

Thomas Vidick

Associate Professor
California Institute of Technology

1200 E. California Blvd.
Pasadena, CA 91125
☎ +1 (310) 735 7850
✉ vidick@cms.caltech.edu
📁 cms.caltech.edu/~vidick/

Nationality: Belgian
Born: 07/13/1982

Research interests

- **Theoretical Computer Science and Quantum Information**

My research is centered around problems at the interface of theoretical computer science, quantum information and cryptography. I like to use complexity theory as a tool to study problems in quantum computing, and quantum mechanical phenomena as a way to gain a new perspective on classical concepts from theoretical computer science.

Education & Employment

- 2017–current **Associate Professor**, *California Institute of Technology*, Pasadena.
- 2014–2017 **Assistant Professor**, *California Institute of Technology*, Pasadena.
- 2011–2013 **Postdoctoral Associate**, *Massachusetts Institute of Technology*, Cambridge, Advised by Scott Aaronson.
- 2007–2011 **Ph.D. in Computer Science**, *University of California*, Berkeley, GPA: 3.97/4.0. Dissertation title: *The Complexity of Entangled Games*. Advisor: Umesh Vazirani.
- 2006–2007 **Masters in Computer Science**, *University Paris 7*, Paris, Ranked 2nd. Master's project: *A study of Entanglement in Quantum Interactive Proof Systems*. Advisor : Julia Kempe.
- 2002–2007 **Magistère [B.Sc.]**, *École Normale Supérieure*, Paris, Ranked 1st. Major in Computer Science, Minor in Mathematics

Scholarships and awards

- Co-winner of the **FOCS'12 best paper award** for the paper “A multi-prover interactive proof for NEXP sound against entangled provers”, with Tsuyoshi Ito [25].
- My Ph.D. thesis was awarded the **Bernard Friedman Memorial Prize** in Applied Mathematics from U.C. Berkeley's Department of Mathematics.
- Berkeley Regent's Graduate Fellowship (2007-2008).

Courses taught at Caltech

- CMS139 Advanced Algorithms. Spring'15, Winter'16, Winter'17.
CS/Phys 120 Quantum Cryptography, Fall'16. Also offered as an EdX MOOC.
CS101 Introduction to Theoretical Cryptography, Spring'16.
CS286 Seminar in Computer Science: Around the quantum PCP conjecture, Fall'14.

Advising

- Postdocs Piyush Srivastava (2014-2016), Omar Fawzi (2015), Gil Cohen (2015-2016), Stacey Jeffery (2015-2016).
Graduate students Jenish Mehta (2014-), Milan Cvitkovic (2015-), Andrea Coladangelo (2015-).
Undergraduates Mahrud Sayrafi (SURG, Summer'14), Shannon Wang (SURF, Summer'15), Nick Haliday (SURF, Summer'15), Chinmay Nirkhe (Spring and Fall'16), Jalex Stark (Spring-Summer'17).

Workshop organization

- Simons Algorithms & Geometry Meeting *Apr. 21st 2017, New York.* Day-long meeting on the topic of "Unitary Correlation Matrices". Co-organized with Oded Regev (NYU).
SoCal Theory Day 2016 *Nov. 11th 2016, Caltech.* Day-long event with theory-oriented talks by Southern California researchers in TCS.
Foundations of Randomness *Oct. 26-28th 2015, Stellenbosch Institute for Advanced Study, South Africa.* Three-day workshop co-organized with A. Ekert, R. Renner and M. Santha as part of a Fall'15 STIAS project on "the nature of randomness and fundamental physical limits of secrecy". Around 20 invited participants.
Quantum Games and Protocols *Feb. 24-28th 2014, Simons Institute, Berkeley.* Week-long workshop co-organized with Dorit Aharonov and John Watrous as part of the special semester on Quantum Hamiltonian Complexity at the Simons Institute. Around 40 invited participants.

Professional service & affiliations

- Visiting Senior Research Fellow Centre for Quantum Technologies, NUS, Singapore.
Visiting Fellow Perimeter Institute, Waterloo, Canada.
Managing Editor Theory of Computing, theoryofcomputing.org
Editor Quantum, quantum-journal.org
Steering Committee Innovations in Theoretical Computer Science (ITCS), itcs-conf.org
PC Chair QCRYPT 2017.

- PC Member QIP 2012, QCRYPT 2012, QIP 2014, STOC 2014, RANDOM 2014, QCRYPT 2014, ITCS 2015, TQC 2015, CCC 2016, QIP 2016, FOCS 2016, ICALP 2017, STOC 2018.
- Reviewer SIAM Journal on Computing, JACM, ToC, Nature, CMP, Complexity, PRL, PRA, PRX, STOC, FOCS, CCC, QIP, Crypto, Quantum Information & Computation.
- Organizer Online seminar series TCS+.
- Organizer Caltech Theory seminar, 2014–present.
Berkeley quantum reading group, Fall '09, Spring '10, Fall '10, Spring '11.
Berkeley Theory Student's seminar, Fall '08.
- Member Association for Computing Machinery (ACM), American Physical Society (APS).

Funding

- PI for AFOSR MURI “Scalable Certification of Quantum Computing Devices and Networks”, 2017-2022.
- co-PI on NSF Physics Frontiers Center “Institute for Quantum Information and Matter (IQIM)”, 2016-2022.
- NSF CAREER “Interactions with Untrusted Quantum Devices”, 2016-2021.
- Air Force Young Investigator Award “Towards a Secure Quantum Network”, 2016-2021.
- Okawa Foundation Research Grant, 2015-2016.

References

- **Scott Aaronson** (Postdoc mentor), University of Texas at Austin, aaronson@cs.utexas.edu
- **Ran Raz**, Princeton University: ran.raz.mail@gmail.com
- **Oded Regev**, Courant Institute, NYU, regev@cims.nyu.edu
- **Umesh Vazirani** (Ph.D. advisor), UC Berkeley, vazirani@cs.berkeley.edu
- **John Watrous**, IQC Waterloo, watrous@cs.uwaterloo.ca

Recent invited talks

- 17th Jul. 2017 **Entanglement Tests from Group Representations**, *Workshop on Probabilistic and Algebraic Methods in Quantum Information Theory*, Texas A&M University.
- 19th Jun. 2017 **Robust and/or efficient tests for high-dimensional entanglement**, *TYQI 2017*, Paris, France.
- 27th Mar. 2017 **Rigorous RG algorithms and area laws for low energy eigenstates in 1D**, *IQC Colloquium*, Waterloo, ON.
- 19th Jan. 2017 **Rigorous RG algorithms and area laws for low energy eigenstates in 1D**, *QIP'17*, Seattle, WA.
- 2nd Dec. 2016 **Overlapping Qubits**, *Theory Colloquium*, UT Austin, TX.

- 9th Oct. 2016 **Overlapping qubits**, *Workshop on Subfactor Theory, Quantum Field Theory, and Quantum Information*, Harvard University.
- 7th Jul. 2016 **Overlapping qubits**, *QuPa day*, Paris.
- 16th Mar. 2016 **Device independent quantum cryptography**, *MIT CIS seminar*, MIT.
- 08th Feb. 2016 **Anchoring games for parallel repetition**, *UCSD theory seminar*, UCSD.
- 1st Oct. 2015 **Interactive proofs for local Hamiltonians**, *Invited talk at the Workshop on the Frontiers of Quantum Information and Computer Science*, QUICS, University of Maryland, USA.
- 4th May 2015 **A multiprover interactive proof system for the local Hamiltonian problem**, *Berkeley, USA*, Quantum Hamiltonian Complexity Reunion at the Simons Institute.
- 22nd Apr. 2015 **Non-Signalling Parallel Repetition Via de Finetti Reductions**, *Berkeley, USA*, Simons Institute workshop on Information Theory in Complexity Theory and Combinatorics.
- 1st Apr. 2015 **Noncommutative Grothendieck inequalities and quantum two-player games**, *Cambridge, UK*, Invited talk in BMC session on Quantum Information.
- 28th Aug. 2014 **The quantum PCP conjecture**, *Paris, France*, invited talk at the PCQC inauguration workshop.
- 20th Aug. 2014 **Tutorial on the quantum PCP conjecture**, *Kyoto, Japan*, AQIS 2014.
- 18th Aug. 2014 **Parallel repetition of entangled projection games**, *Tokyo, Japan*, invited talk at the ELC Workshop at the University of Tokyo on Quantum Complexity Theory.
- 14th May 2014 **A polynomial-time algorithm for the ground state of 1D gapped local Hamiltonians**, *Waterloo, Canada*, PiQuDos seminar, Perimeter Institute.

Publications

Journals (refereed)

- [1] Phong Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*, 2(2):181–207, 2008.
- [2] Guillaume Ricotta and Thomas Vidick. On the asymptotic height of Hseegner points. *Canadian Journal of Mathematics*, 60(6):1406–1436, 2008.
- [3] Julia Kempe, Hirotsada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18:273–307, 2009. Journal version of [25].
- [4] Julia Kempe, Hirotsada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick. Entangled games are hard to approximate. *SIAM Journal on Computing*, 40(3):848–877, 2011. Journal version of [24].
- [5] Thomas Vidick and Stephanie Wehner. Does ignorance of the whole imply ignorance of the parts? large violations of noncontextuality in quantum theory. *Phys. Rev. Lett.*, 107:030402, July 2011.

- [6] Thomas Vidick and Stephanie Wehner. More nonlocality with less entanglement. *Phys. Rev. A*, 83:052310, May 2011.
- [7] Jop Briët, Harry Buhrman, Troy Lee, and Thomas Vidick. All Schatten spaces endowed with the Schur product are Q-algebras. *Journal of Functional Analysis*, 262(1):1 – 9, 2012.
- [8] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan’s Extractor in the Presence of Quantum Side Information. *SIAM Journal on Computing*, 41(4):915–940, 2012.
- [9] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 370(1971):3432–3448, 2012. Nontechnical version of [31].
- [10] Thomas Vidick. A concentration inequality for the overlap of a vector on a large set, with application to the communication complexity of the gap-Hamming-Distance problem. *Chicago Journal of Theoretical Computer Science*, 2012(1), July 2012.
- [11] Jop Briët, Harry Buhrman, Troy Lee, and Thomas Vidick. Multipartite entanglement in XOR games. *Quantum Info. Comput.*, 13(3-4):334–360, March 2013.
- [12] Jop Briët and Thomas Vidick. Explicit lower and upper bounds on the entangled value of multiplayer XOR games. *Communications in Mathematical Physics*, 321(1):181–207, 2013.
- [13] Oded Regev and Thomas Vidick. Elementary proofs of Grothendieck theorems for completely bounded norms. *Journal of Operator Theory*, 71:491–506, 2014.
- [14] Umesh Vazirani and Thomas Vidick. Fully Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014. Journal version of [38].
- [15] Zeph Landau, Umesh Vazirani, and Thomas Vidick. A polynomial time algorithm for the ground state of one-dimensional gapped local Hamiltonians. *Nature Physics*, 2015. Journal version of [36].
- [16] Anurag Anshu, Itai Arad, and Thomas Vidick. Simple proof of the detectability lemma and spectral gap amplification. *Physical Review B*, 93(20):205142, 2016.
- [17] R. Arnon-Friedman, R. Renner, and T. Vidick. Non-signaling parallel repetition using de Finetti reductions. *IEEE Transactions on Information Theory*, 62(3):1440–1457, March 2016.
- [18] Carlos Palazuelos and Thomas Vidick. Survey on nonlocal games and operator space theory. *Journal of Mathematical Physics*, 57(1):015220, 2016.

- [19] Stefano Pironio, Valerio Scarani, and Thomas Vidick. Focus on device independent quantum information. *New Journal of Physics*, 18(10):100202, 2016.
- [20] Thomas Vidick. Three-player entangled XOR games are NP-hard to approximate. *SIAM Journal on Computing*, 45(3):1007–1063, 2016. Journal version of [34].
- [21] Thomas Vidick and John Watrous. Quantum proofs. *Foundations and Trends® in Theoretical Computer Science*, 11(1-2):1–215, 2016.
- [22] Itai Arad, Zeph Landau, Umesh Vazirani, and Thomas Vidick. Rigorous RG algorithms and area laws for low energy eigenstates in 1D. *Communications in Mathematical Physics*, 2017. Journal version of [41].
- [23] David Gosset, Jenish C. Mehta, and Thomas Vidick. QCMA hardness of ground space connectivity for commuting Hamiltonians. *Quantum*, 1:16, July 2017.
- [Conference proceedings \(refereed\)](#)
- [24] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick. Entangled games are hard to approximate. In *IEEE Annual Symposium on Foundations of Computer Science*, FOCS '08, pages 447–456, Los Alamitos, CA, USA, 2008. IEEE Computer Society.
- [25] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using entanglement in quantum multi-prover interactive proofs. In *Proceedings of the 2008 IEEE 23rd Annual Conference on Computational Complexity*, CCC '08, pages 211–222, Washington, DC, USA, 2008. IEEE Computer Society.
- [26] Joshua Brody, Amit Chakrabarti, Oded Regev, Thomas Vidick, and Ronald De Wolf. Better gap-hamming lower bounds via better round elimination. In *Proceedings of the 13th international conference on Approximation, Randomization, and combinatorial optimization: algorithms and techniques*, APPROX/RANDOM'10, pages 476–489, Berlin, Heidelberg, 2010. Springer-Verlag.
- [27] Anindya De and Thomas Vidick. Near-optimal extractors against quantum storage. In *Proceedings of the 42nd ACM symposium on Theory of computing*, STOC '10, pages 161–170, New York, NY, USA, 2010. ACM.
- [28] Julia Kempe and Thomas Vidick. Parallel repetition of entangled games. In *Proceedings of the 43rd ACM symposium on Theory of Computing*, STOC '11, pages 353–362, 2011.
- [29] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for NEXP sound against entangled provers. In *IEEE Annual Symposium on Foundations of Computer Science*, FOCS '12, Los Alamitos, CA, USA, 2012. IEEE Computer Society. Recipient of the Best Paper Award.
- [30] Abel Molina, Thomas Vidick, and John Watrous. Optimal counterfeiting attacks and generalizations for Wiesner's quantum money. In *7th Conference on Theory of*

Quantum Computation, Communication, and Cryptography (TQC'12), volume 7582 of *Lecture Notes in Computer Science*. Springer, 2012.

- [31] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proceedings of the 44th ACM symposium on Theory of Computing*, STOC '12, pages 61–76. ACM, 2012.
- [32] Assaf Naor, Oded Regev, and Thomas Vidick. Efficient rounding for the noncommutative Grothendieck inequality. In *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 71–80, New York, NY, USA, 2013. ACM.
- [33] Oded Regev and Thomas Vidick. Quantum XOR games. In *Computational Complexity (CCC), 2013 IEEE Conference on*, pages 144–155, June 2013.
- [34] Thomas Vidick. Three-player entangled XOR games are NP-hard to approximate. In *IEEE Annual Symposium on Foundations of Computer Science*, FOCS '13, Los Alamitos, CA, USA, 2013. IEEE Computer Society.
- [35] Irit Dinur, David Steurer, and Thomas Vidick. A parallel repetition theorem for entangled projection games. In *Proceedings of the 2014 IEEE 29th Conference on Computational Complexity*, CCC '14, pages 197–208, Washington, DC, USA, 2014. IEEE Computer Society.
- [36] Zeph Landau, Umesh Vazirani, and Thomas Vidick. An efficient algorithm for finding the ground state of 1D gapped local Hamiltonians. In *Proceedings of the 5th Conference on Innovations in Theoretical Computer Science*, ITCS '14, pages 301–302, New York, NY, USA, 2014. ACM.
- [37] Laura Mancinska and Thomas Vidick. Unbounded entanglement can be needed to achieve the optimal success probability. In Javier Esparza, Pierre Fraigniaud, Thore Husfeldt, and Elias Koutsoupias, editors, *Automata, Languages, and Programming*, volume 8572 of *Lecture Notes in Computer Science*, pages 835–846. Springer Berlin Heidelberg, 2014.
- [38] Umesh Vazirani and Thomas Vidick. Robust device independent quantum key distribution. In *Proceedings of the 5th Conference on Innovations in Theoretical Computer Science*, ITCS '14, pages 35–36, New York, NY, USA, 2014. ACM.
- [39] Matthew Coudron and Thomas Vidick. Interactive proofs with approximately commuting provers. In *Automata, Languages, and Programming (ICALP)*, pages 355–366. Springer, 2015.
- [40] Joseph Fitzsimons and Thomas Vidick. A multiprover interactive proof system for the local Hamiltonian problem. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science (ITCS)*, pages 103–112. ACM, 2015.

- [41] Itai Arad, Zeph Landau, Umesh Vazirani, and Thomas Vidick. Rigorous RG algorithms and area laws for low energy eigenstates in 1D. In *Proceedings of the 2017 Conference on Innovations in Theoretical Computer Science (ITCS)*, 2017.
- [42] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Hardness amplification for entangled games via anchoring. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 303–316. ACM, 2017.
- [43] Mohammad Bavarian, Thomas Vidick, and Henry Yuen. Parallel repetition via fortification: analytic view and the quantum case. In *Proceedings of the 2017 Conference on Innovations in Theoretical Computer Science (ITCS)*, 2017.
- [44] Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Overlapping qubits. In *Proceedings of the 2017 Conference on Innovations in Theoretical Computer Science (ITCS)*, 2017.
- [45] Anand Natarajan and Thomas Vidick. A quantum linearity test for robustly verifying entanglement. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1003–1015. ACM, 2017.
- [Preprints \(not refereed\)](#)
- [46] Dorit Aharonov, Itai Arad, and Thomas Vidick. The quantum PCP conjecture, 2013.
- [47] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. Simple and tight device-independent security proofs. *arXiv preprint arXiv:1607.01797*, 2016.
- [48] Steven Heilman and Thomas Vidick. A moment majorization principle for random matrix ensembles with applications to hardness of the noncommutative Grothendieck problem. *arXiv preprint arXiv:1603.05620*, 2016.
- [49] Dimiter Ostrev and Thomas Vidick. Entanglement of approximate quantum strategies in XOR games. *arXiv preprint arXiv:1609.01652*, 2016.
- [50] Rui Chao, Ben W. Reichardt, Chris Sutherland, and Thomas Vidick. Test for a large amount of entanglement, using few measurements. 2017.
- [51] Brenden Roberts, Thomas Vidick, and Olexei I Motrunich. Rigorous renormalization group method for ground space and low-energy states of local hamiltonians. *arXiv preprint arXiv:1703.01994*, 2017.
- [52] Thomas Vidick. Parallel diqkd from parallel repetition. *arXiv preprint arXiv:1703.08508*, 2017.