Phillip Rogaway

Homepage: https://web.cs.ucdavis.edu/∼rogaway
Zoom: https://ucdavis.zoom.us/j/4778298788
Email: rogaway@pm.me
6765 SW Raleighwood Ln
Portland, OR 97225 USA
Cell: +1 530 220 4843

Current interest Grade K-12 math teaching, with an emphasis on creative problem solving and connecting math with the humanities

Last position Professor, Department of Computer Science, University of California, Davis. *1994–2024*
Emeritus since 2024.07.01

Research Cryptography — ethics and technology — privacy — theory of computation

Education
Massachusetts Institute of Technology *1987–1991*
Ph.D. in Electrical Engineering and Computer Science, 1991
University of Wisconsin, Madison *1986–1987*
Graduate student, Department of Mathematics, on leave from MIT
University of California, Berkeley *1980–1984*
B.A. in Computer Science, 1985

Visiting positions
École Normale Supérieure (ENS), France (2015)
ETH Zürich, Switzerland (2014)
Isaac Newton Institute, Cambridge, UK (2012)
Chiang Mai University, Thailand (1999–2005)
Chulalongkorn University, Bangkok, Thailand (2003)
Dartmouth College, USA (1990–1991)

Stats Number of citations to my work: more than 45,000 *Stats and rankings by Google Scholar*
h-index: 83 *maximal h s.t. h most cited papers have $\geq h$ citations each*
Ranking, in the world, among scholars in:
cryptography: #16 ethics and technology: #1 privacy: #8

Awards for research ▷ **Levchin Prize** (2016). "For groundbreaking practice-oriented research that has had an exceptional impact on real-world cryptography." ▷ **PET Award** (2015). For the most important paper on privacy enhancing technology in a calendar year (paper from CRYPTO 2015). ▷ **IACR Fellow** (2012). "For fundamental contributions to the theory and practice of cryptography and for educational leadership in cryptography." ▷ **ACM Paris Kanellakis Theory and Practice Award** (2009). "[For the] development of the field of practice-oriented provable-security and its widespread impact on the theory and practice of cryptography and security." ▷ **RSA Award for Mathematics** (2003). "[For developing] the primary paradigm for reasoning about the properties of cryptographic methods today." ▷ **ACM CCS Test of Time Award** (2011). For for paper from CCS 2001.

Awards for teaching ▷ **ASUCD Excellence in Teaching Award Finalist** (2015). Campus-wide award given to one professor from ∼2,000.
▷ **ASUCD Excellence in Teaching Award Finalist** (2014). Campus-wide award given to one professor from ∼2,000.
▷ **UCD College of Engineering Outstanding Teaching Award** (2010). College-wide award given to one professor from ∼225.

Subjects taught

Algorithms · cryptography · data structures · discrete math (combinatorics, graph theory, logic, number theory, and probability) · ethics and technology · science fiction films · theory of computation. Also, privately, standard K-12 math subjects and math competition problems.

K-12 outreach

▷ Substitute teacher for math classes (Jesuit High School, 2025–present)
▷ Private math tutoring, middle school students (2018–2024)
▷ Private math tutoring, high school students (2020–present)
▷ COSMOS summer program on security (grades 8–12) (2000)
▷ International Mathematical Olympiad (IMO) training (Chiang Mai, 2000, in Thai)
▷ Guest teaching in math classes (California and Thailand, 2013–2024)

Publications

About 135 research publications: DBLP:Rogaway
About 15 U.S. patents: Patents:Rogaway

Lectures

About 160 talks, in 32 countries.
About 20 of these keynotes, and 28 invited talks at conferences.

Grants

PI on grants and gifts totalling more than $3 million. Mostly from the NSF. No military funding.

Standards

Approximately 25 cryptographic standards based on my work.
Schemes standardized by ANSI, IEEE, IETF, ISO, and NIST.

Leadership roles

▷ Chair, Campus Committee on International Studies and Exchanges (2009–2010)
▷ Chair, Department's Undergraduate Affairs Committee (2008–2018)
▷ Chair, Department's Committee of Graduate Advisors (2010–2016)
▷ Chair, Department's Faculty Search Committee (2005–06)
▷ Chair, IACR Fellows Committee (2015) (member, 2012–2014)
▷ Program Chair, Crypto 2011
▷ IACR Board of Directors, 2016, 2017, 2018 (elected position)
▷ Editorial Board, *Journal of Cryptology*, 2009–2017
▷ Editorial Board, *Information and Computation*, 2005–2010
▷ PETs Award Selection Committee, 2016
▷ Program Committee member, various conferences, 20 times
▷ Organizer, Department's Distinguished Lecture Series (2007–08)

Advising

▷ PhD advisor to 9 Ph.D. students, most of whom became professors.
▷ Advised hundreds of undergrads (chaired departmental undergrad committee for years).
▷ Advised hundreds of grad students (chaired departmental grad advising committee for years).

DEI

Experience dealing with students with: autism spectrum · depression · learning disabilities · limited English. Personal experiences with prosopagnosia.

Misc

▷ Three years as a security architect, IBM (1991–1994).
▷ Many years doing private consulting in cryptography.
▷ Lived or worked in more than 70 different countries.
▷ Held appointment at Chiang Mai University, Thailand, for about a decade.
▷ Can speak Thai. Could once speak Persian and Spanish.
▷ Rock climbing, alpine climbing, backpacking.

Teaching evaluations

Median instructor-quality ratings of of 10/10 (old system) and 5/5 (new system) for $\sim 70\%$ of all courses taught
(possibly the highest evaluations in the department)
▷ All evaluations 2001–2024
▷ ECS 127: Cryptography. Winter 2024
A mathematical course typical of my "technical" teaching
▷ ECS 188: Ethics in an Age of Technology. Spring 2023.
The class I have focused on in recent years. More STS than moral philosophy
▷ ECS 189L: Topics in Computer Science: *Black Mirror*. Spring 2024.
Novel experimental class

Available online

Teaching statement
Full CV (∼30 pages)

References

The following individuals can speak to my teaching, not just my research.

Prof. Mihir Bellare — *Closest collaborator for 30 years*
University of California, San Diego, USA
`mihir@eng.ucsd.edu` Personal webpage

Prof. Dipak Ghosal — *Professor and Chair in my home department*
University of California, Davis, USA
`dghosal@ucdavis.edu` Personal webpage

Prof. Norm Matloff — *Senior professor in my home department*
University of California, Davis, USA
`nsmatloff@ucdavis.edu` Personal webpage

Prof. Chanathip Namprempre — *Colleague with whom I discuss teaching*
Currently: Penumbra Security
Formerly: Visiting Professor at Reed College, USA
Formerly: Professor at Thammasat University, Thailand
`cnamprem@gmail.com` DBLP page