Jonathan Katz jkatz2@gmail.com

Education

Ph.D. (with distinction), Computer Science, Columbia University, 2002
Dissertation: *Efficient Cryptographic Protocols Preventing "Man-in-the-Middle" Attacks*
Advisors: Zvi Galil and Moti Yung
Also advised by Rafail Ostrovsky (Telcordia Technologies)

M.Phil., Computer Science, Columbia University, 2001

M.A., Chemistry, Columbia University, 1998

S.B., Mathematics, Massachusetts Institute of Technology, 1996

S.B., Chemistry, Massachusetts Institute of Technology, 1996

Employment History

Senior Staff Research Scientist, Google
November, 2023 – current

Professor Emeritus, University of Maryland
May, 2025 – current

Chief Scientist, Dfns
October, 2022 – November, 2023

(While on leave from the University of Maryland.) Managed five-person research group responsible for the design, analysis, and implementation of cryptographic protocols used by Dfns.

Professor, University of Maryland
July, 2013 – August, 2019; August, 2020 – February, 2025

Professor and
VA Center for Innovative Technology Eminent Scholar in Cybersecurity,
George Mason University
August, 2019 – August, 2020

Director, Maryland Cybersecurity Center (MC2)
October, 2013 – June, 2019

Associate Professor, University of Maryland
July, 2008 – June, 2013

Assistant Professor, University of Maryland
July, 2002 – June, 2008

Responsible for maintaining a world-class research program in cryptography and information security. Duties include supervising graduate students and designing and teaching courses in cryptography, theoretical computer science, and network security.

Independent Cryptography/Cybersecurity Consultant, various positions
August, 2002 – present

I have consulted for several companies and government agencies on the design, analysis, and implementation of cryptographic protocols and algorithms. I have also delivered tailored courses on a wide range of topics in cryptography and cybersecurity to audiences in industry, academia, and government. Finally, I have served as an expert witness in patent cases and other areas.

Visiting Research Scientist, IBM T.J. Watson Research Center (Hawthorne, NY)
August, 2008 – July, 2009

Visited and collaborated with the cryptography research group at IBM.

Visiting Professor, École Normale Supérieure (Paris, France)
June – July, 2008

Presented three lectures on my research; collaborated with the cryptography research group at ENS.

Research Fellow, Institute for Pure and Applied Mathematics, UCLA
September – December, 2006

Invited as a core participant for the Fall 2006 program on "Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security."

Visiting Research Scientist, DIMACS
March – May, 2002

Conducted research in both theoretical and applied cryptography, leading to two published papers.

Instructor, Columbia University
Summer, 1999 – Spring, 2002

Taught *Computability and Models of Computation* (Summer '01, Spring '02), *Introduction to Cryptography* (Spring '01), and *Introduction to Computer Programming in C* (Summer '99, Spring '00).

Research Scientist, Telcordia Technologies
March, 2000 – October, 2001

Member of the Mathematical Sciences Research Center. Conducted basic research in cryptography leading to the filing of two provisional patents. Provided security consulting services for other research groups within Telcordia.

Security Consultant, Counterpane Systems
May, 1999 – March, 2000

Discovered security flaws in email encryption software (PGP); this work was widely covered in the press and led to two published papers and a refinement of the current standards for email encryption. Designed and implemented secure web-based protocols for clients. Contributed to *Secrets and Lies: Digital Security in a Networked World*, by B. Schneier (J. Wiley & Sons, 2000).

Honors and Awards

Recipient of 2025 PKC Test-of-Time Award for the 2009 paper *Signing a Linear Subspace: Signature Schemes for Network Coding* for "its foundational contribution in introducing signature schemes with (linear) homomorphic properties. These ideas have proven to be highly influential, with applications ranging from blockchains to secure outsourced computation."

ACM Fellow (2021), "For contributions to cryptographic protocol design and cryptography education."

Mercator Fellow, German Research Foundation (2019).

ACM SIGSAC Outstanding Contribution Award (2019), "For exemplary commitment to education in cryptography, through teaching and research, and for dedication to the advancement and increased influence of cryptographic research."

IACR Fellow (2019), "For broad contributions, especially in public-key encryption and cryptographic protocols, and for dedication to service and education."

University of Maryland Distinguished Scholar-Teacher Award, 2017–2018

Member, State of Maryland Cybersecurity Council and Chair, Subcommittee on Education and Workforce Development, 2015–2019

Member, steering committee, IEEE Cybersecurity Initiative, 2014–2017

Alexander von Humboldt Research Award, 2015–2016

Named one of Daily Record's "50 Influential Marylanders," 2014

Invited participant, DARPA Computer Science Study Group, 2009–2010

NSF CAREER award, 2005

University of Maryland GRB semester award, 2005–2006

National Defense Science and Engineering Graduate Fellowship, 1996–1999

NSF Graduate Fellowship, 1996 (declined)

Alpha Chi Sigma award for academic excellence, MIT, 1996

Research Grants/Gifts

(Dollar amounts listed reflect my home university's portion of the award, rounded to the nearest dollar. Unless indicated otherwise, I am the sole PI on the award.)

Research gift, G0 Labs, $25,000.
January, 2024

"SaTC: CORE: Medium: Cryptography in a Post-Quantum Future," NSF, $1,000,400.
August, 2022 – July, 2025
PI: Jonathan Katz; co-PIs: Gorjan Alagic and Dana Dachman-Soled

"Proving Security of Algorand (as Deployed)," Algorand Foundation Ltd., $150,668.
September, 2021 – August, 2022

"Bridging Secure Computation and Differential Privacy," Facebook, $100,000.
2021 – 2022

"Formally verified Accelerator for Ring-based Secure Iterative evaluation of Data under Encryption (FARSIDE)," DARPA (via subcontract to SRI International), $447,202.
March, 2021 – February, 2024

"Provable Security of the Algorand Protocol," Algorand Foundation Ltd., $150,000.
September, 2020 – August, 2021

"TAMED: posT quAntuM zEro knowleDge," DARPA (via subcontract to UCLA), $500,259.
April, 2020 – March, 2024

"Foundations for Next-Generation Cryptographic Standards," NIST, $600,000.
September, 2019 – August, 2021
PI: Jonathan Katz; co-PIs: Dana Dachman-Soled and Babis Papamanthou

"Repelling Evasion and Poisoning Attacks: A Principled Way Forward," DARPA, $3,146,359.
December, 2019 – November, 2023
PI: Tom Goldstein; co-PIs: John Dickerson, Furong Huang, David Jacobs, Jonathan Katz, and Abhinav Shrivastava

"Practical Multi-Party Computation for Lightweight Clients," Alibaba, $100,000.
January, 2019 – December, 2020

"Efficient Implementations of Secure Multi-Party Computation," PlatON, $142,214.
September, 2018 – March, 2020

"CPS: Medium: Collaborative Research: Security vs. Privacy in Cyber-Physical Systems," NSF (CNS-1837517), $360,000.
September, 2018 – September, 2021

"Scholarship for Service (SFS) for ACES," NSF (DGE-1753857), $5,046,316.
January, 2018 – December, 2022
PI: Michel Cukier; co-PIs: Jonathan Katz, Lawrence Gordon, William Nolte, and Jan Plane

"LL/University of Maryland Research Collaboration on Secure Multi-Party Computation," Lincoln Laboratory, $49,892.
April, 2017 – May, 2018

"Automated Analysis and Synthesis of Secure Cryptographic Algorithms," NRL, $266,004.
September, 2016 – September, 2019

"TWC: Medium: Collaborative: New Protocols and Systems for RAM-Based Secure Computation," NSF (CNS-1563722), $484,196.
May, 2016 – April, 2019
PI: Jonathan Katz; co-PI: Mike Hicks

"Design and Analysis of (Quantum-Resistant) Hash-Based Signatures," Cisco, $68,694.
April, 2016 – March, 2017

"Provable Security for Next-Generation Cryptography," NIST, $1,097,937.
September, 2015 – August, 2018
PI: Jonathan Katz; co-PIs: Dana Dachman-Soled and Babis Papamanthou

"TWC: Large: Collaborative: The Science and Applications of Crypto-Currency," NSF (CNS-1518765), $1,935,783.
July, 2015 – June, 2018
PI: Elaine Shi; co-PIs: Michael Hicks, Jonathan Katz, and David Van Horn

"TWC: Medium: Apollo: An Architecture for Scalable Verifiable Computing," NSF (CNS-1514261), $1,200,000.
July, 2015 – June, 2018
PI: Babis Papamanthou; co-PIs: Amol Deshpande, Jonathan Katz, and Elaine Shi

"US-Europe Workshop on Cryptography and Hardware Security for the Internet of Things," ARO, $35,000.
June, 2015 – June, 2016
PI: Gang Qu; co-PI: Jonathan Katz

"Secure Information Flows in Hybrid Coalition Networks," US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), $179,708.
May, 2015 – May, 2016
PI: Michael Hicks; co-PI: Jonathan Katz

"Secure Network-Centric Data Distribution and Processing," US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), $64,525.
May, 2015 – May, 2016

"EAGER: Physical, Social, and Situational Factors as Determents of Public WiFi Users' Online Behaviors," NSF (CNS-1444633), $215,002.
October, 2014 – September, 2016
co-PIs: Jonathan Katz and David Maimon

"Establishing a Science of Security Research Lablet at the University of Maryland," NSA, $4,737,089.
March, 2014 – March, 2017
Lead PI: Jonathan Katz

"Automating Secure Computation," DARPA (via subcontract to ACS), $51,213.
January, 2014 – February, 2015
PI: Elaine Shi; co-PI: Jonathan Katz

"Network Security: Efficient Protocols for Message Integrity in DTNs," Laboratory for Telecommunications Sciences, $176,353.
April, 2013 – March, 2015

"Secure Information Flows in Hybrid Coalition Networks," US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), $356,615.
May, 2013 – May, 2015
PI: Michael Hicks; co-PI: Jonathan Katz

"Secure Network-Centric Data Distribution and Processing," US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), $108,016.
May, 2013 – May, 2015

"TWC: Small: Exploring Cryptographic Models and Setup Assumptions," NSF (CNS-1223623), $400,945.
September, 2012 – August, 2015

"Developing a Science of Cybersecurity," US Army Research Laboratory, $2,813,768.
October, 2011 – September, 2013

"TC: Large: Collaborative Research: Practical Secure Two-Party Computation: Techniques, Tools, and Applications," NSF (CNS-1111599), $1,000,000.
August, 2011 – August 2016
PI: Jonathan Katz; co-PI: Michael Hicks

"Delegated, Outsourced, and Distributed Computation," US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), $199,226.
May, 2011 – April, 2013

"Toward Practical Cryptographic Protocols for Secure Information Sharing, Phase II CSSG," DARPA, $400,000.
September, 2010 – August, 2012

"NetSE: Medium: Collaborative Research: Privacy-Preserving Social Systems," NSF (IIS-0964541), $880,000.
September, 2010 – August, 2013
PI: Bobby Bhattacharjee; co-PIs: Jonathan Katz and Neil Spring

Supplement for "CAREER: Models and Cryptographic Protocols for Unstructured, Decentralized Systems," NSF (CNS-0447075), $80,000.
August, 2009 – August, 2010

"Energy Efficient Security Architectures and Infrastructures," US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), $162,450.
May, 2009 – April, 2011

"Cryptographic Primitives and Protocols for Security in Complex Systems," DARPA, $100,000.
March, 2009 – March, 2010

"Understanding Fairness in Secure Two-Party and Multi-Party Computation," NSF (CCF-0830464), $277,782.
September, 2008 – August, 2011

"Collaborative Research: CT-ISG: Efficient Cryptography Based on Lattices," NSF (CNS-0716651), $138,500.
September, 2007 – August, 2010

"Efficient Security Techniques for Information Flows in Coalition Environments," US Army Research Laboratory/UK Ministry of Defence (International Technology Alliance in Network and Information Science), $395,026.
May, 2007 – April, 2009
PIs: Jonathan Katz and Michael Hicks

"Designing Reliable and Secure Tactical MANETs," DoD MURI, $1,442,324.
May, 2007 – April, 2012
PI: Virgil Gligor; co-PIs: John Baras and Jonathan Katz

"New Techniques for Authenticating Humans (and Other Resource-Constrained Devices)," NSF (CNS-0627306), $300,000.
September, 2006 – August, 2009

"Feasibility and Efficiency of Secure Computation," United States-Israel Binational Science Foundation, $120,000.
September, 2005 – August, 2009

"CAREER: Models and Cryptographic Protocols for Unstructured, Decentralized Systems," NSF (CNS-0447075), $400,000.
February, 2005 – January, 2010

"Secure Design and Usage of Cryptographic Hash Functions," University of Maryland GRB semester award.
2005–2006 academic year

"ITR-(ASE+NHS)-(DMC+INT+SOC): Resilient Storage and Querying in Decentralized Networks," NSF (CNS-0426683), $720,000.
September, 2004 – August, 2008
PI: Bobby Bhattacharjee; co-PIs: Sudarshan Chawathe, Jonathan Katz, and Aravind Srinivasan

"Distributed Trust Computations for Decentralized Systems," NSF (CNS-0310499), $375,000.
August, 2003 – July, 2006
PI: Bobby Bhattacharjee; co-PI: Jonathan Katz

"Collaborative Research: Mitigating the Damaging Effects of Key Exposure," NSF (CNS-0310751), $240,000.
August, 2003 – July, 2006

PhD Students (Graduated)

Giorgos Tsimos (graduated in 2025, co-advised with Babis Papamanthou)
Currently scientist at Pod Network

Doruk Gur (graduated in 2025)

Noemi Glaeser (graduated in 2024, co-advised with Giulio Malavolta)

Chen Bai (graduated in 2024, co-advised with Gorjan Alagic)
Currently a postdoc at Virginia Tech

Michael Rosenberg (graduated in 2024, co-advised with Ian Miers)
Currently at Cloudflare

Erica Blum (graduated in 2023)
Currently assistant professor at Reed College

Yupeng Zhang (graduated in 2018, co-advised with Babis Papamanthou)
Recipient of ACM SIGSAC dissertation award (2019)
Currently assistant professor at UIUC

Xiao Wang (graduated in 2018)
Currently assistant professor at Northwestern University

Kartik Nayak (graduated in 2018, co-advised with Elaine Shi)
Currently associate professor at Duke University

Daniel Apon (graduated in 2017)
Currently applied cryptography lead at MITRE

Aishwarya Thiruvengadam (graduated in 2017, co-advised with Dana Dachman-Soled)
Currently assistant professor at IIT Madras

Andrew Miller (graduated in 2016, co-advised with Elaine Shi)
Currently associate professor at UIUC

Alex Malozemoff (graduated in 2016)
Currently at Galois, Inc.

Adam Groce (graduated in 2014)
Currently professor at Reed College

Ranjit Kumaresan (graduated in 2012)
Currently at Visa Research

Arkady Yerukhimovich (graduated in 2011)
Currently associate professor at George Washington University

S. Dov Gordon (graduated in 2010)
Currently associate professor at George Mason University

Omer Horvitz (graduated in 2007, co-advised with Prof. Gligor)
Currently CTO at techmeme.com

Chiu-Yuen Koo (graduated in 2007)
Currently at Google

Ruggero Morselli, (graduated in 2006, co-advised with Prof. Bhattacharjee)
Currently at Google

Postdoctoral Researchers

Alex Block, 2022–2024
Currently assistant professor at UIC

Hendrik Waldner, 2022–2024
Currently research scientist at Nethermind

Andreea Alexandru, 2021 – 2023
Currently cryptography scientist at Duality Technologies

Georgios Zirdelis, 2021 – 2022
Currently cryptographer at Modulus Labs

Julian Loss, 2019 – 2021
Currently assistant professor at CISPA Helmholtz Center for Information Security

Jiayu Xu, 2019 – 2021
Currently assistant professor at Oregon State University

Leo Fan, 2019 – 2021
Currently assistant professor at Rutgers University

Sina Shiehian, 2019 – 2020
Currently privacy engineer at Snap

Daniel Genkin, 2016 – 2018
Currently associate professor at Georgia Tech

Samuel Ranellucci, 2016 – 2018
Currently cryptographer at Unbound Tech

Dimitris Papadopoulos, 2016 – 2017
Currently assistant professor at Hong Kong University of Science and Technology

Jacob Alperin-Sheriff, 2015 – 2016
Currently at EY-Parthenon

Hoang Viet Tung, 2014 – 2015
Currently associate professor at Florida State University

Feng-Hao Liu, 2013 – 2015
Currently associate professor at Washington State University

Jean Paul Degabriele, 2013 – 2014
Currently research group leader at Darmstadt University

Yan Huang, 2012 – 2014
Currently associate professor at Indiana University

Hong-Sheng Zhou, 2010 – 2013
Currently associate professor at Virginia Commonwealth University

Dominique Schröder, 2011 – 2012
Currently professor of privacy enhancing technologies at TU Wien

Raef Bassily, 2012
Current associate professor at The Ohio State University

Seung Geol Choi, 2010 – 2012
Currently professor at the US Naval Academy

Vassilis Zikas, 2010 – 2012
Current associate professor at Georgia Tech

Lior Malka, 2009 – 2010

Ik Rae Jeong, 2005 – 2006
Currently professor at Korea University

Professional Activities

Editor-in-chief:
– Foundations and Trends in Privacy and Security (2023–present)

Editorial board:
– ACM Transactions on Privacy and Security (2024–present)
– IACR Communications in Cryptology (2024)
– Journal of Cryptology (2011–present)
– International Journal of Applied Cryptography (2007–present)
– Proceedings on Privacy Enhancing Technologies (2015–2017)
– Information & Computation (2012–2017)
– Journal of Computer and System Sciences (2013–2014)
– IET Information Security (2005–2012)
– Fundamenta Informaticae (2006–2011)

Program chair:
– Real-World MPC Workshop 2025
– 6th International Symposium on Cyber Security, Cryptology, and Machine Learning (CSCML) 2022
– ACM Conference on Computer and Communications Security 2019–2020
– ACM Conf. on Computer and Communications Security (area chair, cryptography) 2018
– Crypto 2016–2017
– Symposium and Bootcamp on the Science of Security (HoTSoS) 2017
– Intl. Conference on Practice and Theory in Public-Key Cryptography (PKC) 2015
– Conference on Decision and Game Theory for Security (GameSec) 2011
– Cryptography Track, 12th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS) 2010
– Applied Cryptography and Network Security (ACNS) 2007

Organizer:
– Graduate Summer School on Post-Quantum and Quantum Cryptography (IPAM, UCLA), 2022
– Winter School on Cryptocurrency and Blockchain Technologies (Shanghai, China), 2017

Steering committees, etc.:
– Member, Scientific Advisory Board of CISPA Helmholtz Center for Information Security gGmbH, 2025–present
– International Symposium on Cyber Security, Cryptography and Machine Learning (CSCML), 2016–present
– Member, State of Maryland Cybersecurity Council (2015–2019)

– Co-chair, IEEE Cybersecurity Award Selection Committee (2017, 2018)
– IEEE Cybersecurity Initiative (2014–2017)

Program committees:
– ACM Conf. on Computer and Comm. Security (CCS) 2005, 2006, 2011–2013, 2017, 2018, 2022–2026
– USENIX Security 2025, 2026
– IEEE Symposium on Security & Privacy (Oakland) 2009, 2015, 2026
– Eurocrypt 2006, 2008, 2009, 2011, 2013, 2025
– Asiacrypt 2004, 2007, 2008, 2010, 2012, 2024
– International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS) 2017, 2023
– Crypto 2003, 2005, 2006, 2009, 2013, 2020, 2023
– IEEE Conf. on Distributed Computing Systems (ICDCS) 2023
– Theory of Cryptography Conference (TCC) 2006, 2007, 2012, 2016, 2022
– Workshop on Privacy-Enhancing Technologies for the Homeland Security Enterprise 2022
– Real World Cryptography (RWC) 2019, 2020
– IndoCrypt 2017
– IEEE European Symposium on Security & Privacy 2016, 2017
– Network and Distributed System Security (NDSS) 2016
– Mycrypt 2016
– Symposium and Bootcamp on the Science of Security (HotSoS) 2015, 2016, 2018
– European Symposium on Security in Computer Security (ESORICS) 2013
– RSA—Cryptographers' Track 2006, 2007, 2010, 2012
– Financial Cryptography 2012
– ACM-SIAM Symposium on Discrete Algorithms (SODA) 2011
– Intl. Conf. on Cryptology and Network Security (CANS) 2010
– Intl. Conf. on Pairing-Based Cryptography (Pairing) 2010
– Public-Key Cryptography (PKC) 2007, 2010
– ACM Symposium on Theory of Computing (STOC) 2009
– Applied Cryptography and Network Security (ACNS) 2006, 2009
– IEEE Symposium on Foundations of Computer Science (FOCS) 2008
– Security in Communication Networks 2008
– ICALP 2007
– ACM Workshop on Security and Sensor Networks (SASN) 2004, 2005, 2006
– Security and Cryptography for Networks (SCN) 2006
– VietCrypt 2006
– International Conference on Information Security and Cryptology (ICISC) 2005, 2006
– UCLA/IPAM workshop on "Locally decodable codes. . . ," 2006
– Workshop on Cryptography over Ad Hoc Networks (WCAN) 2005, 2006
– International Conference on Cryptology in Malaysia (Mycrypt) 2005
– Workshop on Information Security Applications (WISA) 2004

Courses/Tutorials

Two 1-hour tutorials: "Introduction to (Zero-Knowledge) Proofs" and "The Sum-Check Protocol and Applications," Foundations and Applications of Zero-Knowledge Proofs (Intl. Centre for Mathematical Sciences, Edinburgh, UK), September 2024.

7.5 hours of lectures: "Secure Distributed Computation," Summer School on Cryptography (University of Bonn, Germany), September 2022.

3.5-hour tutorial: "Introduction to (Classical) Cryptography," Graduate Summer School on Post-Quantum and Quantum Cryptography (IPAM, UCLA), July 2022.

3-hour tutorial: "Introduction to Secure Computation," 1st Crypto Innovation School (Shenzhen, China), November 2018.

3-hour tutorial: "Incentives and Game-Theoretic Considerations in Bitcoin," Winter School on Cryptocurrency and Blockchain Technologies (Shanghai, China), January 2017.

7-week on-line course: "Cryptography," Coursera, 2014.

1-hour tutorial: "Message Authentication Codes (an Introduction)," Army Research Laboratory (Adelphi, MD), October 2009.

Half-day tutorial: "Ruminations on Defining Rational Multi-Party Computation," Summer School on Rational Cryptography (Bertinoro, Italy), June 2008.

1-hour tutorial: "The Basics of Public-Key Encryption," Booz Allen Hamilton (Linthicum, MD), October 2007.

2^{+}-hour tutorial: "A Survey of Modern Cryptography," ACM Sigmetrics, June 2007.

Week-long course: "Zero Knowledge: Foundations and Applications," (Bertinoro, Italy), October 2006.

Half-day tutorial: "Black-Box Reductions, Impossibility Results, and Efficiency Lower Bounds," UCLA/IPAM, September 2006.

Invited Panel and Session Participation

IOHK Summit (Miami, Florida): panel participant, "The Future of Blockchain Research," April 2019.

ATARC Federal CISO Summit: moderator, "Addressing the Cybersecurity Skills Gap," January 2018.

Big Data in Finance, University of Michigan: panel participant, October 2016.

3rd Annual Conference on Cyber Security and the Law (French American Foundation, Washington, D.C.): panel participant, September 2016.

11th Colloquium for Information System Security Education (Boston University): panel member, "How to Teach Cryptology," June 2007.

Invited Talks

Silicon Valley Cybersecurity Conference: "Introduction to the NIST Lattice-Based Standards," June 2025.

TU Wien (Vienna, Austria): "Round-Optimal Fully Secure Distributed Key Generation," March 2025.

Public Lecture, Intl. Centre for Mathematical Sciences (Edinburgh, UK): "What do Cryptographers Work on?" September 2024.

DeCompute 2024 (Singapore): "Honest-Majority ECDSA for Signing Networks," September 2024.

Distinguished Computing Lecture, Boise State University: "Round-Optimal Fully Secure Distributed Key Generation," November 2023.

Workshop on Securing the Future of GenAI—Mitigating Security Risks (Google, Reston, VA): "A Watermark for Large Language Models," October 2023.

NIST Workshop on Multi-Party Threshold Schemes (MPTS) 2023: "Standardizing Protocols for Threshold ECDSA," September 2023.

NIST Workshop on Multiparty Threshold Schemes (MPTS) 2023: "Distributed Key Generation in the Discrete-Logarithm Setting," September 2023.

DeCompute 2023 (Singapore): "Securing Wallets in a Federated Key-Management Network," September 2023.

Intl. Workshop on Timed-Release Encryption and its Applications (Oxford, UK): "On the Security of Time-Lock Puzzles and Timed Commitments," June 2023.

Friedrich-Alexander-Universität (Nuremberg, Germany): "Zero-Knowledge Proofs and Potential Legal Applications," December 2022.

Facebook Privacy-Preserving Machine Learning Series (virtual): "Spreading the Privacy Blanket: Differentially Oblivious Shuffling for Differential Privacy," April 2022.

University of Erlangen-Nürnberg, Mercator tutorial (virtual): "Differential Privacy for Distributed Protocols," October 2021.

University of Erlangen-Nürnberg, Mercator tutorial (virtual): "Secure Distributed Protocols," October 2021.

Ruhr University Bochum, CASA Distinguished Lecture (virtual): "Differentially Oblivious Protocols for Differential Privacy," May 2021.

Towson University, REU Colloquium (virtual): "Is RSA Encryption Secure? A Look at Modern Cryptography," April 2021.

University of Maryland, Baltimore County, Cyber Defense Lab (virtual): "Secure Computation: From Theory to Practice," October 2020.

Improving Privacy with Advanced Cryptographic Techniques, JHUAPL (virtual): "Secure Computation: Recent Progress and Future Trends," September 2020.

Crypto 2019: "Secure Multiparty Computation: When Theory Meets. . . ," August 2019.

Nanyang Technological University (Singapore), School of Physical and Mathematical Sciences Distinguished Speaker Series: "Fractal: A High-Performance Proof-of-Stake Blockchain," August 2019.

Singapore University of Technology and Design: "The Network Effect: The Impact of Network Modeling on Cryptographic Feasibility Results," August 2019.

Summer Summit on Cryptocurrency and Blockchain Technologies (City University of Hong Kong): "Incentives and Game-Theoretic Considerations in Bitcoin," August 2019.

Summer Summit on Cryptocurrency and Blockchain Technologies (City University of Hong Kong): "Blockchain and Bitcoin Fundamentals," August 2019.

Chinese University of Hong Kong, Faculty of Engineering Distinguished Lecture Series: "Fractal: A High-Performance Proof-of-Stake Blockchain," July 2019.

Northwestern University, Feinberg School of Medicine: "Privacy-Preserving Analytics for Medical Data," June 2019.

IEEE Conference on Computer and Network Security (CNS) 2019: "The Network Effect: The Impact of Network Modeling on Cryptographic Feasibility Results," June 2019.

IOHK Summit (Miami, Florida): "Practical Secure Computation," April 2019.

Information Technology and Innovation Foundation (Washington, D.C.): "Cryptography and Public Policy," March 2019.

DC-area Security and Privacy Seminar: "How to Hash: Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers," February 2019.

TPMPC Workshop (Aarhus, Denmark): "Optimizing ZK Proofs from Secure Computation," May 2018.

Sandia National Laboratories: "A Survey of Secure Computation," March 2018.

UT Dallas Distinguished Lecture Series: "Post-Quantum Signatures from Secure Computation," November 2017.

New Jersey Institute of Technology Distinguished Speaker Series: "Post-Quantum Signatures from Secure Computation," October 2017.

Cyberweek—Academic Perspectives on Cybersecurity Challenges (Tel Aviv, Israel): "Secure Distributed Computation," June 2017.

2nd Hebrew University Networking Summer (Jerusalem, Israel): "Recent Progress in Generic Secure Computation," June 2017.

MITRE Distinguished Speaker Series (McLean, VA): "Recent Progress in Efficient Secure Computation," May 2017.

IEEE Cybersecurity Development Conference (Boston, MA): "How to Think about Cryptography: Common Crypto Flaws and How to Avoid Them," November 2016.

Cyber Community of Interest Meeting, ONR: "Automated Analysis and Synthesis of Symmetric-Key Modes of Encryption," September 2016.

Computing Research Association: Addressing National Priorities and Societal Needs (Computing Community Consortium, Washington, D.C.): "Better Privacy and Security via Secure Multiparty Computation," May 2016.

Workshop on Human Factors in Cybersecurity Design, Hebrew University (Jerusalem, Israel): "Taking the Human into Account in Cryptographic Design," March 2016.

George Washington University Department of Mathematics: "The Nature of Proofs: A Computational Perspective," February 2016.

Foundations of Cyber Security and Privacy Symposium, Max Planck Society (Munich, Germany): "Cryptography as a Nucleus for Cybersecurity Research," July 2015.

Privacy Enhancing Technologies Symposium (PETS) 2015: "Secure Computation: Where Do We Go From Here?" June 2015.

Naval Postgraduate School Foundation, President's Circle Retreat: "Privacy-Preserving Distributed Computation," April 2014.

Georgetown University: "Secure Computation in the RAM Model," April 2014.

Rutgers University: "Privacy-Preserving Computation: How, What, and Why?" November 2013.

First EasyCrypt workshop (University of Pennsylvania): "EasyCrypt 0.2 Feedback and Recommendations," July 2013.

Workshop on Real-World Cryptography (Stanford): "Practical Anonymous Subscriptions," January 2013.

Workshop on Theory and Practice of Multiparty Computation (Aarhus, Denmark): "Recent Results on Game Theory and Secure Computation," June 2012.

Indiana University: "Is (Generic) Secure Two-Party Computation Practical?" November 2011.

Microsoft Research (Redmond, WA): "(Ever More) Efficient Secure Two-Party Computation," March 2011.

PerAda Workshop on Security, Trust, and Privacy (Rome, Italy): "Privacy, Trust, and Security in Pervasive Computing: Challenges and Opportunities," November 2010.

Tsinghua University (Beijing, China): "Fairness and Partial Fairness in Two-Party Computation," June 2010

Beijing Institute of Technology: "Rational Secret Sharing," June 2010.

SKLOIS: The State Key Laboratory Of Information Security (Beijing, China): "Leakage-Resilient Cryptography," June 2010.

SKLOIS: The State Key Laboratory Of Information Security (Beijing, China): "Rational Secret Sharing," June 2010.

Workshop on Decentralized Mechanism Design, Distributed Computing, and Cryptography (Princeton University): "Rational Secret Sharing: A Survey," June 2010.

Microsoft Research (Cambridge, MA): "Rational Secret Sharing," April 2009.

AT&T Labs: "Fairness and Partial Fairness in Secure Two-Party Computation," February 2009.

University of Toronto: "Fairness and Partial Fairness in Secure Two-Party Computation," February 2009.

Joint Mathematics Meetings, AMS Special Session on Algebraic Cryptography and Generic Complexity: "Public-Key Cryptography from a (Theoretical) Cryptographer's Perspective," January 2009.

Dagstuhl workshop on Theoretical Foundations of Practical Information Security (Germany): "Partial Fairness in Secure Two-Party Computation," December 2008.

École Normale Supérieure (Paris, France): "Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise," July 2008.

École Normale Supérieure (Paris, France): "Predicate Encryption: A New Paradigm for Public-Key Encryption," July 2008.

École Normale Supérieure (Paris, France): "Fairness in Secure Computation," June 2008.

UC Berkeley: "Predicate Encryption: A New Paradigm for Public-Key Encryption," May 2008.

5th Theory of Cryptography Conference (TCC) 2008 (New York): "Bridging Game Theory and Cryptography: Recent Results and Future Directions," March 2008.

MIT Cryptography and Information Security Seminar: "Complete Fairness in Secure Two-Party Computation," March 2008.

11th IMA Intl. Conference on Cryptography and Coding Theory (Cirencester, UK): "Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise," December 2007.

INDOCRYPT 2007 (Chennai, India): "Capability-Based Encryption: A New Paradigm for Public-Key Encryption," December 2007.

Pennsylvania State University: "Universally-Composable Multi-Party Computation using Tamper-Proof Hardware," April 2007.

Workshop on Cryptography: Underlying Mathematics, Provability, and Foundations (Fields Institute, Toronto): "Blind Signatures: Definitions and Constructions," November 2006.

Workshop on Foundations of Secure Multi-Party Computation (UCLA/IPAM): "On Expected Constant-Round Protocols for Broadcast," November 2006.

Workshop on Public-Key Systems with Special Properties (UCLA/IPAM): "Blind Signatures: Definitions and Constructions," October 2006.

13th SIAM Meeting on Discrete Mathematics (Victoria, Canada): "New Techniques for Authenticating Humans," June 2006.

Boston University: "New Techniques for Authenticating Humans (and other Resource-Constrained Devices)," April 2006.

Stevens Institute of Technology: "New Techniques for Authenticating Humans (and other Resource-Constrained Devices)," March 2006.

Georgia Tech: "New Techniques for Authenticating Humans (and other Resource-Constrained Devices)," November 2005.

University of Modena: "Secure Authentication without Traditional Cryptographic Keys," July 2005.

Workshop on the Past, Present, and Future of Oblivious Transfer (Haifa, Israel): "Round-Optimal Secure Two-Party Computation," May, 2005.

UCLA: "Secure Remote Authentication Using Biometric Data," March, 2005.

Luminy Workshop on Cryptography (Marseilles, France): "Secure Remote Authentication Using Biometric Data," November, 2004.

DIMACS Workshop on *Cryptography: Theory Meets Practice*: "Using Biometric Data for Secure Network-Based Authentication," October, 2004.

MIT Cryptography and Information Security Seminar: "Round-Optimal Secure Two-Party Computation," April, 2004.

Korea University: "Scalable and Efficient Protocols for Authenticated Group Key Exchange," November, 2003.

Korea Information Security Agency (KISA): "Efficient Protocols for Password-Only Authenticated Key Exchange," November, 2003.

6th Annual International Conference on Information Security and Cryptology (ICISC 2003): "Binary Tree Encryption: Constructions and Applications," November, 2003.

National Science Foundation (NSF) — Washington Area Trustworthy Systems Hour: "Maintaining Security in the Event of Key Exposure," April, 2003.

New York University: "Efficient and Non-Malleable Proofs of Plaintext Knowledge and Applications," July, 2002.

IBM T.J. Watson Research Center: "A Forward-Secure Public-Key Encryption Scheme," July, 2002.

DIMACS Workshop on *Cryptographic Protocols in Complex Environments*: "Efficient and Non-Malleable Proofs of Plaintext Knowledge and Applications," May, 2002.

IBM T.J. Watson Research Center: "Practical Password-Authenticated Key Exchange Provably Secure Against Off-Line Dictionary Attacks," December, 2000.

MIT Cryptography and Information Security Seminar: "Practical and Provably Secure Password-Authenticated Key Exchange," December, 2000.

Bell Labs (Lucent Technologies) Crypto/Security Seminar: "Cryptographic Counters and Applications to Electronic Voting," November, 2000.

Publications

Books Authored or Edited

1. Shlomi Dolev, Jonathan Katz, and Amnon Meisels, eds. *CSCML 2022: 6th International Symposium on Cybersecurity, Cryptography, and Machine Learning*, LNCS vol. 13301, Springer, 2022.

2. A. Chakraborti, R. Curtmola, J. Katz, J. Nieh, A.-R. Sadeghi, R. Sion, and Y. Zhang. *Cloud Computing Security: Foundations and Research Directions*. Foundations and Trends in Privacy and Security 3(2):103–213, 2022.

3. J. Katz and Y. Lindell. *Introduction to Modern Cryptography, third edition*. Chapman & Hall/CRC Press, 2020. (First edition published in 2007; second edition published in 2014.)

4. J. Katz and G. Vigna, eds. *CCS'20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. ACM Press, 2020.

5. X. Wang and J. Katz, eds. *CCS'19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM Press, 2019.

6. J. Katz and H. Shacham, eds. *Advances in Cryptology—Crypto 2017, Proceedings*. LNCS vols. 10401–10403, Springer, 2017.

7. M. Robshaw and J. Katz, eds. *Advances in Cryptology—Crypto 2016, Proceedings*. LNCS vols. 9814–9816, Springer, 2016.

8. J. Katz, ed. *Public-Key Cryptography (PKC) 2015, Proceedings*. LNCS vol. 9020, Springer, 2015.

9. J.S. Baras, J. Katz, and E. Altman. *Decision and Game Theory for Security, Second Intl. Conference, GameSec 2011, Proceedings*. LNCS vol. 7037, Springer, 2011.

10. J. Katz. *Digital Signatures*. Springer, 2010.

11. J. Katz and M. Yung, eds. *Applied Cryptography and Network Security, 5th International Conference, ACNS 2007, Proceedings*. LNCS vol. 4521, Springer, 2007.

Book Chapters

1. J. Katz. "Privacy-Preserving Distributed Computation." In *Handbook of Sharing Confidential Data: Differential Privacy, Secure Multiparty Computation, and Synthetic Data*, J. Drechsler, D. Kifer, J. Reiter, and A. Slavkovic, eds., Chapman & Hall/CRC Press, 2024.

2. J. Katz. "Cryptography." In *Computing Handbook (3rd edition), vol. 1: Computer Science and Software Engineering*, A. Tucker, T. Gonzalez, and J. Diaz-Herrera, eds., Chapman & Hall/CRC Press, 2014.

3. J. Katz. "Public-Key Cryptography." In *Handbook of Information and Communication Security*, P. Stavroulakis and M. Stamp, eds., Springer, 2010.

4. J. Katz. "Cryptography." In *Wiley Encyclopedia of Computer Science and Engineering*, B.W. Wah, ed., John Wiley & Sons, 2008.

5. J. Katz. "Symmetric-Key Encryption." In *The Handbook of Information Security*, H. Bidgoli, ed., John Wiley & Sons, Inc., 2005.

6. J. Katz. "Cryptography." In *Computer Science Handbook, 2nd edition*, A. Tucker, ed., CRC Press, 2004.

Journal Articles

1. J. Katz and A. Urban. "Honest-Majority Threshold ECDSA with Batch Generation of Key-Independent Presignatures." *Comm. in Cryptology* 2(1), 2024

2. M. Belorgey, S. Carpov, K. Deforth, D. Jetchev, A. Sae-Tang, M. Vuille, N. Gama, J. Katz, I. Leontiadis, and M. Mohammadi. "Manticore: A Framework for Efficient Multiparty Computation Supporting Real Number and Boolean Arithmetic." *J. Cryptology* 36(3): 31, 2024.

3. T. Chakraborty, S. Jajodia, J. Katz, A. Picariello, G. Sperli, and V.S. Subrahmanian. "FORGE: A Fake Online Repository Generation Engine for Cyber Deception." *IEEE Trans. on Dependable and Secure Computing* 18(2): 518–533, 2021.

4. D. Dachman-Soled, N. Fleischhacker, J. Katz, A. Lysyanskaya, and D. Schröder. "Feasibility and Infeasibility of Secure Computation with Malicious PUFs." *J. Cryptology* 33(2): 595–617, 2020.

5. S.G. Choi, J. Katz, D. Schröder, A. Yerukhimovich, and H.-S. Zhou. "(Efficient) Universally Composable Oblivious Transfer Using a Minimal Number of Stateless Tokens." *J. Cryptology* 32:459–497, 2019. **One of three papers from TCC 2014 invited to this journal.**

6. Y. Zhang, C. Papamanthou, and J. Katz. "Verifiable Graph Processing." *ACM Trans. on Privacy and Security* 21(4), article 20, 2018.

7. M. Lee, A. Dunn, J. Katz, B. Waters, and E. Witchel. "Anon-Pass: Practical Anonymous Subscriptions." *IEEE Security & Privacy* 12(3): 20–27, 2014. **Invited to a special issue for papers from the IEEE Symp. on Security & Privacy, 2014.**

8. S. D. Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich. "Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure." *Information & Computation* 234: 17–25, 2014. **Invited to a special issue of this journal for papers from SSS 2010.**

9. D. Apon, J. Katz, and A. Malozemoff. "One-Round Multi-Party Communication Complexity of Distinguishing Sums." *Theoretical Computer Science* 501: 101–108, 2013.

10. J. Katz and V. Vaikuntanathan. "Round-Optimal Password-Based Authenticated Key Exchange." *J. Cryptology* 26(4): 714–743, 2013. **One of three papers from TCC 2011 invited to this journal.**

11. J. Katz, A. Sahai, and B. Waters. "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products." *J. Cryptology* 26(2): 191–224, 2013. **One of four papers from Eurocrypt 2008 invited to this journal.**

12. Y. Dodis, B. Kanakurthi, J. Katz, L. Reyzin, and A. Smith. "Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets." *IEEE Transactions on Information Theory* 58(9): 6207–6222, 2012.

13. J. Katz, P. MacKenzie, G. Taban, and V. Gligor. "Two-Server Password-Only Authenticated Key Exchange." *J. Computer and System Sciences* 78(2): 651–669, 2012.

14. J. Katz. "Which Languages Have 4-Round Zero-Knowledge Proofs?" *J. Cryptology* 25(1): 41–56, 2012. **One of three papers from TCC 2008 invited to this journal.**

15. S.D. Gordon and J. Katz. "Partial Fairness in Secure Two-Party Computation." *J. Cryptology* 25(1): 14–40, 2012.

16. S.D. Gordon, C. Hazay, J. Katz, and Y. Lindell. "Complete Fairness in Secure Two-Party Computation." *J. of the ACM* 58(6): 1–36, 2011.

17. Y. Ishai, J. Katz, E. Kushilevitz, Y. Lindell, and E. Petrank. "On Achieving the 'Best of Both Worlds' in Secure Multiparty Computation." *SIAM J. Computing* 40(1): 122–141, 2011.

18. J. Katz, J.-S. Shin, and A. Smith. "Parallel and Concurrent Security of the HB and HB^+ Protocols." *J. Cryptology* 23(3): 402–421, 2010.

19. O. Horvitz and J. Katz. "Bounds on the Efficiency of 'Black-Box' Commitment Schemes." *Theoretical Computer Science* 411(10): 1251–1260, 2010. **Invited to a special issue of this journal.**

20. J. Katz, R. Ostrovsky, and M. Yung. "Efficient and Secure Authenticated Key Exchange Using Weak Passwords." *J. of the ACM* 57(1): 78–116, 2009.

21. J. Katz, C.-Y. Koo, and R. Kumaresan. "Improving the Round Complexity of VSS in Point-to-Point Networks." *Information & Computation* 207(8): 889–899, 2009.

22. I. Haitner, O. Horvitz, J. Katz, C.-Y. Koo, R. Morselli, and R. Shaltiel. "Reducing Complexity Assumptions for Statistically-Hiding Commitment." *J. Cryptology* 22(3): 283–310, 2009.

23. A. Bender, J. Katz, and R. Morselli. "Ring Signatures: Stronger Definitions, and Constructions Without Random Oracles." *J. Cryptology* 22(1): 114–138, 2009.

24. J. Katz and C.-Y. Koo. "On Expected Constant-Round Protocols for Byzantine Agreement." *J. Computer and System Sciences* 75(2): 91–112, 2009.

25. J. Katz and Y. Lindell. "Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs." *J. Cryptology* 21(3): 303–349, 2008.

26. E.-J. Goh, S. Jarecki, J. Katz, and N. Wang. "Efficient Signature Schemes with Tight Security Reductions to the Diffie-Hellman Problems." *J. Cryptology* 20(4): 493–514, 2007.

27. R. Canetti, S. Halevi, and J. Katz. "A Forward-Secure Public-Key Encryption Scheme." *J. Cryptology* 20(3): 265–294, 2007.

28. J. Katz and M. Yung. "Scalable Protocols for Authenticated Group Key Exchange." *J. Cryptology* 20(1): 85–113, 2007.

29. D. Boneh, R. Canetti, S. Halevi, and J. Katz. "Chosen-Ciphertext Security from Identity-Based Encryption." *SIAM J. Computing* 36(5): 1301–1328, 2007.

30. J. Katz and M. Yung. "Characterization of Security Notions for Probabilistic Private-Key Encryption." *J. Cryptology* 19(1): 67–96, 2006.

31. W. Du, J. Deng, Y.S. Han, P.K. Varshney, J. Katz, and A. Khalili. "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks." *ACM Trans. on Information and System Security* 8(2): 228–258, 2005.

32. R. Gennaro, Y. Gertner, J. Katz, and L. Trevisan. "Bounds on the Efficiency of Generic Cryptographic Constructions." *SIAM J. Computing* 35(1): 217–246, 2005.

Articles in Refereed Conferences and Workshops

1. K. Abbaszadehand J. Katz. "Non-Interactive Zero-Knowledge Arguments with Certified Deletion." *Advaces in Cryptology—Asiacrypt 2025.*

2. E. Crites, J. Katz, C. Komlo, S. Tessaro, and C. Zhu. "On the Adaptive Security of FROST." *Advances in Cryptology—Crypto 2025.*

3. K. Gupta, N. Chandran, D. Gupta, J. Katz, and R. Sharma. "Shark: Actively Secure Inference using Function Secret Sharing." *IEEE Symposium on Security & Privacy (Oakland) 2025.*

4. B. Balle, J. Bell, A. Cheu, A. Gascon, J. Katz, M. Raykova, P. Schoppmann, and T. Steinke. "Hash-Prune-Invert: Improved Differentially Private Heavy-Hitter Detection in the Two-Server Model." *IEEE Symposium on Security & Privacy (Oakland) 2025.*

5. L. Fan, J. Katz, Z. Lu, P. Thai, and H.-S. Zhou. "Best-Possible Unpredictabile Proof-of-Stake: An Impossibility and a Practical Design." *IEEE EuroS&P 2025.*

6. J. Katz and B. Sela. "Secret Sharing with Publicly Verifiable Deletion." *Advances in Cryptology—Eurocrypt 2025.*

7. Y. Sun, J. Katz, M. Raykova, P. Schoppmann, and X. Wang. "Actively Secure Private Set Intersection in the Client-Server Setting." *Proc. 31st ACM Conf. on Computer and Communications Security*, 2024.

8. I. Karantaidou, O. Renawi, N. Kamarinakis, F. Baldimtsi, J. Katz, and J. Loss. "Blind Multi-Signatures for Anonymous Tokens with Decentralized Issuance and Public Verifiability." *Proc. 31st ACM Conf. on Computer and Communications Security*, 2024.

9. K. Abbaszadeh, C. Pappas, J. Katz, and D. Papadopoulos. "Zero-Knowledge Proofs of Training for Deep Neural Networks." *Proc. 31st ACM Conf. on Computer and Communications Security*, 2024.

10. J. Katz. "Round-Optimal Fully Secure Distributed Key Generation." *Advances in Cryptology—Crypto 2024*.

11. J. Katz and M. Rosenberg. "LATKE: A Framework for Constructing Identity-Binding PAKEs." *Advances in Cryptology—Crypto 2024*.

12. A. Block, Z. Fang, J. Katz, J. Thaler, H. Waldner, and Y. Zhang. "Field-Agnostic SNARKs from Expand-Accumulate Codes." *Advances in Cryptology—Crypto 2024*.

13. K.D. Gur, J. Katz, and T. Silde. "Two-Round Threshold Lattice-Based Signatures from Threshold Homomorphic Encryption." PQCrypto 2024.

14. G. Alagic, C. Bai, J. Katz, C. Majenz, and P. Struck. "Post-Quantum Security of Tweakable Even-Mansour, and Applications." *Advances in Cryptology—Eurocrypt 2024*.

15. R. Garg, K. Yang, J. Katz, and X. Wang. "Scalable Mixed-Mode MPC." *IEEE Symposium on Security & Privacy (Oakland) 2024*.

16. A. Block, A. Garreta, J. Katz, J. Thaler, P. Tiwari, and M. Zajac. "Fiat-Shamir Security of FRI and Related SNARKs." *Advaces in Cryptology—Asiacrypt 2023*.

17. E. Blum, J. Katz, J. Loss, K. Nayak, and S. Ochsenreither. "Abraxas: Throughput-Efficient Hybrid Asynchronous Consensus." *Proc. 30th ACM Conf. on Computer and Communications Security*, 2023.

18. E. Blum, J. Katz, D. Leung, J. Loss, and T. Rabin. "Analyzing the Real-World Security of the Algorand Blockchain." *Proc. 30th ACM Conf. on Computer and Communications Security*, 2023.

19. J. Kirchenbauer, J. Geiping, Y. Wen, J. Katz, I. Miers, and T. Goldstein. "A Watermark for Large Language Models." *Intl. Conf. on Machine Learning (ICML) 2023* (accepted for short live presentation). **Recipient of Outstanding Paper Award.**

20. A. Alexandru, E. Blum, J. Katz, and J. Loss. "State Machine Replication under Changing Network Conditions." *Advances in Cryptology—Asiacrypt 2022*.

21. J. Katz, C. Zhang, and H.-S. Zhou. "An Analysis of the Algebraic Group Model." *Advances in Cryptology—Asiacrypt 2022*.

22. A. Alexandru, L. Burbano, A. Cardenas, M. Celiktug, J. Gomez, J. Katz, and M. Kantarcioglu. "Private Anomaly Detection in Linear Controllers: Garbled Circuits vs. Homomorphic Encryption." *61st IEEE Conf. Decision and Control 2022*.

23. J. Katz. "A Provably Secure, Lightweight Protocol for Anonymous Authentication." *13th Conf. on Security and Cryptography for Networks (SCN) 2022.*

24. G. Alagic, C. Bai, J. Katz, and C. Majenz. "Post-Quantum Security of the Even-Mansour Cipher." *Advances in Cryptology—Eurocrypt 2022.* (Also accepted for presentation at *QIP 2022.*)

25. D. Gordon, J. Katz, M. Liang, and J. Xu. "Spreading the Privacy Blanket: Differentially Oblivious Shuffling for Differential Privacy." *Applied Cryptography and Network Security (ACNS) 2022.*

26. J. Katz, J. Loss, and M. Rosenberg. "Boosting the Security of Blind Signature Schemes." *Advances in Cryptology—Asiacrypt 2021.*

27. E. Blum, J. Katz, and J. Loss. "TARDIGRADE: An Atomic Broadcast Protocol for Arbitrary Network Conditions." *Advances in Cryptology—Asiacrypt 2021.*

28. M. Abdalla, M. Barbosa, J. Katz, J. Loss, and J. Xu. "Algebraic Adversaries in the Universal Composability Framework." *Advances in Cryptology—Asiacrypt 2021.*

29. N. Franzese, J. Katz, S. Lu, R. Ostrovsky, X. Wang, and C. Weng. "Constant-Overhead Zero Knowledge for RAM Programs." *Proc. 28th ACM Conf. on Computer and Communications Security*, 2021.

30. M. Barbosa, G. Barthe, X. Fan, B. Grégoire, S.-H. Hung, J. Katz, P.-Y. Strub, X. Wu, and L. Zhou. "EasyPQC: Mechanizing Post-Quantum Cryptography Using Easycrypt." *Proc. 28th ACM Conf. on Computer and Communications Security*, 2021.

31. C. Weng, K. Yang, X. Xie, J. Katz, and X. Wang. "Mystique: Efficient Conversions for Zero-Knowledge Proofs with Applications to Machine Learning." *USENIX Security Symposium 2021.*

32. C. Weng, K. Yang, J. Katz, and X. Wang. "Wolverine: Fast, Scalable, and Communication-Efficient Zero-Knowledge Proofs for Boolean and Arithmetic Circuits." *IEEE Symp. on Security & Privacy (Oakland) 2021.*

33. P. Lazos, F. Marmolejo-Cossio, X. Zhou, and J. Katz. "RPPLNS: Pay-per-last-N-shares with a Randomised Twist." *20th Intl. Conf. on Autonomous Agents and Multiagent Systems (AAMAS) 2021.*

34. E. Blum, J. Katz, C.-D. Liu-Zhang, and J. Loss. "Asynchronous Byzantine Agreement with Subquadratic Communication." *18th Theory of Cryptography Conference (TCC) 2020.*

35. J. Katz, J. Loss, and J. Xu. "On the Security of Time-Lock Puzzles and Timed Commitments." *18th Theory of Cryptography Conference (TCC) 2020.*

36. T. Duong, L. Fan, J. Katz, P. Thai, and H.-S. Zhou. "2-hop Blockchain: Combining Proof-of-Work and Proof-of-Stake Securely." *ESORICS 2020.*

37. C. Guo, J. Katz, X. Wang, C. Weng, and Y. Yu. "Better Concrete Security for Half-Gates Garbling (in the Multi-Instance Setting)." *Advances in Cryptology—Crypto 2020*.

38. M. Abdalla, M. Barbosa, T. Bradley, S. Jarecki, J. Katz, and J. Xu. "Universally Composable Relaxed Password-Authenticated Key Exchange." *Advances in Cryptology—Crypto 2020*.

39. P. Bunn, J. Katz, E. Kushilevitz, and R. Ostrovsky. "Efficient 3-Party Distributed ORAM." *12th Conference on Security and Cryptography for Networks (SCN) 2020*.

40. J. Giraldo, A. Cardenas, M. Kantarcioglu, and J. Katz. "Adversarial Classification Under Differential Privacy." *Network and Distributed System Security Conference (NDSS) 2020*.

41. C. Guo, J. Katz, X. Wang, and Y. Yu. "Efficient and Secure Multiparty Computation from Fixed-Key Block Ciphers." *IEEE Symp. on Security & Privacy (Oakland) 2020*.

42. E. Blum, J. Katz, and J. Loss. "Synchronous Consensus with Optimal Asynchronous Fallback Guarantees." *17th Theory of Cryptography Conference (TCC) 2019*.

43. F. Marmolejo-Cossio, E. Brigham, B. Sela, and J. Katz. "Competing (Semi-)Selfish Miners in Bitcoin." *ACM Conf. on Advances in Financial Technologies 2019*.

44. C. Hong, J. Katz, V. Kolesnikov, W. Lu, and X. Wang. "Covert Security with Public Verifiability: Faster, Leaner, and Simpler." *Advances in Cryptology—Eurocrypt 2019*.

45. D. Apon, D. Dachman-Soled, H. Gong, and J. Katz. "Constant-Round Group Key-Exchange from the Ring-LWE Assumption." *Intl. Conference on Post-Quantum Cryptography 2019*.

46. N. Gupta, J. Katz, and N. Chopra. "Statistical Privacy in Distributed Average Consensus on Finite Real-Valued Inputs." *American Control Conference 2019*.

47. D. Gordon, J. Katz, and X. Wang. "Simple and Efficient Two-Server ORAM." *Advances in Cryptology—Asiacrypt 2018*.

48. H. Chan, J. Katz, K. Nayak, A. Polychroniadou, and E. Shi. "More is Less: Perfectly Secure Oblivious Algorithms in the Multi-Server Setting." *Advances in Cryptology—Asiacrypt 2018*.

49. J. Katz, V. Kolesnikov, and X. Wang. "Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures." *Proc. 25th ACM Conf. on Computer and Communications Security*, 2018.

50. J. Katz, S. Ranellucci, M. Rosulek, and X. Wang. "Optimizing Authenticated Garbling for Faster Secure Two-Party Computation." *Advances in Cryptology—Crypto 2018*.

51. B. Cogliati, Y. Dodis, J. Katz, J. Lee, J. Steinberger, A. Thiruvengadam, and Z. Zhang. "Provable Security of (Tweakable) Block Ciphers Based on Substitution-Permutation Networks." *Advances in Cryptology—Crypto 2018*.

52. Y. Zhang, D. Genkin, J. Katz, D. Papadopoulos, C. Papamanthou. "vRAM: Faster Verifiable RAM with Program-Independent Preprocessing." *IEEE Symp. on Security & Privacy (Oakland) 2018*.

53. J. Katz, M. Maffei, G. Malavolta, and D. Schröder. "Subset Predicate Encryption and Its Applications." *Cryptology and Network Security (CANS)*, 2017.

54. X. Wang, S. Ranellucci, and J. Katz. "Authenticated Garbling and Efficient Maliciously Secure Two-Party Computation." *Proc. 24th ACM Conf. on Computer and Communications Security*, 2017. **Recipient of best paper award.**

55. X. Wang, S. Ranellucci, and J. Katz. "Global-Scale Secure Multi-Party Computation." *Proc. 24th ACM Conf. on Computer and Communications Security*, 2017.

56. D. Maimon, M. Becker, S. Patil, and J. Katz. "Self-Protective Behaviors over Public WiFi Networks." *Learning from Authoritative Security Experiment Results (LASER)*, 2017.

57. C. Freitag, J. Katz, and N. Klein. "Symmetric-Key Broadcast Encryption: The Multi-Sender Case." *Intl. Symp. on Cyber Security, Cryptography, and Machine Learning 2017*.

58. D. Apon, C. Cho, K. Eldefrawy, and J. Katz. "Efficient, Reusable Fuzzy Extractors from LWE." *Intl. Symp. on Cyber Security, Cryptography, and Machine Learning 2017*.

59. Y. Zhang, D. Genkin, J. Katz, D. Papadopoulos, and C. Papamanthou. "vSQL: Verifying General SQL Queries over Dynamic Outsourced Databases." *IEEE Symp. on Security & Privacy (Oakland) 2017*.

60. X. Wang, A. Malozemoff, and J. Katz. "Faster Secure Two-Party Computation in the Single-Execution Setting." *Advances in Cryptology—Eurocrypt 2017*.

61. Y. Dodis, S. Guo, and J. Katz. "Fixing Cracks in the Concrete: Random Oracles with Auxiliary Input, Revisited." *Advances in Cryptology—Eurocrypt 2017*.

62. N. Gupta, J. Katz, and N. Chopra. "Privacy in Distributed Average Consensus." *20th International Federation of Automatic Control (IFAC) World Congress*, 2017.

63. K. Liao and J. Katz. "Incentivizing Blockchain Forks via Whale Transactions." *4th Workshop on Bitcoin and Blockchain Research*, 2017.

64. Y. Zhang, J. Katz, and C. Papamanthou. "An Expressive (Zero-Knowledge) Set Accumulator." *IEEE European Symposium on Security & Privacy 2017*.

65. V.T. Hoang, J. Katz, A. O'Neill, and M. Zaheri. "Selective-Opening Security in the Presence of Randomness Failures." *Advances in Cryptology—Asiacrypt 2016*.

66. J. Katz. "Analysis of a Proposed Hash-Based Signature Standard." *3rd International Conference on Research in Security Standardisation (SSR)*, 2016.

67. K. Lewi, A. Malozemoff, D. Apon, B. Carmer, A. Foltzer, D. Wagner, D. Archer, D. Boneh, J. Katz, and M. Raykova. "5Gen: A Framework for Prototyping Applications Using Multilinear Maps and Matrix Branching Programs." *Proc. 23rd ACM Conf. on Computer and Communications Security*, 2016.

68. X. Wang, S.D. Gordon, A. McIntosh, and J. Katz. "Secure Computation of MIPS Machine Code." *ESORICS 2016*.

69. M.D. Green, J. Katz, A. Malozemoff, and H.-S. Zhou. "A Unified Approach to Idealized Model Separations via Indistinguishability Obfuscation." *10th Conf. on Security and Cryptography for Networks (SCN) 2016*.

70. Y. Zhang, J. Katz, and C. Papamanthou. "All Your Queries are Belong to Us: The Power of File-Injection Attacks on Searchable Encryption." *USENIX Security Symposium 2016*.

71. R. Zhu, Y. Huang, J. Katz, and A. Shelat. "The Cut-and-Choose Game and Its Application to Cryptographic Protocols." *USENIX Security Symposium 2016*.

72. S. Zahur, X. Wang, M. Raykova, A. Gascon, J. Doerner, D. Evans, and J. Katz. "Revisiting Square Root ORAM: Efficient Random Access in Secure Computation." *IEEE Symp. on Security & Privacy (Oakland) 2016*.

73. J. Katz, D. Dachman-Soled, and A. Thiruvengadam. "10-Round Feistel is Indifferentiable from an Ideal Cipher." *Advances in Cryptology—Eurocrypt 2016*.

74. V.T. Hoang, J. Katz, and A. Malozemoff. "Automated Analysis and Synthesis of Authenticated Encryption Schemes." *Proc. 22nd ACM Conf. on Computer and Communications Security*, 2015. **Recipient of best paper award.**

75. Y. Zhang, J. Katz, and C. Papamanthou. "IntegriDB: Verifiable SQL for Outsourced Databases." *Proc. 22nd ACM Conf. on Computer and Communications Security*, 2015.

76. A. Miller, A. Kosba, J. Katz, and E. Shi. "Nonoutsourceable Scratch-Off Puzzles to Discourage Bitcoin Mining Coalitions." *Proc. 22nd ACM Conf. on Computer and Communications Security*, 2015.

77. J. Garay, J. Katz, B. Tackman, and V. Zikas. "How Fair is Your Protocol? A Utility-Based Approach to Protocol Optimality." *ACM Symposium on Principles of Distributed Computing (PODC)* 2015.

78. D. Dachman-Soled, J. Katz, and V. Rao. "Adaptively Secure, Universally Composable, Multi-Party Computation in Constant Rounds." *12th Theory of Cryptography Conference (TCC) 2015*.

79. S.D. Gordon, J. Katz, F.-H. Liu, E. Shi, and H.-S. Zhou. "Multi-Client Verifiable Computation with Stronger Security Guarantees." *12th Theory of Cryptography Conference (TCC) 2015*.

80. J. Katz, S. Lucks, and A. Thiruvengadam. "Hash Functions from Defective Ideal Ciphers." *RSA Conference—Cryptographers' Track 2015*.

81. Y. Zhang, C. Papamanthou, and J. Katz. "Alitheia: Towards Practical Verifiable Graph Processing." *Proc. 21st ACM Conf. on Computer and Communications Security*, 2014.

82. Y. Huang, J. Katz, V. Kolesnikov, R. Kumaresan, and A. Malozemoff. "Amortizing Garbled Circuits." *Advances in Cryptology—Crypto 2014*.

83. D. Dachman-Soled, N. Fleischhacker, J. Katz, Anna Lysyanskaya, and Dominique Schroöder. "Feasibility and Infeasibility of Secure Computation with Malicious PUFs." *Advances in Cryptology—Crypto 2014*.

84. S.G. Choi, J. Katz, A. Malozemoff, and V. Zikas. "Efficient Three-Party Computation from Cut-and-Choose." *Advances in Cryptology—Crypto 2014*.

85. A. Malozemoff, J. Katz, and M. Green. "Automated Analysis and Synthesis of Block-Cipher Modes of Operation." *IEEE Computer Security Foundations Symposium* 2014.

86. J. Katz, A. Kiayias, H.-S. Zhou, and V. Zikas. "Distributing the Setup in Universally Composable Multiparty Computation." *ACM Symposium on Principles of Distributed Computing (PODC)* 2014.

87. C. Liu, Y. Huang, E. Shi, J. Katz, and M. Hicks. "Automating Efficient RAM-Model Secure Computation." *IEEE Symp. on Security & Privacy (Oakland) 2014*.

88. A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz. "PermaCoin: Repurposing Bitcoin Work for Long-Term Data Preservation." *IEEE Symp. on Security & Privacy (Oakland) 2014*.

89. S. Goldwasser, S.D. Gordon, V. Goyal, A. Jain, J. Katz, F.-H. Liu, A. Sahai, E. Shi, and H.-S. Zhou. "Multi-Input Functional Encryption." *Advances in Cryptology—Eurocrypt 2014*.

90. D. Apon, J. Katz, E. Shi, and A. Thiruvengadam. "Verifiable Oblivious Storage." *Public-Key Cryptography (PKC) 2014*.

91. S.G. Choi, J. Katz, D. Schröder, A. Yerukhimovich, and H.-S. Zhou. "(Efficient) Universally Composable Oblivious Transfer with a Minimal Number of Stateless Tokens." *11th Theory of Cryptography Conference (TCC) 2014*, pp. 638–662, LNCS vol. 8349, Springer, 2014. **One of three papers invited to *J. Cryptology*.**

92. A. Miller, M. Hicks, J. Katz, and E. Shi. "Authenticated Data Structures, Generically." *ACM Symp. on Principles of Programming Languages (POPL) 2014*.

93. K.-M. Chung, J. Katz, and H.-S. Zhou. "Functional Encryption from (Small) Hardware Tokens." *Advances in Cryptology—Asiacrypt 2013*.

94. J. Garay, J. Katz, U. Maurer, B. Tackmann, and V. Zikas. "Rational Protocol Design: Cryptography Against Incentive-Driven Attackers." *Proc. 54th Annual Symposium on Foundations of Computer Science (FOCS)*, 2013.

95. R. Bassily, A. Groce, J. Katz, and A. Smith. "Coupled-Worlds Privacy: Exploiting Adversarial Uncertainty in Statistical Data Privacy." *Proc. 54th Annual Symposium on Foundations of Computer Science (FOCS)*, 2013.

96. Y. Huang, J. Katz, and D. Evans. "Efficient Secure Two-Party Computation Using Symmetric Cut-and-Choose." *Advances in Cryptology—Crypto 2013*.

97. M. Lee, A. Dunn, J. Katz, B. Waters, and E. Witchel. "Anon-Pass: Practical Anonymous Subscriptions." *IEEE Symp. on Security & Privacy (Oakland) 2013*. **Invited to a special issue of *IEEE Security & Privacy magazine***.

98. S.G. Choi, J. Katz, R. Kumaresan, and C. Cid. "Multi-Client Non-Interactive Verifiable Computation." *10th Theory of Cryptography Conference (TCC) 2013*.

99. S. Fehr, J. Katz, F. Song, H.-S. Zhou, and V. Zikas. "Feasibility and Completeness of Cryptographic Tasks in the Quantum World." *10th Theory of Cryptography Conference (TCC) 2013*.

100. J. Katz, U. Maurer, B. Tackmann, and V. Zikas. "Universally Composable Synchronous Computation." *10th Theory of Cryptography Conference (TCC) 2013*.

101. S.G. Choi, J. Katz, H. Wee, and H.-S. Zhou. "Efficient, Adaptively Secure, and Composable Oblivious Transfer with a Single, Global CRS." *Public-Key Cryptography (PKC) 2013*.

102. J. Katz, A. Thiruvengadam, and H.-S. Zhou. "Feasibility and Infeasibility of Adaptively Secure, Fully Homomorphic Encryption." *Public-Key Cryptography (PKC) 2013*.

103. D. Gordon, J. Katz, V. Kolesnikov, F. Krell, T. Malkin, M. Raykova, and Y. Vahlis. "Secure Two-Party Computation in Sublinear Amortized Time." *Proc. 19th ACM Conf. on Computer and Communications Security*, 2012.

104. J. Alwen, J. Katz, U. Maurer, and V. Zikas. "Collusion-Preserving Computation." *Advances in Cryptology—Crypto 2012*.

105. A. Groce, J. Katz, A. Thiruvengadam, and V. Zikas. "Byzantine Agreement with a Rational Adversary." *Intl. Colloquium on Automata, Languages, and Programming (ICALP) 2012*, pp. 561–572, LNCS vol. 7392, Springer, 2012.

106. P. Mardziel, M. Hicks, J. Katz, and M. Srivatsa. "Knowledge-Oriented Secure Multiparty Computation." *ACM Workshop on Programming and Analysis for Security (PLAS) 2012*.

107. Y. Huang, J. Katz, and D. Evans. "Quid Pro Quo-tocols: Strengthening Semi-Honest Protocols with Dual Execution." *IEEE Symp. on Security & Privacy (Oakland) 2012*.

108. J.H. Seo, J.H. Cheon, and J. Katz. "Constant-Round Multi-Party Private Set Union Using Reversed Laurent Series." *Public-Key Cryptography (PKC) 2012*, pp. 398–412, LNCS vol. 7293, Springer, 2012.

109. A. Groce and J. Katz. "Fair Computation with Rational Players." *Advances in Cryptology—Eurocrypt 2012*, pp. 81–98, LNCS vol. 7237, Springer, 2012.

110. S.G. Choi, J. Katz, R. Kumaresan, and H.-S. Zhou. "On the Security of the 'Free-XOR' Technique." *9th Theory of Cryptography Conference (TCC) 2012*, pp. 39–53, LNCS vol. 7194, Springer, 2012.

111. S.G. Choi, K.-W. Hwang, J. Katz, T. Malkin, and D. Rubenstein. "Secure Multi-Party Computation of Boolean Circuits with Applications to Privacy in On-Line Marketplaces." *RSA Conference—Cryptographers' Track 2012*, pp. 416–432, LNCS vol. 7178, Springer, 2012.

112. Y. Huang, D. Evans, and J. Katz. "Private Set Intersection: Are Garbled Circuits Better than Custom Protocols?" *Network and Distributed System Security Conference (NDSS) 2012*.

113. Y. Huang, C.-H. Shen, D. Evans, J. Katz, and A. Shelat. "Efficient Secure Computation with Garbled Circuits" (invited paper). *Intl. Conference on Information Systems Security (ICISS)*, pp. 28–48, LNCS vol. 7093, Springer, 2011.

114. J. Katz and L. Malka. "Constant-Round Private-Function Evaluation with Linear Complexity." *Advances in Cryptology—Asiacrypt 2011*, pp. 556–571, LNCS vol. 7073, Springer, 2011.

115. Y. Huang, D. Evans, J. Katz, and L. Malka. "Faster Secure Two-Party Computation Using Garbled Circuits." *20th USENIX Security Symposium*, 2011.

116. J. Garay, J. Katz, R. Kumaresan, and H.-S. Zhou. "Adaptively Secure Broadcast, Revisited." *ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 179–186, ACM, 2011.

117. J. Katz and V. Vaikuntanathan. "Round-Optimal Password-Based Authenticated Key Exchange." *8th Theory of Cryptography Conference (TCC)*, pp. 293–310, LNCS vol. 6597, Springer, 2011. **One of three papers invited to *J. Cryptology*.**

118. A. Groce, J. Katz, and A. Yerukhimovich. "Limits of Computational Differential Privacy in the Client/Server Setting." *8th Theory of Cryptography Conference (TCC)*, pp. 417–431, LNCS vol. 6597, Springer, 2011.

119. Z. Brakerski, J. Katz, G. Segev, and A. Yerukhimovich. "Limits on the Power of Zero-Knowledge Proofs in Cryptographic Constructions." *8th Theory of Cryptography Conference (TCC)*, pp. 559–578, LNCS vol. 6597, Springer, 2011.

120. J. Katz, D. Schröder, and A. Yerukhimovich. "Impossibility of Blind Signatures from One-Way Permutations." *8th Theory of Cryptography Conference (TCC)*, pp. 615–629, LNCS vol. 6597, Springer, 2011.

121. Y. Huang, L. Malka, D. Evans, and J. Katz. "Efficient Privacy-Preserving Biometric Identification." *Network & Distributed System Security Conference (NDSS) 2011.*

122. S.D. Gordon, J. Katz, and V. Vaikuntanathan. "A Group Signature Scheme from Lattice Assumptions." *Advances in Cryptology—Asiacrypt 2010*, pp. 395–412, LNCS vol. 6477, Springer, 2010.

123. Z. Brakerski, Y. Tauman Kalai, J. Katz, and V. Vaikuntanathan. "Public-Key Cryptography Resilient to Continual Memory Leakage." *Proc. 51st Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 501–510, IEEE, 2010.

124. J. Katz and L. Malka. "Secure Text Processing with Applications to Private DNA Matching." *Proc. 17th ACM Conf. on Computer and Communications Security*, pp. 485–492, ACM, 2010.

125. A. Groce and J. Katz. "A New Framework for Efficient Password-Based Authenticated Key Exchange." *Proc. 17th ACM Conf. on Computer and Communications Security*, pp. 516–525, ACM, 2010.

126. S.D. Gordon, J. Katz, R. Kumaresan, and A. Yerukhimovich. "Authenticated Broadcast with a Partially Compromised Public-Key Infrastructure." *12th Intl. Symp. on Stabilization, Safety, and Security of Distributed Systems*, pp. 144–158, LNCS vol. 6366, Springer, 2010. **Invited to a special issue of *Information & Computation.***

127. D. Gordon and J. Katz. "Partial Fairness in Secure Computation." *Advances in Cryptology—Eurocrypt 2010*, pp. 157–176, LNCS vol. 6110, Springer, 2010.

128. R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin. "Secure Network Coding over the Integers." *Public-Key Cryptography (PKC)*, pp. 142-160, LNCS vol. 6056, Springer, 2010.

129. G. Fuchsbauer, J. Katz, and D. Naccache. "Efficient Rational Secret Sharing in Standard Communication Networks." *7th Theory of Cryptography Conference (TCC)*, pp. 419–436, LNCS vol. 5978, Springer, 2010.

130. J. Katz and V. Vaikuntanathan. "Signature Schemes with Bounded Leakage Resilience." *Advances in Cryptology—Asiacrypt 2009*, pp. 703–720, LNCS vol. 5912, Springer, 2009.

131. J. Katz and A. Yerukhimovich. "On Black-Box Constructions of Predicate Encryption Schemes from Trapdoor Permutations." *Advances in Cryptology—Asiacrypt 2009*, pp. 197–213, LNCS vol. 5912, Springer, 2009.

132. J. Katz and V. Vaikuntanathan. "Smooth Projective Hashing and Password-Based Authenticated Key Exchange from Lattices." *Advances in Cryptology—Asiacrypt 2009*, pp. 636–652, LNCS vol. 5912, Springer, 2009.

133. G. Ateniese, S. Kamara, and J. Katz. "Proofs of Storage from Homomorphic Identification Protocols." *Advances in Cryptology—Asiacrypt 2009*, pp. 319–333, LNCS vol. 5912, Springer, 2009.

134. M. Albrecht, C. Gentry, S. Halevi, and J. Katz. "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'." *Proc. 16th ACM Conf. on Computer and Communications Security*, pp. 1–10, ACM, 2009.

135. J. Alwen, J. Katz, Y. Lindell, G. Persiano, A. Shelat, and I. Visconti. "Collusion-Free Multiparty Computation in the Mediated Model." *Advances in Cryptology—Crypto 2009*, pp. 524–540, LNCS vol. 5677, Springer, 2009.

136. D. Boneh, J. Katz, D. Freeman, and B. Waters. "Signing a Linear Subspace: Signatures for Network Coding." *Public-Key Cryptography (PKC)*, pp. 68–87, LNCS vol. 5443, Springer, 2009. **Recipient of PKC Test-of-Time Award, 2025.**

137. Y. Dodis, J. Katz, A. Smith, and S. Walfish. "Composability and On-Line Deniability of Authentication." *6th Theory of Cryptography Conference (TCC)*, pp. 146–162, LNCS vol. 5444, Springer, 2009.

138. S.D. Gordon and J. Katz. "Complete Fairness in Multi-Party Computation Without an Honest Majority." *6th Theory of Cryptography Conference (TCC)*, pp. 19–35, LNCS vol. 5444, Springer, 2009.

139. J. Katz, C.-Y. Koo, and R. Kumaresan. "Improving the Round Complexity of VSS in Point-to-Point Networks." *Intl. Colloquium on Automata, Languages, and Programming (ICALP)*, pp. 499–510, LNCS vol. 5126, Springer, 2008.

140. S.D. Gordon, C. Hazay, J. Katz, and Y. Lindell. "Complete Fairness in Secure Two-Party Computation." *Proc. 40th Annual ACM Symposium on Theory of Computing (STOC) 2008*, pp. 413–422, ACM, 2008.

141. J. Katz, A. Sahai, and B. Waters. "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products." *Advances in Cryptology—Eurocrypt 2008*, pp. 146–162, LNCS vol. 4965, Springer, 2008. **One of four papers invited to *J. Cryptology*.**

142. S. Kamara and J. Katz. "How to Encrypt with a Malicious Random Number Generator." *Fast Software Encryption (FSE)*, pp. 303–315, LNCS vol. 5086, Springer, 2008.

143. J. Katz and Y. Lindell. "Aggregate Message Authentication Codes." *RSA Conference—Cryptographers' Track*, pp. 155–169, LNCS vol. 4964, Springer, 2008.

144. J. Katz. "Bridging Cryptography and Game Theory: Recent Results and Future Directions" (invited paper). *5th Theory of Cryptography Conference (TCC)*, pp. 251–272, LNCS vol. 4948, Springer, 2008.

145. J. Katz. "Which Languages Have 4-Round Zero-Knowledge Proofs?" *5th Theory of Cryptography Conference (TCC)*, pp. 73–88, LNCS vol. 4948, Springer, 2008. **One of three papers invited to *J. Cryptology*.**

146. V. Goyal and J. Katz. "Universally-Composable Computation with an Unreliable Common Reference String." *5th Theory of Cryptography Conference (TCC)*, pp. 142–154, LNCS vol. 4948, Springer, 2008.

147. J. Katz. "Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise" (invited paper). *11th IMA Intl. Conference on Cryptography and Coding Theory*, pp. 1–15, Lecture Notes in Computer Science vol. 4887, Springer, 2007.

148. J. Garay, J. Katz, C.-Y. Koo, and R. Ostrovsky. "Round Complexity of Authenticated Broadcast with a Dishonest Majority." *Proc. 48th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 658–668, IEEE, 2007.

149. O. Horvitz and J. Katz. "Universally Composable Two-Party Computation in Two Rounds." *Advances in Cryptology—Crypto 2007*, pp. 111–129, Lecture Notes in Computer Science vol. 4622, Springer, 2007.

150. R. Morselli, B. Bhattacharjee, J. Katz, and M. Marsh. "Exploiting Approximate Transitivity of Trust" (invited paper). *4th Intl. Conf. on Broadband Communications, Networks, and Systems (BroadNets)*, pp. 515–524, IEEE, 2007.

151. J. Katz. "On Achieving the 'Best of Both Worlds' in Secure Multiparty Computation." *Proc. 39th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 11–20, ACM, 2007.

152. J. Katz. "Universally-Composable Multi-Party Computation using Tamper-Proof Hardware." *Advances in Cryptology—Eurocrypt 2007*, pp. 115–128, Lecture Notes in Computer Science vol. 4515, Springer, 2007.

153. J. Katz and C.-Y. Koo. "Round-Efficient Secure Computation in Point-to-Point Networks." *Advances in Cryptology—Eurocrypt 2007*, pp. 311–328, Lecture Notes in Computer Science vol. 4515, Springer, 2007.

154. C. Hazay, J. Katz, C.-Y. Koo, and Y. Lindell. "Concurrently-Secure Blind Signatures without Random Oracles or Setup Assumptions." *4th Theory of Cryptography Conference (TCC)*, pp. 323–341, Lecture Notes in Computer Science vol. 4391, Springer, 2007.

155. S.D. Gordon and J. Katz. "Rational Secret Sharing, Revisited." *Security and Cryptography for Networks (SCN)*, pp. 229–241, Lecture Notes in Computer Science vol. 4116, Springer, 2006. An extended abstract of this work also appeared at *NetEcon 2006*.

156. J. Katz and C.-Y. Koo. "On Expected Constant-Round Protocols for Byzantine Agreement." *Advances in Cryptology—Crypto 2006*, pp. 445–462, Lecture Notes in Computer Science vol. 4117, Springer, 2006.

157. Y. Dodis, J. Katz, L. Reyzin, and A. Smith. "Authenticated Key Agreement from 'Close' Secrets." *Advances in Cryptology—Crypto 2006*, pp. 232–250, Lecture Notes in Computer Science vol. 4117, Springer, 2006.

158. C.-Y. Koo, V. Bhandari, J. Katz, and N. Vadiya. "Reliable Broadcast in Radio Networks: The Bounded Collision Case." *Proc. 25th Annual ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 258–262, ACM, 2006.

159. J. Katz and J.S. Shin. "Parallel and Concurrent Security of the HB and HB$^+$ Protocols." *Advances in Cryptology—Eurocrypt 2006*, pp. 73–87, Lecture Notes in Computer Science vol. 4004, Springer, 2006.

160. A. Bender, J. Katz, and R. Morselli. "Ring Signatures: Stronger Definitions, and Constructions without Random Oracles." *3rd Theory of Cryptography Conference (TCC)*, pp. 60–79, Lecture Notes in Computer Science vol. 3876, Springer, 2006.

161. J. Katz and J.S. Shin. "Modeling Insider Attacks on Group Key-Exchange Protocols." *Proc. 12th ACM Conf. on Computer and Communications Security*, pp. 180–189, ACM, 2005.

162. O. Horvitz and J. Katz. "Lower Bounds on the Efficiency of 'Black-Box' Commitment Schemes." *International Colloquium on Automata, Languages, and Programming (ICALP)*, pp. 128–139, Lecture Notes in Computer Science vol. 3580, Springer, 2005. **Invited to a special issue of *Theoretical Computer Science*.**

163. J. Katz, P. MacKenzie, G. Taban, and V. Gligor. "Two-Server Password-Only Authenticated Key Exchange." *Applied Cryptography and Network Security (ACNS)*, pp. 1–16, Lecture Notes in Computer Science vol. 3531, Springer, 2005.

164. X. Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith. "Secure Remote Authentication Using Biometric Data." *Advances in Cryptology—Eurocrypt 2005*. pp. 147–163, Lecture Notes in Computer Science vol. 3494, Springer, 2005.

165. R. Canetti, S. Halevi, J. Katz, Y. Lindell, and P. MacKenzie. "Universally Composable Password-Based Key Exchange." *Advances in Cryptology—Eurocrypt 2005*, pp. 404–421, Lecture Notes in Computer Science vol. 3494, Springer, 2005.

166. I. Haitner, O. Horvitz, J. Katz, C.-Y. Koo, R. Morselli, and R. Shaltiel. "Reducing Complexity Assumptions for Statistically-Hiding Commitment." *Advances in Cryptology—Eurocrypt 2005*, pp. 58–77, Lecture Notes in Computer Science vol. 3494, Springer, 2005.

167. R. Canetti, S. Halevi, and J. Katz. "Adaptively-Secure, Non-Interactive Public-Key Encryption." *2nd Theory of Cryptography Conference (TCC)*, pp. 150–168, Lecture Notes in Computer Science vol. 3378, Springer, 2005.

168. J. Katz and Y. Lindell. "Handling Expected Polynomial-Time Strategies in Simulation Based Security Proofs." *2nd Theory of Cryptography Conference (TCC)*, pp. 128–149, Lecture Notes in Computer Science vol. 3378, Springer, 2005.

169. Y. Dodis and J. Katz. "Chosen-Ciphertext Security of Multiple Encryption." *2nd Theory of Cryptography Conference (TCC)*, pp. 188–209, Lecture Notes in Computer Science vol. 3378, Springer, 2005.

170. D. Boneh and J. Katz. "Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption." *RSA Conference—Cryptographers' Track*, pp. 87–103, Lecture Notes in Computer Science vol. 3376, Springer, 2005.

171. J. Katz, R. Ostrovsky, and M.O. Rabin. "Identity-Based Zero Knowledge." *Security in Communication Networks (SCN)*, pp. 180–192, Lecture Notes in Computer Science vol. 3352, Springer, 2004.

172. R. Morselli, J. Katz, and B. Bhattacharjee. "A Game-Theoretic Framework for Analyzing Trust-Inference Protocols." *Second Workshop on the Economics of Peer-to-Peer Systems*, Boston, MA, 2004.

173. J. Katz and R. Ostrovsky. "Round-Optimal Secure Two-Party Computation." *Advances in Cryptology—Crypto 2004*, pp. 335–354, Lecture Notes in Computer Science vol. 3152, Springer, 2004.

174. I.R. Jeong, J. Katz, D.H. Lee. "One-Round Protocols for Two-Party Authenticated Key Exchange." *Applied Cryptography and Network Security (ACNS)*, pp. 220–232, Lecture Notes in Computer Science vol. 3089, Springer, 2004.

175. R. Canetti, S. Halevi, and J. Katz. "Chosen-Ciphertext Security from Identity-Based Encryption." *Advances in Cryptology—Eurocrypt 2004*, pp. 207–222, Lecture Notes in Computer Science vol. 3027, Springer, 2004.

176. R. Morselli, B. Bhattacharjee, J. Katz, and P. Keleher. "Trust-Preserving Set Operations." *Proc. IEEE INFOCOM*, pp. 2231–2241, IEEE, 2004.

177. Y. Dodis, M. Franklin, J. Katz, A. Miyaji, and M. Yung. "A Generic Construction for Intrusion-Resilient Public-Key Encryption." *RSA Conference—Cryptographers' Track*, pp. 81–98, Lecture Notes in Computer Science vol. 2964, Springer, 2004.

178. J. Katz. "Binary Tree Encryption: Constructions and Applications" (invited paper). *6th Intl. Conference on Information Security and Cryptology (ICISC)*, pp. 1–11, Lecture Notes in Computer Science vol. 2971, Springer, 2003.

179. J. Katz and N. Wang. "Efficiency Improvements for Signature Schemes with Tight Security Reductions." *Proc. 10th ACM Conf. on Computer and Communications Security*, pp. 155–164, ACM, 2003.

180. J. Katz and M. Yung. "Scalable Protocols for Authenticated Group Key Exchange." *Advances in Cryptology—Crypto 2003*, pp. 110–125, Lecture Notes in Computer Science vol. 2729, Springer, 2003.

181. R. Gennaro, Y. Gertner, and J. Katz. "Lower Bounds on the Efficiency of Encryption and Digital Signature Schemes." *Proc. 35th Annual ACM Symposium on Theory of Computing (STOC)*, pp. 417–425, ACM, 2003.

182. J. Katz, R. Ostrovsky, and A. Smith. "Round Efficiency of Multi-Party Computation with Dishonest Majority." *Advances in Cryptology—Eurocrypt 2003*, pp. 578–595, Lecture Notes in Computer Science vol. 2656, Springer, 2003.

183. R. Canetti, S. Halevi, and J. Katz. "A Forward-Secure Public-Key Encryption Scheme." *Advances in Cryptology—Eurocrypt 2003*, pp. 255–272, Lecture Notes in Computer Science vol. 2656, Springer, 2003.

184. J. Katz. "Efficient and Non-Malleable Proofs of Plaintext Knowledge and Applications." *Advances in Cryptology—Eurocrypt 2003*, pp. 211–228, Lecture Notes in Computer Science vol. 2656, Springer, 2003.

185. A. Khalili, J. Katz, and W. Arbaugh. "Toward Secure Key Distribution in Truly Ad-Hoc Networks." *2003 Symposium on Applications and the Internet Workshops*, pp. 342–346, IEEE, 2003.

186. Y. Dodis, M. Franklin, J. Katz, A. Miyaji, and M. Yung. "Intrusion-Resilient Public-Key Encryption." *RSA Conference—Cryptographers' Track*, pp. 19–32, Lecture Notes in Computer Science vol. 2612, Springer, 2003.

187. Y. Dodis, J. Katz, S. Xu, and M. Yung. "Strong Key-Insulated Signature Schemes." *Public-Key Cryptography (PKC)*, pp. 130–144, Lecture Notes in Computer Science vol. 2567, Springer, 2003.

188. J. Katz, R. Ostrovsky, and M. Yung. "Forward Secrecy in Password-Only Key-Exchange Protocols." *Security in Communication Networks (SCN)*, pp. 29–44, Lecture Notes in Computer Science vol. 2576, Springer, 2002.

189. J. Katz and M. Yung. "Threshold Cryptosystems Based on Factoring." *Advances in Cryptology—Asiacrypt 2002*, pp. 192–205, Lecture Notes in Computer Science vol. 2501, Springer, 2002.

190. K. Jallad, J. Katz, and B. Schneier. "Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG." *Information Security Conference*, pp. 90–101, Lecture Notes in Computer Science vol. 2433, Springer, 2002.

191. Y. Dodis, J. Katz, S. Xu, and M. Yung. "Key-Insulated Public-Key Cryptosystems." *Advances in Cryptology—Eurocrypt 2002*, pp. 65–82, Lecture Notes in Computer Science vol. 2332, Springer, 2002.

192. E. Buonanno, J. Katz, and M. Yung. "Incremental and Unforgeable Encryption." *Fast Software Encryption (FSE)*, pp. 109–124, Lecture Notes in Computer Science vol. 2355, Springer, 2002.

193. J. Katz, R. Ostrovsky, and M. Yung. "Efficient Password-Authenticated Key-Exchange Using Human-Memorizable Passwords." *Advances in Cryptology—Eurocrypt 2001*, pp. 474–494, Lecture Notes in Computer Science vol. 2045, Springer, 2001.

194. J. Katz, R. Ostrovsky, and S. Myers. "Cryptographic Counters and Applications to Electronic Voting." *Advances in Cryptology—Eurocrypt 2001*, pp. 78–92, Lecture Notes in Computer Science vol. 2045, Springer, 2001.

195. G. Di Crescenzo, J. Katz, R. Ostrovsky, and A. Smith. "Efficient and Non-Interactive, Non-Malleable Commitment." *Advances in Cryptology—Eurocrypt 2001*, pp. 40–59, Lecture Notes in Computer Science vol. 2045, Springer, 2001.

196. J. Katz and B. Schneier. "A Chosen-Ciphertext Attack Against Several E-mail Encryption Protocols." *Proc. 9th USENIX Security Symposium*, pp. 241–246, USENIX, 2000.

197. J. Katz and M. Yung. "Unforgeable Encryption and Chosen-Ciphertext-Secure Modes of Operation." *Fast Software Encryption (FSE)*, pp. 284–299, Lecture Notes in Computer Science vol. 1978, Springer, 2001.

198. J. Katz and M. Yung. "Complete Characterization of Security Notions for Probabilistic, Private-Key Encryption." *Proc. 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pp. 245–254, ACM, 2000.

199. J. Katz and L. Trevisan. "On the Efficiency of Local Decoding Procedures for Error-Correcting Codes." *Proc. 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pp. 80–86, ACM, 2000.

Other

1. S. Schlesinger and J. Katz. "Anonymous Credit Tokens." Internet draft, August 2025.

2. P. Pfeiffenberger, J. Katz, and T. Olsauskas-Warren. "Probabilistic Reveal Tokens." Internet draft, July 2025.

3. M. Chase et al. "The Picnic Signature Scheme, v. 2.2." Submission to Round 2 of the NIST Post-Quantum Cryptography Standardization Effort, 2020.

4. S. Stevens et al. "Quantum Computing Risks to the Financial Services Industry." Informative Report (ASC X9 IR 01-2019), ANSI ASC X9 Quantum Computing Risk Study Group, 2019.

5. Mark Flood, Jonathan Katz, Stephen Ong, and Adam Smith. "Cryptography and the Economics of Supervisory Information: Balancing Transparency and Confidentiality." *Financial Stability Conference: Using the Tools, Finding the Data (2013).*

6. Rajesh Chitnis, MohammadTaghi Hajiaghayi, Jonathan Katz, and Koyel Mukherjee. "A Game-Theoretic Model Motivated by the DARPA Network Challenge." *SPAA*

2013 brief announcement. Also presented at the *Workshop on Risk Aversion in Algorithmic Game Theory and Mechanism Design, 2012.*

7. R. Morselli, B. Bhattacharjee, J. Katz, and M. Marsh, "KeyChains: A Decentralized Public-Key Infrastructure," Technical Report CS-TR-4788, University of Maryland Computer Science Department, March, 2006.

Patents/Patent Applications

- Dan Yadlin, Ben Riva, Alon Navon, Lev Pachmanov, and Jonathan Katz. Techniques for Single-Round Multi-Party Computation for Digital Signatures. US Patents 11,943,346 (Mar. 6, 2024), 11,632,244 (Apr. 14, 2023).
- Dan Yadlin, Ben Riva, Alon Navon, Lev Pachmanov, and Jonathan Katz. Techniques for Securing Digital Signatures Using Multi-Party Computation. US Patent 11,689,371 (June 27, 2023).
- Dan Yadlin, Ben Riva, Alon Navon, Lev Pachmanov, and Jonathan Katz. Techniques for Securing Application Programming Interface Requests using Multi-party Digital Signatures. US Patent 11,444,779 (Sept. 13, 2022).
- Chongwon Cho, Karim El Defrawy, Daniel C. Apon, and Jonathan Katz. Practical Reusable Fuzzy Extractor Based on the Learning-with-Error Assumption and Random Oracle. US Patent 11,101,991 (Aug. 24, 2021).
- Chongwon Cho, Karim El Defrawy, Daniel C. Apon, and Jonathan Katz. Reusable Fuzzy Extractor Based on the Learning-with-Error Assumption Secure Against Quantum Attacks. US Patent 10,778,423 (Sept. 15, 2020).
- Karim El Defrawy, Joshua W. Baron, and Jonathan Katz. Generic Pattern Matching System." US Patent 10,621,364 (Apr. 14, 2020).
- Karim El Defrawy, Chongwon Cho, Daniel C. Apon, and Jonathan Katz. Nonmalleable Obfuscator for Sparse Functions. US Patent 10,198,584 (Feb. 5, 2019).