

Oded Regev – Publication list

Articles in International Refereed Journals

Appeared

34. J. Kempe, O. Regev, and B. Toner
Unique Games with Entangled Provers are Easy
SIAM Journal on Computing 39:7 (2010) 3207–3229.
(See also Conf. Proc. [35](#))
33. J. Kempe, O. Regev, F. Unger, and R. de Wolf
Upper Bounds on the Noise Threshold for Fault-tolerant Quantum Computing
Quantum Information and Computation 10:5 (2010) 361–376.
(See also Conf. Proc. [30](#))
32. A. Chakrabarti and O. Regev
An Optimal Randomised Cell Probe Lower Bound for Approximate Nearest Neighbour Searching.
SIAM Journal on Computing 39:5 (2010) 1919–1940.
(See also Conf. Proc. [16](#))
31. O. Regev and B. Toner
Simulating Quantum Correlations with Finite Communication.
SIAM Journal on Computing 39:4 (2009) 1562–1580.
(See also Conf. Proc. [29](#))
30. O. Regev
On Lattices, Learning with Errors, Random Linear Codes, and Cryptography.
Journal of the ACM 56:6 (2009) 34.
(See also Conf. Proc. [21](#))
29. I. Dinur, E. Mossel, and O. Regev
Conditional Hardness for Approximate Coloring.
SIAM Journal on Computing 39:3 (2009) 843–873.
(See also Conf. Proc. [22](#))
28. I. Haviv, V. Lyubashevsky, and O. Regev
A Note on the Distribution of the Distance from a Lattice.
Discrete and Computational Geometry 41:1 (2009) 162–176.
27. D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf
Bounded-Error Quantum State Identification and Exponential Separations in Communication Complexity
SIAM Journal on Computing 39:1 (2009) 1–24.
(See also Conf. Proc. [23](#))
26. P. Q. Nguyen and O. Regev
Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures.

- Journal of Cryptology* 22:2 (2009) 139–160.
(See also Conf. Proc. [25](#))
25. D. Gavinsky, O. Regev, and R. de Wolf
Simultaneous Communication Protocols with Quantum and Classical Messages.
Chicago Journal of Theoretical Computer Science 2008:7.
 24. I. Dinur, E. Friedgut, and O. Regev
Independent Sets in Graph Powers are Almost Contained in Juntas.
GAF 18:1 (2008) 77–97.
 23. S. Khot and O. Regev
Vertex cover might be hard to approximate to within $2-\epsilon$.
Journal of Computer and System Sciences 74:3 (2008) 335–349.
(See also Conf. Proc. [13](#))
 22. D. Micciancio and O. Regev
Worst-case to Average-case Reductions based on Gaussian Measures.
SIAM Journal on Computing 37:1 (2007) 267–302.
(See also Conf. Proc. [19](#))
 21. D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev
Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation.
SIAM Journal on Computing 37:1 (2007) 166–194.
Also invited to and appears in the SIGEST section of *SIAM Review* 50:4 (2008).
(See also Conf. Proc. [17](#))
 20. I. Haviv, O. Regev, and A. Ta-Shma
On the Hardness of Satisfiability with Bounded Occurrences in the Polynomial-Time Hierarchy.
Theory of Computing 3:3 (2007) 45–60.
 19. E. Mossel, R. O’Donnell, O. Regev, J. Steif, and B. Sudakov
Non-Interactive Correlation Distillation, Inhomogeneous Markov Chains and the Reverse Bonami-Beckner Inequality.
Israel Journal of Mathematics 154 (2006) 299–336.
 18. J. Kempe, A. Kitaev, and O. Regev
The Complexity of the Local Hamiltonian Problem.
SIAM Journal on Computing 35:5 (2006) 1070–1097.
(See also Conf. Proc. [20](#))
 17. Y. Azar and O. Regev
Combinatorial Algorithms for the Unsplittable Flow Problem.
Algorithmica 44:1 (2006) 49–66.
(See also Conf. Proc. [5](#))
 16. I. Dinur, O. Regev, and C. Smyth
The hardness of 3-uniform hypergraph coloring.

- Combinatorica* 25:5 (2005) 519–535.
(See also Conf. Proc. [8](#))
15. D. Aharonov and O. Regev
Lattice Problems in NP intersect coNP
Journal of the ACM 52:5 (2005) 749–765.
(See also Conf. Proc. [18](#))
 14. I. Dinur, V. Guruswami, S. Khot, and O. Regev
A New Multilayered PCP and the Hardness of Hypergraph Vertex Cover.
SIAM Journal on Computing 34:5 (2005) 1129–1146.
(See also Conf. Proc. [11](#))
 13. V. Guruswami, D. Micciancio, and O. Regev
The complexity of the covering radius problem.
Computational Complexity 14:2 (2005) 90–121.
(See also Conf. Proc. [15](#))
 12. O. Regev
New lattice-based cryptographic constructions.
Journal of the ACM 51:6 (2004) 899–942.
(See also Conf. Proc. [10](#))
 11. O. Regev
Improved inapproximability of lattice and coding problems with preprocessing.
IEEE Transactions on Information Theory 50:9 (2004) 2031–2037.
(See also Conf. Proc. [12](#))
 10. O. Regev
Quantum computation and lattice problems.
SIAM Journal on Computing 33:3 (2004) 738–760.
(See also Conf. Proc. [7](#))
 9. J. Balogh, O. Regev, C. Smyth, W. Steiger, and M. Szegedy
Long monotone paths in line arrangements.
Discrete and Computational Geometry 32:2 (2004) 167–176.
(See also Conf. Proc. [9](#))
 8. J. Kempe and O. Regev
3-Local Hamiltonian is QMA-complete.
Quantum Information and Computation 3:3 (2003) 258–264.
 7. A. Armon, Y. Azar, L. Epstein, and O. Regev
Temporary tasks assignment resolved.
Algorithmica 36:3 (2003) 295–314.
(See also Conf. Proc. [6](#))
 6. A. Armon, Y. Azar, L. Epstein, and O. Regev
On-line restricted assignment of temporary tasks with unknown durations.
Information Processing Letters 85:2 (2003) 67–72.

5. O. Regev
Priority algorithms for makespan minimization in the subset model.
Information Processing Letters 84:3 (2000) 153–157.
4. B. Awerbuch, Y. Azar, S. Leonardi, and O. Regev
Minimizing the flow time without migration.
SIAM Journal on Computing 31:5 (2002), 1370–1382.
(See also Conf. Proc. 2)
3. B. Awerbuch, Y. Azar, and O. Regev
Maximizing job benefits on-line.
Journal of Scheduling 4:6 (2001), 287–296.
(See also Conf. Proc. 4)
2. Y. Azar, O. Regev, J. Sgall, and G. Woeginger
Off-line temporary tasks assignment.
Theoretical Computer Science 287:2 (2002) 419–428.
(See also Conf. Proc. 3)
1. Y. Azar and O. Regev
On-line bin-stretching.
Theoretical Computer Science 268:1 (2001) 17–41.
(See also Conf. Proc. 1)

Submitted for Journal Publication

1. I. Haviv and O. Regev
The Euclidean Distortion of Flat Tori
Submitted to *Journal of Topology and Analysis*.

Book Chapters

2. O. Regev
On the Complexity of Lattice Problems with Polynomial Approximation Factors.
In *The LLL Algorithm*, P. Q. Nguyen and B. Vallée (eds.), Springer (2010).
1. D. Micciancio and O. Regev
Lattice-based Cryptography.
In *Post-quantum Cryptography*, D.J. Bernstein and J. Buchmann (eds.), Springer (2009).

Publications in Proceedings of Conferences

44. H. Buhrman, O. Regev, G. Scarpa, and R. de Wolf
Near-Optimal and Explicit Bell Inequality Violations
CCC 2011. Also accepted as a contributed long talk in QIP 2011.¹
43. A. Chakrabarti and O. Regev
An Optimal Lower Bound on the Communication Complexity of Gap-Hamming-Distance
STOC 2011.
42. B. Klartag and O. Regev
Quantum One-Way Communication can be Exponentially Stronger Than Classical Communication
STOC 2011. Also an invited talk in QIP 2011.¹
41. I. Haviv and O. Regev
The Euclidean Distortion of Flat Tori
APPROX 2010, pp. 232–245.
40. J. Brody, A. Chakrabarti, O. Regev, T. Vidick, and R. de Wolf
Better Gap-Hamming Lower Bounds via Better Round Elimination
RANDOM 2010, pp. 476–489.
39. J. Kempe and O. Regev
No Strong Parallel Repetition with Entangled and Non-signaling Provers
CCC 2010, pp. 7–15. Also accepted as a contributed short talk in QIP 2010.¹
38. V. Lyubashevsky, C. Peikert, and O. Regev
On Ideal Lattices and Learning with Errors Over Rings
Eurocrypt 2010, pp. 1–23.
37. N. Gama, P. Nguyen, and O. Regev
Lattice Enumeration using Extreme Pruning
Eurocrypt 2010, pp. 257–278.
36. O. Regev
The Learning with Errors Problem
Invited survey paper, CCC 2010, pp. 191–204.
35. J. Kempe, O. Regev, and B. Toner
Unique Games with Entangled Provers are Easy
FOCS 2008, pp. 457–466. Also accepted as a contributed long talk in QIP 2008.¹
34. B. Barak, M. Hardt, I. Haviv, A. Rao, O. Regev, and D. Steurer
Rounding Parallel Repetitions of Unique Games
FOCS 2008, pp. 374–383.
33. A. Ben-Aroya, O. Regev, and R. de Wolf
A Hypercontractive Inequality for Matrix-Valued Functions with Applications to Quantum Computing and LDCs
FOCS 2008, pp. 477–486. Also invited to QIP 2008.¹

32. L. Eldar and O. Regev
Quantum SAT for a qutrit-cinquit pair is QMA_1 -complete
ICALP 2008, pp. 881–892.
31. O. Regev and L. Schiff
Impossibility of a Grover speed-up with a faulty oracle
ICALP 2008, pp. 773–781.
30. J. Kempe, O. Regev, F. Unger, and R. de Wolf
Upper Bounds on the Noise Threshold for Fault-tolerant Quantum Computing
ICALP 2008, pp. 845–856. Also invited to QIP 2008.¹
29. O. Regev and B. Toner
Simulating Quantum Correlations with Finite Communication
FOCS 2007, pp. 384–394. Also accepted as a contributed long talk in QIP 2008.¹
28. I. Haviv and O. Regev
Tensor-based Hardness of the Shortest Vector Problem to within Almost Polynomial Factors
STOC 2007, pp. 469–477.
27. O. Regev
Lattice-based Cryptography
Invited paper, CRYPTO 2006, pp. 131–141.
26. I. Haviv and O. Regev
Hardness of the Covering Radius Problem on Lattices
CCC 2006, pp. 145–158.
25. P. Q. Nguyen and O. Regev
Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures
Eurocrypt 2006, pp. 271–288.
24. O. Regev and R. Rosen
Lattice Problems and Norm Embeddings
STOC 2006, pp. 447–456.
23. D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf
Bounded-Error Quantum State Identification and Exponential Separations in Communication Complexity
STOC 2006, pp. 594–603. Invited to the special issue (appeared).² Also accepted as a contributed long talk in QIP 2006.¹
22. I. Dinur, E. Mossel, and O. Regev
Conditional Hardness for Approximate Coloring
STOC 2006, pp. 344–353.
21. O. Regev
On Lattices, Learning with Errors, Random Linear Codes, and Cryptography.
STOC 2005, pp. 84–93.

20. J. Kempe, A. Kitaev, and O. Regev
The Complexity of the Local Hamiltonian Problem.
FSTTCS 2004, pp. 372–383.
19. D. Micciancio and O. Regev
Worst-case to Average-case Reductions based on Gaussian Measures.
FOCS 2004, pp. 372–381. Invited to the special issue (appeared).²
18. D. Aharonov and O. Regev
Lattice Problems in NP intersect coNP
FOCS 2004, pp. 362–371. Invited to the special issue (declined).²
17. D. Aharonov, W. van Dam, J. Kempe, Z. Landau, S. Lloyd and O. Regev
Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation.
FOCS 2004, pp. 42–51. Invited to the special issue (appeared).²
16. A. Chakrabarti and O. Regev
An Optimal Randomised Cell Probe Lower Bound for Approximate Nearest Neighbour Searching.
FOCS 2004, pp. 473–482. Invited to the special issue (declined).²
15. V. Guruswami, D. Micciancio and O. Regev
The Complexity of the Covering Radius Problem on Lattices and Codes.
CCC 2004, pp. 161–173. Invited to the special issue (appeared).²
14. D. Aharonov and O. Regev
A Lattice Problem in Quantum NP.
FOCS 2003, pp. 210–219.
13. S. Khot and O. Regev
Vertex cover might be hard to approximate to within $2-\epsilon$.
CCC 2003, pp. 379–386. Invited to the special issue (appeared).²
12. O. Regev
Improved inapproximability of lattice and coding problems with preprocessing.
CCC 2003, pp. 363–370.
11. I. Dinur, V. Guruswami, S. Khot and O. Regev
A New Multilayered PCP and the Hardness of Hypergraph Vertex Cover.
STOC 2003, pp. 595–601.
10. O. Regev
New lattice based cryptographic constructions.
STOC 2003, pp. 407–416.
9. J. Balogh, O. Regev, C. Smyth, W. Steiger and M. Szegedy
Long monotone paths in line arrangements.
SoCG 2003, pp. 124–128. Invited to the special issue (appeared).²
8. I. Dinur, O. Regev and C. Smyth
The hardness of hypergraph coloring.
FOCS 2002, pp. 33–40.

7. O. Regev
Quantum computation and lattice problems.
FOCS 2002, pp. 520–529.
6. A. Armon, Y. Azar, L. Epstein and O. Regev
Temporary tasks assignment resolved.
SODA 2002, pp. 116–124.
5. Y. Azar and O. Regev
Strongly polynomial algorithms for the unsplittable flow problem.
IPCO 2001, pp. 15–29.
4. B. Awerbuch, Y. Azar and O. Regev
Maximizing job benefits on-line.
APPROX 2000, pp. 42–50. Invited to the special issue (appeared).²
3. Y. Azar and O. Regev
Off-line temporary tasks assignment.
ESA 1999, pp. 163–171. Invited to the special issue (appeared).²
2. B. Awerbuch, Y. Azar, S. Leonardi and O. Regev
Minimizing the flow time without migration.
STOC 1999, pp. 198–205.
1. Y. Azar and O. Regev
On-line bin-stretching.
RANDOM 1998, pp. 71–81.

In Preparation

1. O. Regev
Bounds on Dimension Reduction in ℓ_1 using Entropy

Manuscripts

3. O. Regev
Bell Violations through Independent Bases Games
[arXiv:1101.0576v2](https://arxiv.org/abs/1101.0576v2)
2. A. Ambainis and O. Regev
An Elementary Proof of the Adiabatic Theorem
[arXiv quant-ph/0411152](https://arxiv.org/abs/quant-ph/0411152)
1. O. Regev
A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem
with Polynomial Space
[arXiv quant-ph/0406151](https://arxiv.org/abs/quant-ph/0406151)

Lecture Notes

1. O. Regev
Lecture notes for the course “Lattices in Computer Science”
http://www.cs.tau.ac.il/~odedr/teaching/lattices_fall_2009, 2004

Theses

2. Scheduling and load balancing
2001, Ph.D. dissertation, Tel Aviv University
1. On-line bin-stretching
1997, M.Sc. thesis, Tel Aviv University

Notes

¹Running since 1998, QIP is the biggest yearly conference in quantum computing. Since 2006 there is a formal call for papers and the contributions are chosen by a program committee. About 10 results from the preceding year are invited to give long talks, and among the close to 300 submissions, 10 are chosen as long contributed talks, and about 20 more as short contributed talks.

²Special issues are typically dedicated to the best 10% of the papers in the conference.