

Atul Singh ARORA

ADDRESS: 1318 Cordova St, Pasadena, CA 91106, USA

PHONE: +1 626 318 0732, +1 626 515 4073

EMAIL: asarora@caltech.edu, atul.singh.arora@gmail.com

RESEARCH EXPERIENCE

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

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

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

- 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.
- 2016 Top 5% in the physics stream of the *Graduate Aptitude Test in Engineering (GATE)*, India.
Obtained a 92.3 percentile in the national graduate physics exam, *Joint Entrance Screening Test (JEST)*, India.
- 2015 Awarded the *Junior Research Fellowship (JRF-NET)* from the Council of Scientific and Industrial Research, India.
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.

List of Publications

Last updated: 7 November, 2022

Among these [3,6,7] are my favourite.

1 Pre-prints

- 2022 [1] **Nov. 2022** (with Jamie Sikora and Thomas Van Himbeeck). ‘Improving the security of device-independent weak coin flipping protocols’. In: Preparation. URL: <https://www.overleaf.com/read/jhwnvgbntqkd>.
- [2] **5th Jan. 2022** (with Alexandru Gheorghiu and Uttam Singh). ‘Oracle Separations of Hybrid Quantum-Classical Circuits’. In: arXiv:2201.01904. DOI: 10.48550/arXiv.2201.01904.
- [3] **12th Oct. 2022** (with Andrea Coladangelo, Matthew Coudron, Alexandru Gheorghiu, Uttam Singh and Hendrik Waldner). ‘Quantum Depth in the Random Oracle Model’. In: arXiv:2210.06454. DOI: 10.48550/arXiv.2210.06454.
- [4] **16th Mar. 2022** (with Xiao-Min Hu, Yi Xie, Ming-Zhong Ai, Kishor Bharti, Jie Zhang, Wei Wu, Ping-Xing Chen, Jin-Ming Cui, Bi-Heng Liu, Yun-Feng Huang, Chuan-Feng Li, Guang-Can Guo, Jérémie Roland, Adán Cabello and Leong-Chuan Kwek). ‘Self-Testing of a Single Quantum System: Theory and Experiment’. In: arXiv:2203.09003. DOI: 10.48550/arXiv.2203.09003.
- [5] **29th Aug. 2022** (with Jérémie Roland, Chrysoula Vlachou and Stephan Weis). ‘Solutions to Quantum Weak Coin Flipping’. In: Cryptology ePrint Archive, Paper 2022/1101. URL: <https://eprint.iacr.org/2022/1101>.

2 Proceedings

- 2021 [6] **Mar. 2021** (with Jérémie Roland and Chrysoula Vlachou). ‘Analytic Quantum Weak Coin Flipping Protocols with Arbitrarily Small Bias’. In: *Proceedings of the Thirty-Second Annual ACM-SIAM Symposium on Discrete Algorithms*. SODA ’21. USA: Society for Industrial and Applied Mathematics, pp. 919–938. ISBN: 978-1-61197-646-5.
- 2019 [7] **June 2019** (with Jérémie Roland and Stephan Weis). ‘Quantum weak coin flipping’. In: *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing - STOC 2019*. ACM Press. DOI: 10.1145/3313276.3316306.

3 Articles

- 2020 [8] **July 2020** (with Kishor Bharti, Leong Chuan Kwek and Jérémie Roland). ‘Uniqueness of All Fundamental Noncontextuality Inequalities’. In: *Physical Review Research* 2.3, p. 033010. ISSN: 2643-1564. DOI: 10.1103/PhysRevResearch.2.033010. (Visited on 08/06/2022).
- 2019 [9] **Feb. 2019** (with Kishor Bharti and Arvind). ‘Revisiting the admissibility of non-contextual hidden variable models in quantum mechanics’. In: *Physics Letters A* 383.9, pp. 833–837. DOI: 10.1016/j.physleta.2018.11.049.
- 2015 [10] **Dec. 2015** (with Ali Asadian). ‘Proposal for a macroscopic test of local realism with phase-space measurements’. In: *Physical Review A* 92.6. DOI: 10.1103/physreva.92.062107.