

Title: Photonic Quantum Science and Technologies

Speakers: Urbasi Sinha

Series: Colloquium

Date: July 04, 2022 - 11:00 AM

URL: <https://pirsa.org/22070000>

Abstract: Quantum mechanics is a cornerstone of modern physics. Just as the 19th century was called the Machine Age and the 20th century the Information Age, the 21st century promises to go down in history as the Quantum Age. Quantum Computing promises unprecedented speed in solving certain classes of problems while Quantum Cryptography promises unconditional security in communications. In this talk, I will discuss the world of single and entangled photons and also discuss ongoing work towards quantum computing, quantum information and quantum cryptography in our Quantum Information and Computing lab at the Raman Research Institute, Bengaluru. I will end with our broad vision for the future, which includes establishment of long distance secure quantum communications in India and beyond involving satellite based, fibre based as well as integrated photonics based approaches towards the global quantum internet.

Zoom Link: <https://pitp.zoom.us/j/94788493307?pwd=QTIUaTY4Nm1IS3hyeUFibVFKV3RMQT09>

Photonic Quantum Science and Technologies



QuEST



Prof. Urbasi Sinha



RRI



QuIC

π : Quantum Information & Computing (QuIC) Lab

Raman Research Institute (RRI), Bengaluru, India.

Affiliate Faculty at IQC, Waterloo, Canada & CQIQC, Toronto, Canada

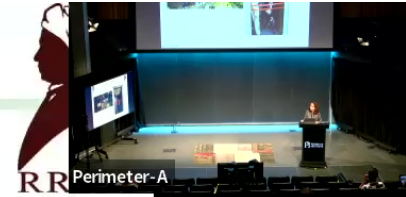
Simon's Emmy Noether fellow at Perimeter Institute, Canada.

Perimeter 2022





And so our journey began....



Perimeter 2022





QuIC



**Today's science is
tomorrow's technology.**

**-Edward Teller, The
Legacy Of Hiroshima**

www.quoteslyfe.com

Perimeter 2022



QulC



केन्द्रीय बजट
UNION BUDGET 2020

Budget 2020 announced Rs 8,000 crore over the next 5-yrs in the National Mission on Quantum technology and its applications

- The areas of focus for the NM-QTA Mission will be in fundamental science, translation, technology development and towards addressing issues concerning national priorities
- The mission can help prepare next generation skilled manpower, boost translational research and also encourage entrepreneurship and start-up ecosystem development.
- Quantum principles will be used for engineering solutions to extremely complex problems in computing, communications, sensing, chemistry, cryptography, imaging and mechanics



- Their applications which will be boosted include those in aero-space engineering, numerical weather predictions, simulations, securing the communications & financial transactions, cyber security, advanced manufacturing, health, agriculture, education
- It can bring India in the list of few countries with an edge in this emerging field will have a greater advantage in garnering multifold economic growth and dominant leadership role

Perimeter 2022





QuIC



The Big Picture.....

Our theoretical understanding of the universe very incomplete. We don't understand more than 80% of what the universe is made of. How well do we understand the laws? A tiny modification of these laws have deep implications in cosmology.

Eg. The Euler-Heisenberg Lagrangian leads to non-linear modifications of electrodynamics and is known to be an important modification in the context of the early universe.

Fundamental tests VERY important.

Perimeter 2022



QuIC



- Quantum Computation is a very important research direction. Quantum computers are projected to be able to solve certain problems for which there is no efficient classical algorithm. Also, some solutions will be exponentially faster than what is possible in classical computation.
- Quantum Cryptography can guarantee perfectly secure communication.

Our lab deals with experimental as well as theoretical problems relating to fundamental tests of quantum mechanics, quantum computation and quantum communication.

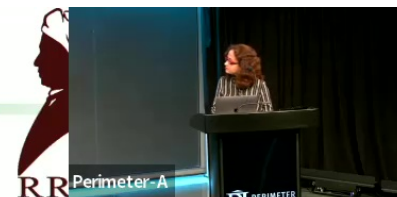
Perimeter 2022





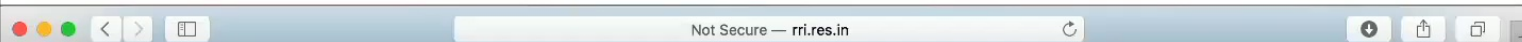
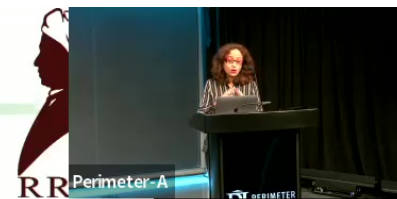
QuIC

<https://wwws.rri.res.in/quic>



- **Quantum Optics lab ----- Class 10000 clean room.**
- **Adjacent lab to be converted to Class 100 clean room – Towards Hybrid Quantum Computing.**
- **Highly modulated environment with precise control on temperature and humidity.**
- **Leading Quantum Optics lab of its kind in India** - primarily dedicated to research in Quantum Information, Computation and Communication.

Perimeter 2022



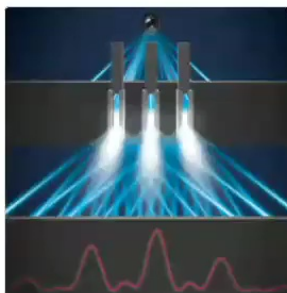
[QuIC](#) [Research](#) [Publications](#) [Lab News](#) [People](#) [Gallery](#) [Job Opportunities](#) [Contact Us](#)

Hi 114.214.254.155, Welcome to QuIC Lab

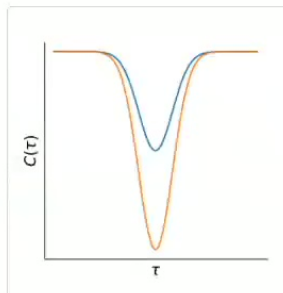
The Quantum Information and Computing (QuIC) lab at the Raman Research Institute, Bangalore is one of the first labs in India to manufacture and establish the usage of heralded and entangled photon sources towards various applications in quantum technologies. We are at present concentrating on four broad themes of research.



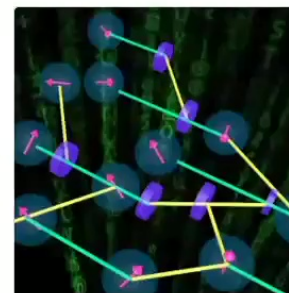
Quantum
Communication



Quantum
Computation

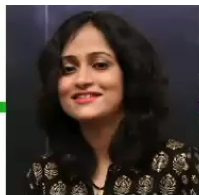


Quantum
Optics

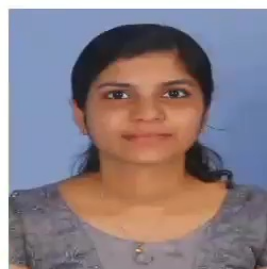
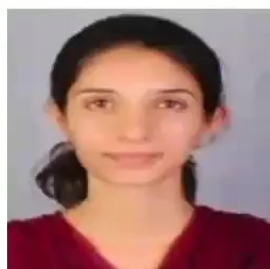
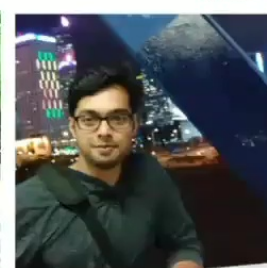
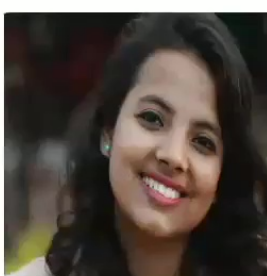
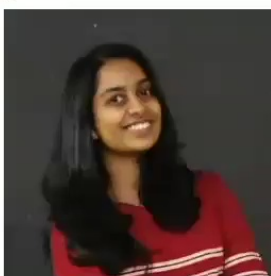
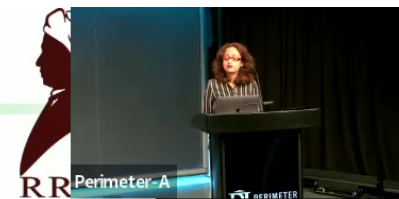


Quantum
Fundamentals & QIP

Perimeter 2022



(Most) Current members of QuIC lab



+ Shashank +
Madhumati

Perimeter 2022



Current members:

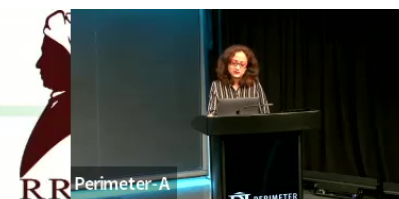
1. Dr. Satyaranjan Behera (Research Scientist C)
2. Dr. Kaumudibikash Goswami (Research Scientist C)
3. Dr. Mandira Pal (senior post doc)
4. Dr. Animesh S Roy (Post Doc)
5. Sourav Chatterjee (Research Scientist C)
6. S. Narayan Sahoo (PhD)
7. R. Chatterjee (PhD)
8. S Chakraborti (PhD)
9. Saumya Ranjan Behera (PhD)
10. Mehak Layal (PhD)
11. Ashlin Jacob (PhD)
12. Prabhakaran S (Project engineer)
13. Bela S Dixit (senior engineer)
14. Melvee George (student visitor)
15. Shashank Ravi (student visitor)
16. Madhumati Seetharaman (student visitor)
17. Sujatha S (Consulting engineer)

Former members:

1. Dr. Simanraj Sadana (post doc, Pavia/Fermilab)
2. Dr. Ashutosh Singh (post doc, Calgary, Canada)
3. Dr. Kausik Joarder (NCU, Poland)
4. Debadrita Ghosh (Gottingen, Germany)
5. A.Rengaraj (LMU)
6. U.Prathwiraj (QuTech, NL)
7. Eneet Kaur (LSU)
8. G Saha (Georgia Tech)
9. Sai Dheeraj Nadela (IIIT)
10. Siva P (INRM, Italy)
11. Karthik Joshi
12. Animesh Aaryan (Japan)
13. Pradeep N
14. Anjali P.S. (IIT M)
15. Shreya Ray (U Texas)
16. Aravind H.V. (TIFR)
17. Sunny Saurabh (Japan)
18. Sudhi Oberoi (IISc)
19. Reena Sayani (IPR)
20. A.Nagalakshmi (Research Scientist B)
21. Rakshita RM
22. A. Anuradha (NCU, Poland)
23. Nandini SG
24. Neha K Nasar (CUSAT)
25. Arghyajoy Mondal (TCS Innovations labs)

Perimeter 2022

To name a few...





Current international collaborators

- Prof. Rafael Sorkin, Perimeter Institute for Theoretical Physics, Waterloo, **Canada**.
- Prof. Barry C. Sanders, Institute for Quantum Science and Technology, Director, University of Calgary, **Canada**.
- Prof. Thomas Jennewein, Institute for Quantum Computing, Waterloo, **Canada**. (also PI of satellite QKD project in Canada).
- Prof. Sougato Bose, University College London, London, **United Kingdom**.
- Dr. Alexandre Matzkin, Centre National de la Recherche Scientifique (CNRS), **France**.
- Prof. A. R. P. Rau, Louisiana State University, Baton Rouge, **USA**.
- Prof. Anupam Majumdar, University of Groningen, **Netherlands**.
- Prof. Lorenzo Macconne, University of Pavia, **Italy**.
- Prof. Lorenzo Pavesi, University of Trento, **Italy** (through the India Trento Programme of Advanced Research, DST-Italy bilateral programme).

Perimeter 2022

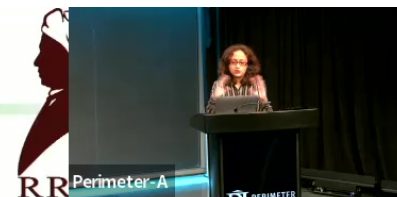


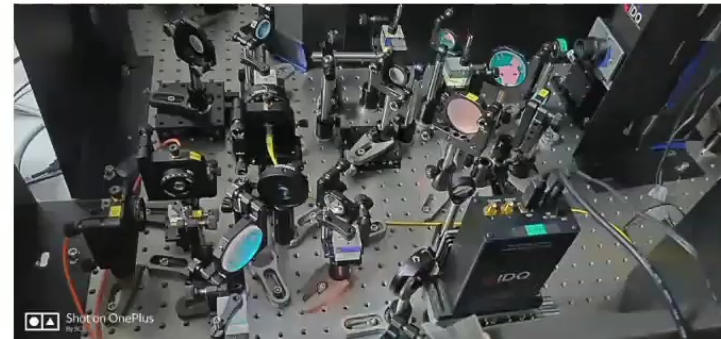
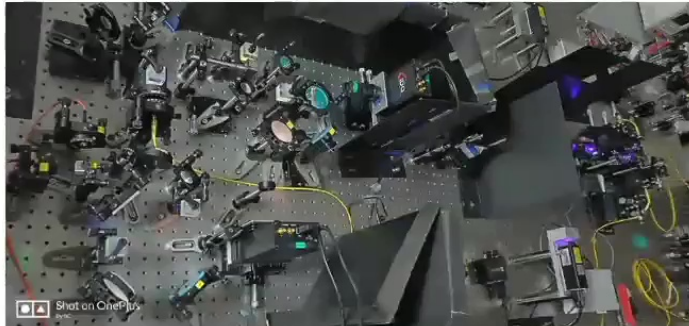
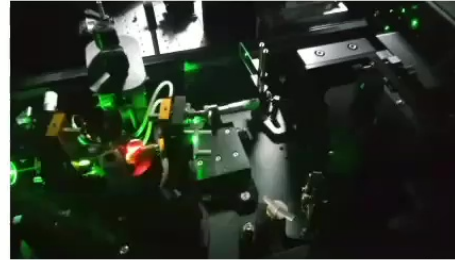
QuIC

Current collaborators in India

- Prof. Dipankar Home, Bose Institute, Kolkata, India.
- Prof. Guruprasad Kar, Indian Statistical Institute, Kolkata, India.
- Prof. Prasanta Panigrahi, Indian Institute of Scientific Education and Research Kolkata, India
- Prof. Arun K. Pati, Harish-Chandra Research Institute, Allahabad, India.
- Prof. Aninda Sinha, Indian Institute of Science, Bangalore, India
- Dr. Debashis Saha, S N Bose Centre for Basic Sciences, India.
- Dr. Som Kanjilal, Harish-Chandra Research Institute, Allahabad, India.
- R. Somashekhar, Raman Research Institute, Bangalore, India.

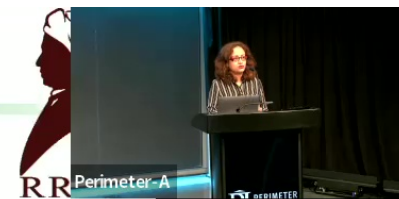
Perimeter 2022





Perimeter 2022

<https://wwws.rri.res.in/quic>



Search All Publications

Options

JOURNALS ▾ PROCEEDINGS ▾ OTHER RESOURCES ▾ My Favorites ▾ Recent Pages ▾

OSA Publishing > Optics and Photonics News > Volume 30 > Issue 9 > Page 32

About All

Single-Photon Sources

Urbasi Sinha, Surya Narayan Sahoo, Ashutosh Singh, Kaushik Joarder, Rishab Chatterjee, and Sanchari Chakraborti

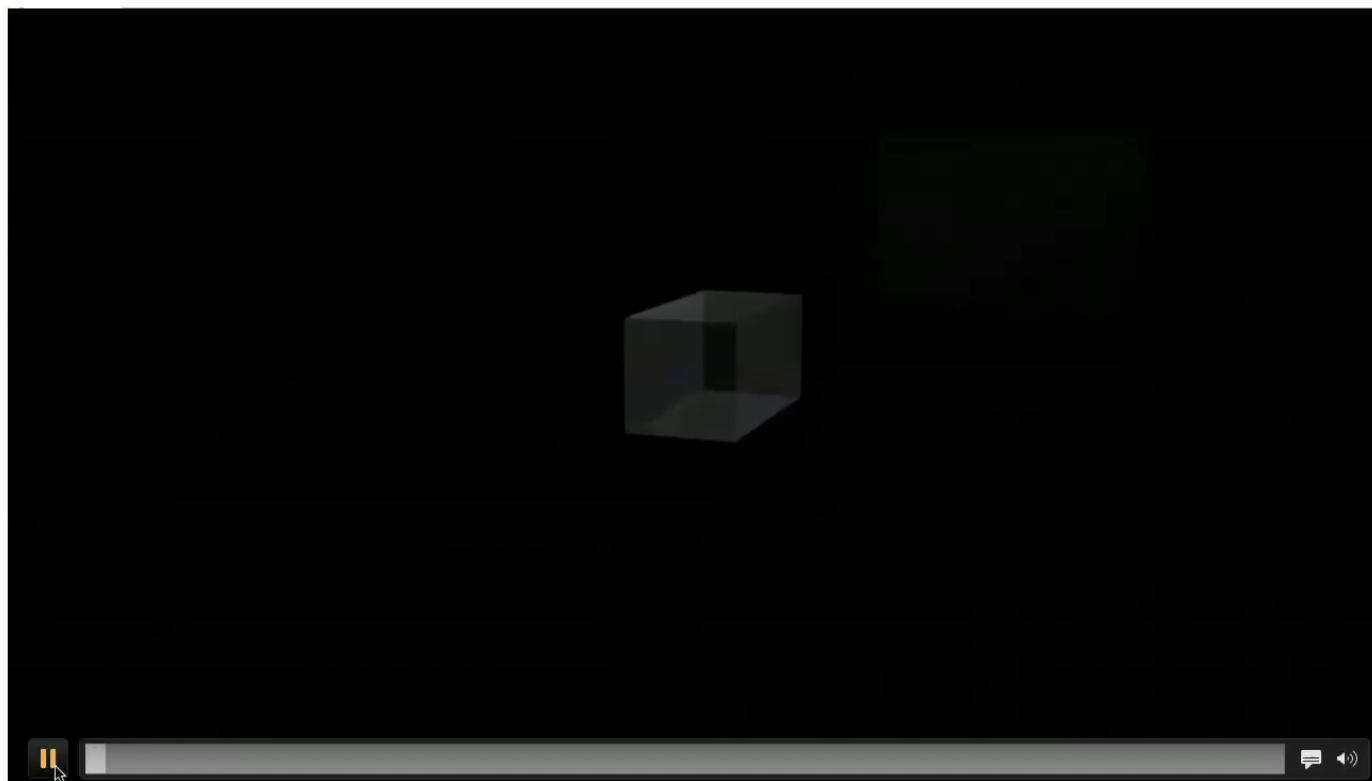
Find other works by these authors ▾

Optics and Photonics News Vol. 30, Issue 9, pp. 32-39 (2019) • <https://doi.org/10.1364/OPN.30.9.000032>

Perimeter 2022



QuIC

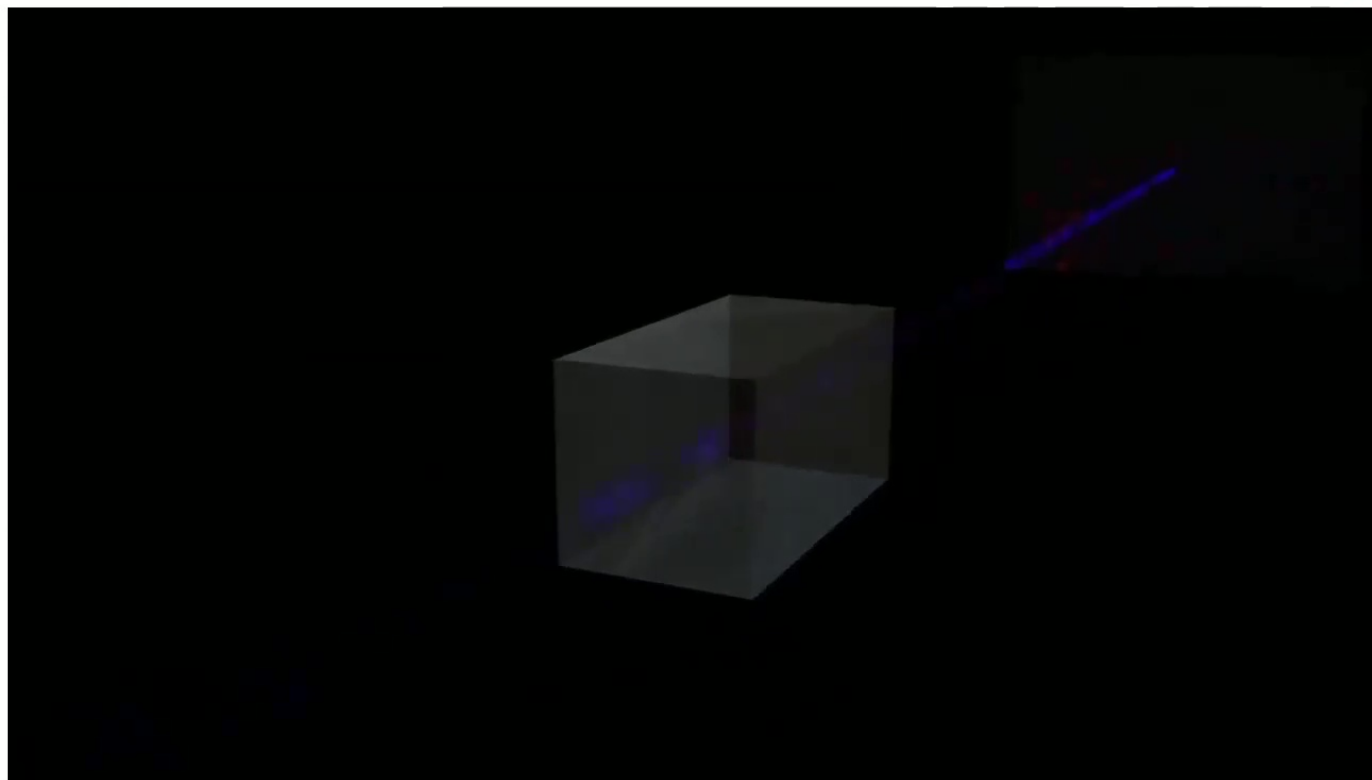
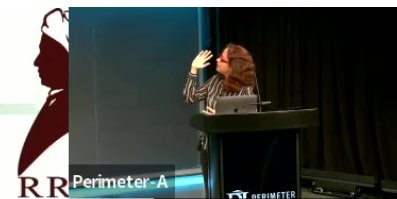


Perimeter 2022





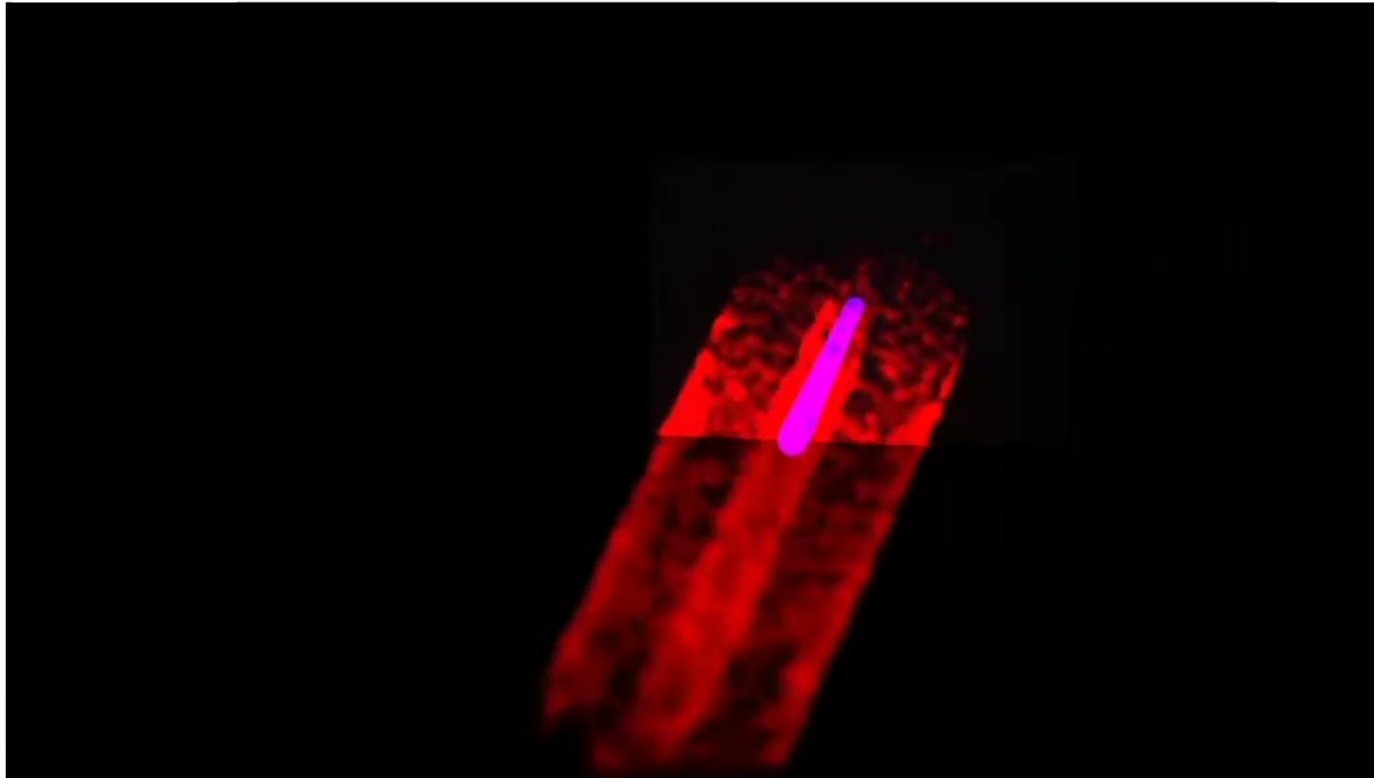
QuIC



Perimeter 2022



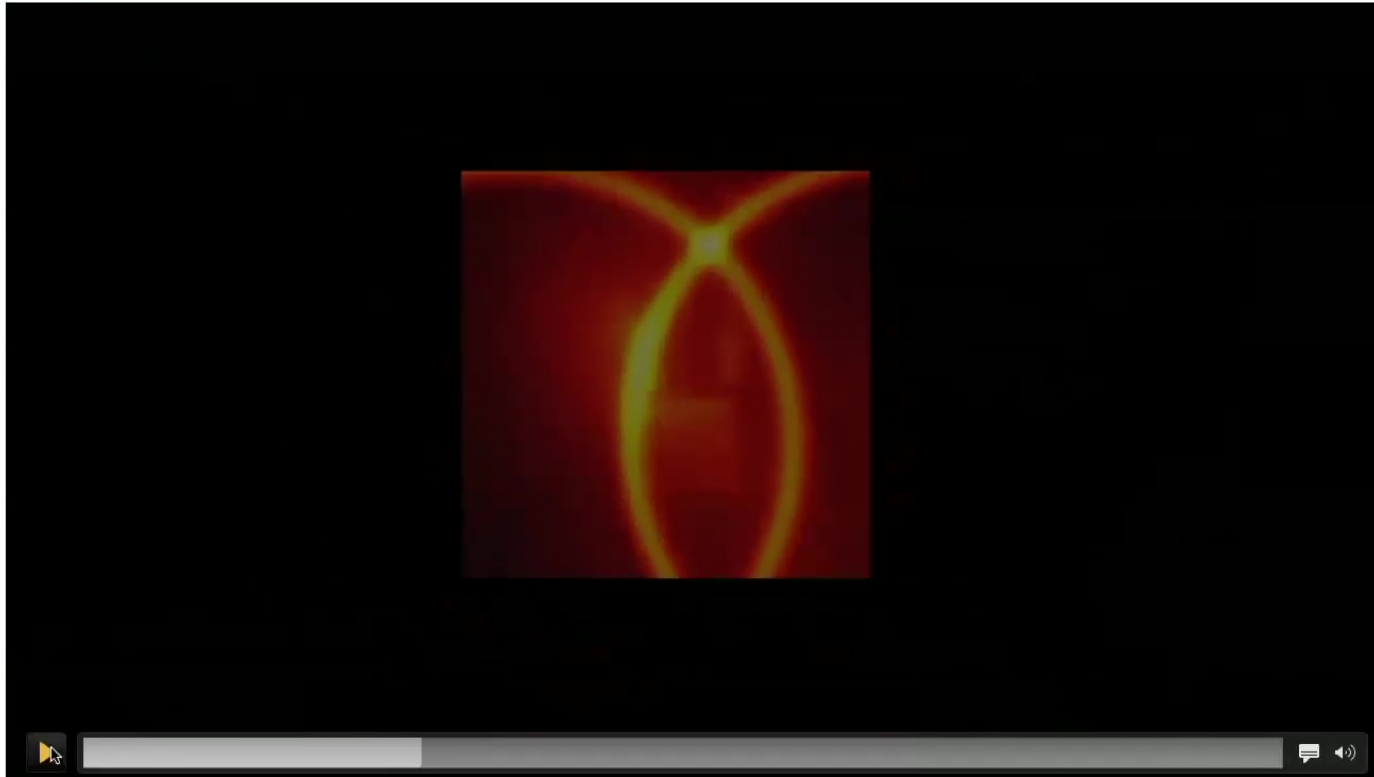
QuIC



Perimeter 2022



QuIC

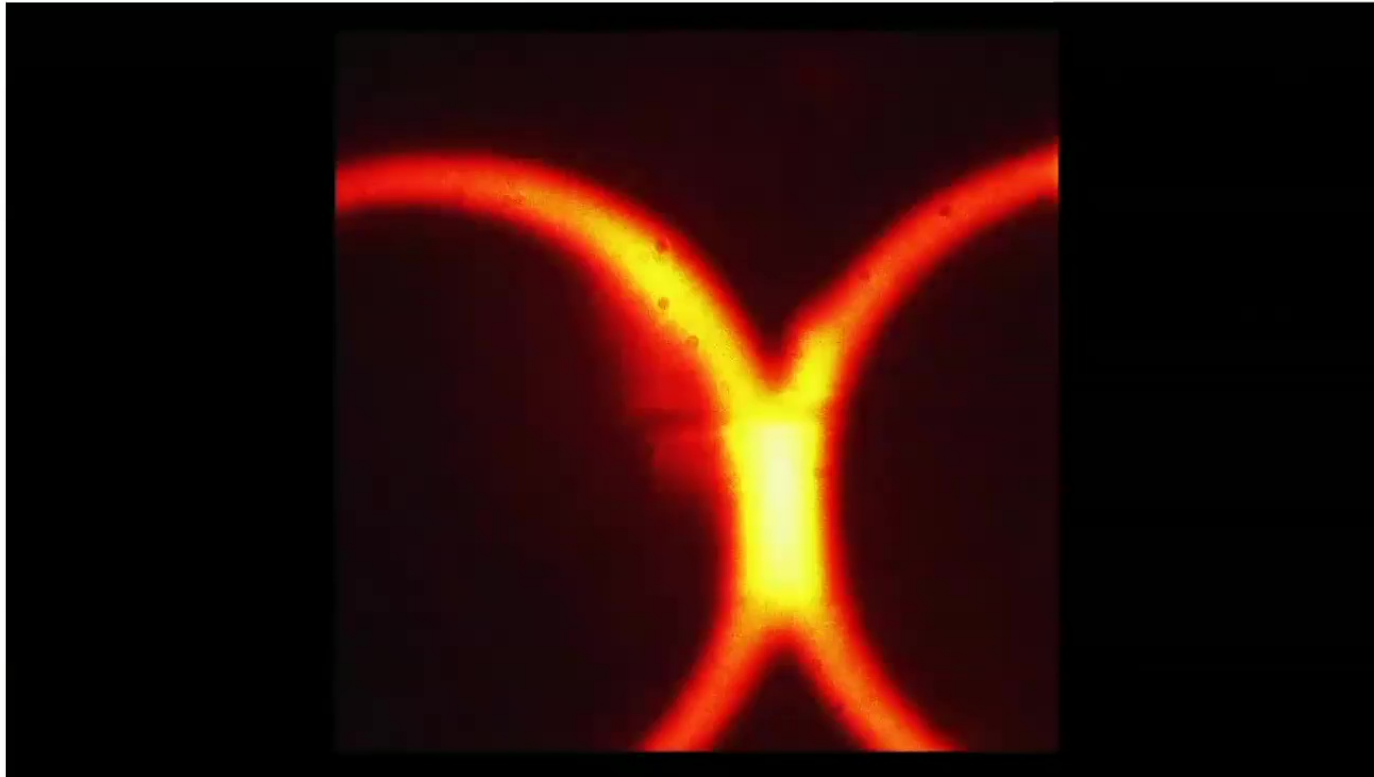
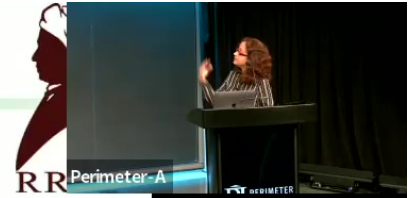


Perimeter 2022





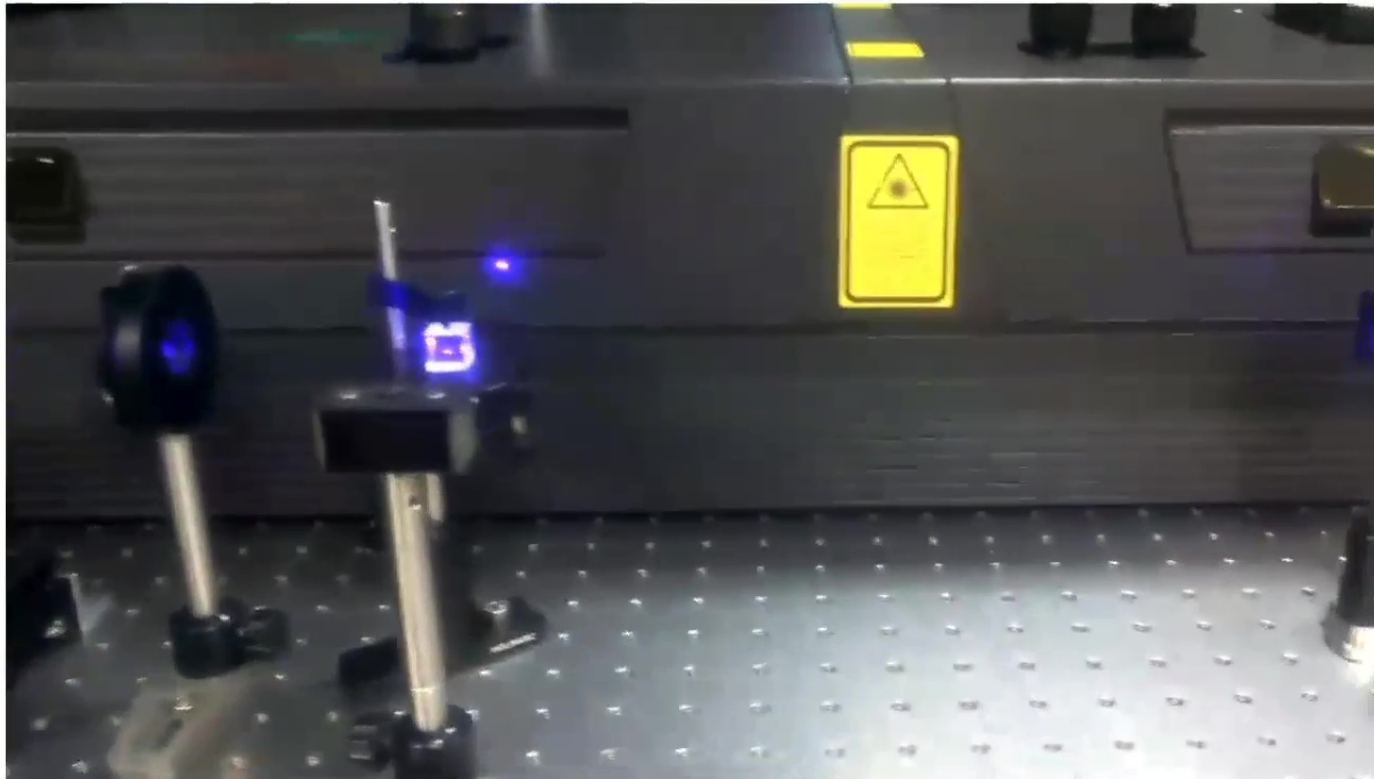
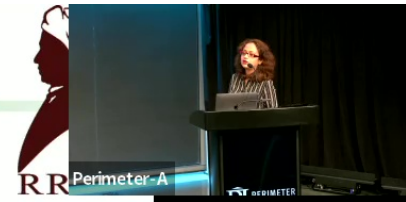
QuIC



Perimeter 2022



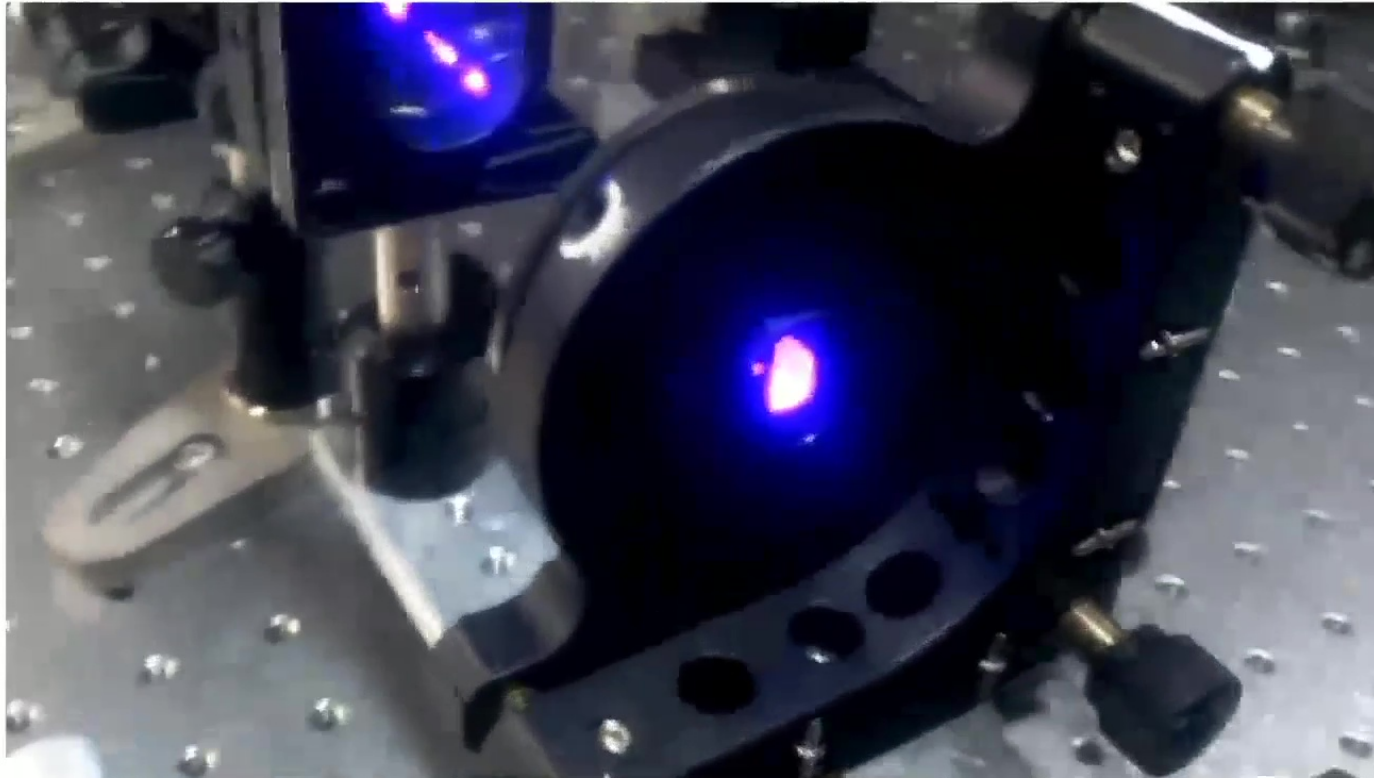
QuIC



Perimeter 2022



QuIC



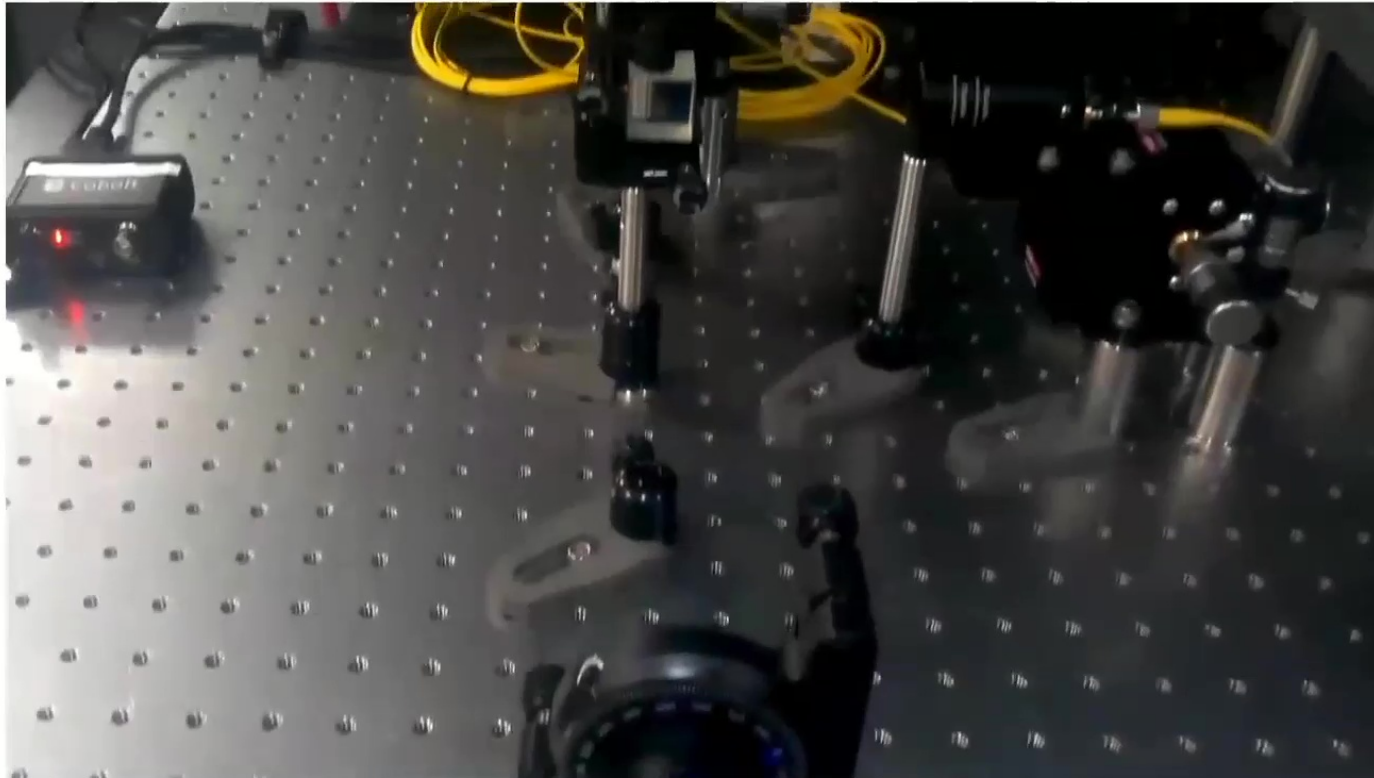
Perimeter 2022



QuIC



Debbie Leung



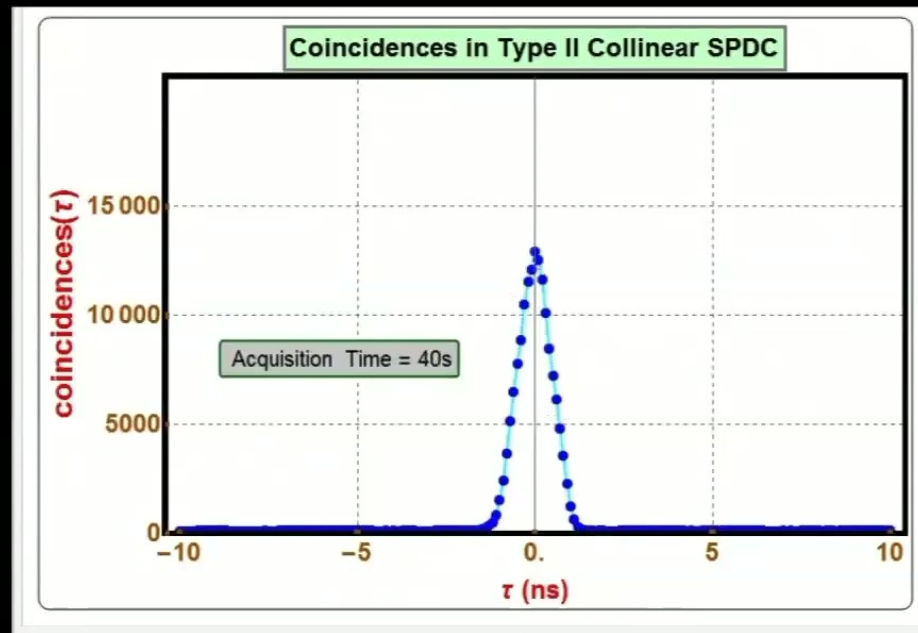
Perimeter 2022



QuIC



*Results
from
our Lab*



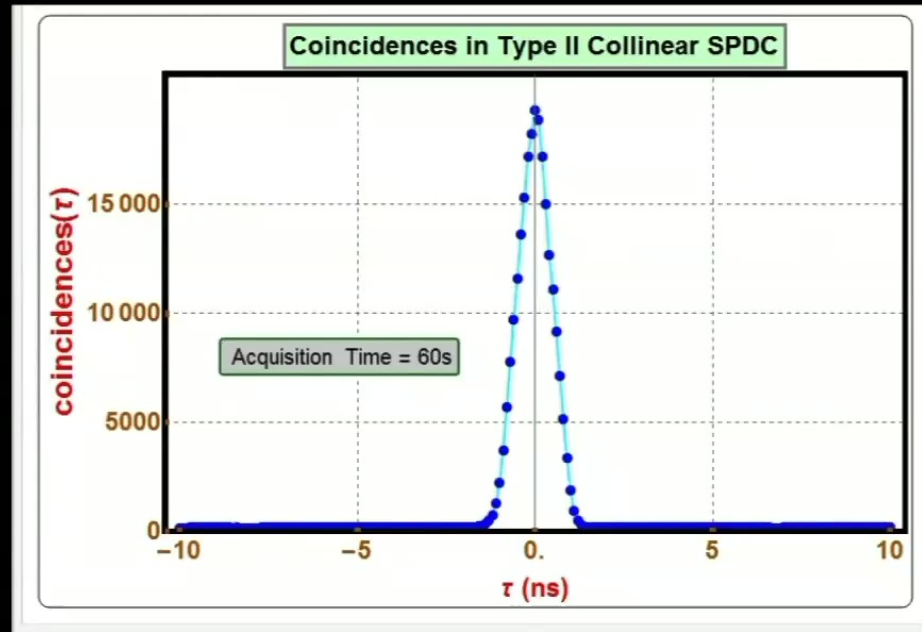
Perimeter 2022



QuIC



*Results
from
our Lab*

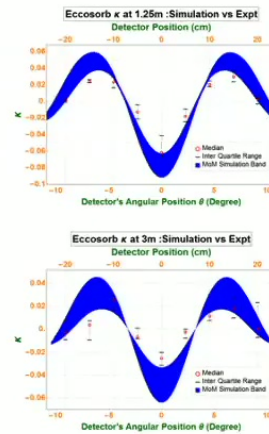


Perimeter 2022



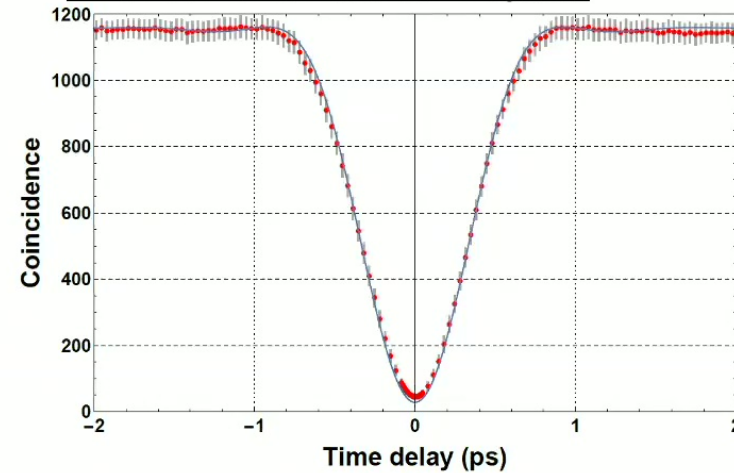
QuIC

Fundamental tests of quantum mechanics.



- *Physical Review Research*, **4** L022001, 2022.
- *New Journal of Physics* **20** 063049, 2018.
- *International Journal of Quantum Information* **14** 1650024, 2016.
- *Scientific Reports*, **5** 10304, 2015.
- *Physical Review Letters*, **113** 120406, 2014 .
- *Science*, **329** 5990 418 – 421, 2010.

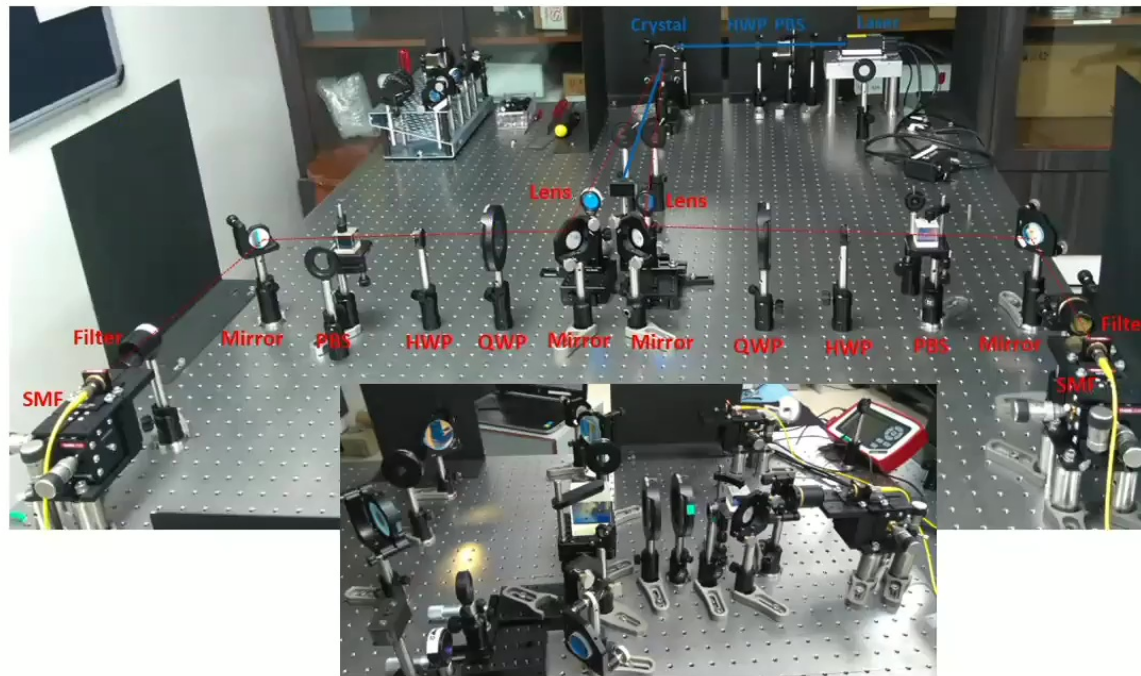
Fundamental Quantum Optics.



- *Physical Review A* **100** 013839, 2019.
- *Physical Review Letters* **125** 123601, 2020
- *Physical Review X Quantum* **3**, 010307, 2022.

Perimeter 2022





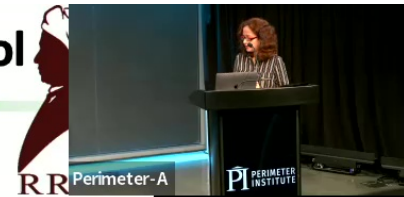
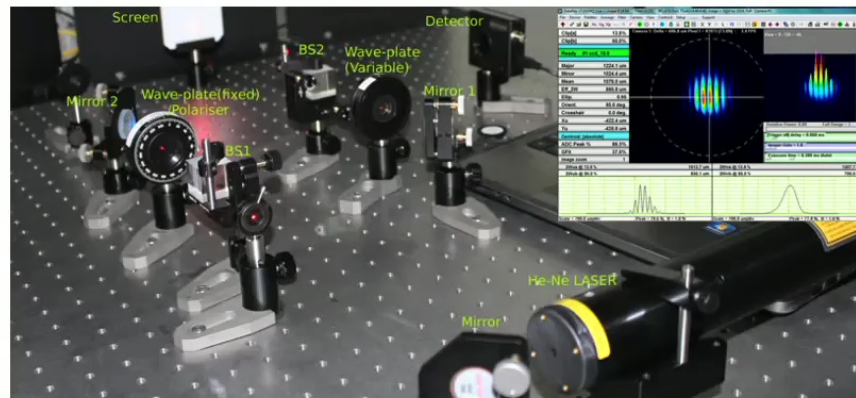
**High
Fidelity
Entangled
Photon
source in
our lab**

- arXiv:2001.07604
- *Journal of Optical Society of America B*, **37** (1), 157 – 166, 2020
- *Journal of Optical Society of America B*, **34**, 681, 2017
- *Physical Review A* **91**, 012120, 2015



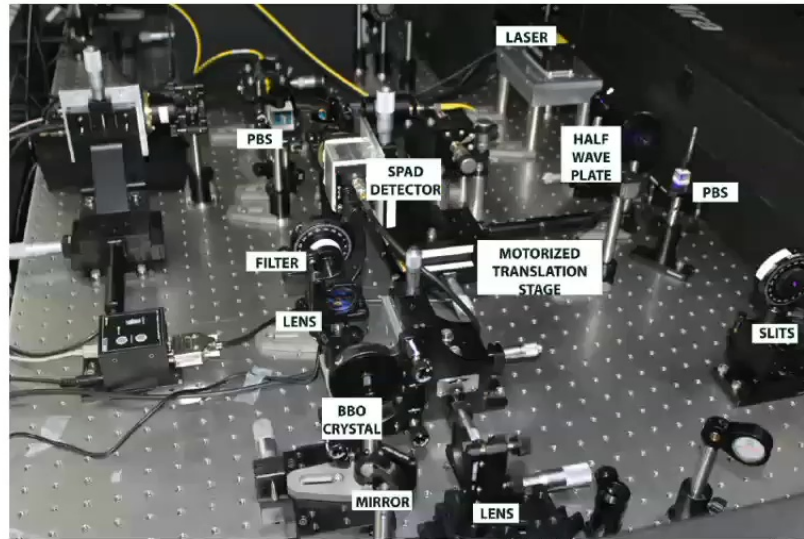
QuIC

Generalized measurements or weak measurements as a tool



- *Physical Review A* **99** 022111, 2019.
- *Annals of Physics*, **391** 1-15, 2018.
- *Physical Review A* **92** 052120, 2015.
- arXiv: 2201.11425 (under review)

Perimeter 2022



Quantum Computing/ QKD in higher dimensions

- arXiv:2201.00131 (2022)
- arXiv: 2201.06188 (2022)
- *Physical Review A* **101** 022112, 2020
- *New Journal of Physics* **21** 113022, 2019.
- *OSA Continuum* **1** (3), 2018.
- *Physical Review A* **86** 012321, 2012.

Perimeter 2022



Quantum Communications overview



India's first project on satellite based QKD

<http://www.rri.res.in/quic/>



Quantum Experiments using Satellite Technology

The age of quantum technologies is imminent and the enhancement in the computational power can pose a threat to the various cryptographic standards currently being used in secure communication, all over the world. The security of most of

Perimeter 2022



Quantum Communications overview



India's first project on satellite based QKD

<http://www.rri.res.in/quic/>



Quantum Experiments using Satellite Technology

The age of quantum technologies is imminent and the enhancement in the computational power can pose a threat to the various cryptographic standards currently being used in secure communication, all over the world. The security of most of

Experimental quantum communications using **integrated photonics**: Project under the India Trento Programme on Advanced Research (ITPAR): Indo-Italian bilateral programme.

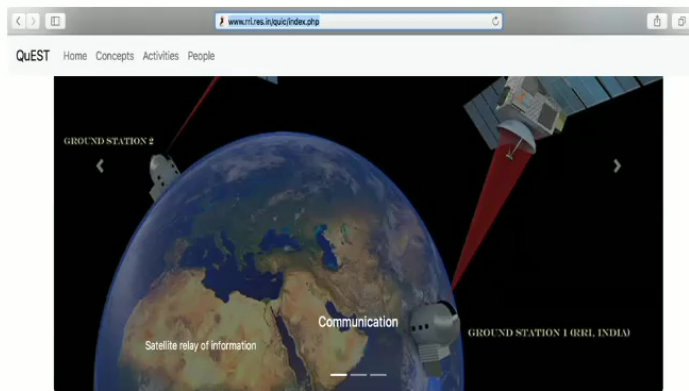
Perimeter 2022

Quantum Communications overview



India's first project on satellite based QKD

<http://www.rri.res.in/quic/>



Quantum Experiments using Satellite Technology

The age of quantum technologies is imminent and the enhancement in the computational power can pose a threat to the various cryptographic standards currently being used in secure communication, all over the world. The security of most of

Experimental quantum communications using **integrated photonics**: Project under the India Trento Programme on Advanced Research (ITPAR): Indo-Italian bilateral programme.

Project under Quantum Enabled Science and Technology programme of the Department of Science and Technology on experimental **Quantum Teleportation**.

Project under Centre for Excellence in Quantum Technologies of the Ministry of Electronics and Information Technology on **Device Independent Random Number Generation**.

Perimeter 2022



Some fundamental quantum questions



- 1. What do the non classical features of Quantum Mechanics (QM) reveal about the nature of physical reality?**
- 2. How to reconcile our everyday experience of the macroscopic world with the weird behaviour of the microphysical world described by QM?**
- 3. To what extent is it possible to test QM in the macrolimit?**

Perimeter 2022

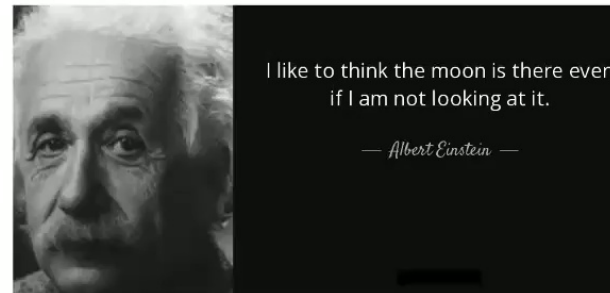


QuIC

Realism



- The classical realist world-view states that a system is in a definite state for which all its observable properties have definite values, independent of measurement.
- Unlike a classical state, the specification of a Quantum state does not, in general, give the values of dynamical variables possessed by a system. Thus, in general, a dynamical variable is taken to have no definite measurement-independent value.
- In other words, a measurement according to quantum mechanics, in general, does not reveal a pre existent value of a dynamical variable.



Perimeter 2022 A. Pais, Rev. Mod. Phys. [51, 863 \(1979\)](#) p.907.



QuIC

Two key notions of our everyday macroscopic world

Local Realism



Local Realist inequalities



Bipartite or Multipartite system

Macrorealism



Macrorealist inequalities



Single system

Why is the notion of Realism important in the context of Quantum Mechanics?

→ Superposition Principle in Quantum Mechanics



$$\frac{1}{\sqrt{2}}|\text{cat alive}\rangle + \frac{1}{\sqrt{2}}|\text{cat dead}\rangle$$

Perimeter 2022





QuIC

Tools for probing aspects of quantum reality



- Bell's inequality and its variants: Testable algebraic consequence (TAC) of the combination of the notions of
Realism + Locality – incompatible with QM
- Leggett-Garg inequality and its variants: TAC of the combination of the notions of
Realism + Noninvasive Measurability (NIM) - incompatible with QM
(Macrorealism)

Perimeter 2022



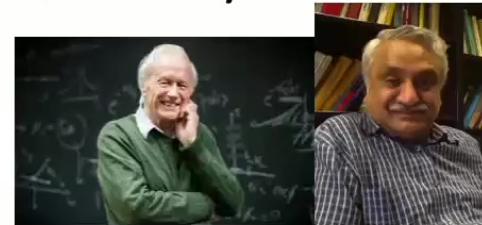
QuIC

Leggett-Garg Inequality (LGI)



- Leggett-Garg inequality (LGI) is a temporal analogue of Bell's inequality (BI) in terms of *time-separated correlation functions* corresponding to successive measurement outcomes for a system whose state evolves in time.
- Notion of *Realism* is invoked in deriving LGI by assuming that a system, during its time evolution, is at *any* given time in a definite one of the “macroscopically separated” available states.
- *Noninvasive Measurability* (NIM) is assumed which means that, in principle, it is possible to determine which of the states the system is in, *without affecting* the state itself or the system's subsequent dynamics.

Perimeter 2022





QuIC

- Original motivation for LGI was to use it for probing the possible limits of QM in the mesoscopic/macroscopic regime, e.g. experiments involving the rf-SQUID device.



Perimeter 2022



QuIC

- In recent years, the QM violation of LGI and its implications have been extensively studied for various types of microsystems to probe their non-classicality, ranging from solid-state qubits to nuclear spins to electrons to photons...



Perimeter 2022



QuIC

- In recent years, the QM violation of LGI and its implications have been extensively studied for various types of microsystems to probe their non-classicality, ranging from solid-state qubits to nuclear spins to electrons to photons...
- All this without involving the notion of locality....



Perimeter 2022

PRX QUANTUM **3**, 010307 (2022)

Loophole-Free Interferometric Test of Macrorealism Using Heralded Single Photons

Kaushik Joarder¹, Debashis Saha², Dipankar Home³ and Urbasi Sinha^{1,*}

¹*Raman Research Institute, C. V. Raman Avenue, Sadashivanagar, Bengaluru, Karnataka 560080, India*

²*Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, Warsaw 02-668, Poland*

³*Center for Astroparticle Physics and Space Science (CAPSS), Bose Institute, Kolkata 700 091, India*

Perimeter 2022



QuIC

Key features of our experiment

- The first loophole-free experiment wherein both the LGI and the WLGI inequalities have been decisively violated.



Perimeter 2022



Key features of our experiment



- The first loophole-free experiment wherein both the LGI and the WLGJ inequalities have been decisively violated.
- Comprehensive refutation of the classical realist worldview along with measurements ensured to be non-invasive.
- Perfect matching of these observed violations with quantum-mechanical predictions incorporating experimental nonidealities, again not analysed in earlier such experiments.
- Powerful platform for harnessing this most general unambiguous signature of nonclassicality of single photon states towards various information theoretic applications wherein the single photon is a ubiquitous workhorse.

Perimeter 2022



Loophole free Bell tests



LE

Loop
elec

B. Hensen
R. N. Scho
S. Wehner

More than
that obeys
quantum
between o
an inequal
Numerous
all experi
tions to o
'loopholes'

PRL 115, 250401 (2015)  Selected for a Viewpoint in *Physics*
PHYSICAL REVIEW LETTERS week ending
18 DECEMBER 2015



Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons

Marissa Giustina,^{1,2,*} Marijn A. M. Versteegh,^{1,2} Sören Wengerowsky,^{1,2} Johannes Handsteiner,^{1,2} Armin Hochrainer,^{1,2}
Kevin Phelan,¹ Fabian Steinlechner,¹ Johannes Kofler,³ Jan-Åke Larsson,⁴ Carlos Abellán,⁵ Waldimar Amaya,⁵
Valerio Pruneri,^{5,6} Morgan W. Mitchell,^{5,6} Jörn Beyer,⁷ Thomas Gerrits,⁸ Adriana E. Lita,⁸ Lynden K. Shalm,⁸
Sae Woo Nam,⁸ Thomas Scheidl,^{1,2} Rupert Ursin,¹ Bernhard Wittmann,^{1,2} and Anton Zeilinger^{1,2,†}

¹*Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences,
Boltzmanngasse 3, Vienna 1090, Austria*

²*Quantum Optics, Quantum Nanophysics and Quantum Information, Faculty of Physics, University of Vienna,
Boltzmanngasse 5, Vienna 1090, Austria*

³*Max-Planck-Institute of Quantum Optics, Hans-Kopfermann-Straße 1, 85748 Garching, Germany*

⁴*Institutionen för Systemteknik, Linköpings Universitet, 581 83 Linköping, Sweden*

⁵*ICFO – Institut de Ciències Fòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Barcelona, Spain*

⁶*ICREA – Institució Catalana de Recerca i Estudis Avançats, 08015 Barcelona, Spain*

⁷*Physikalisch-Technische Bundesanstalt, Abbestraße 1, 10587 Berlin, Germany*

⁸*National Institute of Standards and Technology (NIST), 325 Broadway, Boulder, Colorado 80305, USA*

(Received 10 November 2015; published 16 December 2015)

Local realism is the worldview in which physical properties of objects exist independently of measurement and where physical influences cannot travel faster than the speed of light. Bell's theorem states that this worldview is incompatible with the predictions of quantum mechanics, as is expressed in Bell's inequalities. Previous experiments convincingly supported the quantum predictions. Yet every

Perimeter 2022



Loophole free Bell tests



LE

Loop
elec

B. Hensen
R. N. Scho
S. Wehner

More than
that obeys
quantum
between o
an inequal
Numerous
all experi
tions to o
'loopholes'

PR

PRL 115, 250402 (2015)

Selected for a Viewpoint in *Physics*

Selected for a Viewpoint in *Physics*
PHYSICAL REVIEW LETTERS

week ending
18 DECEMBER 2015



Strong Loophole-Free Test of Local Realism*

Ma

Lynden K. Shalm,^{1,†} Evan Meyer-Scott,² Bradley G. Christensen,³ Peter Bierhorst,¹ Michael A. Wayne,^{3,4} Martin J. Stevens,¹ Thomas Gerrits,¹ Scott Glancy,¹ Deny R. Hamel,⁵ Michael S. Allman,¹ Kevin J. Coakley,¹ Shellee D. Dyer,¹ Carson Hodge,¹ Adriana E. Lita,¹ Varun B. Verma,¹ Camilla Lambrocco,¹ Edward Tortorici,¹ Alan L. Migdall,^{4,6} Yanbao Zhang,² Daniel R. Kumor,³ William H. Farr,⁷ Francesco Marsili,⁷ Matthew D. Shaw,⁷ Jeffrey A. Stern,⁷ Carlos Abellán,⁸ Waldimar Amaya,⁸ Valerio Pruneri,^{8,9} Thomas Jennewein,^{2,10} Morgan W. Mitchell,^{8,9} Paul G. Kwiat,³ Joshua C. Bienfang,^{4,6} Richard P. Mirin,¹ Emanuel Knill,¹ and Sae Woo Nam^{1,‡}

¹National Institute of Standards and Technology, 325 Broadway, Boulder, Colorado 80305, USA

²Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada, N2L 3G1

³Department of Physics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801, USA

⁴National Institute of Standards and Technology, 100 Bureau Drive, Gaithersburg, Maryland 20899, USA

⁵Département de Physique et d'Astronomie, Université de Moncton, Moncton, New Brunswick E1A 3E9, Canada

⁶Joint Quantum Institute, National Institute of Standards and Technology and University of Maryland, 100 Bureau Drive, Gaithersburg, Maryland 20899, USA

⁷Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Drive, Pasadena, California 91109, USA

⁸ICFO-Institut de Ciències Fòniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain

⁹ICREA-Institució Catalana de Recerca i Estudis Avançats, 08015 Barcelona, Spain

¹⁰Quantum Information Science Program, Canadian Institute for Advanced Research, Toronto, Ontario, Canada

(Received 10 November 2015; published 16 December 2015)

Bell's inequalities. Previous experiments convincingly supported the quantum predictions. Yet every

Perimeter 2022



QuIC

Why is a loophole free test such an important achievement?



"The results fulfill a long-standing goal, not so much to squelch any remaining doubts that quantum mechanics is real and complete, but to develop new capabilities in quantum information and security. A loophole-free Bell test demonstrates not only that particles can be entangled at all but also that a particular source of entangled particles is working as intended and hasn't been tampered with. Applications include perfectly secure quantum key distribution and unhackable sources of truly random numbers."

Summarized beautifully in *Physics Today* **69**, 1, 14 (2016)

Perimeter 2022



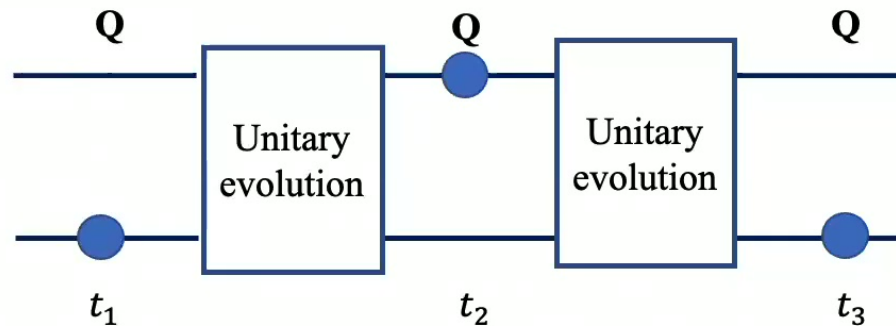


QuIC

Why both LGI and WLGI?

Inequality	Expression & MR bound	QM bound
LGI	$\langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \leq 1$	1.5
WLGI	$P_{t_1, t_3}(-, +) - P_{t_1, t_2}(-, +) - P_{t_2, t_3}(-, +) \leq 0$	0.5

- LGI and WLGI are both necessary but not sufficient conditions of MR. Hence, simultaneous violation provides a more robust violation of the notion of MR.
- WLGI expression involves a significantly lower number of measurable joint probabilities compared to the number of measurable joint probabilities in the LGI expression, thus making it a more experimentally friendly parameter, prone to less error and hence a better match with QM predictions.



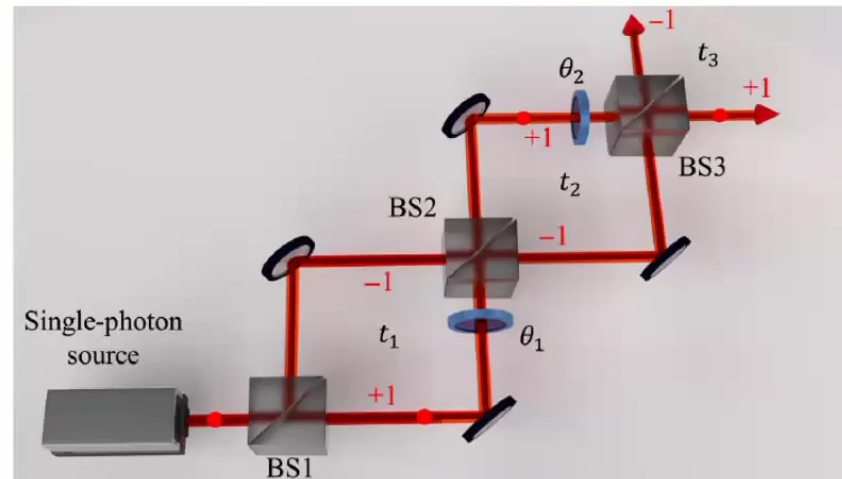
A. J. Leggett and A. Garg, Phys. Rev. Lett. 54, 857–860 (1985).

D. Saha *et al.* Phys. Rev. A, 91:032117.

Perimeter 2022



Experimental proposal



Macroscopicity

$$\sim 1.2 \times 10^4$$

Here characterized by the ratio of the spatial separation of the 2 arms of interferometer to the wavelength of the photon.

- Clumsiness loophole
- Detection efficiency loophole
- Coincidence loophole
- Multiphoton emission loophole
- Preparation state loophole



**Closed/
circumvented
together for the
first time.**

Perimeter 2022





QuIC

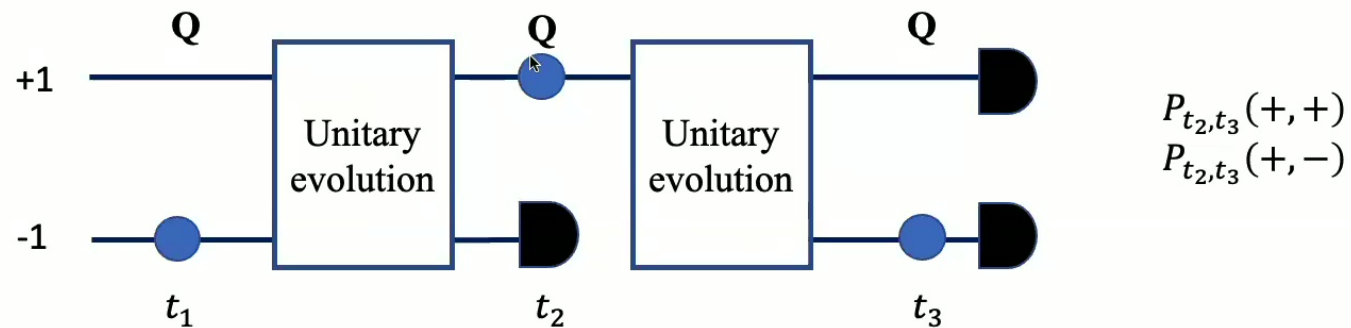
Clumsiness loophole



Negative Result Measurements (NRM): Measurement in which outcome is inferred when the detector is “not” triggered.

NRM is employed to satisfy NIM so that any violation of the inequality can then be solely attributed to the violation of realism.

But, measurements are inherently invasive...Non idealness of NRM can result in classical disturbance that can lead to a false violation – Clumsiness loophole.



Use of perfect blockers

Perimeter 2022





QILC

Clumsiness loophole contd....

Operational/statistical form of NIM \longrightarrow No-signaling in time (NSIT)

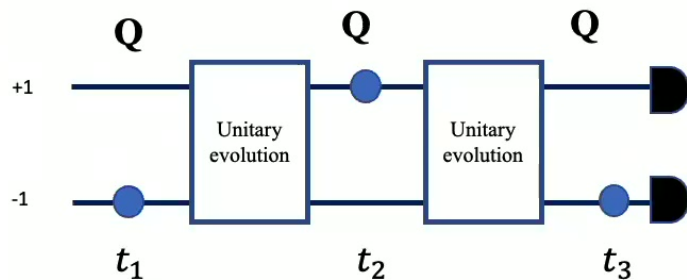
$$P_{t_2}(q_{t_2}) = P_{t_1,t_2}(+, q_{t_2}) + P_{t_1,t_2}(-, q_{t_2}),$$

$$P_{t_3}(q_{t_3}) = P_{t_1,t_3}(+, q_{t_3}) + P_{t_1,t_3}(-, q_{t_3}),$$

$$P_{t_3}(q_{t_3}) = P_{t_2,t_3}(+, q_{t_3}) + P_{t_2,t_3}(-, q_{t_3}).$$

Choice of measurement at any instant does not affect the statistical results of any measurement at a later instant.

Single experimental run



$$\langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle$$

Three experimental runs

$$\text{Exp 1: } \langle Q_{t_1} Q_{t_2} \rangle \quad NSIT_{(t_1)t_2}$$

$$\text{Exp 2: } \langle Q_{t_2} Q_{t_3} \rangle \quad NSIT_{(t_2)t_3}$$

$$\text{Exp 3: } \langle Q_{t_1} Q_{t_3} \rangle \quad NSIT_{(t_1)t_3}$$

Perimeter 2022





QuIC

Fair sampling loophole/ Detection efficiency loophole

- The assumption that all detection efficiencies are 100%.....In reality this is not the case.

1. Calculate minimum detection efficiency using hidden variable model

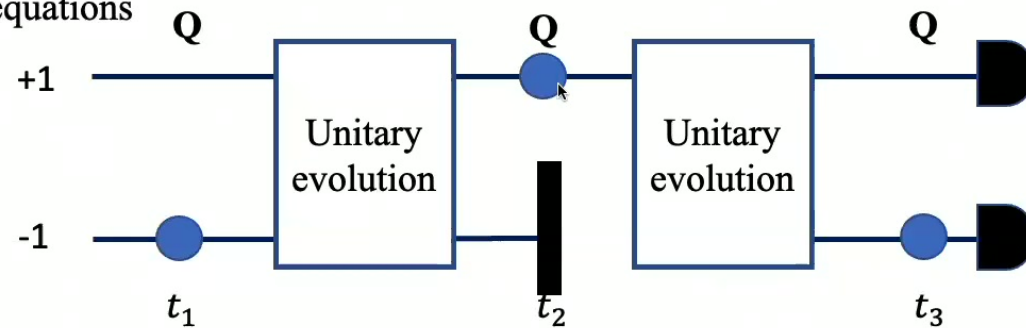
LGI: 85 %

WLG: 78 %

2. Modification in the measurement strategy

- using blocker for NRM
- detectors fixed at time t_3
- NIM assumption
- using AoT/induction equations

$$\langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \leq 1$$



Detection efficiency $\neq 0$

Perimeter 2022





QuIC

Fair sampling loophole/ Detection efficiency loophole

- The assumption that all detection efficiencies are 100%.....In reality this is not the case.

1. Calculate minimum detection efficiency using hidden variable model

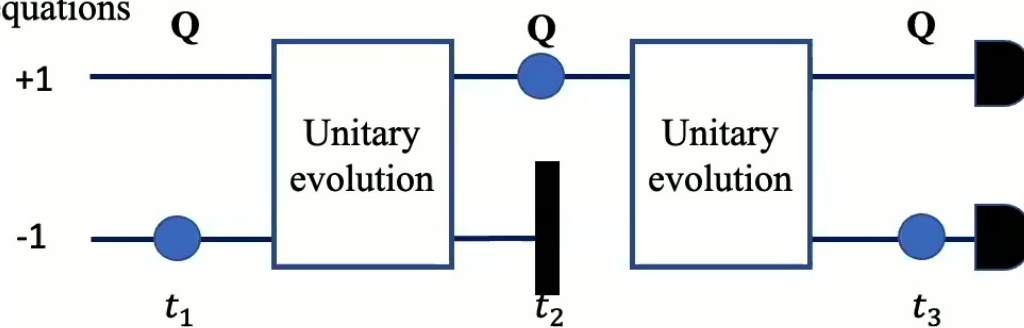
LGI: 85 %

WLG: 78 %

2. Modification in the measurement strategy

- using blocker for NRM
- detectors fixed at time t_3
- NIM assumption
- using AoT/induction equations

$$\langle Q_{t_1} Q_{t_2} \rangle + \langle Q_{t_2} Q_{t_3} \rangle - \langle Q_{t_1} Q_{t_3} \rangle \leq 1$$



Detection efficiency $\neq 0$

Detection efficiency loophole thus irrelevant in this context!

Perimeter 2022





QuIC



TABLE I. Experiments testing LGI based on projective measurements and by addressing the clumsiness loophole in different ways, with the relevant references cited in the text.

System	Macroscopicity parameter	Procedure
Nitrogen-vacancy center in diamond hosting a three-level quantum system [8]	Atomic mass	Testing the macrorealist bound on the success rate in a “three-box” game while satisfying the NSIT conditions
A single cesium atom performing “quantum walk” on a discrete lattice [9]	Atomic mass	Testing the violation of LGI by determining classical invasiveness using control experiments
Spin-bearing phosphorus impurity atom in silicon [10]	Atomic mass	Testing LGI by suitable implementation of controlled-NOT (CNOT) and anti-CNOT gates
Neutrino flavor oscillation [11]	Length scale of the neutrino oscillation	Testing the violation of LGI using the “stationarity” condition
Three-level single photons [16]	Spatial separation between the paths	Testing the violation of modified LGI [28] using ambiguous measurements
Superconducting flux qubit [22]	Difference in the magnetic moments of the two oppositely circulating superconducting superposed current states of the flux qubit	Testing the violation of NSIT as a consequence of macrorealism by determining classical invasiveness using control experiments
Two- and four-qubit “cat states” studied in the cloud-based quantum computing device “IBM QE” [27]	Number of constituent qubits	Testing the violation of the “clumsy-macrorealist” bound of LGI

While clumsiness loophole has been addressed in many earlier experiments, the other loopholes have not garnered much attention, especially the detection efficiency loophole that has played a critical role in analysis of many Bell violation experiments had not been analyzed in earlier LGI experiments.

Perimeter 2022





Qulr

Expression	Experimentally measured value	Macrorealist upper bound	QM predicted range including experimental non-idealities
LGI (1)	1.32 ± 0.04	1	1.34 ± 0.06
WLGI (2)	0.10 ± 0.02	0	0.08 ± 0.03

NSIT expression	Experimentally measured value	QM predicted range including experimental non-idealities
$\text{NSIT}_{(t_1)t_2} (9)$	$ 0.002 \pm 0.017 $	0
$\text{NSIT}_{(t_1)t_3} (10)$	$ 0.002 \pm 0.016 $	0
$\text{NSIT}_{(t_2)t_3} (11)$	$ 0.004 \pm 0.016 $	$ 0 \pm 0.0261 $

Perimeter 2022





← Discussing the Leggett Garg inequality experiment with Leggett himself!



QuIC

n

Ex

na

RE

F

C

Th

ini

NEWSLETTERS

Sign up to read our regular email newsletters

NewScientist

[News](#) [Podcasts](#) [Video](#) [Technology](#) [Space](#) [Physics](#) [Health](#) [More](#) [Shop](#) [Courses](#) [Events](#)

The quantum experiment that could prove reality doesn't exist

We like to think that things are there even when we aren't looking at them. But that belief might soon be overturned thanks to a new test designed to tell us if quantum weirdness persists in macroscopic objects



PHYSICS 3 November 2021



Perimeter 2022



QuIC

Theory and experiments on Quantum Superposition Principle, Born Rule as well as higher order interference in Quantum Mechanics

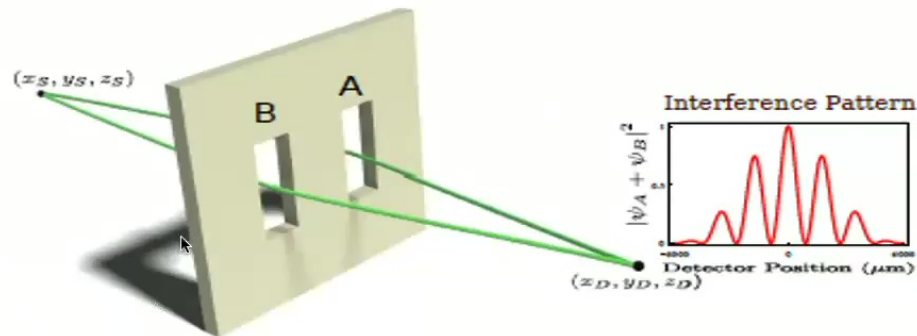


Perimeter 2022



QuIC

Superposition principle in the two slit experiment



- R.P.Feynman, R.Leighton and M.Sands, *The Feynman Lectures on Physics* Vol. 3, 1963.
- C.Cohen-Tannoudji, B.Diu and F.Laloe, *Quantum Mechanics I*, 2005.
- R.Shankar, *Principles of Quantum Mechanics*, 1994.

Perimeter 2022

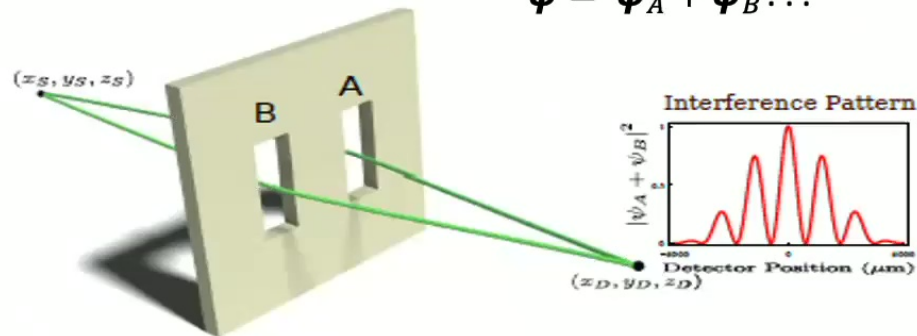




QuIC

Superposition principle in the two slit experiment

$$\psi = \psi_A + \psi_B ???$$



- R.P.Feynman, R.Leighton and M.Sands, *The Feynman Lectures on Physics* Vol. 3, 1963.
- C.Cohen-Tannoudji, B.Diu and F.Laloe, *Quantum Mechanics I*, 2005.
- R.Shankar, *Principles of Quantum Mechanics*, 1994.

Perimeter 2022

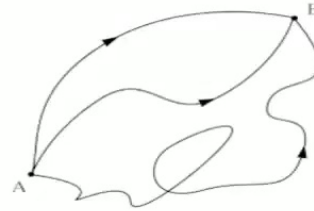




QuIC



Feynman's path integral formalism



$$K(A, B) = \int_A^B \exp^{i/\hbar S[B, A]} Dx(t)$$

An integration over all possible paths that can be taken by the particle in going from A to B.

Perimeter 2022

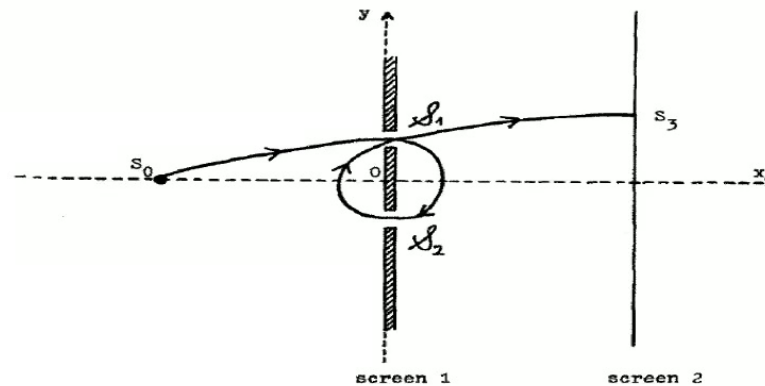


Previous work

1. H. Yabuki, Int. J. Theor. Phys. **25**, 159 (1986).
2. H. DeRaedt, K. Michielsen and K. Hess, Phys. Rev. A **85**, 012101 (2012).

162

Yabuki

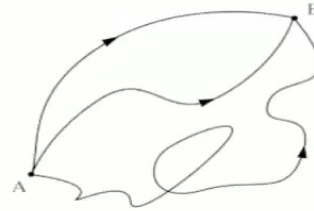


Picture from Yabuki

Perimeter 2022



Feynman's path integral formalism



$$K(A, B) = \int_A^B \exp^{i/\hbar S[B, A]} Dx(t)$$

An integration over all possible paths that can be taken by the particle in going from A to B.



QuIC



Journals ▾

Help/Feedback

Journal, vol, page, DOI, etc. 🔍

PHYSICAL REVIEW LETTERS

[Highlights](#) [Recent](#) [Accepted](#) [Collections](#) [Authors](#) [Referees](#) [Search](#) [Press](#) [About](#) 📶

Featured in Physics

Nonclassical Paths in Quantum Interference Experiments

Rahul Sawant, Joseph Samuel, Aninda Sinha, Supurna Sinha, and Urbasi Sinha
Phys. Rev. Lett. **113**, 120406 — Published 19 September 2014

Physics See Focus story: [Curvy Photon Trajectories Could Be Detectable](#)



Article

References

Citing Articles (1)

Supplemental Material

PDF

HTML

Export Citation



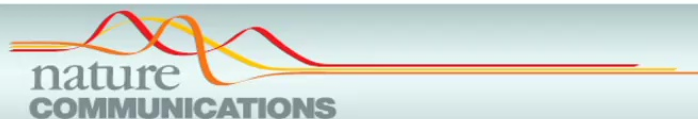
ABSTRACT

In a double slit interference experiment, the wave function at the screen with both slits open is not exactly equal to the sum of the wave functions with the slits individually open one at a time. The three scenarios represent three different boundary conditions and as such, the superposition principle should not be applicable. However, most well-known text books in quantum mechanics implicitly

Issue

Vol. 113, Iss. 12 — 19 September 2014

Perimeter 2022



ARTICLE

Received 16 Sep 2016 | Accepted 16 Nov 2016 | Published 23 Dec 2016

DOI: 10.1038/ncomms13987

OPEN

Exotic looped trajectories of photons in three-slit interference

Omar S. Magaña-Loaiza^{1,*}, Israel De Leon^{2,3,*}, Mohammad Mirhosseini¹, Robert Fickler³, Akbar Safari³, Uwe Mick⁴, Brian McIntyre¹, Peter Banzer^{3,4}, Brandon Rodenburg⁵, Gerd Leuchs^{3,4} & Robert W. Boyd^{1,3}

Perimeter 2022

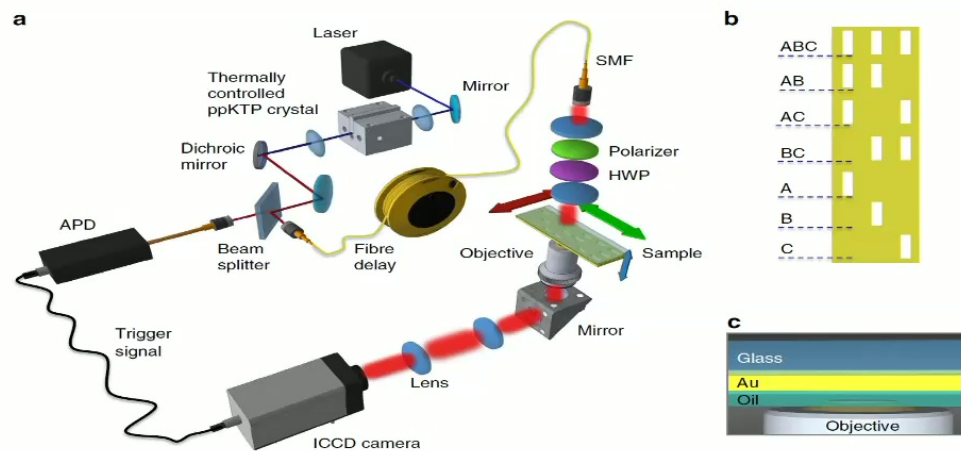
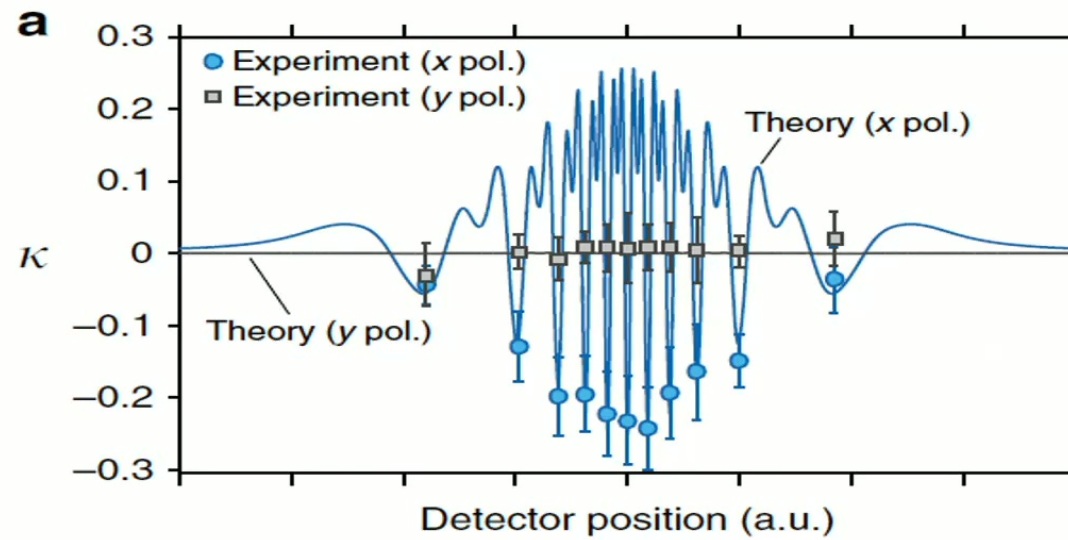


Figure 2 | Experimental set-up utilized to measure exotic trajectories of light. (a) Sketch of the experimental set-up used to measure the far-field interference patterns for the various slit configurations. (b) The seven different slit arrangements used in our study. This drawing is not to scale; in the actual experiment each slit structure was well separated from its neighbors to avoid undesired cross talk. (c) Detail of the structure mounted on the set-up. The refractive index of the immersion oil matches that of the glass substrate creating a symmetric index environment around the gold film.



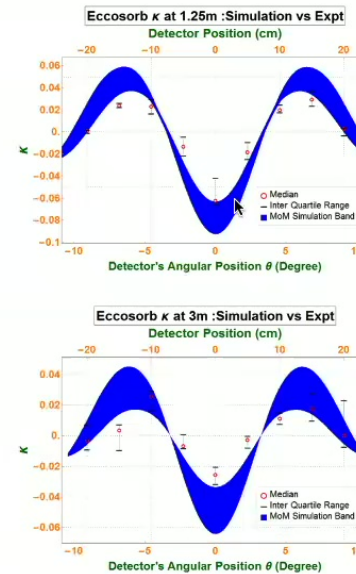
Perimeter 2022



QuIC

First ever measurement of non zero Sorkin parameter

Precision experiment,
Fundamental tests



Measuring the deviation from the Superposition Principle in interference experiments,
A.Rengaraj, U. Prathwiraj, Surya Narayan Sahoo, R. Somshekhar and US, *New Journal of Physics* **20** 2018

Perimeter 2022



Testing quantum foundations with quantum computers

Simanraj Sadana,¹ Lorenzo Maccone,² and Urbasi Sinha^{1,*}

¹*Light and Matter Physics, Raman Research Institute, Bengaluru-560080, India*

²*Dipartimento di Fisica and INFN Sezione di Pavia, University of Pavia, via Bassi 6, I-27100 Pavia, Italy*



(Received 28 November 2021; accepted 23 February 2022; published 1 April 2022)

We present two complementary viewpoints for combining quantum computers and the foundations of quantum mechanics. On the one hand, ideal devices can be used as test beds for experimental tests of the foundations of quantum mechanics: We provide algorithms for the Peres test for complex numbers in quantum superpositions and the Sorkin test of Born's rule. On the other hand, noisy intermediate-scale quantum devices can be benchmarked using these same tests. These are deep quantum benchmarks based on the foundations of quantum theory itself. We present test data from Rigetti hardware.

DOI: [10.1103/PhysRevResearch.4.L022001](https://doi.org/10.1103/PhysRevResearch.4.L022001)



RESEARCH HIGHLIGHT | 25 May 2022

Algorithms to review classic principles of quantum mechanics

The tests can also evaluate the performance of computing systems





Our approach to Quantum Computing



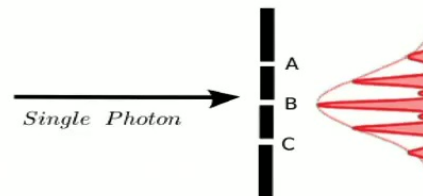
Generation of Spatially Correlated Qutrits and Qudits Using SPDC

Correlated photonic qutrit pairs for quantum information and communication, D.Ghosh, T.Jennewein, P.Kolenderski and U.Sinha, OSA Continuum 1 (3), 2018

Perimeter 2022

What is Qutrit?

- **Qubit** has two orthogonal **basis states**, denoted by $|0\rangle$, $|1\rangle$ and it can also be in a linear combination of states, e.g. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α and β are normalised probability amplitudes.
- **Qutrit** has three orthogonal basis states, often denoted by $|0\rangle$, $|1\rangle$, $|2\rangle$.
- It is also possible to form linear combination of states, called *superposition* e.g. $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle$.



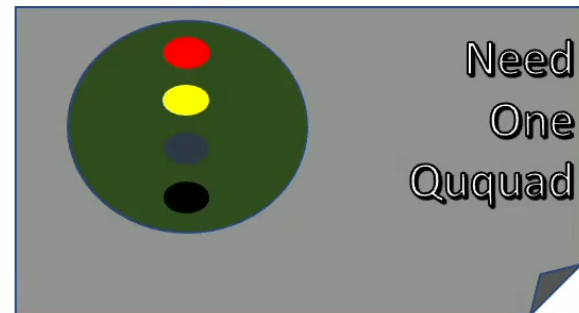
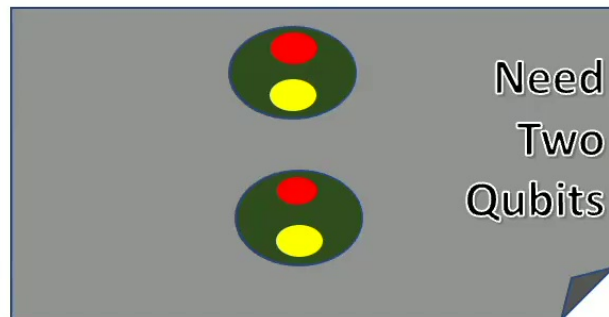


QuIC



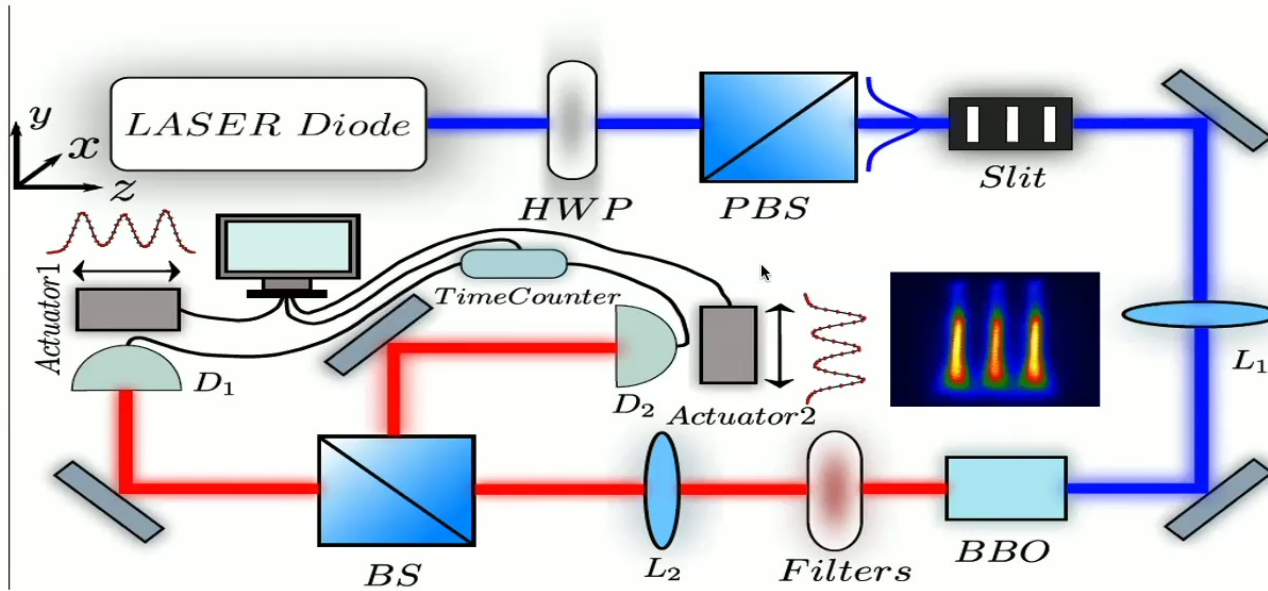
Quantum Computation

- ☐ Hard to maintain large number of particles in a superposition
- ☐ Use qudits - decrease the size of the system



Perimeter 2022

Pump beam modulation: our way of generating qudits

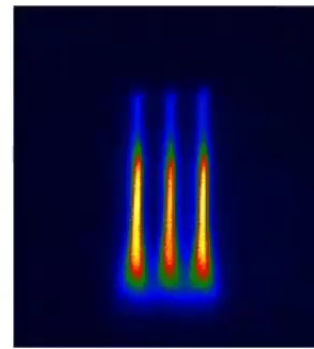


Perimeter 2022

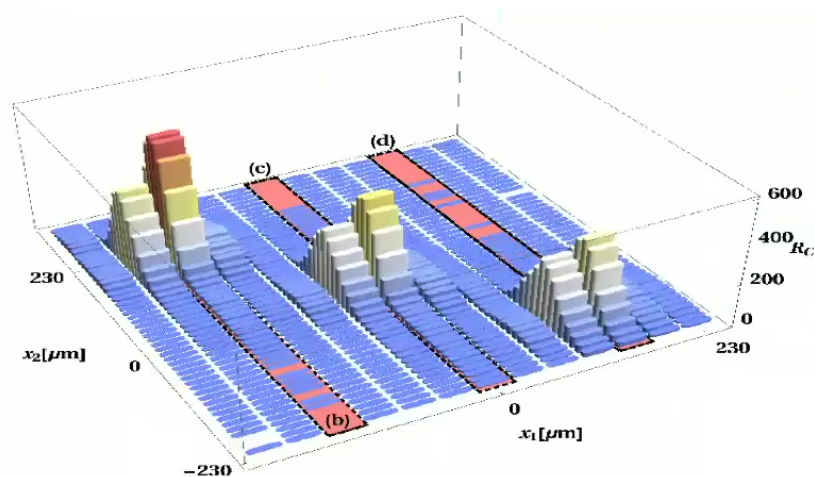
- The **spatial structure of the pump** is carried through faithfully to the resultant **single photons (Signal and idler)**.



Pump Profile At the Crystal



Single Photon Profile At the Detector



Pearson correlation coefficient of 0.902(2)

Correlated photonic qutrit pairs for quantum information and communication, D.Ghosh, T.Jennewein, P.Kolenderski and U.Sinha, OSA Continuum 1 (3), 2018

Perimeter 2022



Hot from the oven...



- Derived a monotonicity relation between Negativity and sum of PCCs for arbitrary dimensions.
- Derived a monotonicity relation between Negativity and sum of Mutual Predictabilities for arbitrary dimensions.
- Determined a monotonicity relation between EOF and Mutual Information for arbitrary dimensions.
- **First direct measurement of an entanglement monotone.**
- **Negativity and EOF are non-equivalent entanglement measures.**
- **First experimental demonstration of non equivalence of different entanglement monotones in higher dimensions.**
- D. Ghosh, T.Jennewein, U.Sinha, *Direct determination of entanglement monotones for arbitrary dimensional bipartite states using statistical correlators and one set of complementary measurements*, [arXiv:2201.00131 \(2022\)](#)
- S. Sadana, S. Kanjilal, D. Home, and U. Sinha, "Relating an entanglement measure with statistical correlators for two-qudit mixed states using only a pair of complementary observables", [arXiv:2201.06188 \(2022\)](#)



WHAT NEXT....

- Working on diffraction based Linear Optics Quantum Information in collaboration with Sougato Bose (UK), Barry Sanders (Canada) and Aninda Sinha (India).
- Proven that a two-slit system acts as a lossy beam splitter:
*Double slit interferometry as a lossy beam splitter, S. Sadana, B.C. Sanders and US, New Journal of Physics **21** 113022, 2019.*
- Investigations of myriad QIP protocols as well as higher dimensional quantum gates over the next few years and experimental implementation in our lab.

Perimeter 2022





Subscribe

Latest Issues

SCIENTIFIC
AMERICAN 175

Cart 0

Sign In | Stay Informed

[THE SCIENCES](#) [MIND](#) [HEALTH](#) [TECH](#) [SUSTAINABILITY](#) [EDUCATION](#) [VIDEO](#) [PODCASTS](#) [BLOGS](#) [PUBLICATIONS](#) [Q](#)

PHYSICS

Quantum Slits Open New Doors

An update to the classic “double-slit” experiment paves the way toward a novel strategy for quantum computing

By Urbasi Sinha on January 1, 2020

Perimeter 2022



Quantum State Estimation: a novel method..



PHYSICAL REVIEW LETTERS **125**, 123601 (2020)

Quantum State Interferography

Surya Narayan Sahoo,¹ Sanchari Chakraborti¹, Arun K. Pati,² and Urbasi Sinha^{1,*}

¹*Light and Matter Physics, Raman Research Institute, Bengaluru 560080, India*

²*Quantum Information and Computation Group, Harish-Chandra Research Institute, HBNI, Allahabad 211019, India*

 (Received 13 March 2020; accepted 11 August 2020; published 16 September 2020)

Quantum state tomography (QST) has been the traditional method for characterization of an unknown state. Recently, many direct measurement methods have been implemented to reconstruct the state in a resource efficient way. In this Letter, we present an interferometric method, in which any qubit state, whether mixed or pure, can be inferred from the visibility, phase shift, and average intensity of an interference pattern using a single-shot measurement—hence, we call it quantum state interferography. This provides us with a “black box” approach to quantum state estimation, wherein, between the incidence of the photon and extraction of state information, we are not changing any conditions within the setup, thus giving us a true single shot estimation of the quantum state. In contrast, standard QST requires at least two measurements for pure state qubit and at least three measurements for mixed state qubit reconstruction. We then go on to show that QSI is more resource efficient than QST for quantification of entanglement in pure bipartite qubits. We experimentally implement our method with high fidelity using the polarization degree of freedom of light. An extension of the scheme to pure states involving $d - 1$ interferograms for

Perimeter 2022



QulC

Why quantum state estimation?

- Wave function is used to completely describe a quantum system and is central to quantum theory.
- In theoretical calculations, one can assume a form of the wave function and then proceed with the calculations.
- **What about experiments??** Ex: Quantum Computing.
- **Precision in knowledge of the state of the system leads to precision in all that follows...**We simply cannot assume something and think that our assumption is right!
- **Once we know the density matrix, we can calculate many important quantities.....**reduced density matrix can be used for calculating entanglement measures like **entanglement entropy** for instance.
- In our work, we use one of the most fundamental phenomena in quantum systems i.e. interference to devise and experimentally demonstrate a new method for quantum state estimation:

Quantum State Interferography.

Perimeter 2022





QuIC

Our Central Question..



'Black-Box' approach to state determination

'single-shot' state determination

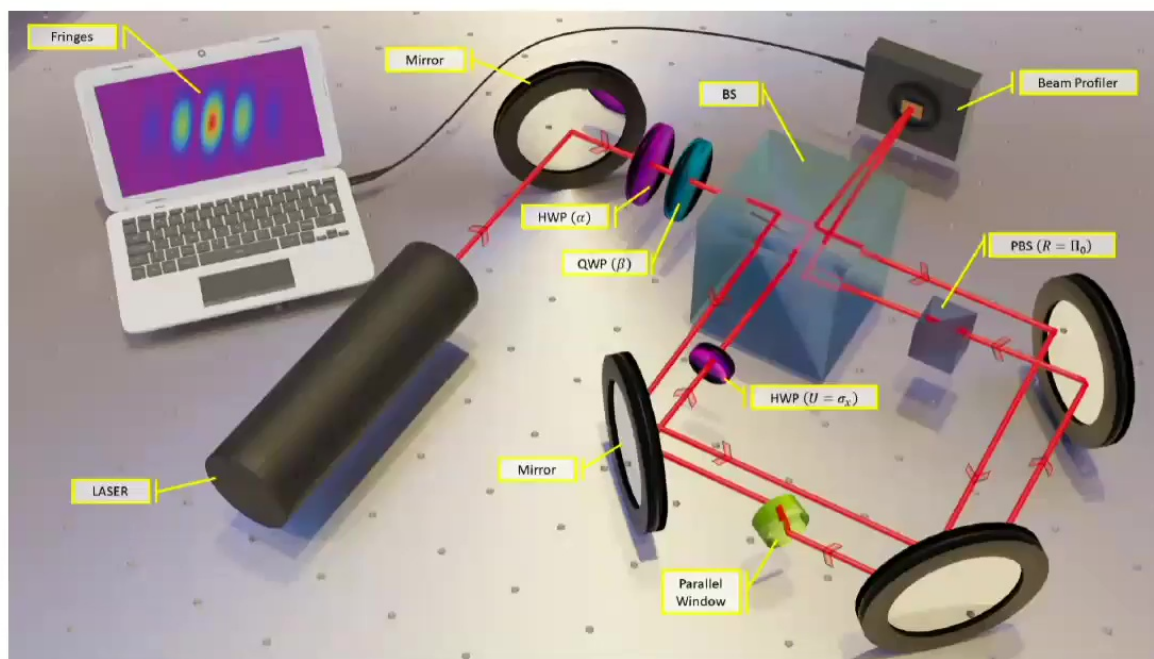


Can we have a device with which, without any change of internal settings by the user, we can determine the quantum state of the system ?

Perimeter 2022

Quantum State Interferography

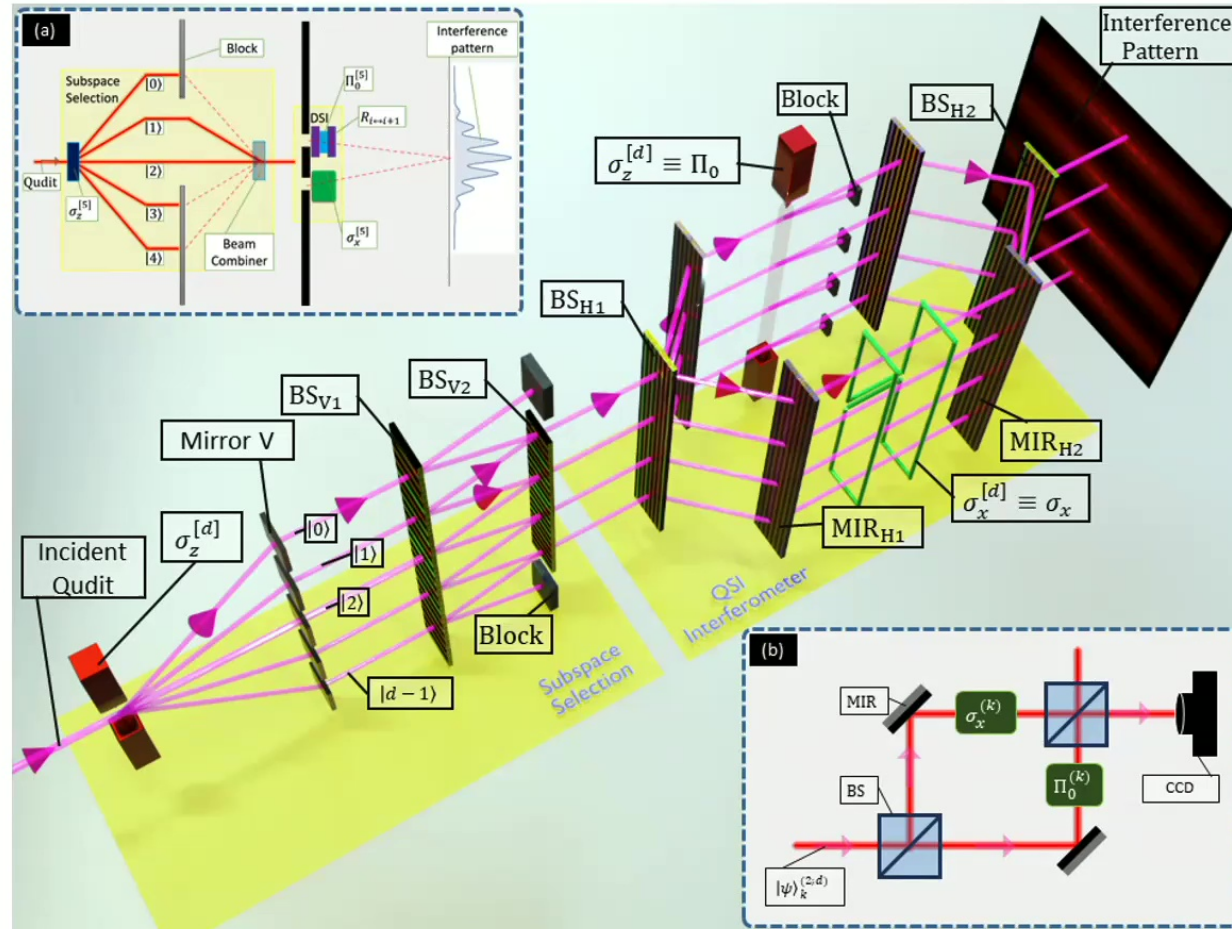
Single-shot quantum state estimation tool



Perimeter 2022



Proposal : Quantum State Interferography for Qudit



Perimeter 2022





- Quantum State Interferography (QSI) can be used to determine an unknown qubit state using a **single-shot measurement**.
- If a bipartite state of qubits is known to be pure, **QSI can quantify the entanglement with a single set-up**.
- With 2 interferometers, any pure qudit state ($d > 2$) can also be determined.
- **Fantastic scaling advantage** over conventional Quantum State Tomography.
- Can be used for quantifying entanglement of a pure bipartite state.
- Interference is a resource, yet again!

Perimeter 2022



nature india

Explore content ▾ About the journal ▾

[nature](#) > [nature india](#) > [research highlights](#) > article

RESEARCH HIGHLIGHT | 23 September 2020

Portable quantum-state estimation tool devised



In quantum mechanics, a photon behaves both like a particle and a wave. The state of a quantum system (such as a photon) carries both its wave and particle information.

Physicists have now devised a novel technique to characterise and estimate the state of such a quantum system¹. This technique, they say, could potentially be used in quantum computing,

Perimeter 2022





Quantum Communication



Quantum Key Distribution (QKD)

The most “practical” quantum technology!

Perimeter 2022



Why you should worry??



- Credit card purchase
- Online Banking
- Electoral polling system
- Defence strategic communication

ALL AT RISK OF BEING COMPROMISED WITH QUANTUM COMPUTERS!!

- Information communicated through Classical Cryptography now.
- This will be compromised with Quantum Computers.
- We need to take steps **now** so that we can prevent this catastrophe.
- The solution is QUANTUM CRYPTOGRAPHY.

Perimeter 2022



What is wrong with Classical Cryptography?



Problem: Unconditional security is not possible.

- Eg: RSA protocol is based on the mathematical complexity of factoring large numbers.
- Shor's algorithm: Algorithm using quantum gates that can perform factorization in polynomial time.



Perimeter 2022





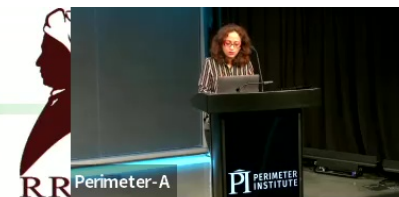
QuIC



1. Computational resources grow very fast and today's hard problem could be solved tomorrow using brute force attack.
2. New algorithms for classical computers.
3. Realization of quantum computers.
4. My security should be independent of future advancements in computational power, new algorithms or new technology. i.e. it should be future secure.
5. This brings forth the need for Quantum Cryptography, where security is based on laws of nature (or laws of Physics) and not on the mathematical complexity of a problem.

Perimeter 2022

The RSA Cryptographic Protocol



- The RSA key length and symmetric key length equivalence and security claim by “RSA Security”¹.

RSA Key Length	Symmetric Key Length	Security Claim
1024 bit	80 bit	Breakable between 2006-2010
2048 bit	112 bit	Secure till 2030
15356 bit	256 bit	Security beyond 2030

“The RSA-2048 Challenge Problem would take 1 billion years with a classical computer. A quantum computer could do it in 100 seconds” - [Dr. Krysta Svore](#), Microsoft Research²

- The current **RSA factorization record** is for [a 768-bit integer](#) by Thorsten Kleinjung *et al.*, announced in Dec 2009, using cluster computing and took two and a half years to solve.³
- A quantum computer will employ Shor’s algorithm to solve the factorization problem. It is estimated that 2048-bit RSA keys could be broken on a quantum computer comprising **4,000 qubits and 100 million gates**.⁴

¹ https://en.wikipedia.org/wiki/Key_size

² <https://medium.com/quantum-bits/break-rsa-encryption-with-this-one-weird-trick>

³ <https://arstechnica.com/information-technology/2010/01/768-bit-rsa-cracked-1024-bit-safe-for-now>

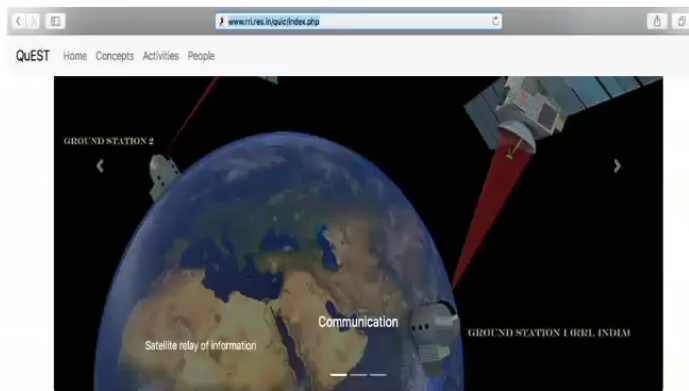
⁴ https://www.entrust.com/wp-content/uploads/2013/05/WP_QuantumCrypto_Jan09.pdf

Quantum Communications overview



India's first project on satellite based QKD

<http://www.rri.res.in/quic/>



Quantum Experiments using Satellite Technology

The age of quantum technologies is imminent and the enhancement in the computational power can pose a threat to the various cryptographic standards currently being used in secure communication, all over the world. The security of most of

Experimental quantum communications using **integrated photonics**: Project under the India Trento Programme on Advanced Research (ITPAR): Indo-Italian bilateral programme.

Project under Quantum Enabled Science and Technology programme of the Department of Science and Technology on experimental **Quantum Teleportation**.

Project under Centre for Excellence in Quantum Technologies of the Ministry of Electronics and Information Technology on **Device Independent Random Number Generation**.

Perimeter 2022



Prepare and Measure based QKD protocols..



Performed with our single photon sources based on spontaneous parametric down conversion and using Uncertainty Principle (non – orthogonality of states) for the security.

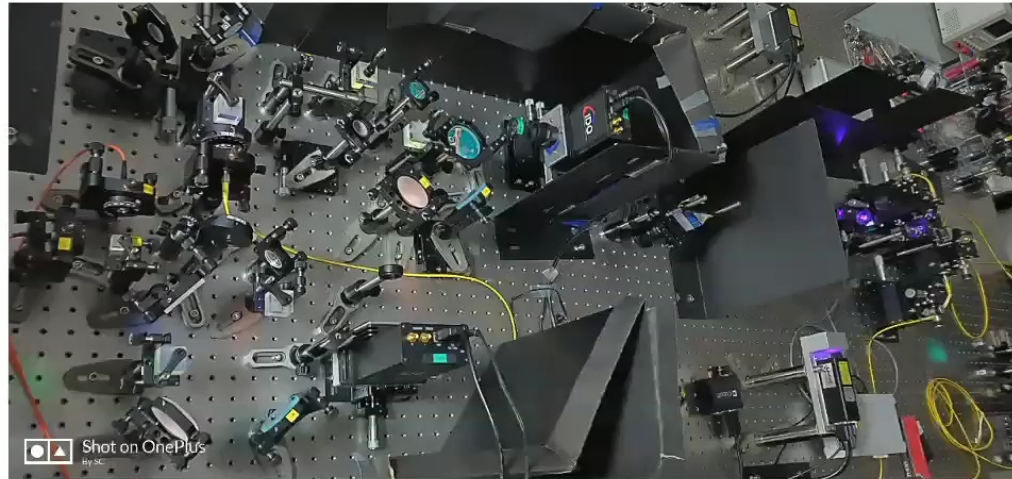
Perimeter 2022



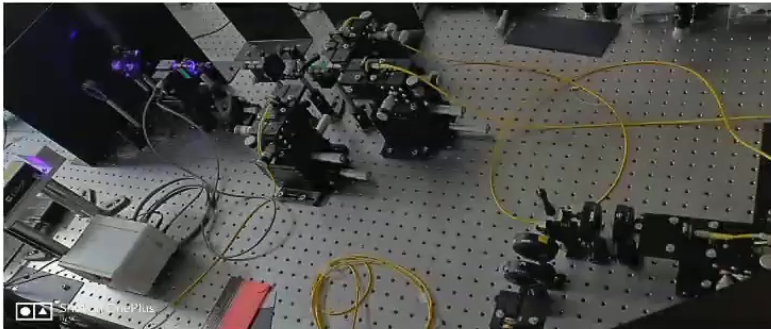
Photographs of B92 setup



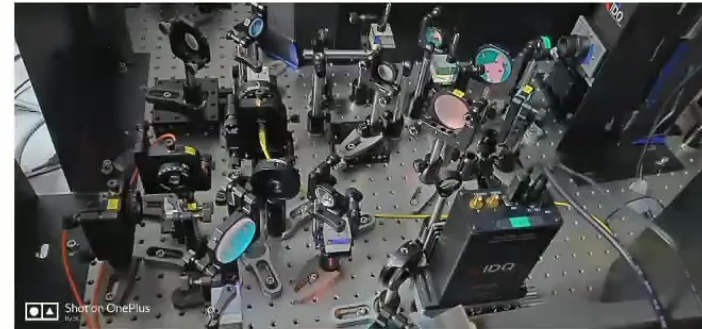
Both: Alice and Bob setup



Alice setup



Bob setup



Perimeter 2022

R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, *Physical Review Applied* **14** 024036, 2020

To our knowledge, till date, the best available B92 setup (using SPDC source) has reported key rate of 31.6 kHz, and QBER 10.5% for 0.4 meters transmission.

Jeffrey Wilson *et al.*, 'Free-space quantum key distribution with a high generation rate potassium titanyl phosphate waveguide photon-pair source', Quant. Comm. & Quant. Imag. XIV, Vol. **9980**, ISOP, 99800U (2016).

Channel length = 2 m, Pump power = 30 mW, Crystal length = 20 mm, Temperature = 40° C

time of the experiment	key rate (kHz)	QBER (%)	symmetry
day	47.8 ± 0.6	4.79 ± 0.01	50.2 : 49.8
night	53.8 ± 0.4	4.79 ± 0.01	53.7 : 46.3

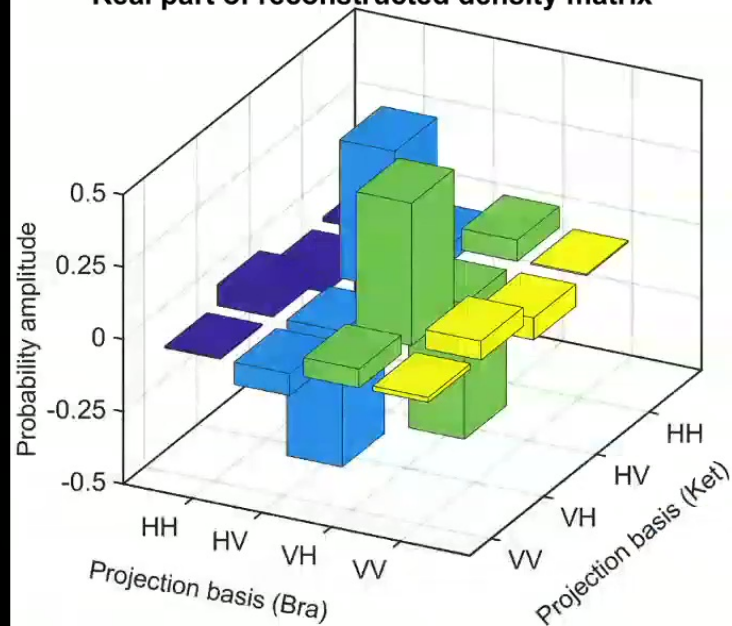
Perimeter 2022



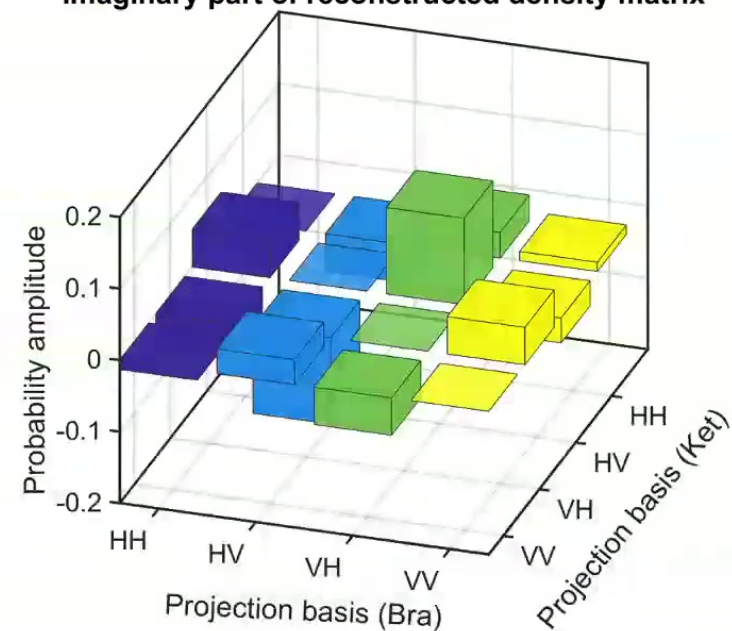
QuIC



Real part of reconstructed density matrix



Imaginary part of reconstructed density matrix



Concurrence of 0.995 achieved in our entangled photon source. Highest possible value being 1.

Perimeter 2022

qkdSim: An experimenter's simulation toolkit for QKD with imperfections, and its performance analysis with a demonstration of the B92 protocol using heralded photons

Rishab Chatterjee,¹ Kaushik Joarder,¹ Sourav Chatterjee,¹ Barry C. Sanders,^{1,2} and Urbasi Sinha^{1,*}

¹Raman Research Institute, C. V. Raman Avenue, Sadashivanagar, Bengaluru, Karnataka 560080, India

²Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada

Physical Review Applied **14** 024036, 2020

An in-lab (free-space) experimental implementation of the B92 protocol has been achieved and reported. This is India's first reported end to end free space QKD experiment, published in internationally peer reviewed journal.


Perimeter 2022

qkdSim, a Simulation Toolkit for Quantum Key Distribution Including Imperfections: Performance Analysis and Demonstration of the B92 Protocol Using Heralded Photons

Rishab Chatterjee,¹ Kaushik Joarder,¹ Sourav Chatterjee²,¹ Barry C. Sanders²,^{1,2} and Urbasi Sinha^{1,*}

¹*Raman Research Institute, C. V. Raman Avenue, Sadashivanagar, Bengaluru, Karnataka 560080, India*

²*Institute for Quantum Science and Technology, University of Calgary, Alberta T2N 1N4, Canada*

 (Received 29 January 2020; revised 22 May 2020; accepted 23 June 2020; published 13 August 2020)

Quantum key distribution (QKD) is one of the most important aspects of quantum cryptography. Using laws of quantum mechanics as the basis for security, the key-distribution process makes information theoretically secure in QKD. With the advancement and commercialization of QKD, an end-to-end QKD simulation software is required that can include experimental imperfections. Software of this kind will ensure that resources are invested only after prior performance analysis, and is faithful to experimental capacities and limitations. In this work, we introduce our QKD simulation toolkit qkdSim, which is ultimately aimed at being developed into such a software package that can precisely model and analyze any generic QKD protocol. We present the design, implementation, and testing of a prototype of qkdSim that can accurately simulate our own experimental demonstration of the B92 protocol. The simulation results

An experimenter's toolkit for simulating Quantum Key Distribution protocol implementations - Indian Patent Application No.: 202141023697 (May, 2021).

Perimeter 2022

Simulation toolkit for QKD: existing in literature

QKD simulator
analyzing Quan
is powered by th
customizing a w
and sub-protoco
Error estimation
simulation provi
final stages of th

Set the initial
Simulator type:
Complete QKD Stack

Parameter
Initial Qubits (n)
Basis choice bias delta
Eve's basis choice bias
Biased error estimator

Quantum Key
OPEN

This mode
QKD key,
developed
(miralem
Sarajevo,

The imple
(AIT) R10
found in o

Prerequ
Quantum
cryptograp
QKD crypt
(OTP) ciph
algorithm and others. First
packet into a byte array which is used as the input

QKD

Our group has
developed a s
protocols, whi

Down
Down

This
does
docu

**A Modeling
Quantum K
Implementa**

LOGAN O. MAILLOUX
JEFFREY D. MORRIS²,
MICHAEL R. GRIMAIL
DOUGLAS D. HODSON,
JOHN M. COLOMBI¹,
COLIN V. MCCLAUGHLI
¹Air Force Institute of Technology, ²
³Army Cyber Institute, West Point, N
⁴Naval Research Laboratory, Washin
Corresponding author: M. R. Gr
This work was supported by the

ABSTRACT Quantu
quantum mechanics to
applications. However,
differ significantly from
work built upon the ON
nonidealities on QKD

OpenQKDNework

Background

Technological advances are bringing large-scale quantum computers closer to reality. While they will bring great benefit to society, they will also undermine some of the key cryptographic pillars of cybersecurity. It is thus imperative that the cryptographic underpinnings of cybersecurity are made resistant to quantum attacks before quantum computers threaten them. Quantum-safe cryptography includes conventional "post-quantum" cryptography (PQC) algorithms (sometimes referred to as "quantum-

Our requirements:

- Quick and precise simulation of physical processes, considering realistic experimental imperfections.
- Simulation of single photon source, detection module and background noise in more details.
- Generalization and applicability to all existing protocols.



C

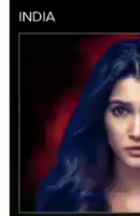


QuEST



Perimeter-A

PERIMETER INSTITUTE



India LAC Face-off

NEWS / INDIA NEWS / R

TOP SEARCHES: Corona

THIS STORY IS FROM

RRI rese
commur

Chethan Kumar | TNN |



Presenting qkdSim: a QK
experimentalists figuring

The novel toolkit c
to ensure online cc
increasing need fo
confines most day-to day business to the digital space.

Qiskit

India Is Amid a Quantum Boom

Qiskit Follow
Aug 19, 2020 · 9 min read



By Ryan F. Mandelbaum, Senior Technical Writer, Qiskit

Qiskit events draw students, researchers, and educators from around the world — but according to our data, interest is spiking in India, both in how users are engaging with the Qiskit open source community and in how often they're running IBM Quantum hardware.

Scientists in India have already started to undertake large-scale quantum projects. Three years ago, researchers began the country's first satellite-based quantum communication experiment — the Quantum Experiments using Satellite Technology, or QuEST project. Another team has been building an advanced new quantum computer. And earlier this year, India gave quantum technology a 80 billion rupee (\$1.07 billion) boost as part of its National Mission on Quantum Technologies and Applications, coordinating stakeholders from across industry, research, and government to spur development in quantum computing, cryptography, communications, and materials science. These efforts are set to have a global impact, while a quantum community is coalescing around newly available opportunities in the field.

"It's a great time to be doing quantum physics because the government is serious about it, the people are serious about it, and we're all excited about what this technology can do for India," said Rishab Chatterjee, a graduate student from the Raman Research Institute in Bangalore, India.

An Advanced New QKD Simulator

Perimeter 2022



C



QuEST



Perimeter-A



THE TIMES OF INDIA



India LAC Face-o

NEWS / INDIA NEWS / RP

TOP SEARCHES: Corona

THIS STORY IS FROM

RRI rese
commur

Chethan Kumar | TNN |



Presenting qkdSim: a QK
experimentalists figuring

The novel toolkit c
to ensure online cc
increasing need fo
confines most day-to day activities to the digital space.

Qiskit

India Is Amid a Quantum Boom



By Ryan

Qiskit ev
world —
users an
often th

Scientist
projects
based q
using Sa
building
gave qu
its Natio
coordin
to spur c
commu
global ir
availabl

"It's a gr
serious i
what thi
student

An Ac

Perimeter 2022

nature india

Home Archives Our picks Blog Podcast About

Global visibility and
impact

BMC Biology

SCIENCE NEWS

India employs home-grown cryptographic scheme for secure communication

K. S. Jayaraman

doi:10.1038/nindia.2020.117 Published online 27 July 2020

Researchers at the Raman Research Institute (RRI) in Bangalore have implemented India's first quantum cryptographic scheme to enable secure communication of sensitive data¹ — an acute need during the COVID-19 pandemic with most government, defence and academic communication going online.

The widely used information transfer protocols employ a secret "key" known only to the communicating parties, who can encrypt and decrypt the messages. The mathematical toolbox used in such protocols is vulnerable to access by eavesdroppers.

"The answer to this lies in using the Quantum Key Distribution or QKD," says Urbasi Sinha, who heads the RRI team.

QKD is a cryptographic method that enhances the security of the communication link by exploiting the principles of quantum mechanics such as the uncertainty principle and no-cloning theorem, Sinha says.



Today's science fiction is
tomorrow's science fact.

Isaac Asimov

quote fancy

Perimeter 2022



Why Satellites for QKD?

Distance Limits for Quantum Channels

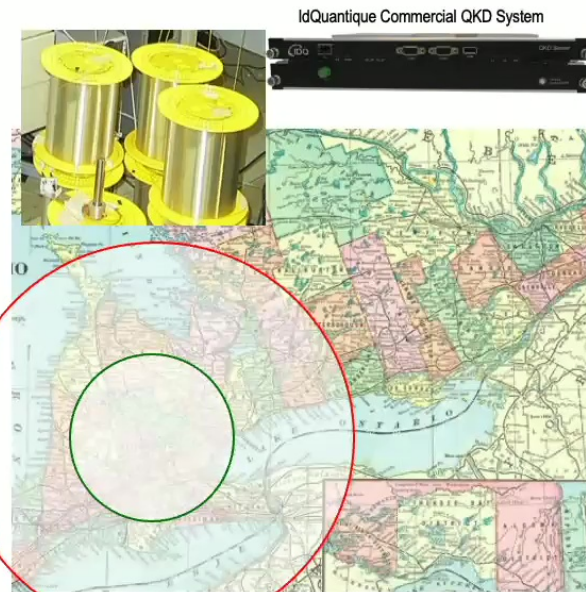


- Ground-based

- typically 100 km
- Demonstrations to max. 300 km
- Optic fibre loss 0.15 dB/km at best
- Free-space limited due to line-of-sight
- Commercial Devices available:
- **Note: Optical amplifiers not possible!**

- Longer distances:

- Trusted Repeaters (> 1000km networks under way)
- Long lived Quantum Memories
- Quantum Repeaters
- **Satellites**



Takesue et al, Nature Photonics 1, 343 - 348 (2007)
Ma, Fung, Lo, Phys. Rev. A 76, 012307 (2007)

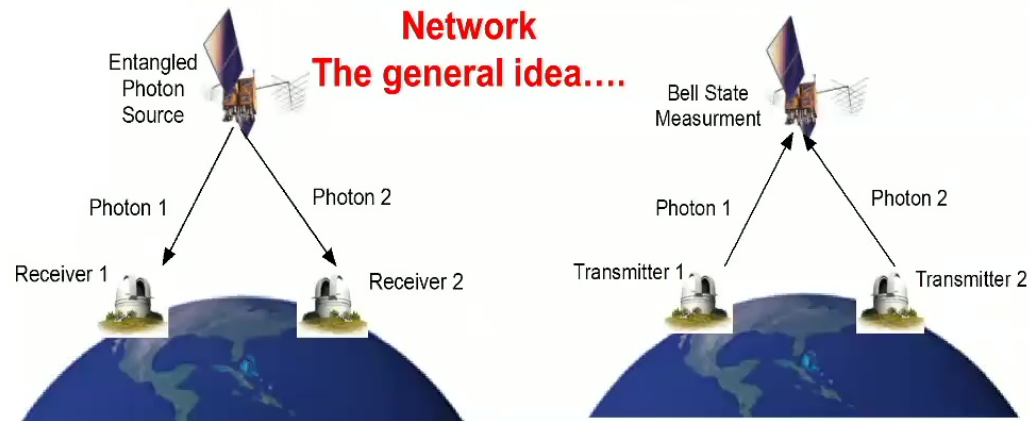
$$T_{geo} \approx \frac{D_R^2 D_T^2}{\lambda^2 L^2}$$

Perimeter 2022

Satellite based Quantum Key Distribution



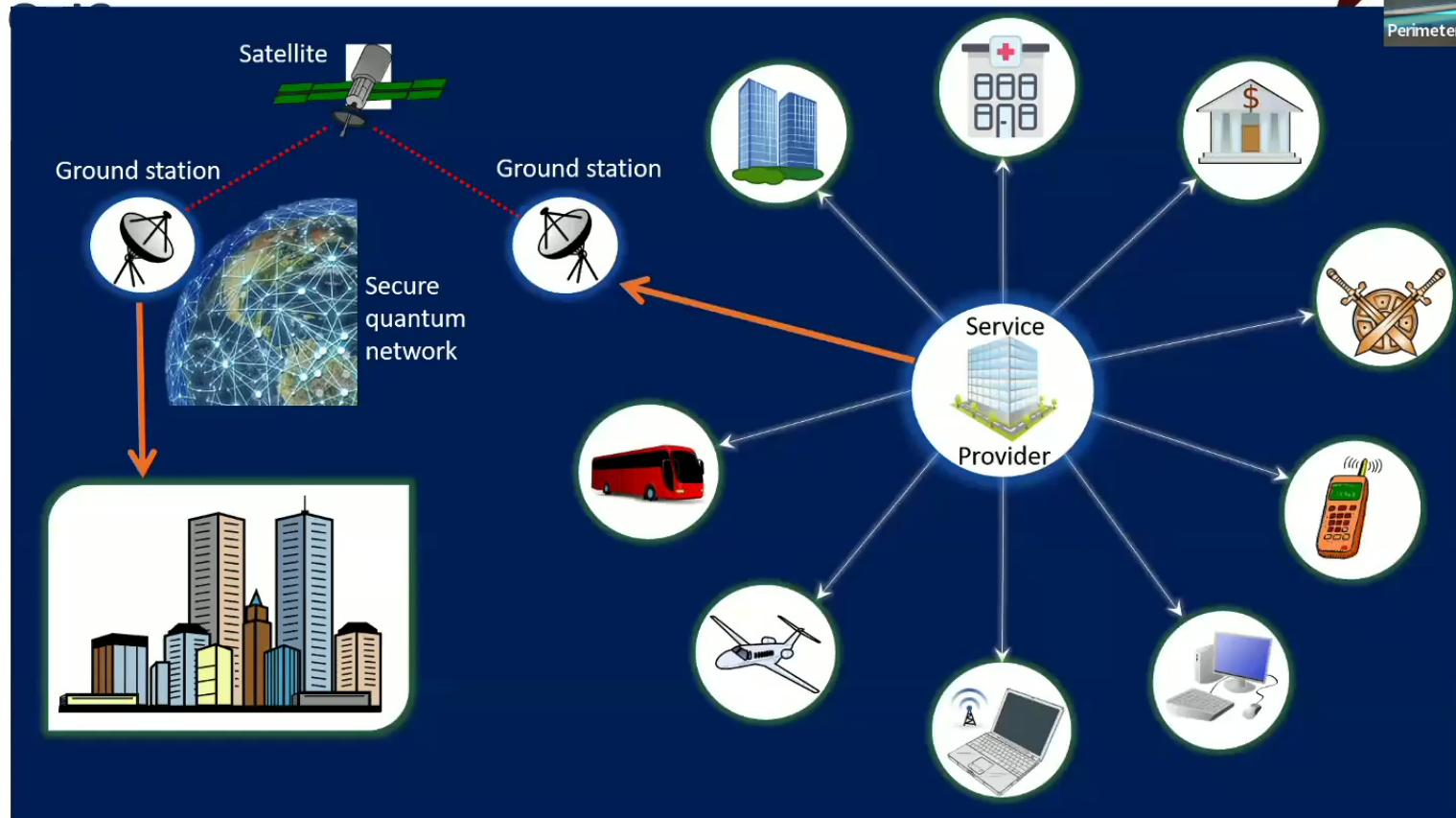
Intercontinental Quantum Secured Network The general idea....



From GEO, almost half the Earth is visible.

- Quantum Repeater: N. Sangouard, C. Simon, et al, Rev. Mod.Phys, 2011
- Detector independent QKD: H.K. Lo, PRL, 2012

Perimeter 2022



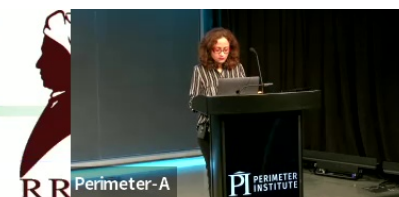
Perimeter-A

PI PERIMETER INSTITUTE

Perimeter 2022



QuIC



Fibre-based QKD record:

Previous distance record was 404 km (Measurement-device-independent quantum key distribution over a 404 km optical fiber) [H.-L. Yin et al., Phys. Rev. Lett. 117(19), 190501 (2016)]

Secure Twin-Field Quantum Key Distribution over 509 km [Jiu-Peng Chen et al., Phys. Rev. Lett. **124**, 070501 (2020). <https://doi.org/10.1103/PhysRevLett.124.070501>]

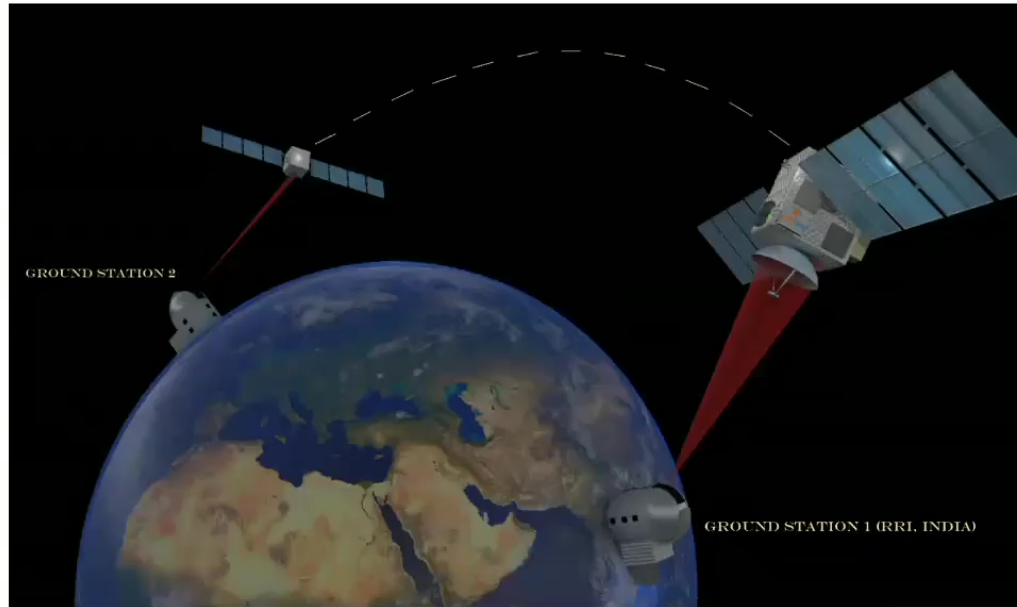
Recently, China successfully completed the 2000-km-long fiber-optic backbone link between Beijing and Shanghai (Y.-A. Chen et al., 2020 **YET TO BE PUBLISHED**). [Source: F. Xu et al., Secure quantum key distribution with realistic devices, Rev. Mod. Phys. 92, 025002 (2020). <https://doi.org/10.1103/RevModPhys.92.025002>]

Free-space QKD record:

Experimental implementation of a Bennett-Brassard 1984 (BB84) protocol type quantum key distribution over a 144 km free-space link using weak coherent laser pulses [Tobias Schmitt-Manderbach et al., Phys. Rev. Lett. 98, 010504 (2007).

<https://doi.org/10.1103/PhysRevLett.98.010504>]

Perimeter 2022



Aim

- ☐ Establishment of information theoretically (satellite-based) secure quantum communication over large distances.
- ☐ Essentially, perform quantum key distribution (QKD) between two ground stations.

QuEST (Quantum Experiments with Satellite Technology)

Collaboration

Raman Research Institute (RRI)



Indian Space Research Organization (ISRO)



Perimeter 2022





Perimeter 2022

4:07 PM

25.8°C

18.4°C

06:27 बजे

06:39 बजे

01:56 बजे

02:19 बजे

राजस्थान पात्रिका

पत्रिका न्यूज नेटवर्क

कोरोना संक्रमण अपडेट

दुनिया

भारत

राजस्थान

बंगलूरु ए.

व्हांटम तकनीक में देश को बड़ी सफलता, 2017 से चल रहा था प्रयोग: आरआरआई के वैज्ञानिकों ने दो भवनों के बीच स्थापित किया व्हांटम संचार

अब देश की कोई भी अहम सूचना नहीं हो पाएगी लीक

वैकिंग, रक्षा, सामरिक क्षेत्र के लिए अत्यंत महत्वपूर्ण

सूचना को डिकोड करना नामुमकिन

आरक्षण प्रवर्ग में बदलाव की मांग: पंचमशाली समुदाय का बंगलूरु में शक्ति प्रदर्शन

नए सरकारी अंतरिक्ष उपग्रह के उपग्रह

Perimeter 2022

Pirsa: 22070000

Page 109/115



QuIC



सत्यमेव जयते

Government of India
Ministry of Science & Technology
Department of Science & Technology



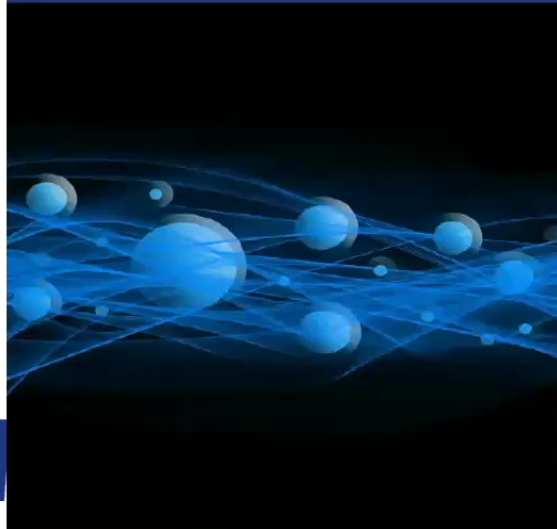
20 Major Success Stories of DST in 2020

Perimeter 2022



QulC

20. RRI ACHIEVES FIRST SUCCESSFUL IMPLEMENTATION OF A HIGHLY SECURE EFFICIENT QUANTUM CRYPTOGRAPHIC SCHEME



The QulC lab at RRI achieved the first successful implementation in India of a highly secure efficient Quantum Cryptographic scheme for an end to end free space QKD under the RRI-ISRO project on "Quantum Experiments using Satellite Technology". The lab has also come up with an end-to-end simulation toolkit named as "qkdSim" to ensure safety in secure quantum communication platforms, a first of its kind that enables Quantum Key Distribution Protocol (QKD) experimentalists to obtain a realistic estimate of the result from an experimental setup meant to demonstrate a QKD protocol. They have also performed an experiment in collaboration with HRI Allahabad that demonstrates a novel quantum state estimation tool opening up a new paradigm in quantum state estimation.

20 /

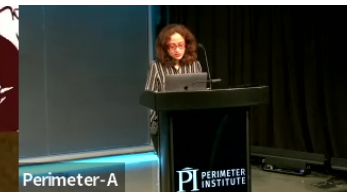
Perimeter 2022





Science This year - 2020 (E)
Science This Year - 2020 (E)

Perimeter 2022





QuIC



varun aggarwal, ASSOC SAMRIDHI GOYAL Kumud Bajaj Dubey Urbasi Sinha Jyoti Arora

ASSOCHAM AWARDS 2021
WOMEN IN CYBER: MAKING A DIFFERENCE

WINNER
Ms. Urbasi Sinha
Raman Research Institute

CATEGORY
Cyber Leading from Front

ASSOCHAM
Celebrating 101 Years

EY
Knowledge Partner
Building a better working world

Urbasi Sinha

+25

Perimeter 2022



QuIC



varun aggarwal, ASSOC SAMRIDHI GOYAL Kumud Bajaj Dubey Urbasi Sinha Jyoti Arora

tcs | **TATA CONSULTANCY SERVICES** | **ASSOCHAM**
Celebrating 101 Years

ASSOCHAM AWARDS 2021

CYBER: MAKING A DIFFERENCE

WINNER

Ms. Urbasi Sinha
Raman Research Institute

CATEGORY
Cyber Leading from Front

ASSOCHAM
Celebrating 101 Years

Knowledge Partner
EY
Building a better working world

Urbasi Sinha

+25

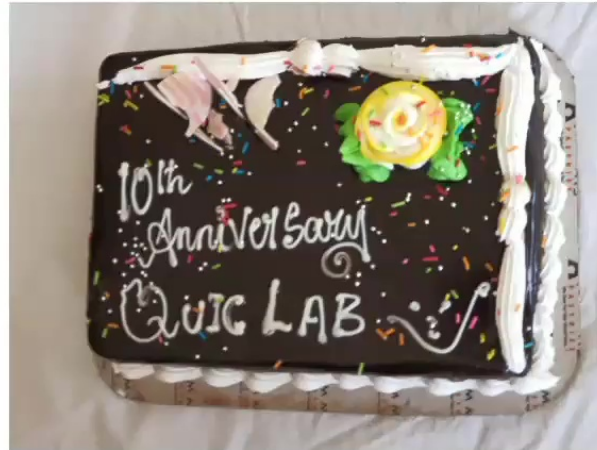
Perimeter 2022



THANK YOU 😊



Come join us!!



Perimeter 2022