Thomas Vidick

Professor
California Institute of Technology

1200 E. California Blvd.
Pasadena, CA 91125
+1 (310) 735 7850
vidick@caltech.edu
users.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

2022–present **Professor**, *Weizmann Institute of Science*, Rehovot

2018–present **Professor**, *California Institute of Technology*, Pasadena

Sept. 2020–Feb. 2021 **FSMP Research Chair**, *Paris, France*

2017–2018 **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, Advisor: 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

- **Held Prize** of the U.S. National Academy of Science, 2023
- **Simons Investigator Award**, 2021-2026
- INRIA International chair. 2020-2025

- Laureate of an FSMP Research Chair, Fall 2020
- **Presidential Early Career Award** (PECASE), 2019.
- 2017-2018 Associated Students of the California Institute of Technology (ASCIT) Teaching Award.
- **CIFAR Azrieli Global Scholar** award, 2017-2019.
- 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.
- My Ph.D. thesis was awarded the **Bernard Friedman Memorial Prize** in Applied Mathematics from U.C. Berkeley's Department of Mathematics.

Courses taught at Caltech

CS38	Introduction to Algorithms. Spring '18.
CMS139	Advanced Algorithms. Spring'15, Winter'16, '17, '18, '19, '20.
CS/Phys 120	Quantum Cryptography. Fall'16, Fall'19. Also offered as an EdX MOOC.
CS152	Introduction to Theoretical Cryptography. Spring'16, Fall'18, Fall'21.
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), Anand Natarajan (2018-2020), Alexandru Gheorghiu (2018-2020), John Wright (2019-2020), Lynn Chua (2020-2021), Ulysses Chabaud (2020-), Atual Arora (2020-), Jiayu Zhang (2021-)
Graduate students	Milan Cvitkovic (2015-2019), Andrea Coladangelo (2015-2019), Jenish Mehta (2014-2021), Spencer Gordon (2017-2022), Alexander Poremba (2018-), Hsin-Yuan Huang (2018-), Jiaqing Jiang (2020-), Danil Akhtiamov (2021-), William King (2021-).
Undergraduates	Mahrud Sayrafi (SURF, Summer'14), Shannon Wang (SURF, Summer'15), Nick Haliday (SURF, Summer'15), Chinmay Nirkhe (Spring and Fall'16), Jalex Stark (Spring-Summer'17), Marc Mulheisen (Summer '19), Tina Zhang (Summer '19), Helena Guan (Fall'19), Jack Maxfield (Summer'20), Laura Lewis (Summer'20).

Workshop organization

IPAM summer school on quantum cryptography	*August 2020, Institute for Pure and Applied Mathematics, Los Angeles.* One-week school addressed at graduate students in mathematics and computer science.
The Quantum Wave in Computing	*Jan. 14 - May. 15 2020, Simons Institute, Berkeley.* Four-month program co-organized with Andrew Childs, Ignacio Cirac and Umesh Vazirani. Includes three international workshops.

Summer Cluster: Challenges in Quantum Computation	*May. 29 - Jul. 20 2018, Simons Institute, Berkeley.* Two month program co-organized with Andrew Childs, Ignacio Cirac and Umesh Vazirani. Around 40 participants and an international week-long workshop.
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.

Affiliations

INRIA International Research Chair	INRIA, France. 2020-2025.
Chaire FSMP	FSMP, France. Fall 2020.
Visiting Senior Research Fellow	Centre for Quantum Technologies, NUS, Singapore. (2016–2022)
Visiting Fellow	Perimeter Institute, Waterloo, Canada. (2017–)

Professional service

Managing Editor	Theory of Computing, `theoryofcomputing.org` (2014–)
Editor	Journal of the ACM (2019–)
Editor	ACM Transactions in quantum computing (2019–)
Editorial Board	Phys. Rev. A, `https://journals.aps.org/pra/` (2018–)
Steering Committee	Innovations in Theoretical Computer Science (ITCS), `itcs-conf.org` (2018-2022)
Steering Committee	Quantum Information Processing (QIP), `qip-conference.org` (2021–)
PC Chair	QCRYPT 2017, ITCS 2020, FOCS 2022
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, ITCS 2019, RANDOM 2019, ITCS 2020, STOC 2021

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	Mathematics of Information seminar, 2018–2022. Caltech Theory seminar, 2014–2018. 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

- ERC Consolidator Award, "Verification of Noisy Quantum Devices at Scale", 2022-2027
- AFOSR Grant FA9550-21-S-0001, "Secure Interactions with Quantum Devices", 2022-2027
- Simons Investigator, 2021-2026.
- co-PI on NSF QLCI and DOE QSA centers, 2020-2025.
- co-PI on DARPA project on post-quantum cryptography, 2020-2024.
- CIFAR QIS program member, 2019-2024.
- Schwartz/Reisman Collaborative Science Program: collaborative grant with Zvika Brakerski, 2019-2020.
- CIFAR Azrieli Global Scholar, QIS program, 2017-2019.
- Lead 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.

Recent invited talks

27, 29 and 31 March 2023	**Connes Embedding Problem, Tsirelson's Problem and MIP*=RE** , *Marston Morse Lectures*, Institute for Advanced Study, Princeton
27 and 28 February 2023	**Verification of quantum computations**, *Technion Graduate Winter School on Challenges and advances in quantum computing*, Sde Boker
22 November 2022	**Quantum soundness of testing tensor codes**, *Tel-Aviv University Theory Seminar*
4 August 2021	**MIP* = RE and Tsirelson's problem**, *ICMP (invited Plenary)*, Geneva
29 June 2021	**Cassical proofs of Quantum Knowledge**, *Dagstuhl Seminar*

17 March 2021 **Cryptographic tests of quantumness**, *Seminaire du DI*, Ecole Normale Superieure, Paris (online)

11 Ferburary 2021 **Testing quantum systems in the high-complexity regime**, *Max Planck distinguished speaker series on quantum computing*, Max Planck Institute, Germany (online)

2 Feburary 2021 **Connes embedding problem, Tsirelson's problem, and MIP* = RE**, *Caltech operator algebras seminar (online)*

1 February 2021 **MIP* = RE and Tsirelson's problem**, *Invited plenary talk at QIP 2021*, Munich, Germany (online)

3 December 2020 **MIP* = RE and Tsirelson's problem**, *Invited plenary talk at IQFA conference*, Grenoble, France (online)

26 November 2020 **MIP* = RE**, *Operator Algebras Seminar*, Université Paris 6, France (online)

28 July 2020 **MIP* = RE: Verifying the halting problem with quantum provers**, *Invited talk at CCC' 2020 conference*, Saarbrucken, Germany (online)

4 May 2020 **Tsirelson's problem in quantum information and connections with operator algebras and quantum complexity theory**, *Math Colloquium*, Tel-Aviv University (online)

8 January 2020 **The complexity-theoretic approach to Connes' Embedding Problem**, *Functional Analysis Seminar*, UCLA

15 December 2019 **Quantum Protocols**, *Three lectures given at the 4th Winter School in Computer Science and Engineering*, Hebrew Univerity, Jerusalem

17 September 2019 **Secure Computation with Quantum Devices: From Device-Independent Cryptography to Verification of Quantum Computers**, *US-Israel Blavatnik Scientific Forum on computer science and its impact on our future*, Jerusalem, Israel

15 July 2019 **A complexity-theoretic approach to disproving Connes' Embedding Problem**, *Workshop on The Many Faceted Connes Embedding Problem*, Banff, Canada

18 June 2019 **Topics in quantum complexity & cryptography**, *Invited survey at It for Qubit summer school*, Kyoto, Japan

15 June 2019 **Survey on quantum program checking and quantum multiprover interactive proof systems**, *Invited talk at HALG 2019*, Copenhagen, Denmark

10 May 2019 **Computationally-secure and composable remote state preparation**, *Bay area crypto day*, Stanford, CA

3 Apr. 2019 **Cryptographic tests of quantumness**, *Invited distinguished lecture*, Hebrew University, Jerusalem

18 Jan. 2019 **Classical verification of quantum computations**, *Invited talk at the JMM 2019*, Baltimore, MD

13 Jan. 2019 **A Cryptographic Test of Quantumness and Certifiable Randomness from a Single Quantum Device**, *Contributed talk at QIP'19*, Boulder, CO

13 Jan. 2019 **Verification of quantum computations**, *Invited tutorial at QIP'19*, Boulder, CO