Thomas Vidick

Postdoctoral Associate, MIT

32 Vassar Street
02139 Cambridge MA, USA
📞 *+1 (310) 735 7850*
✉ *vidick@csail.mit.edu*
🖥 *people.csail.mit.edu/vidick*

Nationality: Belgium
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

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, Grade 19/20.
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, Grade 19/20.
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 [17].

○ 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).

○ 4-year full support undergraduate scholarship from École Normale Supérieure, Paris (2002-2007).

Recent invited talks

Jan. 2013 **Fully device-independent quantum key distribution**, *Beijing, China*, invited **plenary talk** at QIP'13.

Jan. 2013 **NEXP $\subseteq$ MIP***, *Beijing, China*, invited **plenary talk** at QIP'13.

Nov. 2012	**Fully device-independent quantum key distribution**, *Ottawa, Canada*, CIFAR Workshop on quantum information theory.
Oct. 2012	**Efficient rounding for the noncommutative Grothendieck inequality**, *UC Berkeley*, Theory lunch.
Sept. 2012	**Certifiable Quantum Dice**, *Invited talk at QCRYPT'12, Singapore*.
Apr. 2012	**On the complexity of multi-prover interactive proofs with entangled provers**, *IQC Waterloo*, Workshop on Recent Progress in Quantum Algorithms. Talk also given in the CS seminar at CQT, Singapore, Sept. 2012..
Feb. 2012	**Certifiable Quantum Dice**, *MIT, Cambridge*, TOC Colloquium.
Jan. 2012	**Non-commutative Grothendieck inequalities and Quantum XOR games**, *CIRM Marseille*, Workshop on the geometry of entanglement. Talk also given in the joint CS-Math seminar of Northeastern university, Boston, Mar. 2012.

Teaching Experience

Dec. 2012	**Guest lecture on quantum interactive proofs**, *MIT*. Graduate quantum complexity class taught by Scott Aaronson.
Jul. 2012	**Supervised a high-school student from MIT's RSI program on a daily basis.**. Worked on implementing numerical algorithms for estimating Bell inequality violations.
2009-2010	**Tutoring of undergraduate students**, *UC Berkeley*. Introductory computer science courses EECS70 and CS170.
Fall '08	**Teaching Assistant for EECS70**, *UC Berkeley*. Discrete Math and Probability
2003–2006	**Preparation to Oral Exams in Mathematics and Computer Science (Caml)**, *Classes Préparatoires Saint-Louis, Paris*. Given to students in their second year of University.
2004–2006	**Tutoring in mathematics.**. Several private students from college and the two first years of university. Intensive week-long courses given to classes of 7 to 15 students preparing for the "Grandes Écoles".

Professional service

PC Member	QIP 2012, QCRYPT 2012.
Reviewer	SIAM Journal on Computing, JACM, TOC, Complexity, STOC, FOCS, CCC, QIP, Crypto, Quantum Information & Computation.
Organizer	Berkeley quantum reading group, Fall '09, Spring '10, Fall '10, Spring '11. Berkeley Theory Student's seminar, Fall '08.

Professional organizations

Member	Association for Computing Machinery (ACM), American Physical Society (APS).

References

○ **Scott Aaronson** (Postdoc mentor), Massachusetts Institute of Technology, aaronson@csail.mit.edu

○ **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

○ **Andrew Chi-Chi Yao**, Tsinghua University, andrewcyao@yahoo.com

Publications

Journals

[1] Oded Regev and Thomas Vidick. Elementary proofs of Grothendieck theorems for completely bounded norms. *Journal of Operator Theory*, 2012. To appear.

[2] Jop Briët, Harry Buhrman, Troy Lee, and Thomas Vidick. Multipartite entanglement in XOR games. *Quantum Information and Computation*, 2013. To appear.

[3] Jop Briët and Thomas Vidick. Explicit lower and upper bounds on the entangled value of multiplayer XOR games. *Communications in Mathematical Physics*, 2012.

[4] 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.

[5] 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 [19].

[6] 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.

[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] Julia Kempe, Hirotada 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].

[9] 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.

[10] Thomas Vidick and Stephanie Wehner. More nonlocality with less entanglement. *Phys. Rev. A*, 83:052310, May 2011.

[11] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18:273–307, 2009. Journal version of [23].

[12] Phong Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*, 2(2):181–207, 2008.

[13] Guillaume Ricotta and Thomas Vidick. On the asymptotic height of heegner points. *Canadian Journal of Matematics*, 60(6):1406–1436, 2008.

Conference proceedings

[14] Oded Regev and Thomas Vidick. Quantum XOR games, 2013. To appear in CCC'13; accepted for a talk at QIP'13. Technical report arXiv:1207.4939.

[15] Assaf Naor, Oded Regev, and Thomas Vidick. Efficient rounding for the noncommutative Grothendieck inequality, 2013. To appear in STOC'13. Technical report arXiv:1210.7656.

[16] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution, 2013. To appear in STOC'13; selected for a plenary talk at QIP'13. Technical report arXiv:1210.1810.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[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.

Preprints

[25] Thomas Vidick. Three-player entangled XOR games are NP-hard to approximate, 2013. Technical report arXiv:1302.1242.