Thomas Ristenpart

Updated November 1, 2026

Professor
University of Toronto
7268 Bahen Center, 40 St. George St, Toronto, ON M5S 2E4
email: ristenpart@cs.toronto.edu
web: `https://www.cs.toronto.edu/~ristenpart/`

Academic Background

University of California, San Diego. Ph.D. in Computer Science, November 2010.
Advisor: Prof. Mihir Bellare

University of California, Davis. M.S. in Computer Science, June 2005.
Advisor: Prof. Matt Bishop

University of California, Davis. B.S. in Computer Science and Engineering, June 2003.

Work History

Professor
Department of Computer Science, University of Toronto
January 2026 – present

Professor
Cornell Tech & Department of Computer Science, Cornell University
May 2023 – present (on leave)

Associate Professor
Cornell Tech & Department of Computer Science, Cornell University
May 2015 – April 2023

Assistant Professor
Department of Computer Sciences, University of Wisconsin
January 2011 – May 2015

Visiting researcher

Cloudflare
July 2020 – June 2021

Microsoft Research
June 2011

University of Lugano
April 2008 – June 2008

University of Washington
June 2007 – September 2007

Graduate student researcher

UC San Diego
September 2005 – December 2010

UC Davis
July 2003 – June 2005

Software engineering intern

Center for Computing Sciences
Summer 2004

Microsoft
Summers 2001, 2002

Micron Technologies, Inc.
Summers 1999, 2000

Awards

- Test-of-time award for USENIX Security 2016 paper [56]
- Runner up for the Andreas Pfitzmann Best Student Paper Award for PETS 2026 paper [124]
- Distinguished Paper Award for CCS 2025 paper [117]
- Test-of-time award for CCS 2015 paper [48]
- Test-of-time award for USENIX Security 2014 paper [37]
- Distinguished Paper Award for USENIX Security 2023 paper [104]
- Test-of-time award for CCS 2012 paper [25]
- Best Paper Award at CHI 2022 for paper [93]
- Best Paper Award at CSCW 2020 for paper [87]
- Distinguished Paper Award for USENIX Security 2020 paper [86]
- Facebook Internet Defense Prize (third prize) for USENIX Security 2020 paper [86]
- Distinguished Paper Award for USENIX Security 2020 paper [85]
- Test-of-time award for CCS 2009 paper [11]
- Advocate of New York City 2019 award, NYC City Mayor's Office to End Domestic and Gender-Based Violence
- Best Paper Honorable Mention Award for CHI 2020 paper [83]
- Best Paper Honorable Mention Award for CSCW 2019 paper [79]
- Best Paper Award at ACM CHI 2018 for paper [71]
- Distinguished Student Paper Award at IEEE Symposium on Security and Privacy 2016 for paper [54]
- Sloan Foundation Research Fellow 2015
- Best Paper at USENIX Security 2014 for paper [37]
- Runner up for Award for Outstanding Research in Privacy Enhancing Technologies 2014 and New Digital Age grant from Google Executive Chairman Eric Schmidt for paper [30]
- NSF CAREER Award 2013
- Computer Science and Engineering Department Dissertation Award, University of California, San Diego, 2011
- Before graduate school: UC Regents Scholarship (2001-2003), Albert W. Bijou Scholarship (2000), Edward Frank Kraft Prize (2000), UC Davis College of Engineering Annual Fund Scholarship (2000), San Francisco Bay Area Engineering Council Scholarship (1999), Wakeman Scholarship from the UC Regents (1999), UC Davis Alumni Association Leadership Scholarship (1999)

Publications

[1] Mihir Bellare and Thomas Ristenpart. "Multi-Property-Preserving Hash Domain Extension and the EMD Transform". In: *ASIACRYPT*. Vol. 4284. Lecture Notes in Computer Science. Springer, 2006, pp. 299–314.

[2] Francis Hsu, Hao Chen, Thomas Ristenpart, Jason Li, and Zhendong Su. "Back to the Future: A Framework for Automatic Malware Removal and System Repair". In: *ACSAC*. IEEE Computer Society, 2006, pp. 257–268.

[3] Thomas Ristenpart and Scott Yilek. "The Power of Proofs-of-Possession: Securing Multiparty Signatures against Rogue-Key Attacks". In: *EUROCRYPT*. Vol. 4515. Lecture Notes in Computer Science. Springer, 2007, pp. 228–245.

[4] Mihir Bellare and Thomas Ristenpart. "Hash Functions in the Dedicated-Key Setting: Design Choices and MPP Transforms". In: *ICALP*. Vol. 4596. Lecture Notes in Computer Science. Springer, 2007, pp. 399–410.

[5] Thomas Ristenpart and Thomas Shrimpton. "How to Build a Hash Function from Any Collision-Resistant Function". In: *ASIACRYPT*. Vol. 4833. Lecture Notes in Computer Science. Springer, 2007, pp. 147–163.

[6] Thomas Ristenpart, Gabriel Maganis, Arvind Krishnamurthy, and Tadayoshi Kohno. "Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with DHTs". In: *USENIX Security Symposium*. USENIX Association, 2008, pp. 275–290.

[7] Mihir Bellare, Marc Fischlin, Adam O'Neill, and Thomas Ristenpart. "Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles". In: *CRYPTO*. Vol. 5157. Lecture Notes in Computer Science. Springer, 2008, pp. 360–378.

[8] Mihir Bellare and Thomas Ristenpart. "Simulation without the Artificial Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme". In: *EUROCRYPT*. Vol. 5479. Lecture Notes in Computer Science. Springer, 2009, pp. 407–424.

[9] Yevgeniy Dodis, Thomas Ristenpart, and Thomas Shrimpton. "Salvaging Merkle-Damgård for Practical Applications". In: *EUROCRYPT*. Vol. 5479. Lecture Notes in Computer Science. Springer, 2009, pp. 371–388.

[10] Mihir Bellare, Thomas Ristenpart, Phillip Rogaway, and Till Stegers. "Format-Preserving Encryption". In: *Selected Areas in Cryptography*. Vol. 5867. Lecture Notes in Computer Science. Springer, 2009, pp. 295–312.

[11] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds". In: *ACM Conference on Computer and Communications Security*. ACM, 2009, pp. 199–212.

[12] Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek. "Hedged Public-Key Encryption: How to Protect against Bad Randomness". In: *ASIACRYPT*. Vol. 5912. Lecture Notes in Computer Science. Springer, 2009, pp. 232–249.

[13] Thomas Ristenpart and Scott Yilek. "When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography". In: *NDSS*. The Internet Society, 2010.

[14] Marc Fischlin, Anja Lehmann, Thomas Ristenpart, Thomas Shrimpton, Martijn Stam, and Stefano Tessaro. "Random Oracles with(out) Programmability". In: *ASIACRYPT*. Vol. 6477. Lecture Notes in Computer Science. Springer, 2010, pp. 303–320.

[15] Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. "Careful with Composition: Limitations of the Indifferentiability Framework". In: *EUROCRYPT*. Vol. 6632. Lecture Notes in Computer Science. Springer, 2011, pp. 487–506.

[16] Kenneth G. Paterson, Thomas Ristenpart, and Thomas Shrimpton. "Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol". In: *ASIACRYPT*. Vol. 7073. Lecture Notes in Computer Science. Springer, 2011, pp. 372–389.

[17] Qing Zhang, Thomas Ristenpart, Stefan Savage, and Geoff Voelker. "Got Traffic? An Evaluation of Click Traffic Providers". In: *WICOM/AIRWeb Workshop on Web Quality*. 2011.

[18] Benjamin Farley, Ari Juels, Venkatanathan Varadarajan, Thomas Ristenpart, Kevin D. Bowers, and Michael M. Swift. "More for your money: exploiting performance heterogeneity in public clouds". In: *SoCC*. ACM, 2012, p. 20.

[19] Yevgeniy Dodis, Thomas Ristenpart, and Salil P. Vadhan. "Randomness Condensers for Efficiently Samplable, Seed-Dependent Sources". In: *TCC*. Vol. 7194. Lecture Notes in Computer Science. Springer, 2012, pp. 618–635.

[20] Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, and Thomas Shrimpton. "Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail". In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2012, pp. 332–346.

[21] WesLee Frisby, Benjamin Moench, Benjamin Recht, and Thomas Ristenpart. "Security Analysis of Smartphone Point-of-Sale Systems". In: *WOOT*. USENIX Association, 2012, pp. 22–33.

[22] Mihir Bellare, Thomas Ristenpart, and Stefano Tessaro. "Multi-instance Security and Its Application to Password-Based Cryptography". In: *CRYPTO*. Vol. 7417. Lecture Notes in Computer Science. Springer, 2012, pp. 312–329.

[23] Yevgeniy Dodis, Thomas Ristenpart, John P. Steinberger, and Stefano Tessaro. "To Hash or Not to Hash Again? (In)Differentiability Results for H 2 and HMAC". In: *CRYPTO*. Vol. 7417. Lecture Notes in Computer Science. Springer, 2012, pp. 348–366.

[24] Venkatanathan Varadarajan, Thawan Kooburat, Benjamin Farley, Thomas Ristenpart, and Michael M. Swift. "Resource-freeing attacks: improve your cloud performance (at your neighbor's expense)". In: *ACM Conference on Computer and Communications Security*. ACM, 2012, pp. 281–292.

[25] Yinqian Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. "Cross-VM side channels and their use to extract private keys". In: *ACM Conference on Computer and Communications Security*. ACM, 2012, pp. 305–316.

[26] Mihir Bellare, Sriram Keelveedhi, and Thomas Ristenpart. "Message-Locked Encryption and Secure Deduplication". In: *EUROCRYPT*. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 296–312.

[27] Drew Davidson, Benjamin Moench, Thomas Ristenpart, and Somesh Jha. "FIE on Firmware: Finding Vulnerabilities in Embedded Systems Using Symbolic Execution". In: *USENIX Security Symposium*. USENIX Association, 2013, pp. 463–478.

[28] Sriram Keelveedhi, Mihir Bellare, and Thomas Ristenpart. "DupLESS: Server-Aided Encryption for Deduplicated Storage". In: *USENIX Security Symposium*. USENIX Association, 2013, pp. 179–194.

[29] Thomas Ristenpart and Scott Yilek. "The Mix-and-Cut Shuffle: Small-Domain Encryption Secure against N Queries". In: *CRYPTO (1)*. Vol. 8042. Lecture Notes in Computer Science. Springer, 2013, pp. 392–409.

[30] Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, and Thomas Shrimpton. "Protocol misidentification made easy with format-transforming encryption". In: *ACM Conference on Computer and Communications Security*. ACM, 2013, pp. 61–72.

[31] Keqiang He, Alexis Fisher, Liang Wang, Aaron Gember, Aditya Akella, and Thomas Ristenpart. "Next stop, the cloud: understanding modern web service deployment in EC2 and azure". In: *Internet Measurement Conference*. ACM, 2013, pp. 177–190.

[32] Ari Juels and Thomas Ristenpart. "Honey Encryption: Encryption beyond the Brute-Force Barrier". In: *IEEE Security & Privacy* 12.4 (2014), pp. 59–62.

[33] Ari Juels and Thomas Ristenpart. "Honey Encryption: Security Beyond the Brute-Force Bound". In: *EUROCRYPT*. Vol. 8441. Lecture Notes in Computer Science. Springer, 2014, pp. 293–310.

[34] Adam Everspaugh, Yan Zhai, Robert Jellinek, Thomas Ristenpart, and Michael M. Swift. "Not-So-Random Numbers in Virtualized Linux and the Whirlwind RNG". In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2014, pp. 559–574.

[35] Robert Jellinek, Yan Zhai, Thomas Ristenpart, and Michael M. Swift. "A Day Late and a Dollar Short: The Case for Research on Cloud Billing Systems". In: *HotCloud*. USENIX Association, 2014.

[36] Stephen Checkoway, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, Hovav Shacham, and Matthew Fredrikson. "On the Practical Exploitability of Dual EC in TLS Implementations". In: *USENIX Security Symposium*. USENIX Association, 2014, pp. 319–335.

[37] Matthew Fredrikson, Eric Lantz, Somesh Jha, Simon Lin, David Page, and Thomas Ristenpart. "Privacy in Pharmacogenetics: An End-to-End Case Study of Personalized Warfarin Dosing". In: *USENIX Security Symposium*. USENIX Association, 2014, pp. 17–32.

[38] Daniel Luchaup, Kevin P. Dyer, Somesh Jha, Thomas Ristenpart, and Thomas Shrimpton. "LibFTE: A Toolkit for Constructing Practical, Format-Abiding Encryption Schemes". In: *USENIX Security Symposium*. USENIX Association, 2014, pp. 877–891.

[39] Venkatanathan Varadarajan, Thomas Ristenpart, and Michael M. Swift. "Scheduler-based Defenses against Cross-VM Side-channels". In: *USENIX Security Symposium*. USENIX Association, 2014, pp. 687–702.

[40] Daniel Luchaup, Thomas Shrimpton, Thomas Ristenpart, and Somesh Jha. "Formatted Encryption Beyond Regular Languages". In: *ACM Conference on Computer and Communications Security*. ACM, 2014, pp. 1292–1303.

[41] Yinqian Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. "Cross-Tenant Side-Channel Attacks in PaaS Clouds". In: *ACM Conference on Computer and Communications Security*. ACM, 2014, pp. 990–1003.

[42] Liang Wang, Antonio Nappa, Juan Caballero, Thomas Ristenpart, and Aditya Akella. "WhoWas: A Platform for Measuring Web Deployments on IaaS Clouds". In: *Internet Measurement Conference*. ACM, 2014, pp. 101–114.

[43] Yevgeniy Dodis, Chaya Ganesh, Alexander Golovnev, Ari Juels, and Thomas Ristenpart. "A Formal Treatment of Backdoored Pseudorandom Generators". In: *EUROCRYPT (1)*. Vol. 9056. Lecture Notes in Computer Science. Springer, 2015, pp. 101–126.

[44] Rahul Chatterjee, Joseph Bonneau, Ari Juels, and Thomas Ristenpart. "Cracking-Resistant Password Vaults Using Natural Language Encoders". In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2015, pp. 481–498.

[45] Adam Everspaugh, Rahul Chatterjee, Samuel Scott, Ari Juels, and Thomas Ristenpart. "The Pythia PRF Service". In: *USENIX Security Symposium*. USENIX Association, 2015, pp. 547–562.

[46] Venkatanathan Varadarajan, Yinqian Zhang, Thomas Ristenpart, and Michael M. Swift. "A Placement Vulnerability Study in Multi-Tenant Public Clouds". In: *USENIX Security Symposium*. USENIX Association, 2015, pp. 913–928.

[47] David Cash, Paul Grubbs, Jason Perry, and Thomas Ristenpart. "Leakage-Abuse Attacks Against Searchable Encryption". In: *ACM Conference on Computer and Communications Security*. ACM, 2015, pp. 668–679.

[48] Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. "Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures". In: *ACM Conference on Computer and Communications Security*. ACM, 2015, pp. 1322–1333.

[49] Liang Wang, Kevin P. Dyer, Aditya Akella, Thomas Ristenpart, and Thomas Shrimpton. "Seeing through Network-Protocol Obfuscation". In: *ACM Conference on Computer and Communications Security*. ACM, 2015, pp. 57–69.

[50] Bruce Schneier, Matthew Fredrikson, Thomas Ristenpart, and Tadayoshi Kohno. *Surreptitiously Weakening Cryptographic Systems*. Non-peer-reviewed survey. 2015.

[51] Lucas Dixon, Thomas Ristenpart, and Thomas Shrimpton. "Network Traffic Obfuscation and Automated Internet Censorship". In: *IEEE Security & Privacy* 14.6 (2016), pp. 43–53.

[52] Yan Zhai, Lichao Yin, Jeffrey S. Chase, Thomas Ristenpart, and Michael M. Swift. "CQSTR: Securing Cross-Tenant Applications with Cloud Containers". In: *SoCC*. ACM, 2016, pp. 223–236.

[53] Joseph Jaeger, Thomas Ristenpart, and Qiang Tang. "Honey Encryption Beyond Message Recovery Security". In: *EUROCRYPT (1)*. Vol. 9665. Lecture Notes in Computer Science. Springer, 2016, pp. 758–788.

[54] Rahul Chatterjee, Anish Athayle, Devdatta Akhawe, Ari Juels, and Thomas Ristenpart. "pASSWORD tYPOS and How to Correct Them Securely". In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2016, pp. 799–818.

[55] Drew Davidson, Hao Wu, Robert Jellinek, Vikas Singh, and Thomas Ristenpart. "Controlling UAVs with Sensor Input Spoofing Attacks". In: *WOOT*. USENIX Association, 2016.

[56] Florian Tramèr, Fan Zhang, Ari Juels, Michael K. Reiter, and Thomas Ristenpart. "Stealing Machine Learning Models via Prediction APIs". In: *USENIX Security Symposium*. USENIX Association, 2016, pp. 601–618.

[57] Paul Grubbs, Richard McPherson, Muhammad Naveed, Thomas Ristenpart, and Vitaly Shmatikov. "Breaking Web Applications Built On Top of Encrypted Data". In: *ACM Conference on Computer and Communications Security*. ACM, 2016, pp. 1353–1364.

[58] Jay Aikat, Aditya Akella, Jeffrey S. Chase, Ari Juels, Michael K. Reiter, Thomas Ristenpart, Vyas Sekar, and Michael M. Swift. "Rethinking Security in the Era of Cloud Computing". In: *IEEE Security & Privacy* 15.3 (2017), pp. 60–69.

[59] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders". In: *PACMHCI* 1.CSCW (2017), 46:1–46:22.

[60] Paul Grubbs, Thomas Ristenpart, and Yuval Yarom. "Modifying an Enciphering Scheme After Deployment". In: *EUROCRYPT (2)*. Vol. 10211. Lecture Notes in Computer Science. 2017, pp. 499–527.

[61] Paul Grubbs, Thomas Ristenpart, and Vitaly Shmatikov. "Why Your Encrypted Database Is Not Secure". In: *HotOS*. ACM, 2017, pp. 162–168.

[62] Liang Wang, Paul Grubbs, Jiahui Lu, Vincent Bindschaedler, David Cash, and Thomas Ristenpart. "Side-Channel Attacks on Shared Search Indexes". In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2017, pp. 673–692.

[63] Paul Grubbs, Kevin Sekniqi, Vincent Bindschaedler, Muhammad Naveed, and Thomas Ristenpart. "Leakage-Abuse Attacks against Order-Revealing Encryption". In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2017, pp. 655–672.

[64] Paul Grubbs, Jiahui Lu, and Thomas Ristenpart. "Message Franking via Committing Authenticated Encryption". In: *CRYPTO (3)*. Vol. 10403. Lecture Notes in Computer Science. Springer, 2017, pp. 66–97.

[65] Adam Everspaugh, Kenneth G. Paterson, Thomas Ristenpart, and Samuel Scott. "Key Rotation for Authenticated Encryption". In: *CRYPTO (3)*. Vol. 10403. Lecture Notes in Computer Science. Springer, 2017, pp. 98–129.

[66] Joanne Woodage, Rahul Chatterjee, Yevgeniy Dodis, Ari Juels, and Thomas Ristenpart. "A New Distribution-Sensitive Secure Sketch and Popularity-Proportional Hashing". In: *CRYPTO (3)*. Vol. 10403. Lecture Notes in Computer Science. Springer, 2017, pp. 682–710.

[67] Rahul Chatterjee, Joanne Woodage, Yuval Pnueli, Anusha Chowdhury, and Thomas Ristenpart. "The TypTop System: Personalized Typo-Tolerant Password Checking". In: *ACM Conference on Computer and Communications Security*. ACM, 2017, pp. 329–346.

[68] Ivan Pustogarov, Thomas Ristenpart, and Vitaly Shmatikov. "Using Program Analysis to Synthesize Sensor Spoofing Attacks". In: *AsiaCCS*. ACM, 2017, pp. 757–770.

[69] Congzheng Song, Thomas Ristenpart, and Vitaly Shmatikov. "Machine Learning Models that Remember Too Much". In: *ACM Conference on Computer and Communications Security*. ACM, 2017, pp. 587–601.

[70] Liang Wang, Mengyuan Li, Yinqian Zhang, Thomas Ristenpart, and Michael M. Swift. "Peeking Behind the Curtains of Serverless Platforms". In: *USENIX Annual Technical Conference*. USENIX Association, 2018, pp. 133–146.

[71] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology". In: *CHI*. ACM, 2018, p. 667.

[72] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. "The Spyware Used in Intimate Partner Violence". In: *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2018, pp. 441–458.

[73] Yevgeniy Dodis, Paul Grubbs, Thomas Ristenpart, and Joanne Woodage. "Fast Message Franking: From Invisible Salamanders to Encryptment". In: *CRYPTO (1)*. Vol. 10991. Lecture Notes in Computer Science. Springer, 2018, pp. 155–186.

[74] Vincent Bindschaedler, Paul Grubbs, David Cash, Thomas Ristenpart, and Vitaly Shmatikov. "The Tao of Inference in Privacy-Protected Databases". In: *PVLDB* 11.11 (2018), pp. 1715–1728.

[75] Liang Wang, Gilad Asharov, Rafael Pass, Thomas Ristenpart, and Abhi Shelat. "Blind Certificate Authorities". In: *IEEE Symposium on Security and Privacy*. IEEE, 2019, pp. 1015–1032.

[76] Bijeeta Pal, Tal Daniel, Rahul Chatterjee, and Thomas Ristenpart. "Beyond Credential Stuffing: Password Similarity Models Using Neural Networks". In: *IEEE Symposium on Security and Privacy*. IEEE, 2019, pp. 417–434.

[77] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. "Clinical Computer Security for Victims of Intimate Partner Violence". In: *USENIX Security Symposium*. USENIX Association, 2019, pp. 105–122.

[78] Nirvan Tyagi, Paul Grubbs, Julia Len, Ian Miers, and Thomas Ristenpart. "Asymmetric Message Franking: Content Moderation for Metadata-Private End-to-End Encryption". In: *CRYPTO (3)*. Vol. 11694. Lecture Notes in Computer Science. Springer, 2019, pp. 222–250.

[79] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. "'Is my phone hacked?' Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence". In: *PACMHCI* 3.CSCW (2019), 202:1–202:24.

[80] Nirvan Tyagi, Ian Miers, and Thomas Ristenpart. "Traceback for End-to-End Encrypted Messaging". In: *CCS*. ACM, 2019, pp. 413–430.

[81] Lucy Li, Bijeeta Pal, Junade Ali, Nick Sullivan, Rahul Chatterjee, and Thomas Ristenpart. "Protocols for Checking Compromised Credentials". In: *CCS*. ACM, 2019, pp. 1387–1403.

[82] Yiqing Hua, Thomas Ristenpart, and Mor Naaman. "Towards Measuring Adversarial Twitter Interactions against Candidates in the US Midterm Elections". In: *ICWSM*. 2020.

[83] Yiqing Hua, Mor Naaman, and Thomas Ristenpart. "Characterizing Twitter Users Who Engage in Adversarial Interactions against Political Candidates". In: *ACM Conference on Human Factors in Computing Systems – CHI*. 2020.

[84] Kevin A Roundy, Paula Barmaimon Mendelberg, Nicola Dell, Damon McCoy, Daniel Nissani, Thomas Ristenpart, and Acar Tamersoy. "The Many Kinds of Creepware Used for Interpersonal Attacks". In: *IEEE Symposium on Security and Privacy*. 2020.

[85] Paul Grubbs, Anurag Khandelwal, Marie-Sarah Lacharité, Lloyd Brown, Lucy Li, Rachit Agarwal, and Thomas Ristenpart. "Pancake: Frequency smoothing for encrypted data stores". In: *USENIX Security Symposium*. 2020.

[86] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. "The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums". In: *USENIX Security Symposium*. 2020.

[87] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. ""So-called privacy breeds evil" Narrative Justifications for Intimate Partner Surveillance in Online Forums". In: *Proceedings of the ACM on Human-Computer Interaction, Issue CSCW* (2020).

[88] Kurt Thomas, Devdatta Akhawe, Michael Bailey, Dan Boneh, Elie Bursztein, Sunny Consolvo, Nicola Dell, Zakir Durumeric, Patrick Gage Kelley, Deepak Kumar, Damon McCoy, Sarah Meiklejohn, Thomas Ristenpart, and Gianluca Stringhini. "SoK: Hate, Harassment, and the Changing Landscape of Online Abuse". In: *IEEE Symposium on Security and Privacy – Oakland*. 2021.

[89] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. "A Digital Safety Dilemma: Analysis of Remote Computer-Mediated Computer Security Interventions During COVID-19". In: *ACM Conference on Human Factors in Computing Systems – CHI*. 2021.

[90] Julia Len, Paul Grubbs, and Thomas Ristenpart. "Partitioning Oracle Attacks". In: *USENIX Security Symposium*. 2021.

[91] Min Xu, Armin Namavari, David Cash, and Thomas Ristenpart. "Searching Encrypted Data with Size-Locked Indexes". In: *USENIX Security Symposium*. 2021.

[92] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. "The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence". In: *USENIX Security Symposium*. 2021.

[93] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. "Care Infrastructures for Digital Security in Intimate Partner Violence". In: *ACM Conference on Human Factors in Computing Systems – CHI*. 2022.

[94] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A. Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. "Trauma-Informed Computing: Towards Safer Technology Experiences for All". In: *ACM Conference on Human Factors in Computing Systems – CHI*. 2022.

[95] Nirvan Tyagi, Sofía Celi, Thomas Ristenpart, Nick Sullivan, Stefano Tessaro, and Christopher A. Wood. "A Fast and Simple Partially Oblivious PRF, with Applications". In: *Advances in Cryptology – Eurocrypt*. 2022.

[96] Nirvan Tyagi, Julia Len, Ian Miers, and Thomas Ristenpart. "Orca: Blocklisting in Sender-Anonymous Messaging". In: *USENIX Security Symposium*. 2022.

[97] Yiqing Hua, Armin Namavari, Kaishuo Cheng, Mor Naaman, and Thomas Ristenpart. "Increasing Adversarial Uncertainty to Scale Private Similarity Testing". In: *USENIX Security Symposium*. 2022.

[98] Bijeeta Pal, Mazharul Islam, Marina Sanusi, Nick Sullivan, Luke Valenta, Tara Whalen, Christopher Wood, Thomas Ristenpart, and Rahul Chatterjee. "Might I Get Pwned: A Second Generation Compromised Credential Checking Service". In: *USENIX Security Symposium*. 2022.

[99] Marina Sanusi Bohuk, Mazharul Islam, Suleman Ahmad, Michael Swift, Thomas Ristenpart, and Rahul Chatterjee. "Gossamer: Securely Measuring Password-based Logins". In: *USENIX Security Symposium*. 2022.

[100] Yiqing Hua, Manoel Horta Ribeiro, Thomas Ristenpart, Robert West, and Mor Naaman. "Characterizing Alternative Monetization Strategies on YouTube". In: *Proceedings of the ACM on Human-Computer Interaction, Issue CSCW*. 2022.

[101] Julia Len, Paul Grubbs, and Thomas Ristenpart. "Authenticated encryption with key identification". In: *Advances in Cryptology – Asiacrypt*. 2022.

[102] Mazharul Islam, Marina Sanusi Bohuk, Paul Chung, Thomas Ristenpart, and Rahul Chatterjee. "Araña: discovering and characterizing password guessing attacks in practice". In: *USENIX Security Symposium*. 2023.

[103] Sanketh Menda, Julia Len, Paul Grubbs, and Thomas Ristenpart. "Context Discovery and Commitment Attacks: How to Break CCM, EAX, SIV, and More". In: *Advances in Cryptology – Eurocrypt*. 2023.

[104] Alaa Daffalla, Marina Bohuk, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. "Account Security Interfaces: Important, Unintuitive, and Untrustworthy". In: *USENIX Security Symposium*. 2023.

[105] Rosanna Bellini, Kevin Lee, Megan A. Brown, Jeremy Shaffer, Rasika Bhalerao, and Thomas Ristenpart. "The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence". In: *USENIX Security Symposium*. 2023.

[106] Andrès Fàbrega, Carolina Ortega Pérez, Armin Namavari, Ben Nassi, Rachit Agarwal, and Thomas Ristenpart. "Injection Attacks against End-to-End Encrypted Applications". In: *IEEE Symposium on Security and Privacy – Oakland*. 2024.

[107] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Kelley, Michelle Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. "SoK: Safer Digital-Safety Research Involving At-Risk Users". In: *IEEE Symposium on Security and Privacy – Oakland*. 2024.

[108] Armin Namavari, Barry Wang, Sanketh Menda, Ben Nassi, Nirvan Tyagi, James Grimmelmann, Amy Zhang, and Thomas Ristenpart. "Private Hierarchical Governance for Encrypted Messaging". In: *IEEE Symposium on Security and Privacy – Oakland*. 2024.

[109] Emily Tseng, Rosanna Bellini, Yeuk Yu Lee, Alana Ramjit, Thomas Ristenpart, and Nicola Dell. "Data Stewardship in Clinical Computer Security: Balancing Burden and Benefit in Participatory Systems". In: *Proceedings of the ACM on Human-Computer Interaction – CSCW*. 2024.

[110] Andrès Fàbrega, Armin Namavari, Rachit Agarwal, Ben Nassi, and Thomas Ristenpart. "Exploiting Leakage in Password Managers via Injection Attacks". In: *USENIX Security Symposium*. 2024.

[111] Lana Ramjit, Natalie Dolci, Francesca Rossi, Ryan Garcia, Thomas Ristenpart, and Dana Cuomo. "Navigating Traumatic Stress Reactions During Computer Security Interventions". In: *USENIX Security Symposium*. 2024.

[112] Avital Shafran, Eran Malach, Thomas Ristenpart, Gil Segev, and Stefano Tessaro. "Is ML-Based Cryptanalysis Inherently Limited? Simulating Cryptographic Adversaries via Gradient-Based Methods". In: *Advances in Cryptology – Crypto*. 2024.

[113] Emily Tseng, Thomas Ristenpart, and Nicola Dell. "Mitigating Trauma in Qualitative Research Infrastructure: Roles for Machine Assistance and Trauma-Informed Design". In: *Proceedings of the ACM on Human-Computer Interaction – CSCW*. 2025.

[114] Sophie Stephenson, Lana Ramjit, Thomas Ristenpart, and Nicola Dell. "Digital Technologies and Human Trafficking: Combating Coercive Control and Navigating Digital Autonomy". In: *ACM Conference on Human Factors in Computing Systems – CHI*. 2025.

[115] Alaa Daffalla, Arkaprabha Bhattacharya, Jacob Wilder, Rahul Chatterjee, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. "A Framework for Abusability Analysis: The Case of Passkeys in Interpersonal Threat Models". In: *USENIX Security Symposium*. 2025.

[116] Avital Shafran, Roei Schuster, Thomas Ristenpart, and Vitaly Shmatikov. "Rerouting LLM Routers". In: *COLM*. 2025.

[117] Sanketh Menda, Mihir Bellare, Viet Tung Hoang, Julia Len, and Thomas Ristenpart. "The OCH Authenticated Encryption Scheme". In: *CCS*. ACM, 2025.

[118] Carolina Ortega Pèrez, Julia Len, and Thomas Ristenpart. "Interoperable Symmetric Message Franking". In: *CCS*. ACM, 2025.

[119] Armin Namavari and Thomas Ristenpart. "Transcript Franking for Encrypted Messaging". In: *Advances in Cryptology – Asiacrypt*. 2025.

[120] Haesoo Kim, Thomas Ristenpart, and Nicola Dell. "AI-Facilitated Coercive Control: An Experimental Study". In: *ACM Conference on Human Factors in Computing Systems – CHI*. 2026.

[121] Andrès Fàbrega, Julia Len, Thomas Ristenpart, and Greg Rubin. "Random-Access AEAD for Fast Lightweight Online Encryption". In: *Advances in Cryptology – Eurocrypt*. 2026.

[122] Arkaprabha Bhattacharya, Alaa Daffalla, Kevin Lee, Rosanna Bellini, Nicola Dell, and Thomas Ristenpart. "Inconsistent, Incomplete, and Insecure: A Survey of Account Security Interfaces". In: *USENIX Security Symposium*. 2026.

[123] Alaa Daffalla, Grace Myers, Rosanna Bellini, Thomas Ristenpart, and Nicola Dell. ""Maybe there's only one passkey?": Challenges Investigating and Remediating Adversarial Passkeys". In: *USENIX Security Symposium*. 2026.

[124] Akshaya Kumar, Carolina Ortega Pérez, Joseph Jaeger, Thomas Ristenpart, and Michael Specter. "SoK: Offline Finding Protocols for Lightweight Location Tracking". In: *Proceedings on Privacy Enhancing Technologies* (2026).

Research Impact & Media Attention

- Results from [1, 4, 9] used during NIST SHA-3 competition to analyze new cryptographic hash function standard
- Adeona privacy-preserving device tracking software [6] covered by *The New York Times*, *Technology Review*, *ABC News*, and many others. Adeona downloaded >113,000 times since July 2008.
- Mozilla, Google developers acknowledge security vulnerabilities found in [13]
- Cloud computing attacks [11] featured in *Technology Review*, *PC World*, and others. European Network and Information Security Agency cites our work [11] in report on best practices for cloud computing security. Cross-VM cryptographic side-channel attack [25] led to discussions with industry vendors regarding implications, and has been covered by *Hackernews*, *Threatpost*, *Technology Review*, *DarkReading*, and others.
- Proposed standard FFX for encryption methods for credit cards, SSNs, healthcare records based on [10]. Companies now deploy FFX widely to protect credit card data and other sensitive information. Algorithms for FPE and FTE with regular expression formats [30, 38] used by Skyhigh Networks for rapid deployment.
- Hedged cryptography first explored in [12, 13] on track for standardization via RFC draft[1]
- TLS vulnerability found in [16] acknowledged by standardizers
- Point-of-sale vulnerabilities found in [21] acknowledged and fixed by Intuit and IDTech.[2] Bugs found by our tool Fie [27] fixed by TI.
- Format-transforming encryption [30] deployed with Tor. Our regular language tools for building FPE and FTE schemes [38] used in industry.
- Discussion of issues uncovered in [34] with Linux kernel developers and Microsoft security, vulnerabilities in Microsoft patched. Recent redesign of Linux random number generator informed by our work.
- Honey encryption [33] reported on by *Technology Review*, *Business Week*, *Slashdot*, *Boston Globe*, and others.
- Study on typo tolerance in password entry [54] spawned changes in production Dropbox password login system (added a caps lock indicator). Typo tolerance reported on by *Technology Review*, *Threatpost*, *Slashdot*, and others. TypTop [67] released as public, open source software (`https://typtop.info/`).
- Results on machine learning model confidentiality [56] reported on by *Quartz*, *Wired*, *Medium.com*, *ACM.org*, *The Register*.

[1] https://datatracker.ietf.org/doc/draft-irtf-cfrg-det-sigs-with-noise/

[2] `https://security.intuit.com/index.php/home/alerts/95-security-update-for-gray-gopayment-card-reader`

- Collaboration between Cornell Tech (led primarily by Nicola Dell, with some help from me) and the New York City's Office to Combat Domestic Violence lead to NYC Hope web portal (`https://www1.nyc.gov/nychope/site/page/home`).
- Paper [72] led Google to restrict advertisements on google.com and the Google Play store for search terms related to intimate partner violence, as well as changes to Play store policy. This work was reported on by the *New York Times*, *Le Monde*, *The Times*, and more. Our work helped motivate antivirus launch features to flag intimate partner violence (IPV) spyware.
- Recognized as Advocate of New York City in 2019 by the New York City Mayor's Office to End Domestic and Gender Based Violence (ENDGBV) (formerly the Office to Combat Domestic Violence) for our work on clinical computer security [77, 79]. This work led to founding the Clinic to End Tech Abuse (CETA), which has handled referrals for hundreds of IPV survivors requesting help with technology issues.
- Based on our experience with CETA, we wrote a guidebook to help others with setting up tech abuse clinics (`https://www.techabuseclinics.org/`). There are now CETA-inspired clinics across North America including in in Wisconsin, Wisconsin, and British Columbia. Nascent clinics are in the process of being setup elsewhere in North America and Europe.
- Paper [81] helped motivate changes to Google's breached password checking service, integrated into Google Chrome. Paper [98] deployed as breach alerting service at Cloudflare.
- 3HashSDHI construction [95] integrated into upcoming IETF standard, and being prototyped for use by several companies.
- Research and advocacy on technology abuse in intimate partner violence helped motivate and inform United States' Safe Connections Act of 2022.
- Results in [106] led to deployed improvements in design of Signal's encrypted backups, and in [110] to improvements in various password managers.
- Open source implementations of FLOE encryption scheme analyzed in [121] publically available; scheme is on track for use in production systems.

Invited Talks (selected)

- University of Waterloo, CrySP Speaker on Privacy, *For All Tomorrow's Survivors: Computer Security in Interpersonal Threat Models*, 2026
- Max Planck Institute, Symposium on Systems Security, *For All Tomorrow's Survivors: Building Clinical Interventions for Technology Abuse*, 2024
- Google, Tech Days at Google NYC, *For All Tomorrow's Survivors: Building Clinical Interventions for Technology Abuse*, 2023
- Duke University, Triangle Computer Science Distinguished Lecture Series, *Mitigating Technology Abuse in Intimate Partner Violence and Encrypted Messaging*, 2023
- Princeton University, CITP Distinguished Lecture Series, *Mitigating Technology Abuse in Intimate Partner Violence and Encrypted Messaging*, 2023
- CISPA, Distinguished Lecture Series, *Improving Password-based Authentication*, 2022
- SOUPS Conference, Keynote, *Mitigating Technology Abuse in Intimate Partner Violence*, 2021
- North Carolina State University, Data Privacy Month Keynote, *Mitigating Technology Abuse in Intimate Partner Violence*, 2021
- ETH Zurich, Distinguished Lecture Series, *Mitigating Technology Abuse in Intimate Partner Violence and Encrypted Messaging*, 2020

- University of Illinois, Urbana Champaign, ITI Distinguished Lecture Series, *Computer Security for Victims of Abuse*, October 2019
- Princeton University, *Tech Privacy and Safety in Intimate Partner Violence*, February 2018
- Facebook, *Tech Privacy and Safety in Intimate Partner Violence*, October 2017
- Google, *Tech Privacy and Safety in Intimate Partner Violence*, October 2017
- University of Chicago, *Making Password Checking Systems Better*, November 2016
- DIMACS Workshop on Cryptography and its Interactions: Learning Theory, Coding Theory, and Data Structures, *Stealing Machine Learning Models and Using Them to Violate Privacy*, July 2016
- DIMACS/MACS Workshop on Cryptography for the RAM Model of Computation, *Making Password Checking Systems Better*, June 2016
- Carnegie Mellon University, *Making Password Systems Better*, March 2016
- Crypto for Big Data Workshop at Columbia University, *Exploiting Leakage in Searchable Encryption and Machine Learning*, December 2015
- EPFL, *Model Inversion and other Threats in Machine Learning*, September 2015
- ETH Zurich, *Honey Encryption: Security Beyond the Brute-force Bound*, September 2015
- Fast Software Encryption 2014, *New Encryption Primitives for Uncertain Times*, March 2014
- DIMACS Workshop on Current Trends in Cryptography, *Message-locked Encryption and Secure Deduplication*, April 2013
- Royal Holloway University of London, *Message-locked Encryption and Secure Deduplication*, April 2013
- Real World Cryptography, *Message-locked Encryption and Secure Deduplication*, January 2013
- Microsoft Research, *Practice-driven Cryptographic Theory*, August 2012
- Stanford University, *Practice-driven Cryptographic Theory*, June 2012
- Qualcomm, *Practice-driven Cryptographic Theory*, June 2012
- NSF Workshop for Security of Cloud Computing, *New Problems in Security for Cloud Computing*, February 2012
- Isaac Newton Institute for Mathematical Sciences, *Practice-driven Cryptographic Theory*, January 2012
- Dagstuhl Workshop on Public-key Cryptography, *Careful with Composition: Limitations of the Indifferentiability Framework*, September 2011
- Microsoft Research, *Tag Size Does Matter: Attacks and Proofs for the TLS Record Protocol*, June 2011
- Microsoft Research, *Careful with Composition: Limitations of the Indifferentiability Framework*, June 2011
- VMWare, *Virtual Security: Data Leakage in Third-Party Clouds and VM Reset Vulnerabilities*, September 2010
- U. of Washington, *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Clouds*, November 2009
- U. of Washington, *Virtual Machine Reset Vulnerabilities and Hedged Cryptography*, November 2009
- Microsoft Research, *Virtual Security: Data Leakage in Third-Party Clouds and VM Reset Vulnerabilities*, November 2009
- Dagstuhl Workshop on Symmetric Cryptography, *Salvaging Merkle-Damgård for Practical Applications*, January 2009
- Lorentz Center Workshop on Hash Functions, *Design Paradigms for Building Multi-Property Hash Functions*, June 2008

- Ecole Polytechnique Fédérale de Lausanne, *Privacy-Preserving Location Tracking of Lost or Stolen Devices*, May 2008
- Echternach Symmetric Cryptography Seminar, *Design Paradigms for Building Multi-Property Hash Functions*, January 2008
- Microsoft Research, *New Approaches for Building Cryptographic Hash Functions*, August 2007
- U. of Bristol, *New Approaches for Building Cryptographic Hash Functions*, May 2007
- U. of California, Davis, *New Approaches for Building Cryptographic Hash Functions*, March 2007

Professional Activities

- *Steering committee*: USENIX Security 2017–2023; Real-World Cryptography Symposium 2013–2020; DIMACS Workshop on Secure Cloud Computing 2014
- *Program co-Chair*: Cloud Computing Security Workshop 2011; USENIX Security Symposium 2017; Crypto 2020; Symposium on Security and Privacy (Oakland) 2022–2023
- *Program committee*: Fast Software Encryption 2009, 2010; Cloud Computing Security Workshop 2010, 2012, 2013, 2014; Selected Areas in Cryptology 2010; Financial Cryptography and Data Security 2011; HotCloud 2011, 2012; Computer and Communications Security 2011, 2012; Eurocrypt 2012, 2014, 2016, 2018; Symposium on Security and Privacy (Oakland) 2012, 2013, 2015, 2019, 2020, 2026; Network and Distributed Security Symposium 2013, 2014, 2015, 2016; Crypto 2013; HotDep 2013; Dependable Systems and Networks 2014; USENIX Security Symposium 2014, 2015, 2016, 2018, 2019, 2021, 2025; FOCI 2014, 2016; Symposium on Cloud Computing 2014; Real World Cryptography 2024, 2025, 2026
- *Journal reviewer*: Journal of Computer Security; Journal of Cryptology; Designs, Codes and Cryptography
- *Invited panelist*: "How to Choose SHA-3", Lorentz Center Workshop on Hash Functions, June 2008; Electronic Transactions Association
- *Invited participant*: DARPA ISAT Future Ideas Symposium, June 2010; NSF Workshop on the Security of Cloud Computing 2012; DARPA ISAT Workshop 2013

University Service

- *Graduate student relations, University of Toronto*: 2026–2027
- *Security Council, University of Toronto*: 2026–2027
- *Faculty Director of Security, Trust, and Safety (SETS) Initiative*: 2022–2025.
- *Cornell University Research Integrity Council*: 2022–2025. Standing committee to perform inquiries and investigations into alleged scientific misconduct. Participated in one inquiry committee 2023–2024.
- *Cornell University Computer Science Diversity, Equity, and Inclusion Committee*: 2021–2022, 2024–2025
- *Cornell Tech Computer Science PhD Director of Graduate Studies Liaison*: 2017–2018, 2018–2019, 2021–2022. Helping the departmental Director of Graduate Studies with Cornell Tech specific PhD student issues and situations.
- *Cornell Tech Faculty Recruiting Committee*: 2018–2019, 2022–2023 (chair)
- *Cornell Computer Science Faculty Recruiting Committee*: 2018–2019, 2022–2023
- *Jacobs Institute Faculty Recruiting Committee*: 2021–2022
- *Cornell Computer Science field requirements committee*: Spring 2018

- *Cornell Computer Science committee on improving Ithaca / NYC interactions*: Fall 2018, 2019–2020
- *Cornell Computer Science PhD admissions committee*: 2015–2016, 2016–2017
- *Cornell Computer Science PhD admissions process improvements*: 2016. I helped oversee hiring a PhD student as part time developer, and worked with them and faculty to develop a customized HotCRP-based platform for PhD admissions reviewing. We deployed it for the 2016–2017 admissions and it was a substantial improvement on our prior approach; it is the basis for admissions to this day.
- *Cornell Tech faculty liaison regarding move to new campus*: 2015–2016

Teaching Experience

- Cornell Tech, masters "Algorithms", Fall 2023
- Cornell Tech, masters "Computer Security" (a.k.a. Security and Privacy in the Wild), Fall 2019, Spring 2024
- Cornell Tech, graduate "Designing Secure Cryptography", Spring 2019, Spring 2023
- Cornell Tech, masters "Practicum in Computer Security", Fall 2018
- Cornell Tech, masters "Cryptography", Spring 2016, Spring 2017, Spring 2018, Summer 2021, Spring 2022, Fall 2022
- Cornell Tech, graduate "Computer Security", Fall 2015, Fall 2016, Spring 2018, Fall 2021, Fall 2024
- Cornell Tech, masters "Building Startup Systems", Fall 2015, Fall 2016 (academic coordinator for class)
- University of Wisconsin–Madison, graduate "Information Security", Fall 2013
- University of Wisconsin–Madison, "Information Security", Fall 2011, 2012, Spring 2014
- University of Wisconsin–Madison, graduate "Applied Cryptography", Spring 2011,2012
- *Teaching Assistant*, UC San Diego, undergraduate "Modern Cryptography", 2006, 2008, 2010
- *Teaching Assistant*, UC San Diego, graduate "Modern Cryptography", 2008
- *Teaching Assistant*, UC Davis, undergraduate "Intro. to Programming and Problem Solving", 2001.

Advising

Current:

- Arkaprabha Bhattacharya (PhD, Cornell University)
- Alaa Daffalla (PhD, Cornell University)
- Andrés Fábrega (PhD, Cornell University)
- Carolina Ortega Pérez (PhD, Cornell University)

Alumni:

Below are former members of my group or those I spent significant time mentoring, as well as what they did afterwards. Some advisees/mentees accepted positions and deferred them for a year, so I list both the postdoc and accepted tenure-track position under "Placement". Except where indicated otherwise with a footnote, I was the primary adviser.

Advisee	Position	Year	Placement
Sanketh Menda	PhD, Cornell	2025	Amazon Web Services
Armin Namavari	PhD, Cornell	2025	Meta Research Scientist
Lana Ramjit*	Postdoc, Cornell	2024	AEquitas
Rosanna Bellini*	Postdoc, Cornell	2024	New York University (assistant professor)
Julia Len	PhD, Cornell	2024	MIT (postdoc) & UNC Chapel Hill (assistant professor)
Ben Nassi	Postdoc, Cornell	2024	Technion (research fellow)
Emily Tseng*	PhD, Cornell	2024	Microsoft Research (postdoc) & University of Washington (assistant professor)
Marina Sanusi	PhD, Cornell	2024	Meta CTF (co-founder)
Barry Wang	MS, Cornell	2024	CMU PhD program
Nirvan Tyagi	PhD, Cornell	2023	Stanford University (postdoc) & University of Washington (assistant professor)
Bijeeta Pal	PhD, Cornell	2022	Snap Inc.
Yiqing Hua†	PhD, Cornell	2022	Google
Paul Grubbs	PhD, Cornell	2020	New York University (postdoc) & University of Michigan (assistant professor)
Samuel Havron*	MS, Cornell	2020	Squarespace
Lucy Li	MS, Cornell	2020	Addepar
Anurag Khandelwal	Postdoc, Cornell	2019	Yale University (assistant professor)
Rahul Chatterjee	PhD, Cornell	2019	University of Wisconsin–Madison (assistant professor)
Ian Miers	Postdoc, Cornell	2019	University of Maryland (assistant professor)
Liang Wang	PhD, Wisconsin	2018	Princeton University (postdoc)
Ivan Pustogarov‡	Postdoc, Cornell	2017	University of Toronto (postdoc)
Adam Everspaugh	PhD, Wisconsin	2017	Uptake
Matthew Fredrikson**	PhD, Wisconsin	2015	Carnegie Mellon University (assistant professor)
Venkatanathan Varadarajan	PhD, Wisconsin	2015	Oracle Labs
Robert Jellinek	MS, Wisconsin	2014	Amazon
Benjamin Moench	BS, Wisconsin	2014	Symantec
Alexis Fisher	MS, Wisconsin	2013	Sandia National Laboratories
Benjamin Farley	MS, Wisconsin	2012	Amazon AWS
WesLee Frisby	MS, Wisconsin	2012	Sandia National Laboratories
Thawan Kooberat	MS, Wisconsin	2012	Facebook
Adam Vail	BS, Wisconsin	2012	University of Wisconsin (masters)

⋆ Co-advised with Nicola Dell

† Co-advised with Mor Naaman

‡ Co-advised with Vitaly Shmatikov

* Advised by Nicola Dell

** Advised by Somesh Jha

Interns:
Sophie Stephenson (Intern, Summer 2024), Avital Shafran (Intern, Summer 2023), Eman Maali (Intern, Summer 2023), Barry Wang (Intern, Summer 2022), Kaishuo Cheng (Intern, 2021), Julio Poveda (Intern, 2019-2020), Andrea Gallardo (Intern, 2019-2020), Hadas Orgad (Intern, Summer 2017), Ayush Agarwal (Intern, Summer 2017), Jacqueline Palmer (Intern, 2016-2017), Muhammad Haris Mughees (Visiting PhD student, Summer 2017), Guy Galun (Intern, Summer 2016), Jiahui Lu (Intern, Summer 2016), Yuval Pneuli (Intern, Summer 2016), Joanne Woodage (Visiting PhD student, 2016), Giovanni Cherubin (Visiting PhD student, Summer 2016)

Funding

- Google, AI for Trust, Safety, Security and Privacy Award, Sep. 2026 – Sep. 2027. $139,300 CAD. PI: Thomas Ristenpart
- Qualcomm, Faculty Award, 2025–2026. $75,000 USD. With Nicola Dell.
- NSF SaTC: CORE: Medium: Improving Personal Account Security, Jul. 1, 2025 – Jun. 30, 2028, $700,000 USD. PI: Nicola Dell. co-PI: Thomas Ristenpart
- NSF SaTC: CORE: Medium: Building the Next Generation of Authenticated Encryption, Mar. 1, 2025 – Feb. 28, 2029, $1,199,988 USD (award total to Cornell; $733,778 USD subawarded to the University of Toronto). PI: Thomas Ristenpart. co-PI: Shay Gueron
- Google, Cyber NYC Research Award, 2025. $80,000 USD. PI: Nicola Dell. co-PI: Thomas Ristenpart. (Part of Cyber NYC funding listed below.)
- Google, Academic Research Award, 2024–2025. $100,000 USD. With Nicola Dell.
- Google, Cyber NYC Research Award, 2024. $80,000 USD. PI: Thomas Ristenpart. (Part of Cyber NYC funding listed below.)
- Google, Cyber NYC Research Award, 2023. $80,000 USD. PI: Nicola Dell. co-PI: Thomas Ristenpart. (Part of Cyber NYC funding listed below.)
- JP Morgan, Faculty Research Award, 2023–2024. $70,000 USD. PI: Nicola Dell. co-PI: Thomas Ristenpart
- Google, Award for Inclusion Research, 2022–2023. $60,000 USD. PI: Nicola Dell. Co-PI: Thomas Ristenpart.
- Google, Cyber NYC Research Gift, 2022. $3,480,000 USD overall institutional gift (expected over three years); Thomas Ristenpart's allocation: $240,000 USD through the three $80,000 USD awards listed above. PI: Greg Morrisett. co-PI: Nate Foster, Thomas Ristenpart.
- NSF SaTC: CORE: Large: Privacy-Preserving Abuse Prevention for Encrypted Communications Platforms, Aug. 1, 2021 – Jan. 31, 2027, $2,628,174 USD (to Cornell). PI: Thomas Ristenpart. co-PI: James Grimmelmann, Mor Naaman, Nathan Mathias, Amy Zhang
- NSF SaTC: CORE: Medium: Mixed Distribution Models for Encrypted Data Stores, Jul. 15, 2021 – Jun. 30, 2025, $666,666 USD (to Cornell). PI: Thomas Ristenpart. co-PI: Rachit Agarwal, Anurag Khandelwal
- JP Morgan, Faculty Research Award, 2021–2023. $120,000 USD. PI: Thomas Ristenpart. co-PI: Nicola Dell
- Google, AI for Social Good, 2020–2021. $122,574 USD. With Nicola Dell.
- Google, Faculty Research Award, 2020–2021. $73,706 USD. PI: Nicola Dell. co-PI: Thomas Ristenpart
- NSF SaTC: CORE: Medium: Collaborative: Safety and Security for Targets of Digital Violence, Oct. 1, 2019 – Sep. 30, 2023, $849,913 USD. PI: Nicola Dell. co-PI: Karen Levy, Thomas Ristenpart.
- Facebook, Award for Content Policy Research on Social Media Platforms, 2019–2020. $85,968 USD. PI: Nicola Dell. Co-PI: Thomas Ristenpart

- Facebook Secure the Internet Grant, Improving Encrypted Messaging, 2018, $80,000 USD. PI: Thomas Ristenpart. co-PI: Yevgeniy Dodis
- Google, Research Award, 2018. $40,000 USD. PI: Nicola Dell. co-PI: Thomas Ristenpart
- NSF SaTC: CORE: Large: Collaborative: Accountable Information Use: Privacy and Fairness in Decision-Making Systems, May 18, 2017 – May 17, 2022, $899,999 USD. PI: Helen Nissenbaum. co-PI: Thomas Ristenpart
- NSF SaTC: CORE: Medium: Collaborative: Cryptographic Data Protection in Modern Systems, May 31, 2017 – May 30, 2021, $800,000 USD. PI: Vitaly Shmatikov. co-PI: Thomas Ristenpart
- Schmidt Sciences. Apr. 25, 2017 – Apr. 25, 2019, $200,000 USD. PI: Vitaly Shmatikov. co-PI: Thomas Ristenpart.
- ARO Toward Principled Foundations for Honey Objects in Information Security, Apr. 1, 2016 – Mar. 31, 2019, $388,795 USD. PI: Ari Juels. co-PI: Thomas Ristenpart.
- TTP: Medium: Democratizing Secure Password Management, Aug. 11, 2011 – Aug. 31, 2019, $1,197,699 USD. PI: Ari Juels. co-PI: Thomas Ristenpart
- Google, Gift, 2016, $20,000 USD
- Google, Research Award, 2016, $56,500 USD
- TWC: Medium: Collaborative: Distribution-Sensitive Cryptography, Nov. 16, 2015 – Aug. 31, 2019, $399,833 USD (to Cornell). PI: Ari Juels. co-PIs: Thomas Ristenpart, Thomas Shrimpton
- Microsoft, Gift, 2015, $60,000 USD
- Sloan Fellow, Gift, 2015, $50,000 USD
- Microsoft, Gift, 2014, $50,000 USD
- NSF TWC: Frontier: Collaborative: Rethinking Security in the Era of Cloud Computing, Sept. 1, 2013 – Aug. 31, 2018, $1,995,068 USD (to Wisconsin). PI: Michael Reiter. co-PIs: Srinivasa Akella, Jay Aikat, Jeffrey Chase, Peng Ning, Thomas Ristenpart, Vyas Sekar, Michael Swift
- DoD Air Force: Mathematical Foundations of Secure Computing Clouds, Mar. 25, 2013 – Mar. 14, 2018, $338,443 USD ($56,925 USD to Cornell). PI: Benjamin Recht. Co-PIs: Stark Draper, Jordan Ellenberg, Robert Nowak, Christopher Re, Thomas Ristenpart, Steven Wright
- NSF CAREER: Infrastructure for Secure Cloud Computing, 2013 – 2017, $480,620 USD. PI: Thomas Ristenpart
- Microsoft, Gift, 2013, $50,000 USD (to Wisconsin)
- Microsoft, Gift, 2012, $50,000 USD (to Wisconsin)
- NSF TC: Medium: Collaborative Research: Random Number Generation and Use in Virtualized Environments, Sept. 1, 2011 – Aug. 31, 2015, $749,149 USD (to Wisconsin). PI: Thomas Ristenpart. Co-PIs: Yevgeniy Dodis, Michael Swift
- RSA Laboratories, Gift, 2011, $20,000 USD (to Wisconsin)