Curriculum Vitae

CARL A. MILLER
National Institute of Standards and Technology
100 Bureau Dr.
Mail Stop 8930
Gaithersburg, MD 20899-8930
carl.miller@nist.gov
https://camiller.iacs.umd.edu

Employment:

National Institute of Standards and Technology
Mathematician, Computer Security Division (2016-present)

University of Maryland, College Park
Co-Director, Joint Center for Quantum Information and Computer Science (2025-present)
Fellow, Joint Center for Quantum Information and Computer Science (2016-present)
Adjunct Associate Professor in Computer Science and UMIACS (2020-present)
Adjunct Assistant Professor in Computer Science and UMIACS (2017-2020)

University of Michigan, Ann Arbor
Assistant Research Scientist in Computer Science (2013-2016)
Research Fellow in Computer Science (2010-2013)
Postdoc Assistant Professor of Mathematics (2007-2010)

Visiting position:

Research Fellow, Simons Institute for Theoretical Computer Science, Spring 2014

Education:

University of California-Berkeley
Ph.D. in Mathematics, 2007
Thesis title: *Cohomology of p-torsion sheaves on characteristic-p curves*
Thesis advisor: Arthur Ogus
Thesis committee members: Martin Olsson, Ori Ganor
Qualifying exam topics: algebraic geometry, commutative algebra, algebraic topology (minor)

Duke University
B.S. in Mathematics, magna cum laude, 2001. Graduated with highest distinction.

Thesis title: *Exponential iterated integrals and solvable completions of the fundamental group of a manifold*
Thesis advisor: Richard Hain

Awards:

2025 Cyber Policy Research Impact Award from the Institute for Security and Technology (awarded to the NIST Post-Quantum Cryptography team)
2025 NIST ITL Outstanding Conference Paper (for "Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model")
2021 NIST ITL Outstanding Conference Paper (for "The Impossibility of Efficient Quantum Weak Coin-Flipping")
2001 The Julia Dale Prize (top graduating math major at Duke University)
2001 "Outstanding" designation in COMAP Contest in Modeling
2001 National Defense Science & Engineering Graduate Fellowship
2000 Top 16 on William Lowell Putnam exam
2000 First Place, Virginia Tech Regional Mathematics Competition
1996 Top 8 on USA Math Olympiad and silver medal at International Math Olympiad

Citizenship:

USA

Research interests:

Quantum cryptography
Post-quantum cryptography
Quantum communication

Activities:

Program Committee Member for QIP 2026 (29th Conference on Quantum Information Processing), Riga, Latvia.

Scientific Lead for the MathQuantum RTG (Research Training Group) at the University of Maryland, College Park, 2023-Present.

Program Committee Member for QCRYPT 2023 (13th International Conference on Quantum Cryptography), College Park, MD.

Program Committee Member for QIP 2023 (26th Conference on Quantum Information Processing), Ghent, Belgium.

Program Committee Member for TQC 2022 (17th Conference on the Theory of Quantum Computation, Communication, and Cryptography), Urbana-Champaign, IL.

Program Chair for QCRYPT 2021 (11th International Conference on Quantum Cryptography), Amsterdam, The Netherlands.

Local Committee Member for TQC 2019 (14th Conference on the Theory of Quantum Computation, Communication, and Cryptography), College Park, MD.

Program Committee Member for QCRYPT 2018 (8th International Conference on Quantum Cryptography), Shanghai, China.

Team Member for the NIST Postquantum Cryptography Project, 2017 – Present.

Co-Leader of the Math Research Interaction Team Seminar on Quantum Information at the University of Maryland, 2016 – Present.

Committee Member for the UMD High School Mathematics Competition, 2016 – Present.

Program Committee Member for QCRYPT 2016 (6th International Conference on Quantum Cryptography), Washington, DC.

Program Committee Member for TQC 2016 (11th Conference on Theory of Quantum Computation, Communication and Cryptography), Freie Universitaet Berlin, Germany.

Scientific Organizer for TYQI 2016 (2nd International Workshop on Trustworthy Quantum Information), University of Science and Technology, Shanghai, China.

Program Committee Member for QIP 2016 (19th Conference on Quantum Information Processing), Banff Centre, Alberta, Canada.

Local Organizer for TYQI 2015 (1st International Workshop on Trustworthy Quantum Information), University of Michigan, Ann Arbor.

Co-Leader of the Seminar on Theory of Quantum Information Processing at University of Michigan, Ann Arbor, Winter 2011 – Winter 2015.

Refereed Conference Presentations:

SQuInT 2025 (Southwest Quantum Information and Technology)
Albuquerque, NM, USA, October 9-11, 2025
“Hidden-State Proofs of Quantumness.” C. Miller.
(Given virtually.)

QIP 2025 (the 28th Annual Conference on Quantum Information Processing)
Raleigh, NC, USA, February 24-28, 2025
"Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model."
K. Jackson, C. Miller, D. Wang.
(Speaker: Kelsey Jackson.)

EUROCRYPT 2024 (the 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques)
Zurich, Switzerland, May 26-30, 2024
"Evaluating the security of CRYSTALS-Dilithium in the quantum random oracle model."
K. Jackson, C. Miller, D. Wang.
(Speaker: Kelsey Jackson.)

QIP 2021 (the 24th Annual Conference on Quantum Information Processing)
Munich, Germany, February 1-5, 2021
"The membership problem of constant-sized quantum correlations is undecidable."
H. Fu, C. Miller, W. Slofstra.
(Given virtually. Speaker: Honghao Fu.)

STOC 2020 (the 52nd Annual ACM Symposium on Theory of Computing)
Chicago, IL, USA, June 22-26, 2020
"The Impossibility of Efficient Quantum Weak Coin Flipping." C. Miller.
(Given virtually.)

Short plenary talk at QIP 2020 (the 23rd Annual Conference on Quantum Information Processing)
Shenzhen, China, January 6-10, 2020
"The Impossibility of Efficient Quantum Weak Coin-Flipping." C. Miller.

QCRYPT 2019 (the 9th International Conference on Quantum Cryptography)
Montreal, Canada, August 26-30, 2019
"Efficient randomness certification by quantum probability estimation." Y. Zhang, et al.
(Speaker: Yanbao Zhang.)

QCRYPT 2018 (the 8th International Conference on Quantum Cryptography)
Shanghai, China, August 27-31, 2018
"Parallel Device-Independent Quantum Key Distribution." R. Jain, C. Miller, Y. Shi.
(Speaker: Rahul Jain.)

QPL 2018 (the 15th International Conference on Quantum Physics and Logic)
Dalhousie University, Halifax, Canada, June 3-7, 2018
"Three Party Quantum Self-Testing with a Proof by Diagrams." S. Breiner, A. Kalev, C. Miller.

QCRYPT 2017 (the 7th International Conference on Quantum Cryptography),
University of Cambridge, England, September 18-22, 2017.

"Randomness in nonlocal games between mistrustful players." H. Fu, C. Miller, Y. Shi. (Speaker: Honghao Fu.)

QIP 2015 (the 18th Conference on Quantum Information Processing)
Sydney, Australia, January 12-16, 2015.
"Universal security for randomness expansion." C. Miller, Y. Shi.

STOC 2014 (the 46th Annual ACM Symposium on Theory of Computing)
New York City, NY, USA, May 31-June 3, 2014.
"Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices." C. Miller, Y. Shi.

Plenary talk at QIP 2014 (the 17th Conference on Quantum Information Processing)
Barcelona, Spain, February 3-7, 2014.
"Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices." C. Miller, Y. Shi.
(Merged with work by K. Chung, Y. Shi, and X. Wu.)

TQC 2013 (8th Conference on Theory of Quantum Computation, Communication, and Cryptography)
University of Guelph, Canada, May 21-23, 2013.
"Optimal robust self-testing by binary nonlocal XOR games." C. Miller, Y. Shi.

Invited Talks:

Quantum Meets Colloquium, June 3, 2026. (Given virtually.)

Montgomery College, Germantown, MD, September 11, 2025.

Topos Institute Colloquium, November 8, 2024. (Given virtually.)

Distributed Quantum Computing and Cryptography Workshop, Virginia Tech Research Center, Arlington, VA, June 11, 2024.

Zebra Technologies Privacy and Security Summit, October 24, 2023. (Given virtually.)

CISCO Quantum and Photonics Research Seminar, April 8, 2022. (Given virtually.)

Duke University, Department of Mathematics Seminar, December 11, 2020. (Given virtually.)

Computing Colloquium at Boise State University, September 24, 2020. (Given virtually.)

Colloquium at Institute for Quantum Computing, University of Waterloo, June 29, 2020. (Given virtually.)

TYQI 2017 (3rd International Workshop on Trustworthy Quantum Information), Universitie Pierre et Marie Curie, June 19, 2017.

CalTech, Institute for Quantum Information, March 14, 2017.

Institute for Quantum Computing and Department of Combinatorics & Optimization, University of Waterloo, March 9 & 10, 2016.

Joint Center for Quantum Information and Computer Science, University of Maryland, January 27, 2016.

Workshop on Quantum Nonlocality, Causal Structures and Device-Independent Quantum Information, National Cheng Kung University, Taiwan, December 14, 2015.

Workshop on the Foundations of Randomness, Stellenbosch Institute, Cape Town, South Africa, October 27, 2015.

QCRYPT 2015 (5th International Conference on Quantum Cryptography), Tokyo, Japan, October 2, 2015.

CalTech, Institute for Quantum Information, July 22, 2014.

University of Guelph, Canadian Quantum Summer School, June 18, 2014
(with Yaoyun Shi).

Colloquium at Institute for Quantum Computing, University of Waterloo, June 16, 2014.

Workshop on Quantum Games and Protocols, Simons Institute for Theoretical Computer Science, February 26, 2014.

University of Southern California, Dept. of Electrical Engineering, April 13, 2013.

University of Illinois, Chicago, Applied Mathematics Seminar, February 13, 2013.

Perimeter Institute for Theoretical Physics, November 7, 2012.

Tsinghua University, Institute for Interdisciplinary Information Sciences, September 6, 2012.

Multimedia:

Quantum Choreographies (filmed dance piece), presented at Quantum World Congress, September 17-19, 2025, in Tysons, VA. Jonathan David Martin, Carl A. Miller, Adriane

Fang, Samuel Crawford, Timothy Kelly, Mark Sherwood.

Publications:

Honghao Fu, Carl A. Miller, and William Slofstra. The Membership Problem for Constant-Sized Quantum Correlations is Undecidable. *Communications in Mathematical Physics* 406, no. 96 (2025).

Yusuf Alnawakhtha, Atul Mantri, Carl A. Miller, and Daochen Wang. Lattice-Based Quantum Advantage from Rotated Measurements. *Quantum* 8, 1399 (2024).

Kelsey A. Jackson, Carl A. Miller, and Daochen Wang. Evaluating the Security of CRYSTALS-Dilithium in the Quantum Random Oracle Model. *Advances in Cryptology – EUROCRYPT 2024*, pp. 418-446. Lecture Notes in Computer Science, vol 14656 (2024).

Carl A. Miller. The Mathematics of Quantum Coin-Flipping. *Notices of the American Mathematical Society* 69, no. 11, pp. 1908-1917 (2022).

Yusuf Alnawakhtha and Carl A. Miller. Where we are with quantum. *Nature Physics* 18, pp. 611–612 (2022).

Rahul Jain, Carl A. Miller, and Yaoyun Shi. Parallel Device-Independent Quantum Key Distribution. *IEEE Transactions on Information Theory* 66, no. 9, pp. 5567-5584 (2020).

Carl A. Miller. The impossibility of efficient quantum weak coin flipping. *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC '20)*, pp. 916-929 (2020).

Yanbao Zhang, et al. Experimental Low-Latency Device-Independent Quantum Randomness. *Physical Review Letters* 124, 010505 (2020).

Spencer Breiner, Carl A. Miller, and Neil J. Ross. Graphical Methods in Device-Independent Quantum Cryptography. *Quantum* 3, 146 (2019).

Spencer Breiner, Amir Kalev, and Carl A. Miller. Parallel Self-Testing of the GHZ State with a Proof by Diagrams. *Proceedings of the 15th International Conference on Quantum Physics and Logic (QPL 2018),* Electronic Proceedings in Theoretical Computer Science 287, pp. 43-66.

Honghao Fu, Carl A. Miller. Local randomness: Examples and application. *Physical Review A* 97, 032324 (2018).

Carl A. Miller, Roger Colbeck, and Yaoyun Shi. Keyring models: an approach to steerability. *Journal of Mathematical Physics* 59, 022103 (2018).

Amir Kalev, Carl A. Miller. Rigidity of the magic pentagram game. *Quantum Science and Technology* 3, No. 1, 015002 (2018).

Carl A. Miller, Yaoyun Shi. Universal Security for Randomness Expansion from the Spot-Checking Protocol. *SIAM Journal on Computing* 46, No. 4, pp. 1304-1335 (2017).

Carl A. Miller, Yaoyun Shi. Randomness in nonlocal games between mistrustful players. *Quantum Information and Computation*, Vol. 17, No. 7&8, pp. 0595-0610 (2017).

Carl A. Miller, Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices.
Journal of the ACM, Vol. 63, Issue 4, Article No. 33 (2016).
Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC '14), pp. 417-426 (2014).

Carl A. Miller. Evasiveness of Graph Properties and Topological Fixed-Point Theorems. *Foundations and Trends in Theoretical Computer Science*, volume 7, issue 4 (2013).

Carl A. Miller, Yaoyun Shi. Optimal robust quantum self-testing by binary nonlocal XOR games. *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*, vol. 22, 254-262 (2013).

Brett Hemenway, Carl A. Miller, Yaoyun Shi, and Mary Wootters. Optimal entanglement-assisted one-shot classical communication. *Physical Review A* 87, 062301 (2013).

Eric Chitambar, Carl A. Miller, and Yaoyun Shi. Deciding Unitary Equivalence Between Matrix Polynomials and Sets of Bipartite Quantum States. *Quantum Information and Computation 11*, no. 9&10, 0813-0819 (2011).

Eric Chitambar, Carl A. Miller, and Yaoyun Shi. Matrix Pencils and Entanglement Classification. *Journal of Mathematical Physics* 51, 072205 (2010).

Carl A. Miller. An Euler-Poincare bound for equicharacteristic etale sheaves. *Algebra & Number Theory* 4, no. 1, 21-45 (2010).

Carl Miller. Exponential iterated integrals and the relative solvable completion of the fundamental group of a manifold. *Topology* 44, no. 2, 351-373 (2005).

NIST Reports and Standards:

Gorjan Alagic, Maxime Bros, Pierre Ciadoux, Quynh Dang, Thinh Hung Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, Noah Waller. Status

Report on the Second Round of the Additional Digital Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8610. May 2026.

Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Yi-Kai Liu, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, Noah Waller. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Project Standardization Process. NISTIR 8545. March 2025.

Gorjan Alagic, Maxime Bros, Pierre Ciadoux, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Angela Robinson, Hamilton Silberg, Daniel Smith-Tone, Noah Waller. Status Report on the First Round of the Additional Signature Schemes for the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8528. October 2024.

National Institute of Standards and Technology. Module-Lattice-Based Digital Signature Standard. FIPS 204. August 2024.

Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey, Jacob Lichtinger, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, Yi-Kai Liu. Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8413. July 2022.

David Cooper, Daniel Apon, Quynh Dang, Michael Davidson, Morris Dworkin, Carl Miller. Recommendation for Stateful Hash-Based Signature Schemes. NIST SP 800-208. October 2020.

Dustin Moody, Gorjan Alagic, Daniel C. Apon, David A. Cooper, Quynh H. Dang, John M. Kelsey, Yi-Kai Liu, Carl A. Miller, Rene C. Peralta, Ray A. Perlner, Angela Y. Robinson, Daniel C. Smith-Tone, Jacob Alperin-Sheriff. Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8309, July 22, 2020.

Gorjan Alagic, Jacob M. Alperin-Sheriff, Daniel Apon, David Cooper, Quynh H. Dang, Carl Miller, Dustin Moody, Rene Peralta, Ray Perlner, Angela Robinson, Daniel Smith-Tone, Yi-Kai Liu. Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process. NISTIR 8240, January 31, 2019.

Grants:

Army Research Office and National Security Agency. "Quantum Algorithms for Algebra and Discrete Optimization." Co-PI. January 15, 2020 – January 14, 2023. $743,000.

NSF STARSS: TTP. "A Quantum Approach to Hardware Security: from Theory to Optical Implementation." Co-PI. September 1, 2015 – August 31, 2018. $388,333.

NSF PFI: AIR-TT. "Prototyping Untrusted-Device Quantum Cryptography." Co-PI. April 1, 2015 – March 31, 2016. $211,924.

NSF I-Corps Program. "Practical and Provably Secure Random Number Generator." Entreprenurial Lead. Dec. 1, 2014 – May 31, 2015. $50,000.

Teaching Experience:

Courses taught at the University of Michigan:
EECS 203, **Discrete Mathematics**, fall 2013.
EECS 376, **Foundations of Computer Science**, winter 2010.
Math 312, **Applied Modern Algebra**, fall 2009.
Math 567, **Introduction to Coding Theory**, winter 2009.
Math 425, **Introduction to Probability**, fall 2008.
Math 217, **Linear Algebra**, winter 2008.
Math 115, **Calculus I**, fall 2007.

Teaching assistant at UC-Berkeley for four semesters (2005-2006).

Undergraduate seminar leader for Math 149S (Problem-Solving Seminar) at Duke, fall 1998 and fall 1999.

Counselor at the Ross Young Scholars Program at Ohio State University, summer 1998 and summer 1999.

Other Employment:

Participated in the SCAMP summer program at the Center for Communications Research in Princeton, NJ, summer 2002.

Worked on voice-recognition software at the Duke University Computer Science Department under Prof. Alan Biermann during the summer of 2001.

Participated in the PRUV Program at Duke University (under Prof. Richard Hain) and the Discrete Random Structures REU at East Tennessee State University (under Prof. Anant Godbole), summer 2000.