Jonathan Adam Poritz
Curriculum Vitæ

Office Address:
Department of Mathematics and Physics
Colorado State University–Pueblo
2200 Bonforte Blvd.
Pueblo, CO 81001-4901
USA

Home Address:
635 E. Boulder Street
Colorado Springs, CO 80903
USA
+1 (719) 337-1210
WEB: www.poritz.net/jonathan
TWITTER: @poritzj

EDUCATION:

University of Chicago (1986–1992)
Ph.D. in Mathematics, 1992
THESIS: *The moduli space of stable vector bundles over a punctured Riemann surface*
THESIS ADVISOR: Karen K. Uhlenbeck
S.M. in Mathematics, 1987

Harvard University (1981–1985)
Honors A.B. in Mathematics, 1985
THESIS ADVISOR: Raoul Bott

ACADEMIC EXPERIENCE:

Fall 2006- -present: Colorado State University–Pueblo, CO, USA
Associate Professor, Department of Mathematics and Physics
Data Analyst, Center for Teaching and Learning
Courses: College Algebra, Precalculus, Calculus I and II, Real Analysis, Complex Analysis, Statistics, Number Theory and Cryptology, Vectors and Matrices, Linear Algebra, Math Explorations, Mathematical Programming, Algorithms and Data Structures, Think Like a Greek [seminar on history, philosophy, and math of the Hellenistic Age], Higher Geometry, Topology, Introduction to Cryptography [short course for "Cyber-defense Certificate" program]
Service: faculty senator, 2013-15; senate vice-president, 2014/15; faculty handbook committee co-chair, 2013/14; information technology board member and chair, 2013-16; organized department research seminar; honors program oversight committee; CSU-Pueblo AAUP chapter vice-president
Supervision: several student research projects and independent studies, including fractal geometry, computational linear algebra, bioinformatics, and cryptology

2016: Reykjavik University ["Háskólinn í Reykjavík"], Reykjavik, Iceland
Visiting Instructor, School of Computer Science
Course: Cryptocurrencies [three-week, intensive, masters-level course]

2006: University of Colorado at Colorado Springs, CO, USA
Lecturer, Department of Mathematics
Courses: Statistics for the Sciences, Calculus for Business and Economics

2002–2004: Swiss Federal Institute of Technology ["Eidgenössische Technische Hochschule"], Zürich, Switzerland
Visiting Instructor, Department of Computer Science
Course: Introduction to Quantum Computation (offered twice)

1997–2000: Georgetown University, Washington, DC, USA
Visiting Assistant Professor, Department of Mathematics
Courses: Calculus I and II, Undergraduate Differential Geometry, Probability and Statistics
Supervision: student programming project, funded by the National Science Foundation, developing **Java** software to visualize 3-dimensional hyperbolic geometry, exploring and analyzing fundamental domains of cyclic groups

1993–1997: University of Maryland, College Park, MD, USA
Lecturer, Department of Mathematics
Courses: Graduate Topics in Geometry, Linear Algebra, Complex Analysis, Ordinary Differential Equations, Calculus III, Mathematical Modelling for Non-scientists

1992–1993: Institute for Advanced Study, Princeton, NJ, USA
Member, School of Mathematics

SCHOLARLY ACTIVITY:

Citation counts, where computable from *Google Scholar* as of 23 May 2017, appear as "{n}" [total: 529].

Refereed Publications:

[1] *Open Access to Technology: Shared Governance of the Academy's Virtual Worlds*, **J. Acad. Freedom**, Vol. 5 (2014)

[2] *Universal Gates in Other Universes*, **Springer Lecture Notes in Computer Science**, Vol. 7948, 5^{th} *Conference on Reversible Computation*, (2013), Pp. 155-167

[3] *On entropy-preserving stochastic averages*, with Alan Poritz, **Lin. Alg. Appl.**, Vol. 434, No. 6 (2010), Pp. 1425-1443 {10}

[4] *Who searches the searchers?: community privacy in the age of monolithic search engines*, **The Information Society**, Vol. 23, No. 5 (2007), Pp. 383-389 {13}

[5] *Intrusion-Tolerant Middleware: The Road to Automatic Security*, with Christian Cachin, Yves Deswarte, Nuno Neves, David Powell, Robert Stroud, Paulo Verissimo and Ian Welch, **IEEE Security&Privacy**, Vol. 4 (2006), Pp. 54-62 {99}

[6] *Trust[ed| in] computing, signed code and the heat death of the Internet*, **Proc. 2006 ACM Symp. Applied Computing "ACM SAC06"** (2006), Pp. 1855-1859 {16}

[7] *Secure intrusion-tolerant replication on the Internet*, with Christian Cachin, **Proc. Intl. Conf. Dependable Systems and Networks "DSN-2002"** (2002), Pp. 167-176 {133}

[8] *Social preferences and price cap regulation*, with Alberto Iozzi and Edilio Valentini, **J. Public Economic** Th., Vol. 4 (2002), Pp. 93-112 {25}

[9] *Around polygons in* $\mathbb{R}^3$ *and* S^3, with John Millson, **Comm. Math. Phys.**, Vol. 218 (2001), Pp. 315-331 {5}

[10] *The moduli space of boundary compactifications of* $SL(2)$, with Alessandra Iozzi, **Geom. Dedicata**, Vol. 76, No. 1 (1999), Pp. 65-79 {5}

[11] *Boundary compactifications of* $SL(2,\mathbb{R})$ *and* $SL(2,\mathbb{C})$, with Alessandra Iozzi, **Forum Math.**, Vol. 11, No. 3 (1999), Pp. 385-397 {4}

[12] *Ford and Dirichlet domains for cyclic subgroups of* $PSL(2,\mathbb{C})$ *acting on* $H^3_{\mathbb{R}}$ *and* $\partial H^3_{\mathbb{R}}$, with Todd Drumm, **Conform. Geom. Dynam.**, Vol. 3 (1999), Pp. 116-150, available in interactive on-line form at `http://www.ams.org/jourcgi/amsjournal?fn=120&pg1=pii&s1=S1088-4173-99-00042-9` {16}

[13] *Parabolic vector bundles and Hermitian-Yang-Mills connections over a Riemann surface*, **Internat. J. Math.**, Vol. 4, No. 3 (1993), Pp. 467-501 {24}

Expository (Non-refereed) Publications:

[A] *Academic Governance on the Virtual Shop Floor*, with Jonathan Rees, **Academe: Magazine of the AAUP**, May/June, 2017

[B] *Lies, Damned Lies, or Statistics: How to Tell the Truth with Statistics*, undergraduate textbook released under a Creative Commons **BY-SA 4.0** license, `poritz.net/jonathan/share/ldlos`, May, 2017.

[C] *The Tenured IT Expert? Technology experts should have the academic freedom to speak on behalf of what's best for education, not just a university's bottom line.*, with Jonathan Rees, in **Inside Higher Ed**, 20 September 2016.

[D] *Education is Not an App: The Future of University Teaching in the Internet Age*, with Jonathan Rees, **Routledge**, London, UK, 2016.

[E] *Yet Another Introductory Number Theory Textbook*, undergraduate textbook released under a Creative Commons **BY-SA 4.0** license, `poritz.net/jonathan/share/yaintt`, March, 2014.

[F] *Information Technology Wants to Be Free*, **Academe: Magazine of the AAUP**, Sept./Oct., 2012 {4}

[G] *Hash woes*, with Morton Swimmer, **Virus Bulletin**, Oct., 2004

[H] *Property attestation–scalable and privacy-friendly security assessment of peer computers*, with Matthias Schunter, Els Van Herreweghen and Michael Waidner, **IBM Research Report RZ3548** (2004) {167}

[I] *Alternative computational devices and architectures*, with Giovanni Cherubini, Heike Riel and Gian Salis, [confidential] **IBM Research Report** (2003)

[J] *Full Design of Dependable Third Party Services*, with Christian Cachin (editor), and Klaus Kursawe, **Deliverable D5, Project MAFTIA IST-1999-11583**, 2002 {4}

[K] *First specification of APIs and protocols for the MAFTIA middleware*, with Nuno Ferreira Neves and Paulo Verissimo (editors), *et al.*, **Deliverable D24, Project MAFTIA IST-1999-11583**, 2001 {4}

[L] *Specification of dependable trusted third parties*, with Christian Cachin (editor), *et al.*, **Deliverable D26, Project MAFTIA IST-1999-11583**, 2001

Patents [owned by IBM, on which I am a co-inventor]:

[I] *Method and device for verifying the security of a computing platform*, with Matthias Schunter, Elsie Van Herreweghen and Michael Waidner, US Patent No. 7770000, issued August 3, 2010

[II] *Attestation of computing platforms*, with Jan Camenisch and Roger Zimmermann; under review by USPTO, see Pub. No. US 2009/0271616; follows European Patent Office application No. WO2008026086, 2008

[III] *Method and system to authenticate an application in a computing platform operating in Trusted Computing Group (TCG) domain*, with Bernhard Jansen, Luke J. O'Connor, and Elsie Van Herreweghen; under review by USPTO, see Pub. No. 2008/0288783; follows European Patent Office application No. 06126246.5, 2006

SCHOLARLY ACTIVITY (continued):

Fellowships, Prizes and Grants:

*CC*DNI Campus Networking Upgrade, NSF grant 1541373*

- $306,663 was awarded to CSU-Pueblo to upgrade campus bandwidth, partly on the strength of my research proposals and courses I will team-teach remotely, via video classroom

High Performance Computing Infrastructure for Science & Engineering Research Projects, CNS-0923386

- $627,326 awarded to CSU-Ft Collins with CSU-Pueblo as junior partner; hardware is located in Ft Collins
- contributed one of the NSF-recognized scientific proposals in the grant application
- acting as an ongoing liaison between campuses by attending management meetings in Ft Collins and bringing information to Pueblo HPC researchers, supported in part by a CSU-Pueblo faculty development grant

Pikes Peak Regional Undergraduate Mathematics Conference 2010

- PI on Mathematical Association of America grant, funds from National Science Foundation grant DMS-0846477
- co-PI with Drs Barnett and Funk-Neubauer on Mathematical Association of American Section Activity Grant from the Rocky Mountain Section

Non-traditional project proposal on "Developing and proselytizing security-aware software engineering, practices," with Moishe Rappoport, chosen as an IBM Zurich Research Laboratory internal Innovations Contest winner, 2004.

Distributing trust on the Internet – SINTRA project, with Christian Cachin, Klaus Kursawe and Victor Shoup, judged an "IBM Research Division Technical Accomplishment" for 2003

National Science Foundation Research Grant DMS-9806408 in the Mathematics of Computation and Topology/Foundations for 1998–2001

National Science Foundation Research Grant DMS-9403784 in Geometric Analysis for 1994–1996

Presentations (Selections):

Domains 2017: Indie EdTech and Other Curiosities, June 2017

AAUP Colorado Conference Symposium on Academic Freedom, April 2017

AAUP Shared Governance Conference and Workshops, October 2016

"Fearless Friday" Undergraduate Mathematics Seminar, Colorado College, Colorado Springs, December 2013

5^{th} Conference on Reversible Computation, July 2013

AAUP Shared Governance Conference and Workshops, October 2012

Mathematical Association of America Rocky Mountain Section Meeting, April 2010

Mathematical Association of America Rocky Mountain Section Meeting, April 2007

"Slow Pitch" Undergraduate Mathematics Colloquium, University of Colorado at Boulder, December 2006

Mathematics Department Colloquium, University of Colorado, Colorado Springs, November 2006

"Fearless Friday" Undergraduate Mathematics Seminar, Colorado College, Colorado Springs, October 2006

Graduate Seminar, University of Denver, September 2006

2^{nd} ACM Symposium on Applied Computing TRECK Track, April 2006

Mathematics Department Colloquium, University of Colorado, Colorado Springs, January 2006

Special Session on Holomorphic Vector Bundles and Complex Geometry, American Mathematical Society Central Section Meeting, March 1999

Barrett Lectures Conference on Discrete Conformal Geometry, University of Tennessee at Knoxville, June 1998

Workshop on Complex Differential Geometry, Mathematics Institute, University of Warwick, July 1997

R51 Colloquium, National Security Agency, July 1997

Special Session on Vector Bundles with or without Extra Structure, American Mathematical Society Eastern Section Meeting, October 1996

First Brazil/USA Workshop on Geometry, Topology and Mathematical Physics, Campinas, Brazil, July 1996

Relativity and Particle Theory Seminar, University of Maryland, February 1995

Workshop in Gauge Theory, Park City/Institute for Advanced Study Mathematics Institute, Park City, July 1994

Workshop on Harmonic Maps, Minimal Submanifolds, and Rigidity Questions, Mathematical Sciences Research Institute, April 1994

SCHOLARLY ACTIVITY (continued):

Service to the Scientific Community:

Interview, *News 5 Investigates: FBI shuts down illegal drug web site* with Eric Ross, on KOAA-TV Colorado Springs, November, 2013

Interview, *La cryptographie quantique entre dans le commerce*, with Anna Hohler, in "Tracés – Bulletin technique de la Suisse romande", July, 2004

Reviewer for Mathematical Reviews (approximately 30 reviews)

Referee for various US National Science Foundation programs and journals of mathematics, physics, and computer science (approximately 30 in the last five years; most recently for, *e.g.,* **Physic Letters A**, **The Information Society**, the **Journal of the American Society for Information Science and Technology**, the **Journal of Learning Analytics**, and the **IEEE** journals **Computer**, **Transactions on Dependable and Secure Computing**, and **Transactions on Parallel and Distributed Systems**)

Professional Memberships:

American Association of University Professors since 2006
Association for Computing Machinery since 2005
Mathematical Association of America since 2005
American Mathematical Society since 1990

Employment in IT:

2000–2005: IBM Zurich Research Laboratory, Rüschlikon, Switzerland
Research Staff Member
Network Security and Cryptography Group, 2000-2003
Identity Management and Privacy Group, 2003-2005
Projects:
- coding new cryptographic algorithms, the "SINTRA" mid-level communications protocol stack, a test suite and demonstrator scenario, in **Java**, working with one other scientist
- making an interdisciplinary project plan for research in new computational devices and architectures with three other scientists
- as part of IBM's contribution to the Trusted Computing Group (TCG) consortium, doing protocol and algorithm design, working in a small team
- lone representative of IBM on the TCG Best Practices Working Group
- design and implementation of a new multi-party security attestation protocol for the TCG, supervising a small team in construction of a demonstrator (in **Java**) with GUI, complex threading, inter-platform communications, maintenance/ processing of certificate databases, and including general tinkering with and extension of a custom Linux kernel (in **C**)
- as part of IBM's work in the "**PRIME**" European Union-funded project, working on theory of certificate schemes and Zero-Knowledge Proof of Knowledge protocols using pairing-based elliptic curve cryptography and, working with one other scientist, designing and realizing (in **C++**) trial comparative implementations of these techniques to explore performance issues in different parts of the parameter space of such approaches

1985–1986: Greystone Technology Corporation, Wakefield, MA, USA
Software Engineer/Architect
Project: design and implementation (in **C**) of a compiling interpreter for the MUMPS computer language/database environment, working in a small team

1984: Thinking Machines Corporation, Cambridge, MA, USA
Summer Intern
Projects: artificial intelligence research (*e.g.*, computer vision) and numerical solutions of differential equations, on massively parallel architectures in **Lisp** and **C**

1983: Continuum Dynamics, Incorporated, Princeton, NJ, USA
Summer Intern
Projects: large-scale numerical modelling of fluid flows in jet engines and nuclear power plant safety systems, in **Fortran** on supercomputers

1979–1983: Princeton University, Princeton, NJ, USA and Harvard University, Cambridge, MA, USA
Part-time and Contract Programmer
Projects: design and implementation (in **C**, **Fortran** and assembler) of real-time data acquisition and analysis software for various scientific experiments

SCHOLARLY ACTIVITY (continued):

Organization of Professional Meetings:

Pikes Peak Regional Undergraduate Mathematics Conference [PPRUMC]

- steering committee since 2008
- host committee (with Drs Barnett and Funk-Neubauer) for the 7^{th} PPRUMC at CSU-Pueblo in 2010 and for the 13^{th} PPRUMC at CSU-Pueblo in 2016
- panelist, discussion session on mathematical and IT careers, 2009

Mathematical Association of America Rocky Mountain Section Meeting

- leader for discussion "promoting student success in mathematics", April 2009 meeting at CSU-Ft Collins
- session chair, April 2007 meeting at CSU-Pueblo

Program committee member, *Association for Computing Machinery Symposium on Applied Computing* TRECK Track, 2007

Organizer of the special session "Partial Differential Equations" at the American Mathematical Society Eastern Section meeting, College Park, MD, April 1997

Co-organizer of the special session "Harmonic Maps, Locally Symmetric Spaces and Related Issues" at the American Mathematical Society Eastern Section meeting, Boston, MA, October 1995

Educational Outreach:

Hampshire College Summer Studies in Mathematics senior staff at this summer program for gifted high school math students, 2011

- ran a "maxi" workshop on number theory and cryptology
- ran a "mini" on hyperbolic geometry
- co-organized and -ran a "mini" on theory of complexity

MathSciFest afternoon cryptology lab, 2011

Pikes Peak Regional Science Fair judge, 2010/11

Bridges to Biomedical Careers mathematics sessions in summer programs 2009/10/11

Science Day mathematics session, 2009

Packard Foundation grant to support the high school-to-college transition, 2008

Professional Development:

Successfully completed MOOCs:

edX:

HLS1x: Copyright, on copyright law from Harvard Law School, June 2013

Denial 101x, on climate science and its denial from the University of Queensland, June 2015

Coursera:

Surveillance Law, from Stanford Law School, December 2014

Professional Enhancement Programs from the Mathematical Association of America (MAA PREPs):

Authoring Effective Homework Problems with WeBWorK, June 2014

Becoming a Successful WeBWorK System Administrator, July 2015

NSF-sponsored computer science pedagogical enrichment:

Professor's Open Source Software Experience [POSSE], June 2016

PERSONAL MISCELLANEA:

Fluent in Italian, comfortable in French, moderate knowledge of German and Japanese

Dual US/Italian citizen

My Erdös number is **5**, via at least half a dozen distinct geodesics in the Math Reviews collaboration graph