

# Atul Singh ARORA

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

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

EMAIL: [asarora@caltech.edu](mailto:asarora@caltech.edu), [atul.singh.arora@gmail.com](mailto: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.<sup>1</sup></p> <p>Characterised quantum depth, relative to a random oracle.<sup>2</sup></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).<sup>3</sup></p> <p>Introduced methods to improve the security of device-independent weak coin flipping protocols, resulting in an improvement after a decade.<sup>4</sup></p> <p>Solutions to Quantum Weak Coin Flipping—collected all our previous results on the topic into a journal version.<sup>5</sup></p> <p><sup>1</sup> ASA, A. Gheorghiu, U. Singh. <a href="https://arxiv.org/abs/2201.01904">arXiv:2201.01904</a> (submitted; <a href="#">web</a>)</p> <p><sup>2</sup> ASA, Coladangelo, Coudron, Gheorghiu, Singh, Waldner. <a href="https://arxiv.org/abs/2210.06454">arXiv:2210.06454</a></p> <p><sup>3</sup> X. Hu, Y. Xie, ASA, M. Ai, K. Bharti, et. al. <a href="https://arxiv.org/abs/2203.09003">arXiv:2203.09003</a> (submitting)</p> <p><sup>4</sup> ASA, J. Sikora, T Van Himbeeck (submitting; <a href="#">overleaf</a>, <a href="#">web</a>)</p> <p><sup>5</sup> ASA, J. Roland, C. Vlachou, S. Weis. <a href="https://arxiv.org/abs/2202.1101">cryptoeprint:2022/1101</a> (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, <math>\epsilon</math>. The best known had <math>\epsilon \rightarrow 1/6</math> by C. Mochon in 2005.</p> <p>Protocols with <math>\epsilon \rightarrow 1/10</math> were found<sup>1</sup>.</p> <p>An algorithm to numerically find protocols with <math>\epsilon \rightarrow 0</math> was given<sup>1</sup>.</p> <p>An exact (geometric) solution to the problem was found<sup>2</sup>.</p> <p>A simpler, exact (algebraic) solution to the problem was found<sup>3</sup>.</p> <p>On the side, investigated foundational aspects of quantum mechanics<sup>4</sup>.</p> <p><sup>1</sup>ASA, J. Roland, S. Weis. <a href="https://arxiv.org/abs/1811.02984">arXiv:1811.02984</a> (QIP '19 STOC '19 <a href="#">web</a>)</p> <p><sup>2</sup>ASA, J. Roland, C. Vlachou. <a href="https://arxiv.org/abs/1911.13283v1">arXiv:1911.13283v1</a> (<a href="#">web</a>)</p> <p><sup>3</sup>ASA, J. Roland, C. Vlachou. <a href="https://arxiv.org/abs/1911.13283v2">arXiv:1911.13283v2</a> (QCrypt '20 QIP '21 SODA '21 <a href="#">web</a>)</p> <p><sup>4</sup>K. Bharti, A.S.A, L. C. Kwek, J. Roland. <a href="https://arxiv.org/abs/1811.05294">arXiv:1811.05294</a> (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. <a href="https://arxiv.org/abs/1607.03498">arXiv:1607.03498</a>; <a href="#">Physics Letters A. (Nov 2018)</a></p>
SUMMER 2015	<p>Internship UNIVERSITY OF SIEGEN, Germany</p> <p><i>Towards a macroscopic test of local realism</i></p> <p>Advisor: Prof. Otfried GÜHNE</p>

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.