Daniel S. Roche

Last updated April 2022

Contact

United States Naval Academy
Computer Science Department
597 McNair Rd
Annapolis, MD 21402

Office: 438 Hopper Hall
+1 (410) 293-6814
Email: roche@usna.edu
Web: https://roche.work/

Employment

United States Naval Academy, Annapolis, MD, USA.
Professor, Computer Science Department, Fall 2022–present.
Associate Professor, Computer Science Department, Fall 2016–Spring 2022.
Assistant Professor, Computer Science Department. Fall 2011–Spring 2016.

Education

University of Waterloo, Waterloo, ON, Canada. Degree conferred June 2011.
Ph.D., Computer Science
Thesis: Efficient Computation with Sparse and Dense Polynomials

- Supervisors: Mark Giesbrecht and Arne Storjohann

University of Delaware, Newark, DE, USA. Degrees conferred May 2006.
B.S., Computer and Information Sciences
B.S., Mathematical Sciences
B.Music, Applied Music Instrumental, Tuba

Significant Funding and Awards

Plenary Speaker at ACM ISSAC 2024.

ACM ISSAC Distinguished Paper Award. For "Sparse Polynomial Interpolation and Division in Soft-linear Time" with Pascal Giorgi, Bruno Grenet, and Armelle Perret du Cray, 2022.

Office of Naval Research Grant. "New Oblivious Algorithms for Practical Applications", 2019-2022.

National Science Foundation Award, Secure and Trustworthy Cyberspace (SaTC). Award #1618269: "Achieving Practical Privacy for the Cloud", 2016–2020.

Apgar Award for Excellence in Teaching, USNA, March 2016.

Office of Naval Research, UMBC-USNA Cyber Innovation Grants. Co-PI, 2015–2018. "Ensuring Secure Cloud Services using Policy Based Approaches".

National Science Foundation Award, Computing and Communication Foundations (CCF), Algorithmic Foundations (AF). Principal Investigator, 2013–2016.
Award #1319994: "Faster Arithmetic for Sparse Polynomials and Integers".

NSERC Vanier Canada Graduate Scholarship, Spring 2009–Winter 2011.

Selected Publications

Pascal Giorgi, Bruno Grenet, Armelle Perret du Cray, and Daniel S. Roche. **Fast interpolation and multiplication of unbalanced polynomials**. *International Symposium on Symbolic and Algebraic Computation* (ACM ISSAC) 2024, to appear.

Pascal Giorgi, Bruno Grenet, Armelle Perret du Cray, and Daniel S. Roche. **Random primes without primality testing**. *International Symposium on Symbolic and Algebraic Computation* (ACM ISSAC) 2022, pp. 207–215.

Pascal Giorgi, Bruno Grenet, Armelle Perret du Cray, and Daniel S. Roche. **Sparse Polynomial Interpolation and Division in Soft-linear Time**. *International Symposium on Symbolic and Algebraic Computation* (ACM ISSAC) 2022, pp. 459–468.

Linsheng Liu, Daniel S. Roche, Austin Theriault, and Arkady Yerukhimovich. **Fighting Fake News in Encrypted Messaging with the Fuzzy Anonymous Complaint Tally System (FACTS)**. *Network and Distributed System Security Symposium* (NDSS) 2022.

David Lucas, Vincent Neiger, Clément Pernet, Daniel S. Roche, and Johan Rosenkilde. **Verification protocols with sub-linear communication for polynomial matrix operations**. *Journal of Symbolic Computation* 105, 2021, pp. 165–198.

Ian Martiny, Gabriel Kaptchuk, Adam J. Aviv, Daniel S. Roche, and Eric Wustrow: **Improving Signal's Sealed Sender**. *Network and Distributed System Security Symposium* (NDSS) 2021.

Gaspard Anthoine, Jean-Guillaume Dumas, Mélanie de Jonghe, Aude Maignan, Clément Pernet, Michael Hanling, and Daniel S. Roche. **Dynamic proofs of retrievability with low server storage**. USENIX Security Symposium, 2021, pp. 537–554.

Pascal Giorgi, Bruno Grenet, and Daniel S. Roche. **Fast in-place algorithms for polynomial operations: division, evaluation, interpolation**. *International Symposium on Symbolic and Algebraic Computation* (ACM ISSAC) 2020, pp. 210-217.

Anrin Chakraborti, Adam J. Aviv, Seung Geol Choi, Travis Mayberry, Daniel S. Roche, and Radu Sion. **rORAM: Efficient Range ORAM with O(log2 N) Locality**. *Network and Distributed System Security Symposium* (NDSS) 2019.

Claude-Pierre Jeannerod, Théo Mary, Clément Pernet, and Daniel S. Roche. **Improving the Complexity of Block Low-Rank Factorizations with Fast Matrix Arithmetic**. *SIAM J. Matrix Anal. Appl.* 40(4), 2019, pp. 1478–1496.

Jean-Guillaume Dumas, Joris van der Hoeven, Clément Pernet, and Daniel S. Roche. **LU Factorization with Errors**. *International Symposium on Symbolic and Algebraic Computation* (ACM ISSAC) 2019, pp. 131–138.

Pierre Karpman and Daniel S. Roche. **New Instantiations of the CRYPTO 2017 Masking Schemes**. ASIACRYPT 2018, pp. 285–314.

Daniel S. Roche, Adam J. Aviv, Seung Geol Choi, and Travis Mayberry.
Deterministic, Stash-Free, Write-Only ORAM. *ACM Conference on Computer and Communications Security* (ACM CCS) 2017, pp. 507–521.

Adam J. Aviv, Seung Geol Choi, Travis Mayberry, and Daniel S. Roche.
ObliviSync: Practical Oblivious File Backup and Synchronization.
Network and Distributed System Security Symposium (NDSS) 2017.

Daniel S. Roche, Daniel Apon, Seung Geol Choi, and Arkady Yerukhimovich.
POPE: Partial Order-Preserving Encoding, ACM CCS 2016, pp. 1131–1142.

A. Whitman Groves and Daniel S. Roche. **Sparse Polynomials in FLINT**.
ISSAC 2016 Software Presentations.
Appears in *ACM Communications in Computer Algebra*, Vol. 50, Issue 3, Sept. 2016.

Andrew Arnold, Mark Giesbrecht, and Daniel S. Roche.
Faster sparse multivariate polynomial interpolation of straight-line programs.
Journal of Symbolic Computation, Vol. 75, Jul.-Aug. 2016, pp. 4–24.

Daniel S. Roche, Adam J. Aviv, and Seung Geol Choi. **A Practical Oblivious Map Data Structure with Secure Deletion and History Independence**.
IEEE Symposium on Security and Privacy (S&P) 2016, pp. 178–197.

Mohamed Khochtali, Daniel S. Roche, and Xisen Tian. **Parallel sparse interpolation using small primes**. *Parallel Symbolic Computation* (PASCO) 2015, pp. 70–77.

Andrew Arnold and Daniel S. Roche. **Output-sensitive algorithms for sumset and sparse polynomial multiplication**. *International Symposium on Symbolic and Algebraic Computation* (ACM ISSAC) 2015, pp. 29–36.

Andrew Arnold and Daniel S. Roche. **Multivariate sparse interpolation using randomized Kronecker substitutions**. ACM ISSAC 2014, pp. 35–42.

Andrew Arnold, Mark Giesbrecht, and Daniel S. Roche. **Faster sparse polynomial interpolation of straight-line programs over finite fields**. ACM ISSAC 2014, pp. 27–34.

Mark Giesbrecht, Daniel S. Roche, and Hrushikesh Tilak.
Computing sparse multiples of polynomials.
Algorithmica, Vol. 64, No. 3, Nov. 2012, pp. 454–480.

Mark Giesbrecht and Daniel S. Roche.
Detecting lacunary perfect powers and computing their roots
Journal of Symbolic Computation, Vol. 46, Issue 11, Nov. 2011, pp. 1242–1259.

Mark Giesbrecht and Daniel S. Roche. **Diversification improves interpolation**. ACM ISSAC 2011, pp. 123–130.

Daniel S. Roche. **Chunky and Equal-Spaced Polynomial Multiplication**.
Journal of Symbolic Computation, Vol. 46, Issue 7, Jul. 2011, pp. 791–806.

Mark Giesbrecht and Daniel S. Roche.
Complexity of Shifted-Lacunary Polynomial Interpolation
Computational Complexity, Vol. 19 No. 3, 2010, pp. 333–354.

David Harvey and Daniel S. Roche. **An in-place truncated Fourier transform and applications to polynomial multiplication**. ACM ISSAC,, 2010, pp. 325–329.

Daniel S. Roche. **Space- and Time-Efficient Polynomial Multiplication**.
ACM ISSAC, 2009.

Selected Teaching

Course designer and instructor

- SD 212: Data Science & Programming II (2023–2024)
- SI 486I: Randomized and Blockchain Technology (2022)
- SI 486H: Randomness and Computing (2016, 2013)
- SI 485J: Computer Algebra and C++ Template Programming (2014)

Course coordinator and instructor

- SI 413: Programming Languages and Implementation (2023, 2021, 2018, 2011–2013)
- IC 312: Data Structures (2022, 2014–2015)
- SI 335: Computer Algorithms (2021, 2012–2016)
- IC 210: Introduction to Computing (2020)
- SI 204: Introduction to Computer Science (2017)
- SY 301: Data Structures for Cyber Operations (2016)

Service and other activities

ACM Special Interest Group on Symbolic and Algebraic Manipulation (SIGSAM), treasurer (2018–2021); acting vice chair (2024–).

ACM ISSAC, steering committee (2015–2018), program committee (2016, 2021, 2024), treasurer (2013), poster committee (2011).

Privacy Enhancing Technologies (PETS), program committee, 2019–2022.

PASCO, publicity chair (2015).

SYNASC, program committee (2013–2021).

National Science Foundation, panelist (multiple years).

ECCAD, organizer (2011, 2012), general chair (2013).

Referee for ANTS, CASC, FOCS, ISAAC, ISSAC, JACM, J. Complexity, JSC, MICA, PASCO, SNC, SODA, STACS, TCS