007.

Invited Lectures

Practicing Law Institute, New York NY *Computer Security and Healthcare: A Computer Scientist's Perspective* June 2018.

EMCS, Brown University, Providence, RI *Keynote: Authorized but Anonymous — Taking Charge of Your Personal Data* October 2017.

Apple Inc., Cupertino, CA *The John Podesta Project* January 2017.

Duke University Computer Science Special Talk, Durham, NC *A Whirlwind Tour of Anonymous Credentials* March 2016.

Grace Hopper Celebration of Women in Computing, Houston, TX *Authorized but Anonymous: Taking Charge of Your Personal Data* October 2015.

DIMACS/Columbia Data Science Institute Workshop on Cryptography for Big Data, New York, NY *A Whirlwind Tour of Anonymous Credentials* December 2015.

Bristol University Information Security Seminar, Bristol University, Bristol, UK *Anonymous Credentials Light* May 2014.

DIMACS Workshop on Current Trends in Cryptology *Controlled Malleability for NIZK and Signatures: Constructions and Applications* April 2013.

Smith College Club of Rhode Island Lecture Series, Providence, RI *They Don't Need to Know Your Date of Birth -or- Taking Charge of Your Personal Data* April 2013.

3rd Bar-Ilan Winter School on Cryptography: Bilinear Pairings in Cryptography, Bar-Ilan University, Israel *Anonymous Credentials and Ecash* February 2013.

Computer Science Seminar, Johns Hopkins University, Baltimore, MD *From Signatures to Anonymous Credentials to Anonymous Delegation* November 2012.

Academy in Context Dinner Series, Graduate School, Brown University *They Don't Need to Know Your Date of Birth -or- Taking Charge of Your Personal Data* November 2012.

Privacy-Oriented Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany *On The Security of One-Witness Blind Signature Schemes, and on Some Alternatives* September 2012.

Cryptographic Key Management Workshop, National Institute of Standards and Technology, Gaithersburg, MD *How to Balance Privacy and Key Management in User Authentication* September 2012.

Colloquium, Microsoft Research, Redmond, WA *On The Security of One-Witness Blind Signature Schemes* August 2012.

Cryptography Seminar, University of Maryland, College Park, MD *On The Security of One-Witness Blind Signature Schemes* June 2012.

Seminar, IBM Zurich Research Lab, Ruschlikon, Switzerland *Tamper and Leakage Resilience in the Split-State Model* June 2012.

Summer School on Cryptography, Pennsylvania State University, State College, PA *How to Reconcile Anonymity with Accountability* May 2012.

Cryptography Seminar, IBM T.J.Watson Research, Hawthorne, NY *On The Security of One-Witness Blind Signature Schemes* May 2012.

Theory Seminar, Computer Science Department, Columbia University *Tamper and Leakage Resilience in the Split-State Model* May 2012.

Cybersecurity and International Relations Conference, Brown University, Providence, RI *Cybersecurity: Challenges and Solutions* May 2012.

Cryptography Reading Group, National Institute of Standards and Technology, Gaithersburg, MD *Survey on Anonymous Credentials* March 2012.

Meeting on Privacy-Enhancing Technologies, National Institute of Standards and Technology, Gaithersburg, MD *Conditional and Revocable Anonymity* December 2011.

PrimeLife/IFIP Summer School 2010, Helsingborg, Sweden *Keynote Address: Balancing Privacy and Accountability* August 2010.

PrimeLife/IFIP Summer School 2010, Helsingborg, Sweden *Tutorial: Anonymous Credentials* August 2010.

NTT Research, Tokyo, Japan *Tutorial: A Survey of Privacy-Preserving Authentication* July 2010.

Pay-As-You-Go Kickoff Workshop, Amherst, MA *Survey of Electronic Cash* June 2010.

Identity Management Workshop, State Department, Washington, DC *Privacy Landscape* November 2009.

Kerberos Conference, MIT, Cambridge, MA *The Future of Security and Identity on the Internet (Panel Discussion)* October 2009.

Young Engineering Scientists Symposium on Identity Management, Embassy of France, Washington DC *How to Reconcile Anonymity with Accountability* July 2009.

Computer Science Seminar, University of Rome, Rome, Italy *How to Reconcile Anonymity with Accountability* May 2009.

Public-Key Cryptography 2009, Irvine, CA *From Signatures to Anonymous Credentials and Anonymous Delegation (Invited Talk)* March 2009.

Computer Science Department Undergraduate Group, Brown University, Providence, RI *Cryptographic diversions for Valentine's Day – OR – How to be a successful matchmaker without breaching your friends' trust* February 2009.

Microsoft Research Cryptography Seminar, Redmond, WA *Fair Exchange with a Distributed Offline TTP* December 2008.

Workshop on Protecting Subject Privacy, Berkman Center for Internet and Society, Harvard University, Cambridge, MA *The Amazing World of Modern Cryptography* November 2008.

New York University Computer Science Colloquium, New York, NY *How to Reconcile Anonymity with Accountability* November 2008.

Kavli Frontiers of Science Symposium, National Academy of Science, Irvine, CA *The Amazing World of Modern Cryptography and Computer Security* November 2008.

School on Rational Cryptographic Protocols, Bertinoro International Centre for Informatics, Bertinoro, Italy *Incentivizing Distributed Computation* June 2008.

Bristol University Information Security Seminar, Bristol University, Bristol, UK *Compact E-Cash and Applications* January 2008.

Security Research Seminar, Microsoft Research, Cambridge, UK *Compact E-Cash and Applications* January 2008.

TRUST Seminar, University of California, Berkeley, CA *Authentication without Identification* October 2007.

SMath: A Conference of Smith Mathematicians, Smith College, Northampton, MA *How to Be Persuasive While Keeping a Poker Face* September 2007.

Stanford Security Seminar, Stanford University, Stanford, CA *Compact E-Cash and Applications* August 2007.

Computer Science Lecture Series, ITA Software, Cambridge, MA *Authentication without Identification* July 2007.

Invited Talk at the First International Workshop on Group-Oriented Cryptographic Protocols (GOCP), Wrozlaw, Poland *Compact E-Cash and Applications* July 2007.

Ronfest: a Celebration in Honor of Ron Rivest's 60th birthday, MIT, Cambridge, MA *Compact E-Cash and Applications* May 2007.

Wayland Collegium Luncheon Speaker Series, Brown University, Providence, RI *How to Be Persuasive While Keeping a Poker Face* April 2007.

Computer Science Theory Seminar, University of Texas, Austin, TX *Compact E-Cash and Applications* March 2007.

Information Security Seminar, Georgia Tech, Atlanta, GA *Compact E-Cash and Applications* March 2007.

Information Security Seminar, Carnegie-Mellon University, Pittsburgh, PA *Authentication without Identification* March 2007.

Workshop on cryptographic protocols, Bertinoro International Centre for Informatics, Bertinoro, Italy *Simulatable VRFs and applications to NIZK* March 2007.

UCLA IPAM Culminating Workshop on Securing Cyberspace, UCLA, Lake Arrowhead, CA *Compact E-Cash and Applications* December 2006.

Fields Institute Workshop on Foundations of Cryptography, University of Toronto, Toronto, Canada *Compact E-Cash and Applications* November 2006.

UCLA IPAM Workshop on Multi-Party Computation, UCLA, Los Angeles, CA *On Signatures of Knowledge* November 2006.

UCLA IPAM Securing Cyberspace Seminar, UCLA, Los Angeles, CA *Secure Multi-party Computation as a Game* October 2006.

Foundations of Computer Science Seminar, Weizmann Institute of Science, Rehovot, Israel *Compact E-Cash* March 2006.

Foundations of Computer Science Seminar, Weizmann Institute of Science, Rehovot, Israel *On Signatures of Knowledge* February 2006.

Boston University Computer Science Department and Reliable Information Systems and Cyber Security Center, Boston University, Boston, MA *Authentication without Identification: from Theory to Practice* December 2005.

Workshop on Anonymous Communication and Its Applications, International Conference and Research Center for Computer Science, Dagstuhl, Germany *A Formal Treatment of Onion Routing* October 2005.

Laboratory for Secure Systems Seminar, Stevens Institute of Technology, Hoboken, NJ *Authentication without Identification: from Theory to Practice* October 2005.

Crypto Reading Group, NYU, New York, NY *A Formal Treatment of Onion Routing* September 2005.

Five-College Speaker Series on Information Assurance, University of Masshachusetts, Amherst, MA *Authentication without Identification* September 2005.

Computer Science Siesta Seminar, IBM Zurich Research Laboratory, Zurich, Switzerland *A Formal Treatment of Onion Routing* July 2005.

Cryptography and Information Security Seminar, Eidgenossische Technische Hochschule (ETH), Zurich, Switzerland *Compact E-Cash* June 2005.

Cryptography and Information Security Seminar, MIT, Cambridge, MA *A Formal Treatment of Onion Routing* May 2005.

Computer Security and Cryptography Informal Talk, U.C.Berkeley, Berkeley, CA *Signature Schemes with Efficient Protocols, and Applications to Trusted Computing, Anonymous Credentials, and Electronic Cash* March 2005.

Computer Security Seminar, Stanford University, Palo Alto, CA *Compact E-Cash* March 2005.

Workshop on Cryptography, Centre International de Rencontres Mathématiques (CIRM), Marseille, France *On Signature Schemes with Efficient Protocols from Bilinear Maps* November 2004.

Computer Science Department Seminar, Ecole Polytechnique Federale (EPFL), Lausanne, Switzerland *Signature Schemes with Efficient Protocols and Applications to Anonymous Credentials* June 2004.

Computer Science Siesta Seminar, IBM Zurich Research Laboratory, Zurich, Switzerland *Multicast Authentication in Fully Adversarial Networks* June 2004.

Cryptography and Information Security Seminar, Eidgenossische Technische Hochschule (ETH), Zurich, Switzerland *Zero-Knowledge Sets from General Assumptions* June 2004.

Computer Science Talk, Technion, Haifa, Israel *A Signature Scheme with Efficient Protocols* June 2003.

Computer Science Colloquium, Boston University, Boston, MA *On the Composition of Authenticated Byzantine Agreement* October 2002.

Cryptography and Information Security Seminar, Massachusetts Institute of Technology, Cambridge, MA *Unique Signatures and Verifiable Random Functions from the DH-DDH Separation* October 2002.

Workshop on Cryptography, International Conference and Research Center for Computer Science, Dagstuhl, Germany *A Signature Scheme with Efficient Protocols* September 2002.

Service to the Profession

- Program committees of Crypto 2003, Eurocrypt 2004, International Conference on Theory and Practice of Public-Key Cryptography (PKC) 2005, Theory of Cryptography Conference (TCC) 2005, International Symposium on Distributed Computing (DISC) 2006, Security and Cryptography for Networks (SCN) 2006, PKC 2007, Eurocrypt 2007, IEEE Symposium on Security and Privacy 2007, International Colloquium on Automata, Languages and Programming (ICALP) 2007, IEEE Symposium on Foundations of Computer Science (FOCS) 2007, Asiacrypt 2007, Eurocrypt 2008, IEEE ICDCS 2008, ICALP 2008, Eurocrypt 2009, Crypto 2009, NetEcon 2009, Asiacrypt 2010, RSA Cryptographers' Track 2011, TCC 2011, Eurocrypt 2011, Asiacrypt 2013, RSA Cryptographers' Track 2014, ACM CCS 2014, PKC 2015, RSA Cryptographers' Track 2015, PETS 2015, Eurocrypt 2017, Crypto 2018, TCC 2018.
- Member of the Board of Directors, International Association for Cryptologic Research (IACR), 2012-present.
- Member of the IACR Fellows' Committee, 2015-present.
- Member of the Academic Advisory Board, MIT Internet Trust Consortium (formerly the Kerberos Consortium), 2012-present.
- Member of the Electronic Privacy Information Center (EPIC) Advisory Board, 2014-present.
- Secretary and Treasurer, ACM SIGACT, 2009-2012.
- Organizer of the Kavli/National Academic of Sciences Annual Frontiers of Science Symposium, 2009, 2010.
- Organizer, Bertinoro Workshop on Cryptography, May 2009 and Dagstuhl Workshop of Cryptography, September 2011.
- Associate Editor for the IEEE Transactions on Computers, 2006-2008.
- Local organizer of the IEEE Foundations of Computer Science (FOCS) 2007 and the Theory of Cryptography Conference (TCC) 2011.
- Co-organizer for Dagstuhl Seminars 11391 (2011) and 19042 (2019).