

Atul Singh ARORA

ADDRESS: 166 N Allen Av., Pasadena, CA 91106, USA
PHONE: +1 626 318 0732, +1 626 515 4073
EMAIL: asarora@caltech.edu, atul.singh.arora@gmail.com
WEB: AtulSinghArora.github.io

RESEARCH EXPERIENCE

- 2021-present | PostDoc, CALIFORNIA INSTITUTE OF TECHNOLOGY, United States
Advisor: Prof. Thomas VIDICK
Primarily studied hybrid models where depth bounded quantum circuits, can be interleaved with BPP machines.
Showed oracle separations among the different hybrid models.¹
Characterised quantum depth, relative to a random oracle.²
On the side, worked on quantum foundations and quantum coin flipping.
Motivated by contextuality, demonstrated self-testing of a single quantum system (includes both theory and experiment).³
Introduced methods to improve the security of device-independent weak coin flipping protocols, resulting in an improvement after a decade.⁴
Solutions to Quantum Weak Coin Flipping—collected all our previous results on the topic into a journal version.⁵
- ¹ ASA, A. Gheorghiu, U. Singh. [arXiv:2201.01904](https://arxiv.org/abs/2201.01904) (submitted; [web](#))
² ASA, Coladangelo, Coudron, Gheorghiu, Singh, Waldner. [arXiv:2210.06454](https://arxiv.org/abs/2210.06454) (STOC '23)
³ X. Hu, Y. Xie, ASA, M. Ai, K. Bharti, et. al. [arXiv:2203.09003](https://arxiv.org/abs/2203.09003) (submitting)
⁴ ASA, J. Sikora, T Van Himbeeck (submitting; [overleaf](#), [web](#))
⁵ ASA, J. Roland, C. Vlachou, S. Weis. [cryptoeprint:2022/1101](https://arxiv.org/abs/2012.1101) (submitting)
- 2016-20 | PhD Thesis, UNIVERSITÉ LIBRE DE BRUXELLES (ULB), Belgium
Quantum Weak Coin Flipping
Advisor: Prof. Jérémie ROLAND
Primarily worked on quantum weak coin flipping, a cryptographic primitive. Its figure of merit is called the bias, ϵ . The best known had $\epsilon \rightarrow 1/6$ by C. Mochon in 2005.
Protocols with $\epsilon \rightarrow 1/10$ were found¹.
An algorithm to numerically find protocols with $\epsilon \rightarrow 0$ was given¹.
An exact (geometric) solution to the problem was found².
A simpler, exact (algebraic) solution to the problem was found³.
On the side, investigated foundational aspects of quantum mechanics⁴.
- ¹ASA, J. Roland, S. Weis. [arXiv:1811.02984](https://arxiv.org/abs/1811.02984) (QIP '19 STOC '19 [web](#))
²ASA, J. Roland, C. Vlachou. [arXiv:1911.13283v1](https://arxiv.org/abs/1911.13283v1) ([web](#))
³ASA, J. Roland, C. Vlachou. [arXiv:1911.13283v2](https://arxiv.org/abs/1911.13283v2) (QCrypt '20 QIP '21 SODA '21 [web](#))
⁴K. Bharti, A.S.A, L. C. Kwek, J. Roland. [arXiv:1811.05294](https://arxiv.org/abs/1811.05294) (Phys. Rev. Res. 2, 033010)
- 2015-16 | Master's Thesis, INDIAN INSTITUTE OF SCIENCE EDUCATION AND RESEARCH (IISER), MOHALI, India
Contextuality in a Deterministic Quantum Theory
Advisor: Prof. Arvind
Concluded that contextuality is not a necessary feature of quantum mechanics and proposed an alternative, non functional-consistency, bolstered by an explicit construction.
ASA, K. Bharti, Arvind. [arXiv:1607.03498](https://arxiv.org/abs/1607.03498); [Physics Letters A. \(Nov 2018\)](#)
- SUMMER | Internship UNIVERSITY OF SIEGEN, Germany

- 2015 | *Towards a macroscopic test of local realism*
 Advisor: Prof. Otfried GÜHNE
 Constructed a Bell inequality using observables bounded in phase space to probe local realism using macroscopic variables.
 ASA, A. Asadian. [arXiv:1508.04588](https://arxiv.org/abs/1508.04588); *Phys. Rev. A* **92**, 061207
- 2011-14 | Internships
 IISER MOHALI, India. Quantum simulation (theory). Advisor: Prof Arvind.
 NATIONAL PHYSICAL LABORATORY (NPL), New Delhi, India. Set up an experiment to study the dynamics of a dipole lattice. Advisor: Dr Ravi MEHROTRA.
 INDIAN INSTITUTE OF TECHNOLOGY (IIT), BOMBAY, INDIA. Yarn defect recognition using OpenCV. Advisor: Prof Anirban GUHA.

EDUCATION

- SEP 2020 | Doctorat en Sciences de l'ingénieur et technologie,
 OCT 2016 | **Université libre de Bruxelles (ULB)**, Belgium.
- JULY 2016 | Bachelor and Master of Science with PHYSICS major,
 JULY 2011 | **Indian Institute of Science Education and Research (IISER), Mohali**, India.
 CPI: 9.4 /10. Graduated with *rank two*.

CONFERENCES AND SEMINARS

- 2023 | **Talk** (Scheduled). *Quantum Depth in the Random Oracle Model*
 Symposium on Theory of Computing (STOC). Orlando, Florida, USA.
- 2022 | **Poster**. *Oracle separations of hybrid quantum-classical circuits*
 Quantum Information Processing (QIP). Caltech, USA
- 2022 | **Poster**. *Improving the security of device independent weak coin flipping protocols.*
 Quantum Information Processing (QIP). Caltech, USA
- 2021 | **Talk**. *Analytic quantum weak coin flipping protocols with arbitrarily small bias.*
 ACM-SIAM Symposium on Discrete Algorithms (SODA). Virtual.
- 2021 | **Invited Seminar**. *Analytic quantum weak coin flipping protocols ...*
 University of Ottawa (Online). Prof. Broadbent's group.
- 2021 | **Talk**. *Analytic quantum weak coin flipping protocols ...*
 Quantum Information Processing (QIP). Online/Munich, Germany.
- 2020 | **Talk**. *Analytic quantum weak coin flipping protocols ...*
 QCRYPT. Online/Amsterdam, Netherlands.
- 2020 | **Invited Seminar**. *Quantum weak coin flipping*
 Perimeter Institute, Canada.
- 2019 | **Participant**.
 QUANTALGO Workshop. CWI, Amsterdam, Netherlands.
- 2019 | **Participant**.
 (Physics) Lindau Nobel Laureate Meeting (LINO). Lindau, Germany.
- 2019 | **Talk**. *Quantum Weak Coin Flipping.*
 Symposium on Theory of Computing (STOC). Phoenix, Arizona, USA.
- 2019 | **Talk**. *Quantum Weak Coin Flipping.*
 Quantum Information Processing (QIP). University of Colorado, USA.
- 2018 | **Talk**. *Quantum Weak Coin Flipping beyond bias 1/6.*
 QUANTALGO Workshop. Université Paris-Diderot, Paris, France.

- 2018 **Poster.** *Quantum Weak Coin Flipping with bias 1/10.*
Quantum Information Processing (QIP). TU Delft, Netherlands.
- 2017 **Participant.**
Theory of Quantum Computation, Communication and Cryptography (TQC). Paris, France.

RECOGNITION

- 2023 *Hartree Postdoctoral Fellowship*, University of Maryland.
- 2020 *IQIM Postdoctoral Scholarship*, California Institute of Technology.
- 2020 Offered. *Hartree Postdoctoral Fellowship*, University of Maryland.
- 2019 Granted financial support for attending the *(Physics) Lindau Nobel Laureate Meeting, 2019.*
- 2018 Renewed. Two year research fellowship from the Belgian *Fonds National Recherche de Science (FNRS)*, through the FRIA grant.
- 2016 Awarded. Two year research fellowship from the Belgian *Fonds National Recherche de Science (FNRS)*, through the FRIA grant.
- 2015 Awarded the *Junior Research Fellowship (JRF-NET)* from the Council of Scientific and Industrial Research, India.
- 2015 Awarded the *DAAD WISE* fellowship for a summer internship by and in Germany.
- 2013-16 Awarded the Certificate of Merit for the best academic performance in a semester, twice by IISER. Was among the highest scorers four other times.
- 2012 Awarded the *KVPY* fellowship for my work on Stepper Motor Control, by DST, India.
- 2010 Granted financial support for attending the Bright Green Youth climate summit, Denmark.

TEACHING

- 2022 Tutor. Week-long graduate school on post-quantum cryptography. IPAM, UCLA.
- 2019 Teaching Assistant. Information Quantique (graduate). ULB, Brussels.
- 2016 Teaching Assistant. Thermodynamics (undergraduate). IISER, Mohali.
- 2015 Teaching Assistant. Classical Mechanics (undergraduate). IISER, Mohali.

REVIEW

Reviewed articles for the following conferences/journals.

- 2022 MFCS, JACM and QIP
- 2021 QCrypt
- 2019 QIP, STOC

LANGUAGES

- ENGLISH: Fluent
- HINDI: Fluent
- FRENCH: Intermediate
- PUNJABI: Intermediate
- GERMAN: Beginner

INTERESTS & EXTRACURRICULAR

Technology, Open-Source, Programming (C/C++, Python, Fortran, Javascript);
Philosophy, Reading;
Fitness; Piano, Guitar, Violin.