# Curriculum Vitae

Oded Regev

Webpage: http://www.cims.nyu.edu/~regev/ Email: regev@cims.nyu.edu

## 1 Curriculum Vitae

### 1.1 Academic positions

| | |
|---|---|
| *09/12–* | Full Professor, Courant Institute, New York University |
| *10/10–8/12* | Directeur de recherche de 2e classe au CNRS, ENS, Paris |
| *8/06–10/11* | Associate Professor with tenure, Tel Aviv University |
| *3/04–8/06* | Senior Lecturer (equivalent to Assistant Professor), Tel Aviv University |
| *6/03–2/04* | Postdoc, UC Berkeley, USA |
| *9/01–6/03* | Postdoc, Institute for Advanced Study, Princeton NJ, USA |

### 1.2 Education

| | |
|---|---|
| *1997–2001* | Ph.D., Computer Science<br>Tel Aviv University<br>Title of dissertation: “Scheduling and load balancing”<br>Supervisor: Prof. Yossi Azar |
| *1995–1997* | M.Sc., Computer Science (summa cum laude)<br>Tel Aviv University<br>Title of thesis: “On-line bin-stretching”<br>Supervisor: Prof. Yossi Azar |
| *1992–1995* | B.Sc., Mathematics and Computer Science (summa cum laude)<br>Tel Aviv University |

### 1.3 Honors & awards

| | |
|---|---|
| *2018* | The Gödel Prize |
| *2017* | The Ruth and Irving Adler Expository Lecture, Institute for Advanced Study, Princeton |
| *2007* | The Rector’s Excellence in Teaching Award, Tel Aviv University<br>(awarded yearly to 2% of the faculty in the university) |
| *2006* | Best paper award, “Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures”, Eurocrypt 2006, coauthored with P. Nguyen |
| *2005* | Raymond and Beverly Sackler Career Development Chair<br>(awarded yearly to two faculty in exact sciences in Tel Aviv University) |

*2005* Bergmann Memorial Research Award
(awarded yearly to two or three young scientists who are recipients of new Binational Science Foundation grants; includes a $5,000 grant)

*2005* Krill Prize for Excellence in Scientific Research
(awarded yearly by the Wolf foundation to 6 Israeli young scientists across all sciences)

*2004* Yigal Alon Fellowship for young scientists, 2004–2007
(prestigious grant given to a few leading new faculty recruits for 3 years)

*2003* Best paper award, “New lattice-based cryptographic constructions”, STOC 2003

*2000* Prize for Excellence, Tel Aviv University

*1999* Wolf Foundation Prize for Excellence

*1997* Marcus and Celia Maus Prize in Computer Science, Tel Aviv University

*1993–1997* Dean’s list of honor, Tel Aviv University

### 1.4 Grants

*2014* Simons Collaboration on Algorithms and Geometry, five years, $8M shared among 14 PIs

*2013* National Science Foundation (SMALL), $500,000, three years.

*2009* Wolfson Family Charitable Trust, 125,000 British pounds, two years, joint with Julia Kempe.

*2008* Israeli Science Foundation grant, “Lattices in Computer Science”, four years, sole PI, 184,000NIS per year.

*2008* European Research Council (ERC) Starting Grant, “Lattices in Computer Science”, five years, sole PI, total amount 822,000Euro.

*2005* European FP6 integrated project “Qubit Applications”, four years, PI (workpackage leader), total amount 30,000Euro per year, shared with Julia Kempe, Amnon Ta-Shma, and Lev Vaidman.

*2005* Binational Science Foundation grant, “Inapproximability, Unique Games, and Analysis of Boolean Functions”, four years, PI, total amount $30,000 per year, joint with Irit Dinur and Elchanan Mossel.

*2004* Israeli Science Foundation grant, “Lattices in Computer Science”, four years, sole PI, 180,000NIS per year.

### 1.5 Plenary speaker in scientific meetings

6. “Lattices and Lattice-based Cryptography”
Bellaires Research Institute of McGill University, Barbados, February 2013.

5. “On Ideal Lattices and Learning with Errors Over Rings”
ANTS-IX, Nancy, France, July 2010.

4. “The Learning with Errors Problem”
CCC 2010, Cambridge, MA, June 2010.

3. "The Learning with Errors Problem"
   PQCrypto 2010, Darmstadt, Germany, May 2010.

2. "Lattice-based cryptography"
   CRYPTO 2006, Santa Barbara, California, August 2006.

1. "Quantum Algorithm: What's Next?"
   PQCrypto 2006, Leuven, Belgium, May 2006.

# 2 Supervision and Teaching

## 2.1 Postdoctoral researchers mentored

*2018-2020* Euiwoong Lee (Ph.D. 2017, CMU)

*2015-2017* Omri Weinstein (Ph.D. 2015, Princeton; now assistant professor in Columbia)

*2014-2015* Aravindan Vijayaraghavan (Ph.D. 2013, Princeton; now assistant professor in Northwestern)

*2013-2013* Anindya De (Ph.D. 2013, UC Berkeley; now assistant professor in Northwestern)

*2013-2015* Jop Briët, joint with Assaf Naor (Ph.D. 2011, CWI, Amsterdam; now tenure track researcher in CWI)

*2012-2014* Daniel Dadush, joint with Assaf Naor (Ph.D. 2012, Georgia Tech; now tenure track researcher in CWI)

*2012-2013* Divesh Aggarwal, main host Yevgeniy Dodis (Ph.D. 2012, ETH Zurich; now assistant professor in NUS)

*2008-2010* Vadim Lyubashevsky (Ph.D. 2008, UC San Diego; now researcher in IBM Zurich)

*2009* Dan Gutfreund (Ph.D. 2005, Hebrew University)

## 2.2 Doctoral students supervised

*2013–2018* Shravas Rao

*2012–2017* Noah Stephens-Davidowitz (joint with Yevgeniy Dodis)

*2012–2017* Alexander Golovnev (joint with Yevgeniy Dodis)

*2009–2012* Klim Efremenko, "Coding Theory", Tel Aviv University (joint with Amnon Ta-Shma). Won the prestigious Adams fellowship and the Fulbright post-doctoral fellowship.

*2006–2011* Ishay Haviv, "Lattices and Computational Complexity", Tel Aviv University. Won the prestigious Adams fellowship. Now faculty in Tel Aviv College.

*2006–2011* Avraham Ben-Aroya, "Quantum Computation", Tel Aviv University (joint with Amnon Ta-Shma). Won the prestigious Adams fellowship.

*2006–2010* Iftah Gamzu, "Web Search Ranking and Allocation Mechanisms", Tel Aviv University (joint with Yossi Azar).

*2005–2010* Ricky Rosen, "Computational Complexity", Tel Aviv University (joint with Ran Raz).

### 2.3 Invited speaker in schools

- "Lattices and Cryptography"
  Swedish Summer School in Computer Science, August 2018.
- "Lattice-based Cryptography"
  Winter school for graduate students, Bar-Ilan University, Israel, February 2012.
- "Lattices and Cryptography"
  Three lectures in Mathematical Foundations in Cryptography, a winter school for doctoral students, EPFL, Lausanne, February 2009.
- "Harmonic Analysis and Lattices"
  Three lectures in DOCCOURSE 2006, a school for doctoral students, Prague, February 2006.

### 2.4 News articles that mention my work

*2015* A Tricky Path to Quantum-Safe Encryption, by Natalie Wolchover

## 3 Service

### 3.1 Editorial activity

| | |
|---|---|
| *2011–* | Associate Editor-in-Chief, Theory of Computing |
| *2013–2016* | Editorial Board, SIAM Journal on Computing |
| *2009–* | Scientific Board, Electronic Colloquium on Computational Complexity (ECCC) |
| *2008–2011* | Managing Editor, Theory of Computing |
| *2004–2008* | Associate Editor, Theory of Computing |

### 3.2 Program committees

| | |
|---|---|
| *2012* | ACM Symposium on Theory of Computing (STOC 2012) |
| *2010* | ACM Symposium on Theory of Computing (STOC 2010) |
| *2009* | IEEE Conference on Computational Complexity (CCC 2009) |
| *2008* | ACM Symposium on Theory of Computing (STOC 2008) |
| *2008* | Algorithmic Number Theory Symposium (ANTS 2008) |
| *2006* | Theory of Cryptography Conference (TCC 2007) |
| *2005* | IEEE Conference on Computational Complexity (CCC 2005) |
| *2004* | ACM Symposium on Theory of Computing (STOC 2004) |

Last updated: March 26, 2018