# Curriculum Vitae

Joan Boyar

September 21, 2023

Dept. of Mathematics and Computer Science
University of Southern Denmark
Campusvej 55
DK-5230 Odense M
Denmark

Lindvedhave 65
5260 Odense S
Denmark

phone: +45 6618 3458

Email: joan@imada.sdu.dk
URL: https://imada.sdu.dk/u/joan/
ORCID: 0000-0002-0725-8341
phone: +45 6550 2338

## Personal

Born: April 18, 1955, Chicago, Illinois, USA.
Citizenship: USA and Denmark.
Former name: Joan Boyar Plumstead.
Marital status: Married to Kim Skak Larsen.
Child: Marianne Boyar Larsen, born March 11, 1993.

## Education

Ph.D., Computer Science, University of California, Berkeley, June 1983.
M.S., Computer Science, University of California, Berkeley, December 1981.
A.B., Mathematics, University of Chicago, June 1977.

## Work Experience

Professor, Institut for Matematik og Datalogi, University of Southern Denmark, 2017-present.
Visiting Professor, Department of Computer Science, University of Toronto, May 2023.
Visiting Professor, Department of Computer Science, University of Toronto, fall semester 2017.
Lektor (Associate Professor), Institut for Matematik og Datalogi, University of Southern Denmark, 1992-2017.
Visiting Professor, David R. Cheriton School of Computer Science, University of Waterloo, and Department of Computer Science, University of Toronto, fall semester 2012.
Visiting Associate Researcher, Department of Computer Science, University of California – Irvine, fall semester 2007.
Visiting Faculty Member, Department of Computer Science, University of Toronto, fall semester 2002.
Visiting Associate Professor, Computer Sciences Department, University of Wisconsin – Madison, spring semester 1997.
Lektorvikar (Visiting Associate Professor), Institut for Matematik og Datalogi, Odense University, 1991-1992.
Associate Professor, Department of Mathematical Sciences, Loyola University Chicago, 1990-1991.
Lektorvikar (Visiting Associate Professor), Datalogisk Afdeling, Aarhus University, 1989-90.
Assistant Professor, Department of Computer Science, University of Chicago, 1983-89.
Research Assistant, University of California, Berkeley, summer 1981 and 1982-83.

Teaching Associate, Computer Science Division, University of California, Berkeley, winter quarter 1982.
Programmer/Analyst, Laboratory for Astrophysics and Space Research, University of Chicago, February 1978 - August 1979.
Teaching Assistant, Computer Science Department, University of Wisconsin, Madison, fall semester 1977.
Research Associate, Undergraduate Research Participant, and Student Aide; Applied Mathematics Division, Center for Educational Affairs, and Applied Physics Division; Argonne National Laboratory, Argonne, Illinois, summers of 1975, 1976, 1977, and half-time 1976-77.

## Professional Activities

Invited speaker: 48th International Symposium on Mathematical Foundations of Computer Science (MFCS 2023).
Pacific Institute for the Mathematical Science Distinguished Lecture at University of Manitoba, October 18, 2018.
Senior keynote speaker and member of the scientific committee for EURO Summer Institute on Online Optimization at the University of Szeged, June 2015.
Member of the Danish Natural Sciences Research Council (SNF), 1997-2001.
Member of the Computer Science Group for the national Bibliometric Research Indicator, under the Ministry of Higher Education and Science, 2017-2021.
Member of Digital Democracy Center, University of Southern Denmark, 2021-current.
Contributing researcher in the Efficient Algorithms and Data Structures workstream of the Digital Research Centre Denmark (DIREC), 2021-current.
Contributing researcher in the PhD Training Network workstream of the Digital Research Centre Denmark (DIREC), 2021-current.
Member of committees evaluating doctoral theses at University of Chicago, Norwegian University of Science and Technology, Trondheim, University of Aarhus, University of Southern Denmark, Lund University.
Member of program committees: CRYPTO 85, EUROCRYPT 90, WEA 2003, OLA 2004 (chair), ICALP 2007, LATIN 2010, LATIN 2014, WADS 2017, MOLI 2018, SWAT 2018, SOFSEM 2019, WAOA 2019, SWAT 2020, OLAWA 2020, MFCS 2024.
Co-organizer of special session on Online Algorithms (by invitation): CiE 2014.
Member of organizing committees:
22nd ARCO Workshop Spring 2016 (chair);
Trends in Online Algorithms, TOLA 2014 (chair);
SWAT 2004; Workshop on On-Line Algorithms, OLA 2004 (chair);
10th ARCO Workshop on Combinatorial Optimization, 2003;
Algorithms in Quantum Information Processing '98, Aarhus University;
Chicago Workshop on Computational Complexity, 1985.
Member of steering committee for ARCO (Algorithmic Research: Cooperation around Oresound), 2015-current.
Member of editorial board for *Information Processing Letters* (2021-2024).
External reviewer for grants for Israel, Israel/USA, Switzerland, Poland, The Netherlands.
Member of evaluation committees for positions:
(førsteamanuensis i informatikk) at the University of Bergen, Norway, 1997 and 1998,
(universitetslektorat i datalogi) at Lund University, Sweden, 1998.
(postdoc) at Aarhus University, Denmark, 2013.
(associate professor) at Technical University of Denmark, 2014.
Some universities at which I have given talks:
Cambridge University, Cornell University, Lund University, University of California - Berkeley, University of Chicago, University of Manitoba, University of Southern Denmark, University of Toronto, University of Waterloo, University of Wisconsin - Madi-

son, University of Wisconsin - Milwaukee, Yale University, Aalborg University, Aarhus University.

## Major University Services

Coordinator for computer science group, University of Southern Denmark, 2018-2021.
Member of the department's executive committee, University of Southern Denmark, 2018-2019.
Head of algorithms group, University of Southern Denmark, 2018-2019.
Member of the department's executive committee (forskningsleder for datalogi), University of Southern Denmark, 2007-2011.
Member of the Natural Sciences PhD Study Board (and chairman of the local PhD committee), University of Southern Denmark, 2005-2007, 2014-2017.
Member of the Natural Sciences Study Board, University of Southern Denmark, 2000-2002.
Member of the College Council of the University of Chicago, 1986-89.

## Courses Taught (some several times)

Undergraduate:
Introduction to Information Technology I, Introduction to Computer Science, Introduction to Computer Programming I and II, Data Structures, Advanced Data Structures, Discrete Mathematics, Languages and Models, Theory of Algorithms, Graph Theory, Algorithms and Complexity, Algorithms and Probability, Complexity and Computability, Theory of Computation I, Cryptology, Computer Security, Network Security.
Graduate:
Online Algorithms, Cryptology, Cryptography and Complexity, Cryptographic Protocol Theory, Zero-Knowledge Seminar, Structural Complexity, Randomized Algorithms, Geometry and Linear Programming, Combinatorial Optimization, Algorithmic Number Theory.
Pedogogical advisor for assistant professors:
Jing Qin, 2014; Luís Cruz-Filipe, 2018.

## Awards and Funding

Center for Digital Democracy, 2021-2026, member of Trust and News Authenticity project.
Grant from TrygFonden, 2022-2024, member of project "News Trust in the Digital World" (2,300,000 Dkr).
Grant from FNU, 2020-2023, member of project "Online Algorithms with Machine Learning Predictors" (770,400 Dkr).
Grant from FNU, 2017-2020, principal investigator of project "Online Algorithms and Cheminformatics Meet Concurrency" (1,382,962 Dkr).
Rammebevilling (grant) from FNU, 2014-2016, member of project "Algorithmic Challenges" (1,036,800 Dkr).
Grant from Villum Fonden, 2013-2017, principal investigator of project "On-Line Algorithms and Advice" (2,900,101 Dkr).
Velux Visiting Professor grant for Faith Ellen from April 1 to June 30, 2014 (103,264.88 Dkr).
Rammebevilling (grant) from FNU, 2012, principal investigator of project "Online Algorithms at Waterloo and Toronto" (163,754 Dkr).
Rammebevilling (grant) from FNU, 2011-2013, principal investigator of project "On-Line Algorithms, Bioinformatics, and SAT Solving" (1,267,200 Dkr).
Mobility stipends (5 Ph.D. stipends) from The Danish Research Coordination Committee, 2010–2014, responsible for grant application for the project "Efficient Algorithms and High Quality Solutions" (12,000,000 Dkr).
Velux Visiting Professor grant for Faith Ellen from April 11 to June 11, 2010 (130,000 Dkr).
Rammebevilling (grant) from FNU, 2008-2010, member of project

"Fundamental Problems in Online, String, and Wireless Network" (994,875 Dkr).
Rammebevilling (grant) from SNF, 2005-2007, principal investigator of project "Algorithmics" (480,000 Dkr).
Grant from SNF to support SWAT 2004, and the associated workshop and summer school, principal investigator of "Scandinavian Algorithm Week" (95,400 Dkr).
Rammebevilling from SNF, 2002-2004, member of project "Algoritmik" (400,000 Dkr).
Rammebevilling from SNF, 1999-2001, principal investigator of project "Algorithmics" (300,000 Dkr).
Rammebevilling from SNF, 1996-1998, member of project "Algebraic groups and algebraic geometry over finite fields".
ALCOM-FT, the IST Programme of the EU under contract number IST-1999-14186, 2000-03, member of the Aarhus group.
ALCOM-IT, the ESPRIT Long Term Research Programme of the EU under project number 20233, 1995-99, member of the Aarhus group.
NSA Grant No. MDA904-90-H-4016 entitled, "The Complexity of Zero-Knowledge Proofs", 1990-92 ($ 67,652): principal investigator.
NSA Grant No. MDA904-88-H-2006 entitled, "Interactive Proof Systems and Zero-Knowledge", 1987-89 ($ 103,056): principal investigator.
NSA Grant No. MDA904-85-H-0017 entitled, "Cryptographic Security of Pseudo-Random Number Generators", 1985-87 ($ 154,080): principal investigator.
Graduate Opportunity Fellowship; University of California, Berkeley, 1980-82.
Eugene C. and Mona Fay Gee Scholarship; University of California, Berkeley, 1979-80.
Regents Fellowship; University of California, Berkeley, 1979-80.
Graduation with General Honors, Phi Beta Kappa, Sigma Xi; University of Chicago, 1977.

## Patents

Patent No. US 8,316,338 B2, granted November 20, 2012, "Method of optimizing combinational circuits", with René Peralta from NIST.
Patent No. US 8,707,224 B2, granted April 22, 2014, division of patent application above.

## Official Public Challenge Solved

Solved the first challenge by the inventors of Keccak, the winner of the hash function competition by NIST in 2012. Solved with René Peralta on March 6, 2013. Recognized on: http://keccak.noekeon.org/crunchy_contest.html.

## Current Research Interests

Online algorithms, cryptology, combinatorial optimization, data structures, Boolean functions, and computational complexity.

## Outreach

Gave feedback to the winners of SDU's award for high school "researchers" working on the Strategic Development Goals. Talked with the two students about cryptography and quantum computation in my office for 45 minutes, June 24, 2021.
Computer science minor subject representative for 2019-2020, meeting students September 1, 2019.
Final address for TalentCampDK (gymnasium students) entitled "Cryptography Based on Hard Problems", two hours May 10 and two on May 12, 2019.
Faculty member advising groups on the technical content of their ideas for the Innovation course, April 7, 2016
Member of scientific panel judging posters from first year students, June 13, 2014, and June 12, 2015.

Faculty member attending sessions where second year students gave their pitches, in the Innovation course, June 4, 2014.

Workshop leader for three repetitions of the same workshop, "Korttricks og koder" (Card tricks and codes), for Greenlight@Odense Day 2012. This is organized by Greenlight for Girls, and the purpose was to interest girls between 11 and 15 years old in science.

Quoted by journalist for Version2 about insecure keys for RSA due to poor randomness in keys. URL=http://www.version2.dk/artikel/manglende-tilfaeldighed-i-web-kryptering-er-alvorligt-men-kan-rettes-43625.

Science Day presentation (for high school teachers), "Evolution and Pancake Sorting" (for Daniel Merkle), on October 10, 2011.

Presentation and exercises for 8 high school students starting on "Studieretningsprojekter" (senior year projects), "RSA and primality testing", 5 hours on November 30, 2010 (8 more students in 2011 and helping 1 student in 2015).

Talk to visiting high school students about algorithms and coding on October 28, 2011.

Lecture for visiting professors from China, entitled "Quality Measures for On-Line Algorithms", on June 15, 2010.

Lecture at the Nordic Chapter of Sigma Xi's first annual meeting in Copenhagen, May 18, 2010, entitled "Quality Measures for On-Line Algorithms".

"DANAIM's state-of-the-art encryption research", article written with a journalist for the research results section in *ERCIM Innovation*, issue 2, page 8, 2009. http://www.ercim.org/publications/ercim-innovation

Initiator of and moderator for a mailing list for algorithms researchers in Denmark (algoritmik@imada.sdu.dk), so that the community can hear about activities elsewhere and make plans to attend.

Founding member of the Nordic Chapter of Sigma Xi, 2009.

Lecture March 2, 2009, on Primality Testing, at a program for the winners of the Georg Mohr Competition (Georg Mohr-Konkurrencens Vinderseminar) at SDU.

Lecture in Math Club, an initiative intended for first year students at SDU who were potentially interested in studying mathematics, September 25, 2008.

Talk to visiting high school students about primality testing on October 25, 2006 and about cryptography on October 27, 2005.

Datatek '99 organizer and lecturer, October 1999, for high school students interested in datalogi or datateknologi.

Datatek '98 organizer and lecturer, October 1998, for high school students interested in datalogi or datateknologi.

Aktiv efterårsferie for matematik- og datalogiinteresserede på de gymnasiale uddannelser, lecturer, October 1997, for high school students interested in computer science or mathematics.

## Formal training in advising

Two day course on advising PhD students, January 2012.

Half day courses on holding development interviews with PhD students, September 2013 and November 2019.

Half day course on holding development interviews in general, October 2019.

Half day course on advising assistant professors on teaching, January 2014.

## Students advised (degrees completed)

22 bachelor students completed.

32 speciale (masters) students completed.

12 PhD students completed.

Carsten Lund*, Ph.D. 1991, University of Chicago.
Currently researcher at AT&T Labs.
Rolf Fagerberg, Ph.D. 1996, Odense University.
Currently professor at University of Southern Denmark.
Peter Høyer*, Ph.D. 2000, University of Southern Denmark.
Currently associate professor at University of Calgary.
Morten Nyhave Nielsen*, Ph.D. 2002, University of Southern Denmark.
Currently "Afdelingschef" (head of division) at DSB.
Lene Monrad Favrholdt, Ph.D. 2002, University of Southern Denmark.
Currently associate professor at University of Southern Denmark.
Sanne Wøhlk*, Ph.D. 2005, University of Southern Denmark.
Currently professor at Aarhus University.
Uffe Flarup*, Ph.D. 2008, University of Southern Denmark.
Currently Sr. Technical Lead at Multiscription.
Sushmita Gupta*, Ph.D. 2013, University of Southern Denmark.
Currently faculty member at the Institute of Mathematical Sciences, India.
Abyayananda Maiti*, Ph.D. 2013, University of Southern Denmark.
Currently assistant professor at IIT Patna, India.
Magnus Gausdal Find, Ph.D. 2015, University of Southern Denmark.
Currently forward deployed engineer at Palantir, Denmark.
Christian Kudahl*, Ph.D. 2017, University of Southern Denmark.
Currently data scientist at Universal Robots A/S.
Jesper With Mikkelsen*, Ph.D. 2017, University of Southern Denmark.

* These students had more than one advisor.