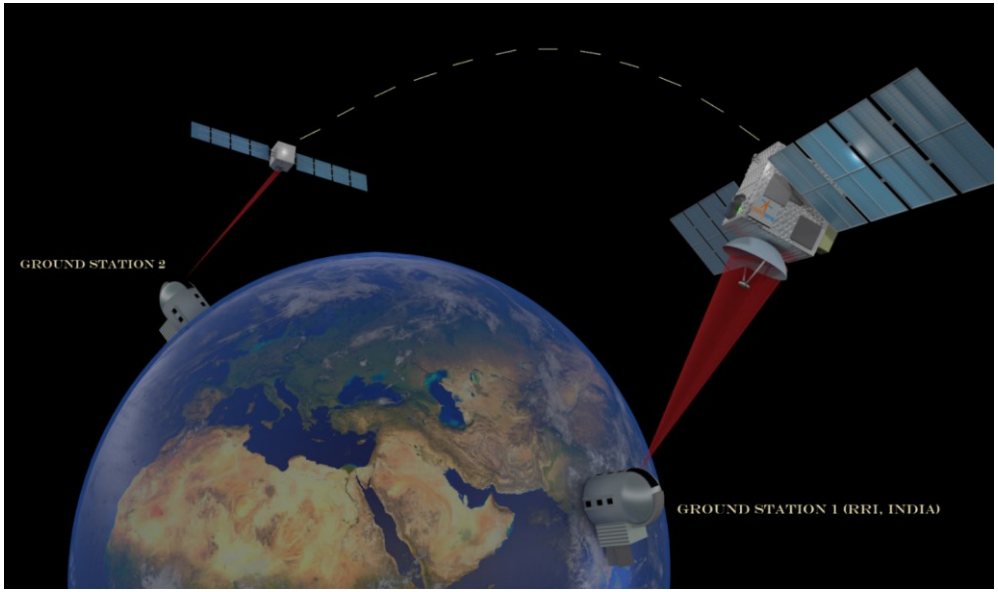
Satellite based quantum communications

QuEST

ISRO



RRI

QuIC

Prof. Urbasi Sinha

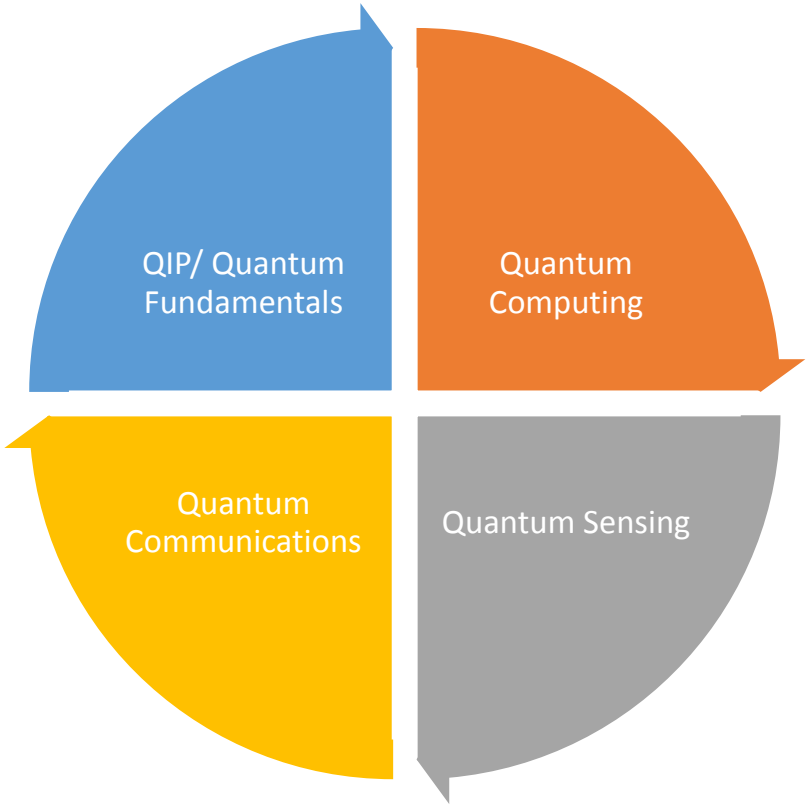
π: Quantum Information & Computing (QuIC) Lab

Raman Research Institute (RRI), Bengaluru, India.

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

Simon's Emmy Noether fellow, Perimeter Institute, Canada

With Photons….



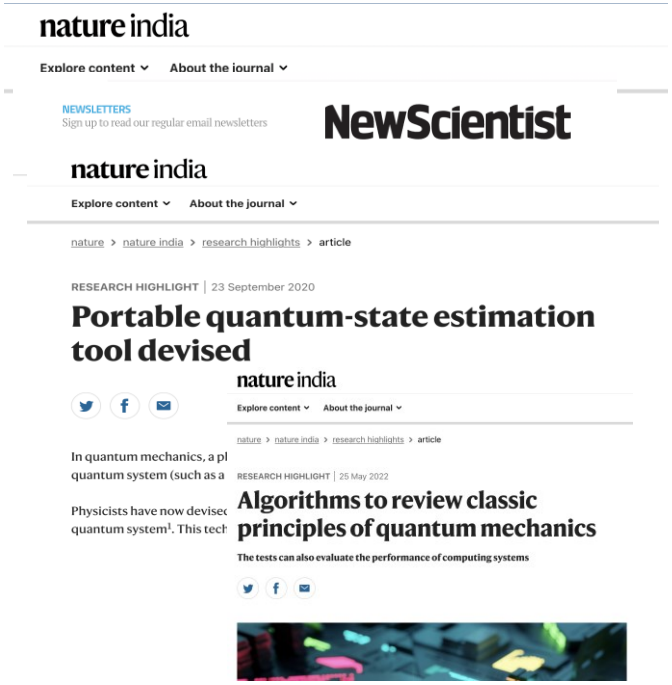
In a nutshell…

Quantum Communications

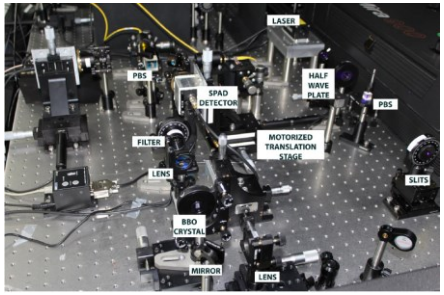
- **Satellite based QKD: Quantum Experiments with Satellite Technology (India's first funded satellite QKD project)**
- **DST-QuEST project on Quantum Relays and Repeater technologies (Theme 1 Q-97)**
- **DST-ITPAR project on Integrated Photonics based QKD (Indo-Italian collaboration)**
- **Long Distance Quantum Teleportation and Device Independent Random Number generation (CEQT grant from MEITY)**

First demonstration of quantum key distribution **between two buildings using an atmospheric free space channel** in India (February 2022).

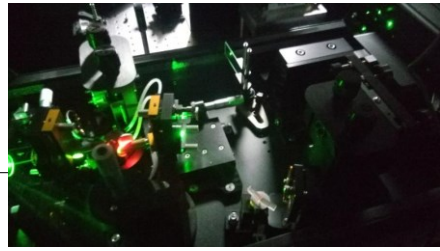
First lab in India dedicated to Photonic Quantum Science and technologies

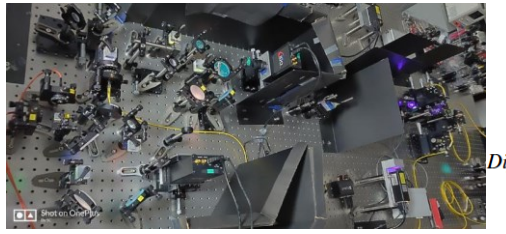


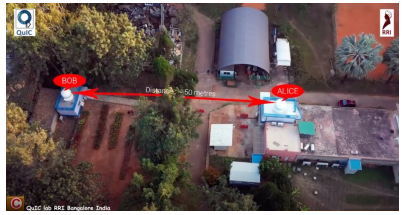
Higher dimensional Quantum Computing and Quantum Information



Effective interplay between fundamental science and novel technologies







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

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

PHYSICAL REVIEW APPLIED **14,** 024036 (2020)

PHYSICAL REVIEW RESEARCH **4**, L022001 (2022)

Letter

Testing quantum foundations with quantum computers

Simanraj Sadana,[1] Lorenzo Maccone,[2] and Urbasi Sinha[1,*]

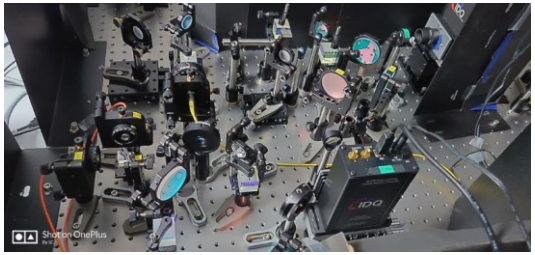
[1]*Light and Matter Physics, Raman Research Institute, Bengaluru-560080, India*

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)

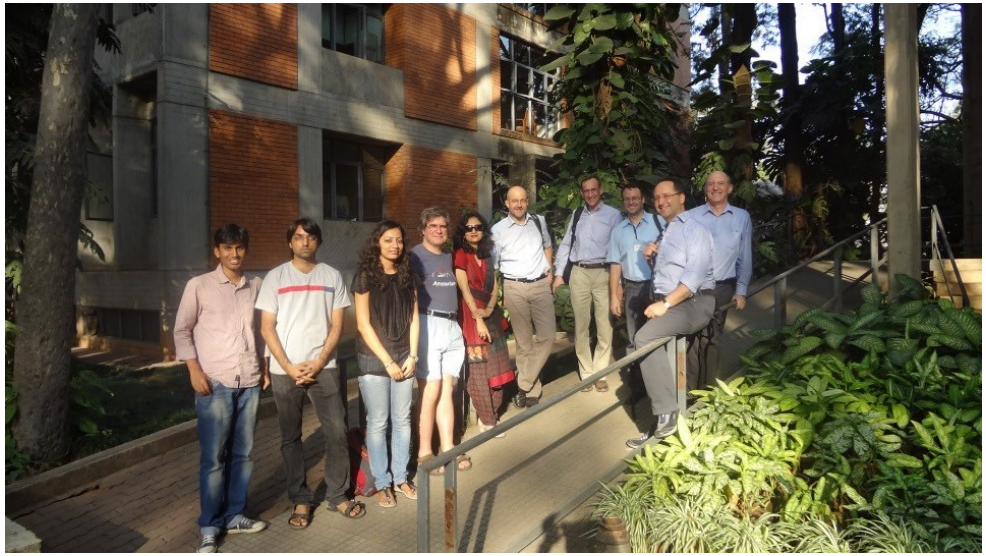
We present two complementary viewpoints for combining quantum computers and the foundations of quantum mechanics. On the one hand, ideal devices can be used as test beds for experimental tests of the foundations of quantum mechanics: We provide algorithms for the Peres test for complex numbers in quantum 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://wwws.rri.res.in/quic

And so our journey began….



Quantum Communication experiments at RRI Bangalore








Current members

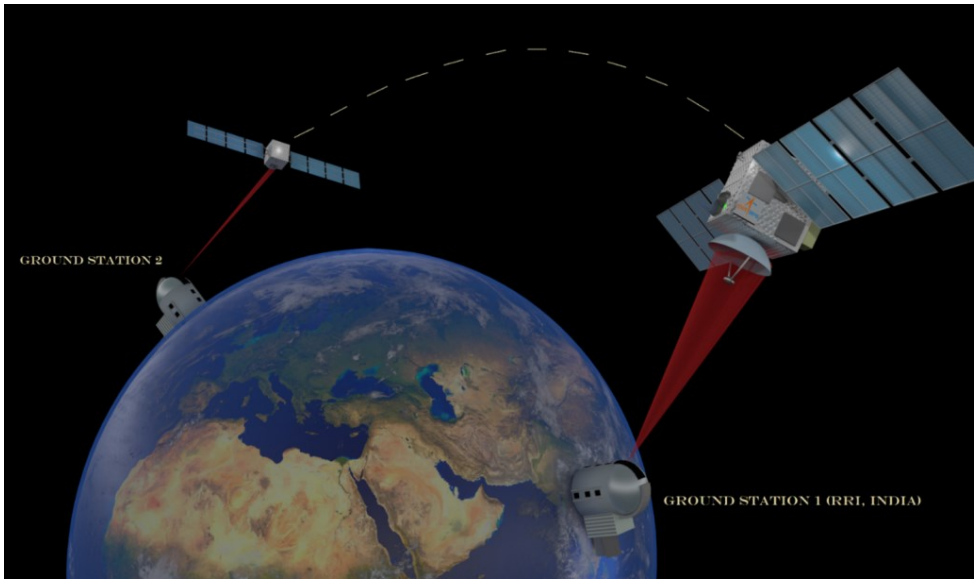
Quantum Experiments using Satellite technology (QuEST)

QuIC

RRI

QuEST

ISRO



Aim

- Establishment of information theoretically (satellite-based) secure quantum communication over large distances.
- Essentially, perform entanglement based Quantum Key Distribution (QKD) between two Indian ground stations using an Indian satellite as a trusted node.

QuEST (Quantum Experiments with Satellite Technology) Collaboration

Raman Research Institute (RRI) [redacted] Indian Space Research Organization (ISRO)

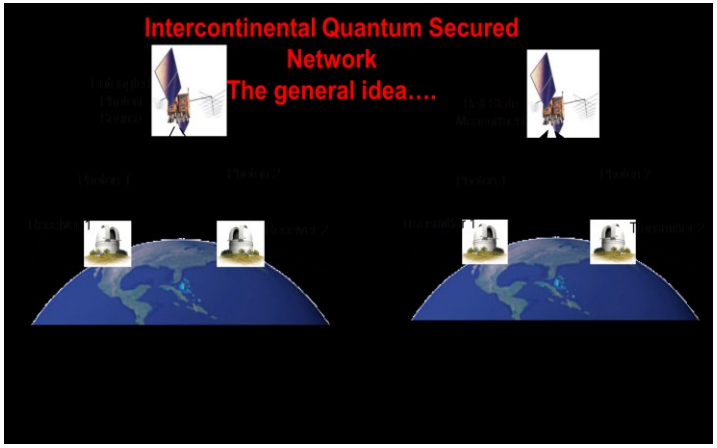
PI: Prof. Urbasi Sinha
Quantum Information and Computing lab, RRI Bengaluru.
usinha@rri.res.in

Why is this experiment exceptional?

- Security in communications is a top priority for various strategic applications including military, banking and many more.
- Current means of securing communications using public key cryptography stand to be compromised with the advent of algorithmic breakthroughs including quantum computing.
- Secure quantum communications thus becomes the need of the hour.
- The security should be operational across long distances, between countries and beyond.
- Using a satellite as a trusted node is a novel means towards long distance secure quantum communications.

QuEST is India's first project on satellite based quantum communications (Sep 2017 -). Started at a time when the field was not that popular, its achievements have played a major role towards putting India on the global map for quantum communications research.

The Chinese satellite demonstrated down link based QKD[1,2,3].



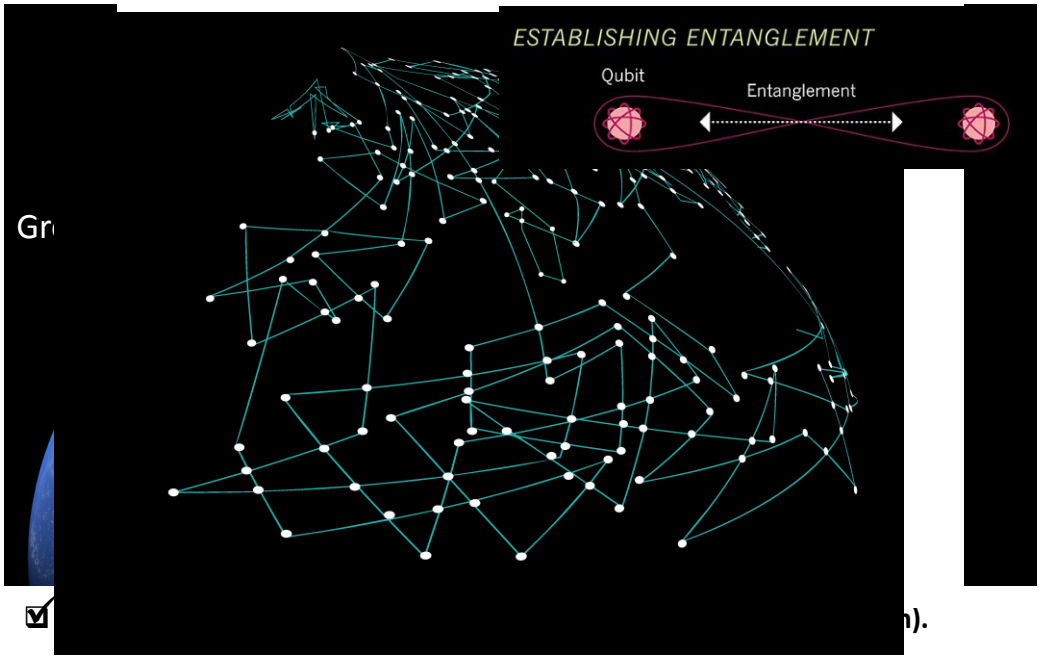
QuEST aims at demonstrating uplink based QKD – never been shown before globally.

- **Uplink allows for photon source to be at the ground based lab.**
- **More flexibility with changing the source even after the satellite has been launched.**
- **Can include quantum memory components also after satellite launch.**
- **Tremendous scope for novel, first-in-the-world science.**

1. Liao, S.K., et al.: Satellite-to-ground quantum key distribution. Nature. 549(7670), 43–47 (2017)
2. Chen, Y.A., et al.: An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature. 589(7841), 214–219 (2021)
3. Yin, J., et al.: Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature. 582(7813), 501–505 (2020)

Project Overview

India's first project on satellite based quantum communications



- ☑ **Prototype for an entanglement-based QKD protocol over an:**
  - **in-lab transmission channel.**
  - **atmospheric channel.**
- ❑ **Prototype for the QKD protocol from a moving receiver platform..**

☑ **).**

☑ **Performance analysis of qkdSim via an in-lab B92 protocol implementation.**

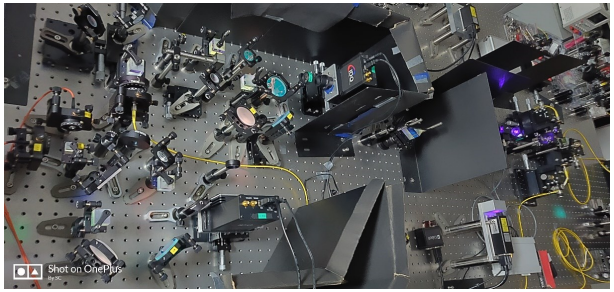
☑ **Development of an entangled bi-photon source.**

☑ **Free-space atmospheric channel characterization.**

Overall milestones achieved so far…

QuIC

Alice and Bob setup



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,*]

[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*

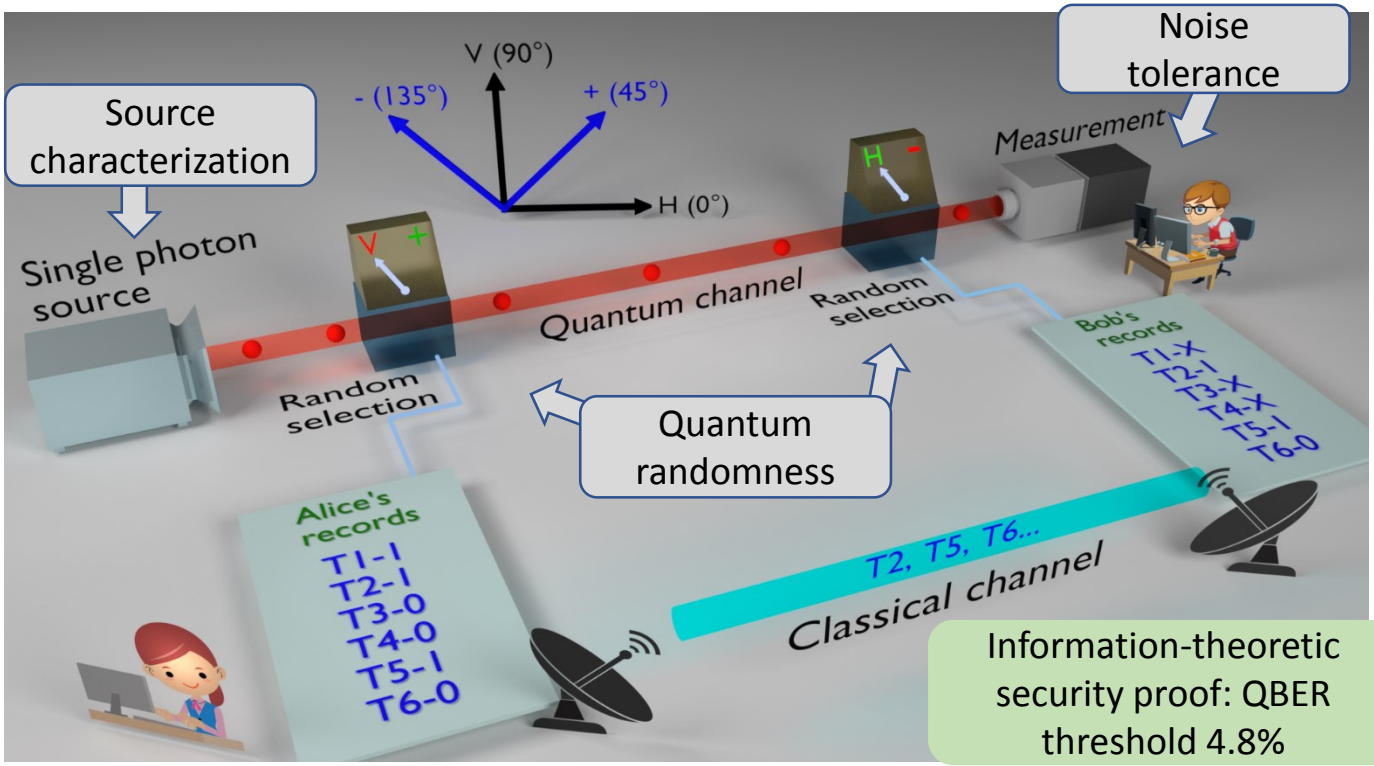
Physical Review Applied **14** 024036, 2020

- **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. The protocol established globally competitive keyrate of 51± 0.5 KHz and a QBER of 4.79±0.01%.**

- **First demonstration** of quantum key distribution **between two buildings using an atmospheric free space channel** in India (February 2021), using Entanglement (https://www.rri.res.in/quic/qkdactivities.php)
- *Polarization correction towards satellite-based QKD without an active feedback*, S. Chatterjee, K. Goswami, R. Chatterjee and U. Sinha, to appear in *Communications Physics (Nature)*
- [**Novel entanglement Based QKD protocol**]

- *R. Chatterjee, S. Chatterjee, B. C. Sanders, and U. Sinha, "An experimenter's toolkit for simulating quantum key distribution protocol implementations",* **Indian Patent Application No. 202141023697 (2021)** [**Novel software development for QKD with device and process imperfections].**

QKD: polarization-encoded B92 protocol



- Single photon generation
- State preparation by Alice
- Transmission
- Measurement by Bob
- Classical post-processing

$+ \rightarrow 0 \longleftrightarrow |H><H|$

$V \rightarrow 1 \longleftrightarrow |-><-|$

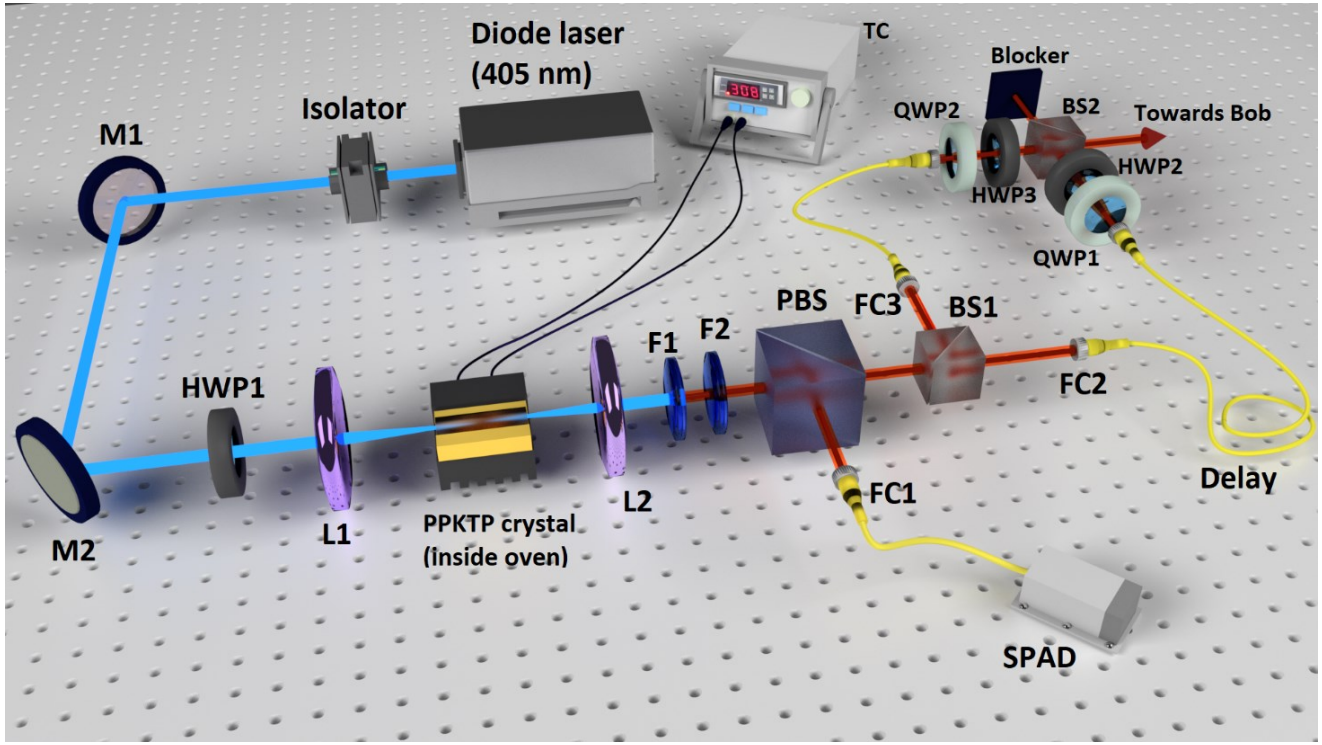
25% success rate

110010	110010
110010	100011

Measurements by an eavesdropper introduces detectable errors, because of Heisenberg's uncertainty principle.

C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
R. Renner, N. Gisin, B. Kraus, Phys. Rev. A **72**, 012332 (2005).

Schematic of B92 experimental setup: Alice's module



Components:

M1, M2: dielectric mirrors

HWP1:half-waveplate for pump light

L1: focusing lens

L2: collimating lens

F1: long pass filter

F2: band pass filter

PBS: polarizing beam splitter

FC1, FC2, FC3: fibre couplers

BS1, BS2: 50-50 beam splitter

HWP2, HWP3: half-waveplates

QWP1, QWP2: quarter-waveplates

SPAD: single photon avalanche detector

TC: temperature controller

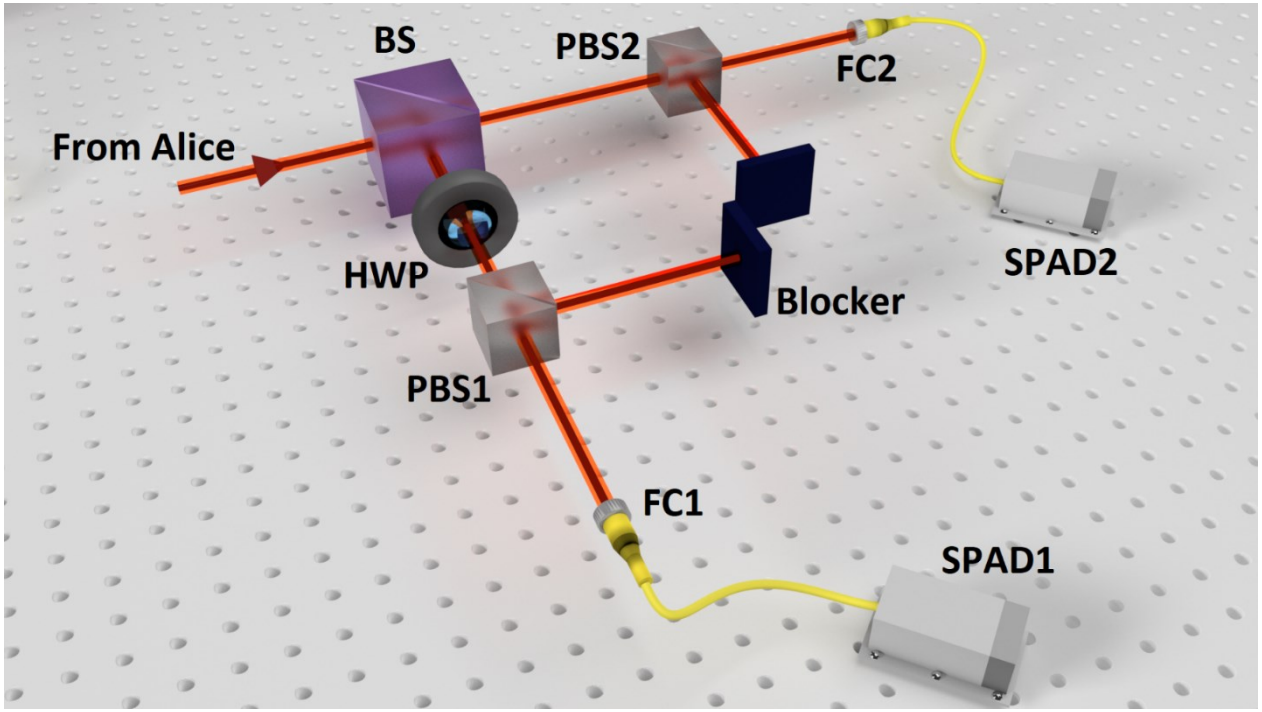
- Heralded single photon using SPDC (continuous pumping)
- Passive quantum randomness

Eavesdropping attacks:

1) PNS type attack
2) Attacks based on active random basis selection

R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, Phys. Rev. App. **14**, 024036 (2020).

Schematic of B92 experimental setup: Bob's module



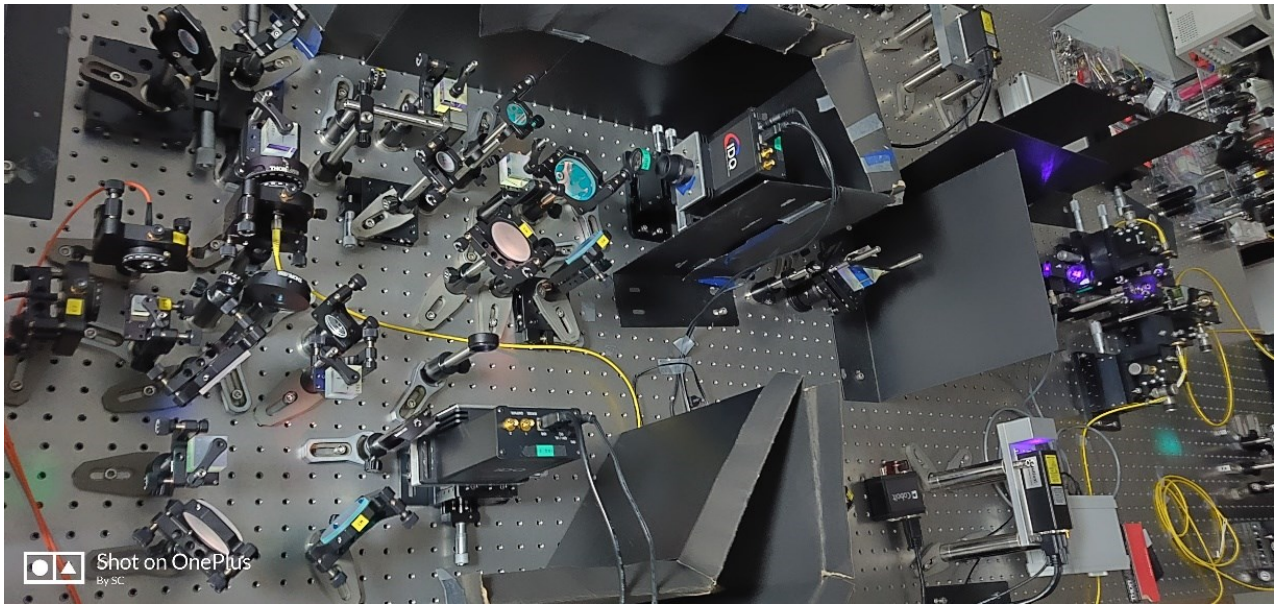
- Passive quantum randomness
- No gated detection required
- Continuous record of time-stamps

Components:
BS: 50-50 non-polarizing beamsplitter
HWP: half-wave plate
PBS1, PBS2: polarizing beamsplitters
FC1, FC2: fibre couplers
SPAD1, SPAD2: single photon avalanche detector

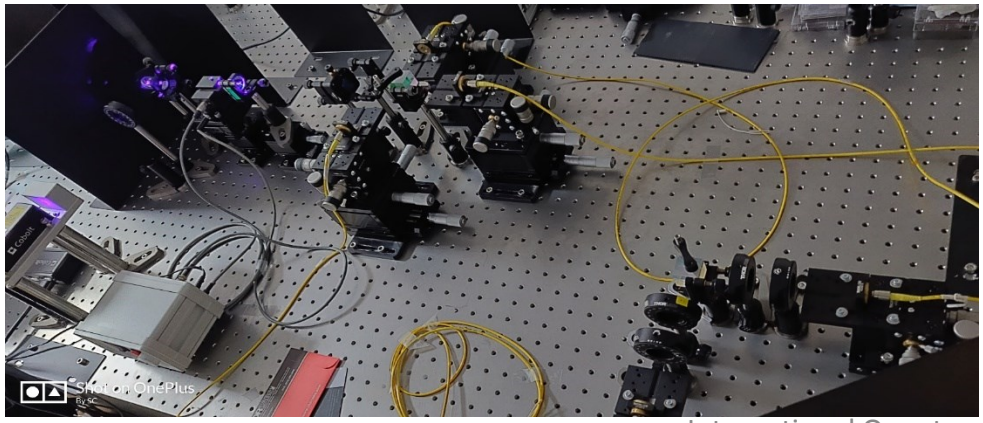
R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, Phys. Rev. App. **14**, 024036 (2020).

Snapshots of the actual B92 setup

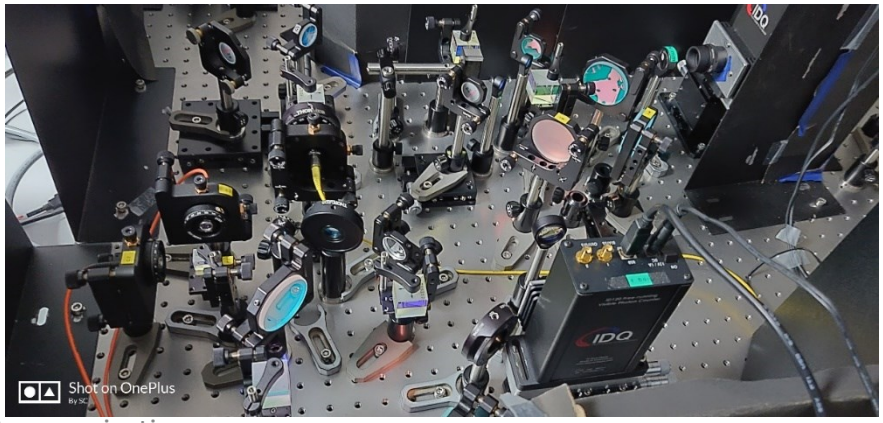
Combined setup



Alice's setup



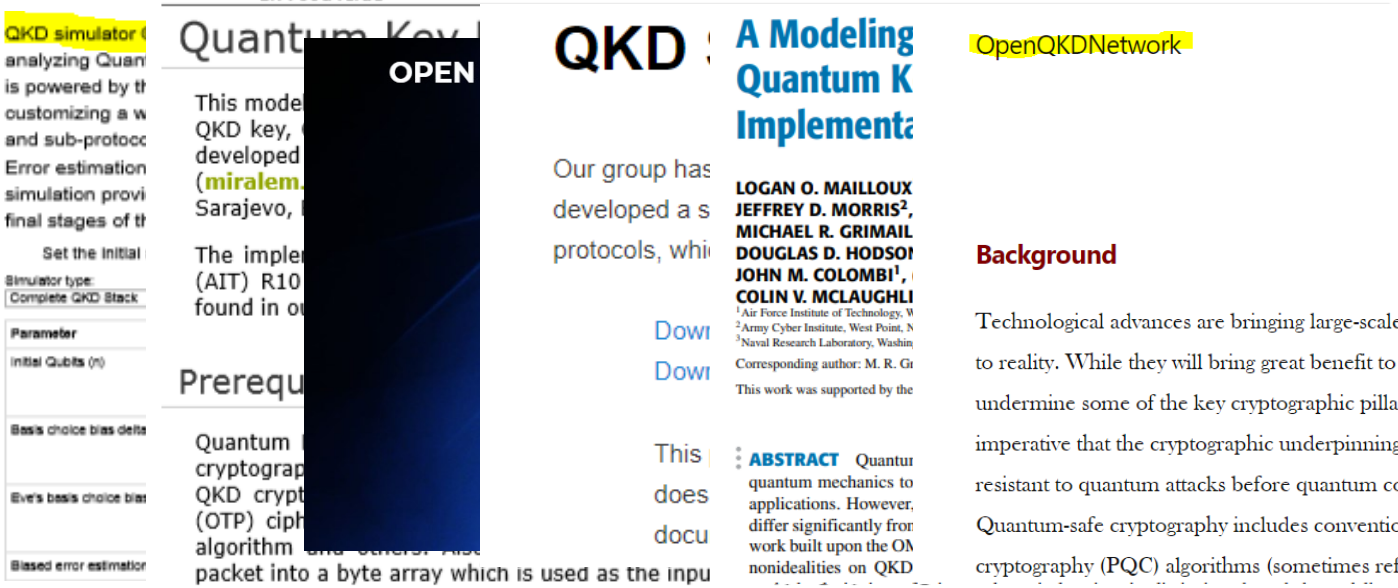
Bob's setup



R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, Phys. Rev. App. **14**, 024036 (2020).

Competing QKD simulation toolkits in literature

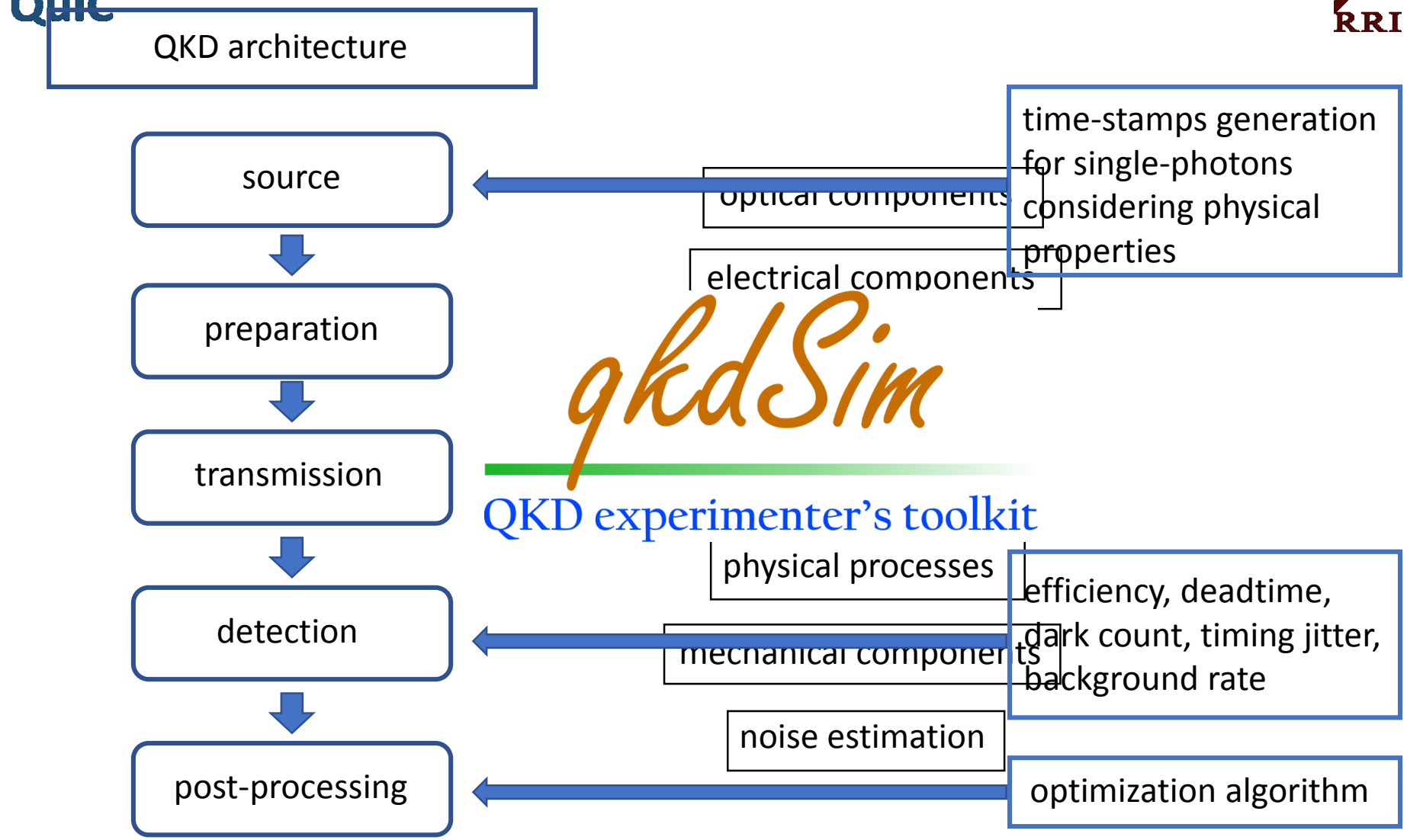
- With QKD becoming commercially viable, advanced engineer techniques are being proposed.
- Direct testing of these techniques in an optical setup is not very cost effective.
- A simulator that can accurately pre-evaluate the performance of these setups/designs.



Missing requirements:

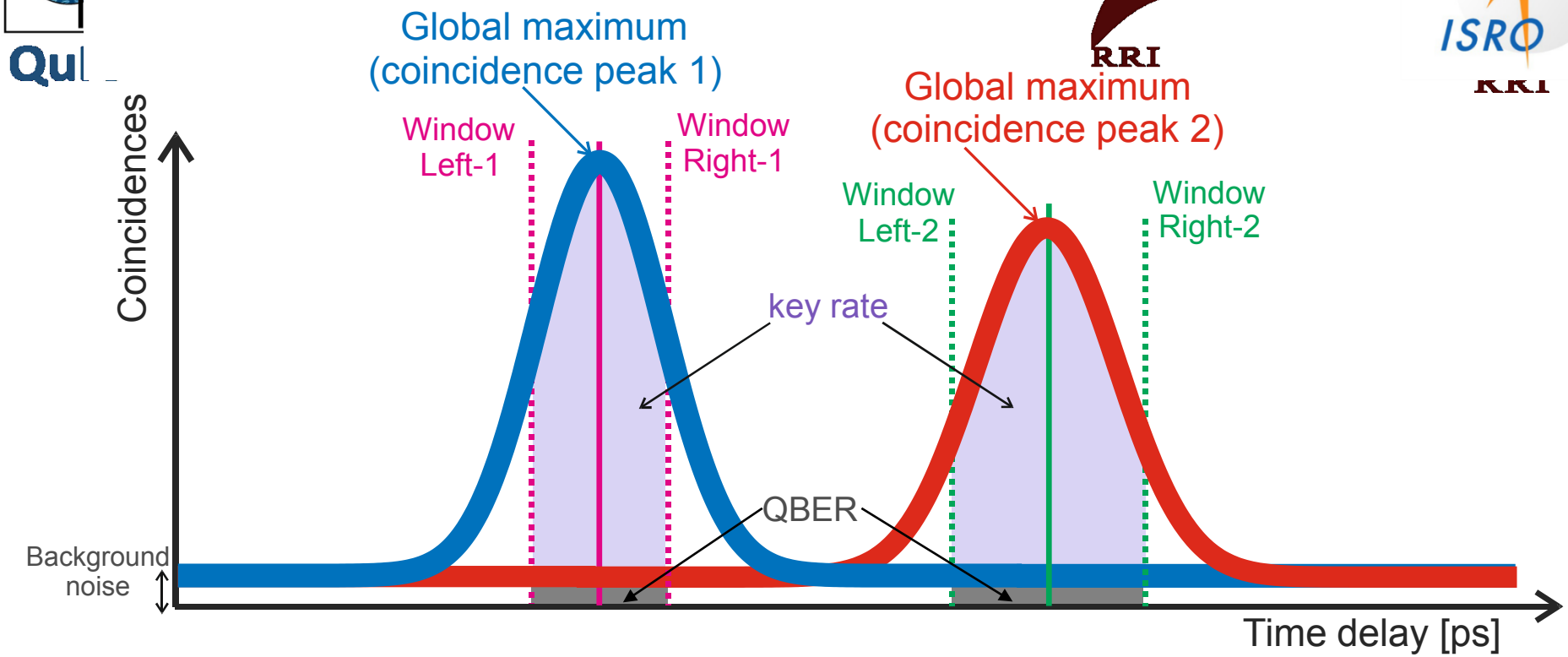
- Quick and precise simulation of physical processes.
- Consideration of experimental non-idealities.

In-house developed QKD simulation toolkit



R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, Phys. Rev. App. **14**, 024036 (2020).
R. Chatterjee, S. Chatterjee, B. C. Sanders, and U. Sinha, Indian Patent Application No. 202141023697 (2021).

Classical post-processing: optimized results

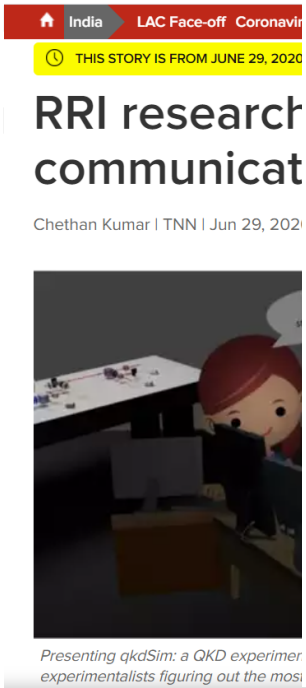


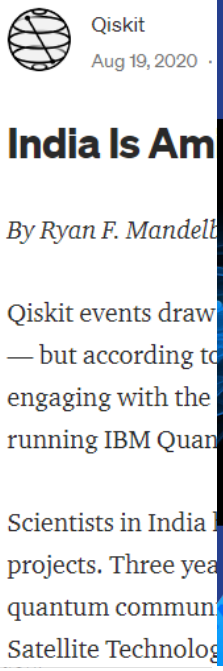
Optimization strategy	Implementation	key rate [Kbps]	QBER [%]	key symmetry
A: optimize SNR, maximize key rate, maintain QBER <= 4.8 %, and ensure key-symmetry 50:50	Experiment	51.0 ± 0.5	4.79 ± 0.01	50.2 : 49.8
	Simulation	52.8 ± 0.4	4.79 ± 0.01	50.1 : 49.9
B: equalize window size, maximize key rate, maintain QBER <= 4.8 %	Experiment	53.8 ± 0.4	4.79 ± 0.01	53.7 : 46.3
	Simulation	59.8 ± 0.3	4.79 ± 0.01	56.9 : 43.1

R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, Phys. Rev. App. **14**, 024036 (2020).

B92 implementational novelties & highlights

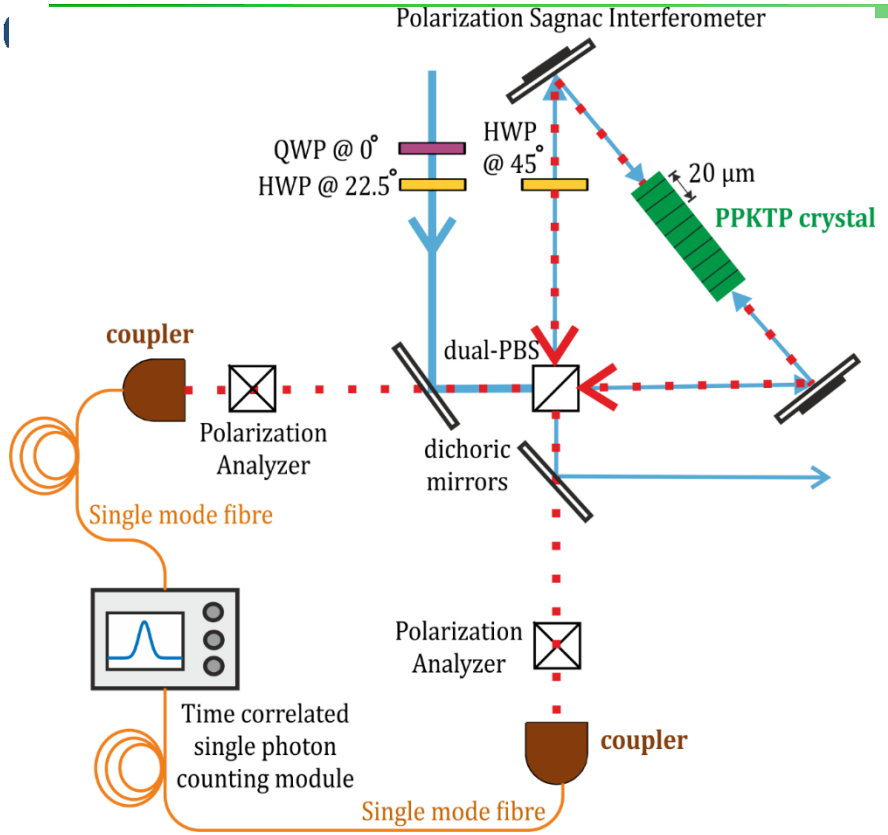
SPDC-based B92 implementation	Key rate [Kbps]	QBER [%]	Transmission channel length [m]
J. Wilson et al. (2016)	31.6	10.5	0.4
R. Chatterjee et al. (2020)	53.8	4.79	2





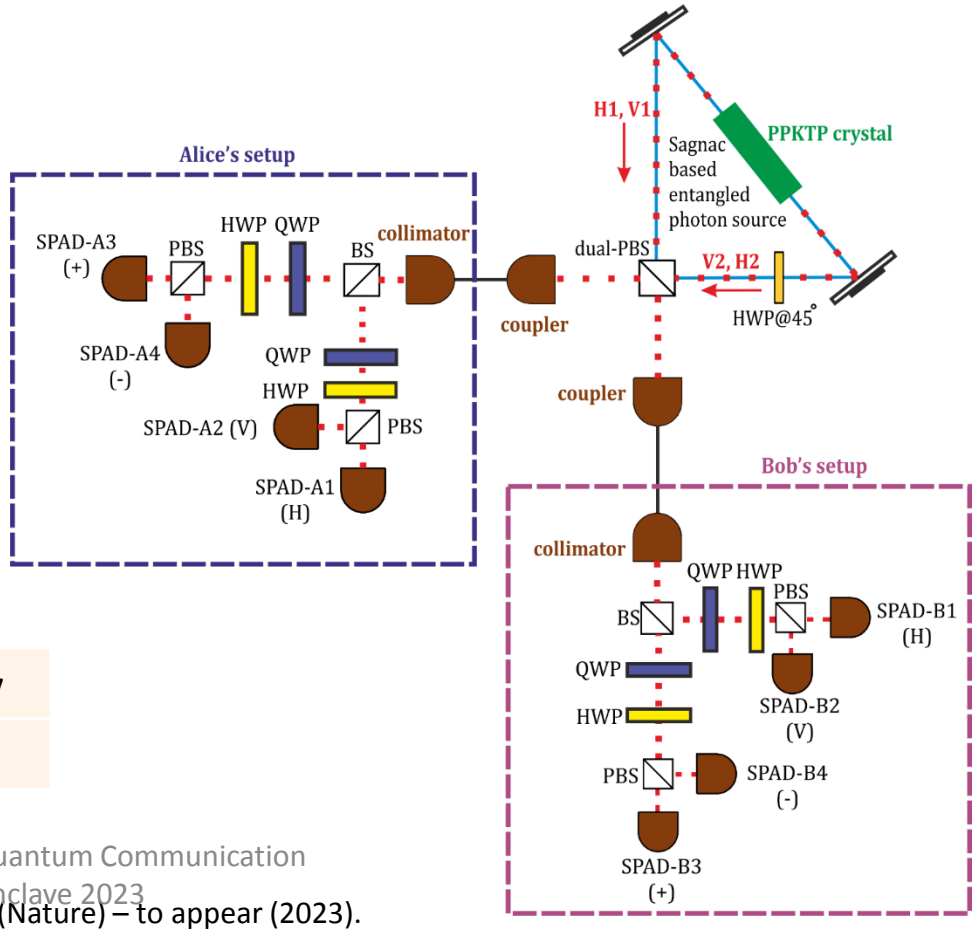
J. Wilson et al., Quant. Comm. & Quant. Imag. XIV, Vol. 9980, ISOP, 99800U (2016).
R. Chatterjee, K. Joarder, S. Chatterjee, B. C. Sanders, and U. Sinha, Phys. Rev. App. **14**, 024036 (2020).

In-lab BBM92 protocol implementation



Source performance metrics:

Fidelity	Concurrence	Purity
94%	92%	91%



Protocol performance metrics:

Key rate	QBER	Key symmetry
96.1 [Kbps]	10.3 [%]	50.04 : 49.96

S. Chatterjee, K. Goswami, R. Chatterjee, and U. Sinha, Comm. Phys. (Nature) – to appear (2023).

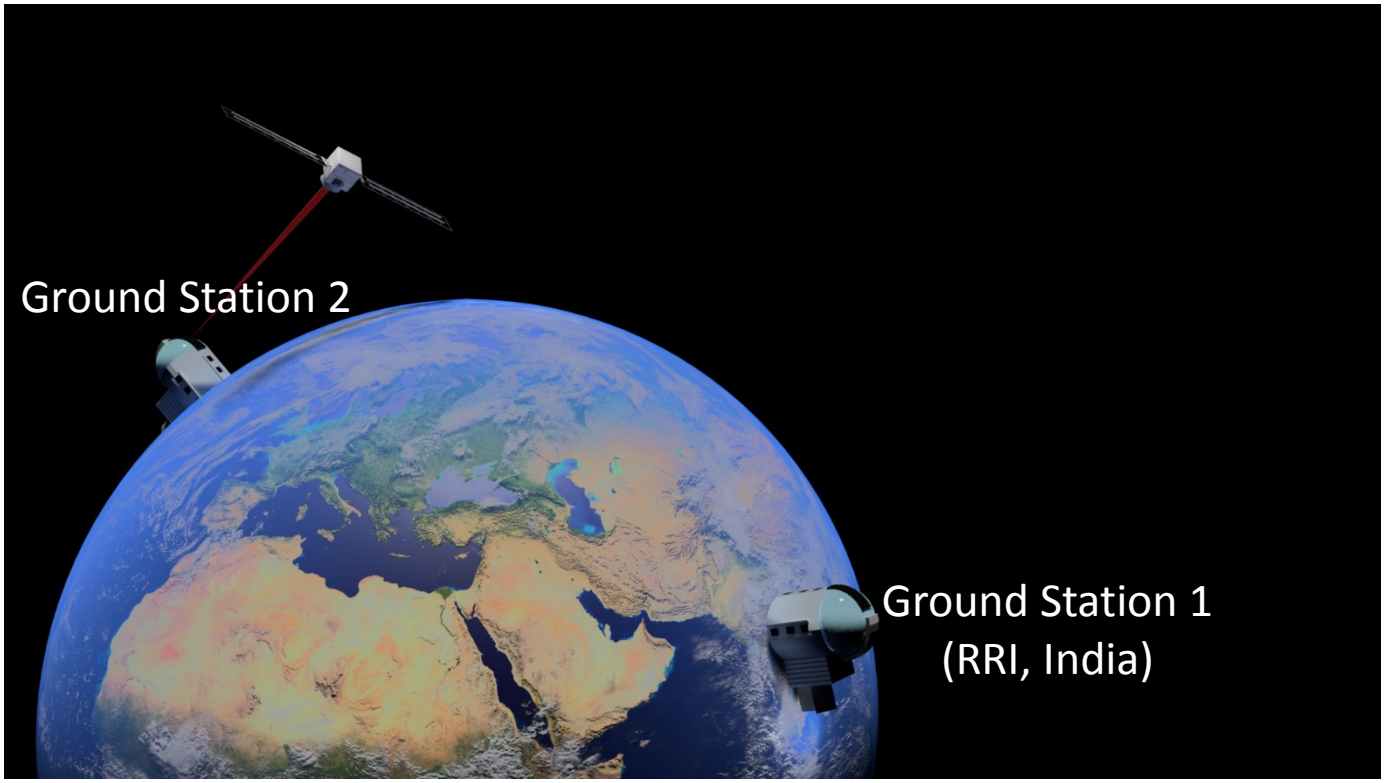
Performance analysis: in-lab implementations

- SPDC-based type-II heralded single-photon source (B92 protocol)
- Bright entangled photon source created out of collinear type-II SPDC process (BBM92 protocol)

Performance metric	In-lab B92 protocol	In-lab BBM92 protocol
Source type	Heralded single-photons	Entangled photons
Wavelength	810 nm	810 nm
Channel length	2 metres	2 metres (fibre-based)
Key rate	53.8 Kbps	96.1 Kbps
QBER	4.79 %	10.3 %
Timeline	Oct. 2019	Feb. 2022

R. Chatterjee, K. Joarder, S. Chatterjee, B. Sanders, and U. Sinha, Phys. Rev. Appl. **14**, 024036 (2021).
S. Chatterjee, K. Goswami, R. Chatterjee, and U. Sinha, Comm. Phys. (Nature) – to appear (2023).

A novel technique...



- **Conventionally, active feedback-based mechanism are employed for real-time polarization tracking.**
- **We employ a polarization bases compensation method that obviates the need for active polarization tracking in satellite-QKD implementations.**

- **Long-distance QKD implementation, in which polarization of light is commonly used degree of freedom, is becoming increasingly important.**
- **A significant challenge:**
  - **photon-polarization gets affected due to birefringence in fibre-based implementations.**
  - **Variation of reference frames due to satellite movement in long-haul demonstrations.**

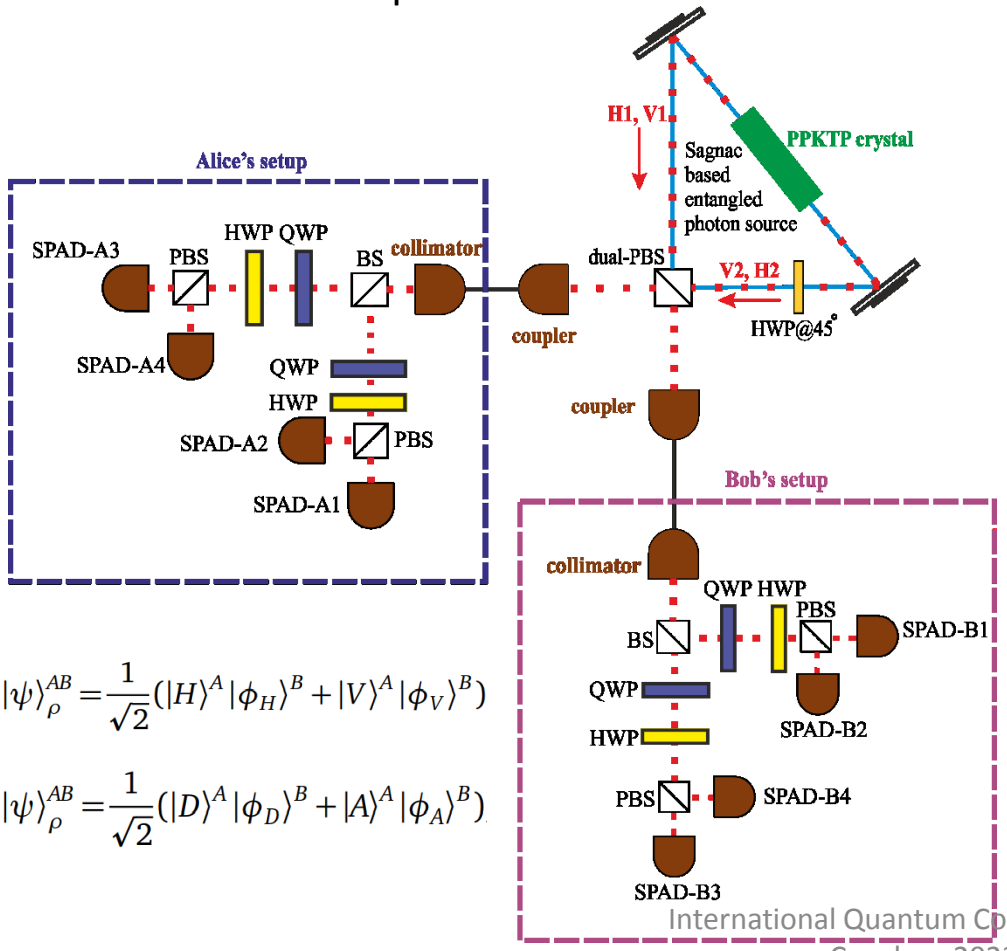
Our method's performance is independent of any local polarization rotation.

S. Chatterjee, K. Goswami, R. Chatterjee, and U. Sinha, Comm. Phys. (Nature) – to appear (2023).

Concept

Conventional (active) methods of polarization tracking:

- Stochastic algorithm to dynamically compensate for any polarization fluctuations.
- Robotized polarization correction based on an active control system



$$|\psi\rangle_{\rho}^{AB} = \frac{1}{\sqrt{2}}(|H\rangle^{A}|\phi_{H}\rangle^{B} + |V\rangle^{A}|\phi_{V}\rangle^{B})$$

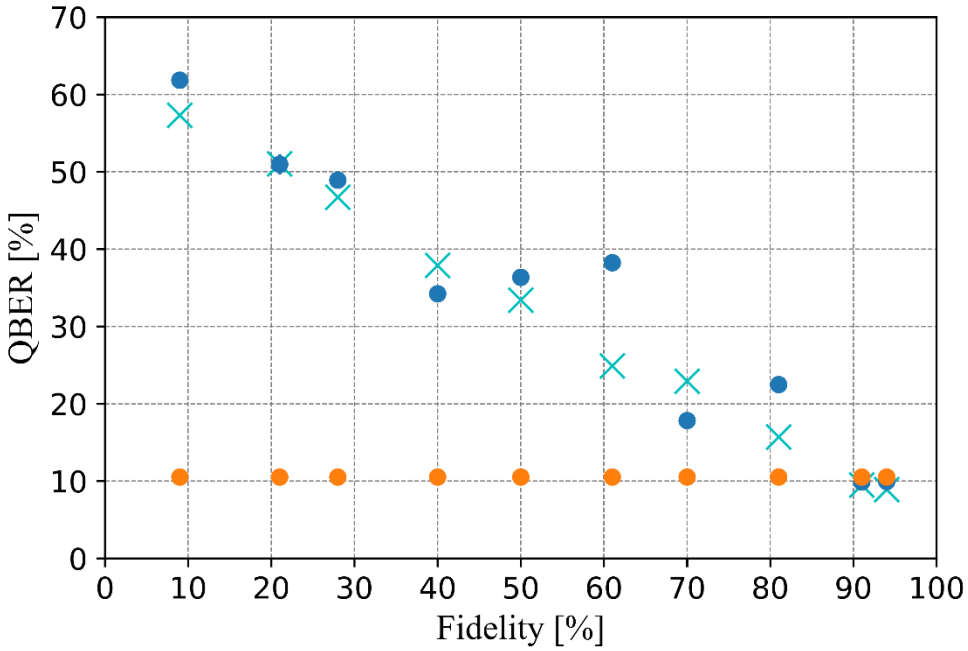
$$|\psi\rangle_{\rho}^{AB} = \frac{1}{\sqrt{2}}(|D\rangle^{A}|\phi_{D}\rangle^{B} + |A\rangle^{A}|\phi_{A}\rangle^{B})$$

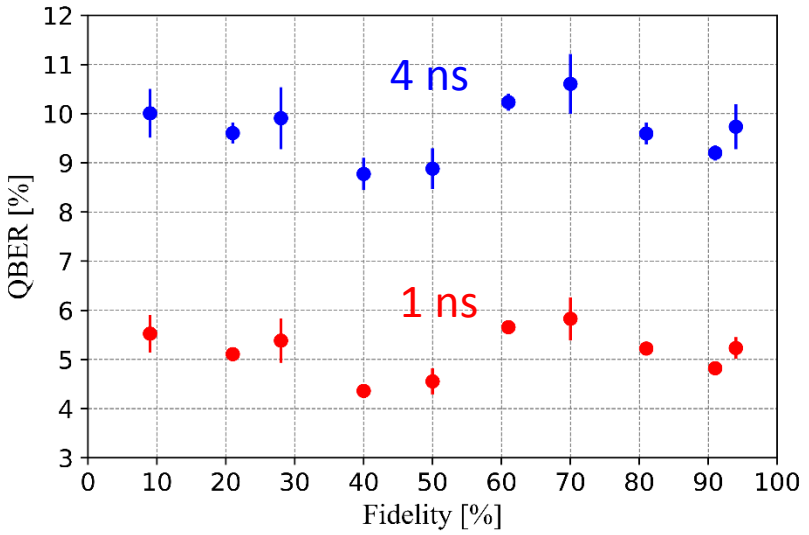
Our approach without an active feedback:

- Perform a quantum state tomography at the output and obtain the reconstructed the density matrix.
- Evaluate the optimal measurement bases choice that leads to a high (anti-) correlation in outcomes.
- Achieve the best trade-off between the key rate, QBER, and balanced key symmetry.

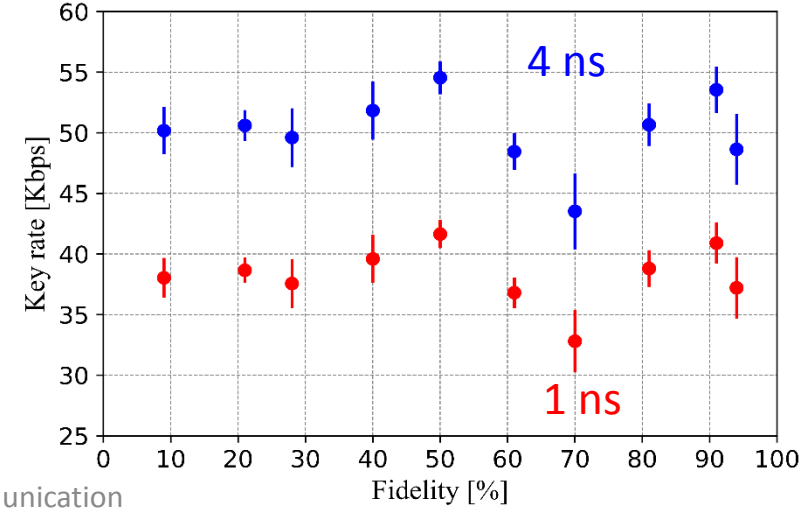
S. Chatterjee, K. Goswami, R. Chatterjee, and U. Sinha, Comm. Phys. (Nature) – to appear (2023).

Results





- Unoptimized QBERs (blue dots) measured in conventional measurement bases.
- Unoptimized QBERs (orange dots) measured in optimized measurement bases.
- Unoptimized QBERs (cyan crosses) measured in Pauli bases – chosen to provide best SNR.



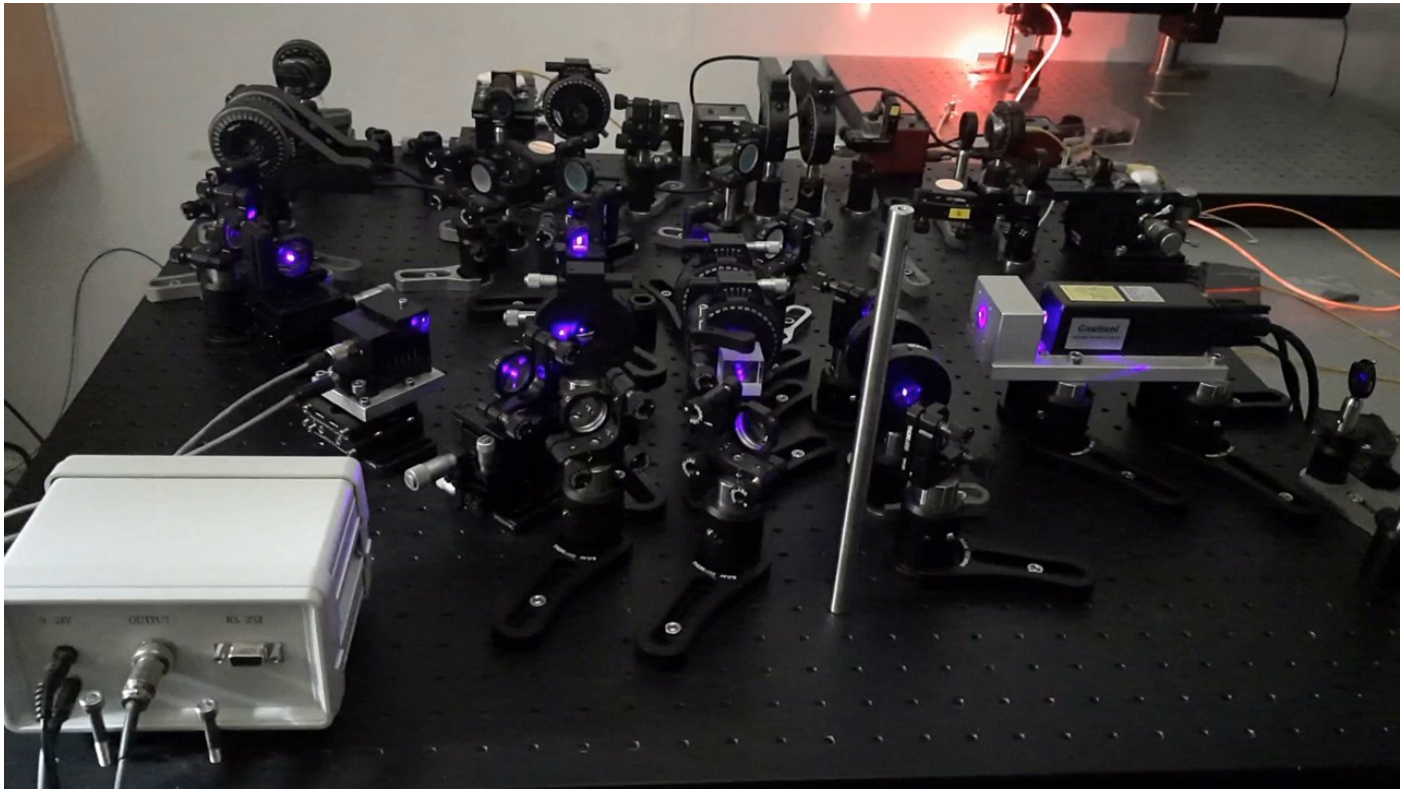
S. Chatterjee, K. Goswami, R. Chatterjee, and U. Sinha, Comm. Phys. (Nature) – to appear (2023).

Usefulness

- Our method addresses important practical challenges in QKD demonstrations: correcting the polarization of light which gets inevitably affected during long distance transmission.
- Active control systems having more parts than the raw system, are more prone to faults over our method, which can lead to instability of the (closed) stabilization loop.
- Our method is cost-effective as the conventional active feedback system-based polarization tracking techniques are resource intensive, resulting in additional maintenance cost.
- Active control systems often employ trial & error methods to nullify the output deviations which leads to the oscillatory response of the closed loop. This is not the case for our method.
- In summary, our method thus serves as an effective tool towards enabling efficient long range QKD implementations for both fibre-based and free-space approaches.

S. Chatterjee, K. Goswami, R. Chatterjee, and U. Sinha, Comm. Phys. (Nature) – to appear (2023).

Free space quantum communications through an atmospheric channel



erformance analysis: free-space implementations

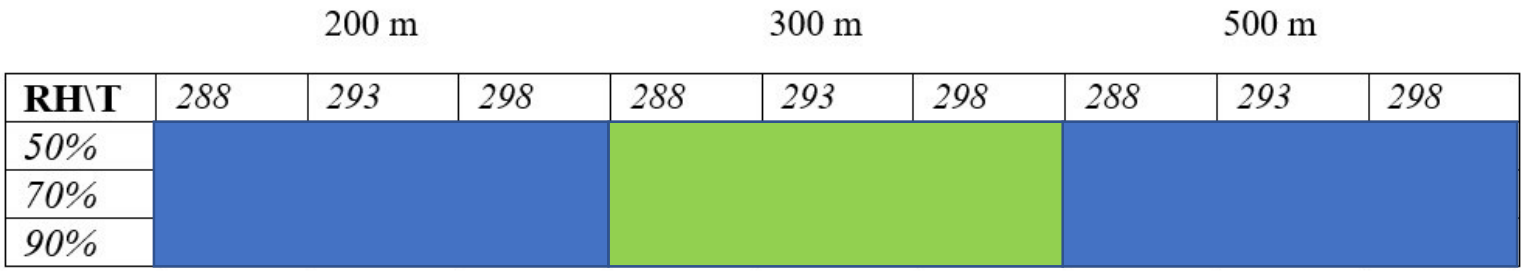
- Bright entangled photon source created out of collinear type-II SPDC process (BBM92 protocol)

Performance metric	Free-space BBM92 protocol	Free-space BBM92 protocol
Source type	Entangled photons	Entangled photons
Wavelength	810 nm	810 nm
Channel length	50 metres	50 metres
Key rate	1.6 Kbps	9.9 Kbps
QBER	11 %	8.9 %
Timeline	Feb. 2021	Nov. 2022

https://timesofindia.indiatimes.com/india/in-a-first-rri-transfers-quantum-encryption-key-safely-between-buildings/articleshow/81138499.cms

Simulating long distance results from real data

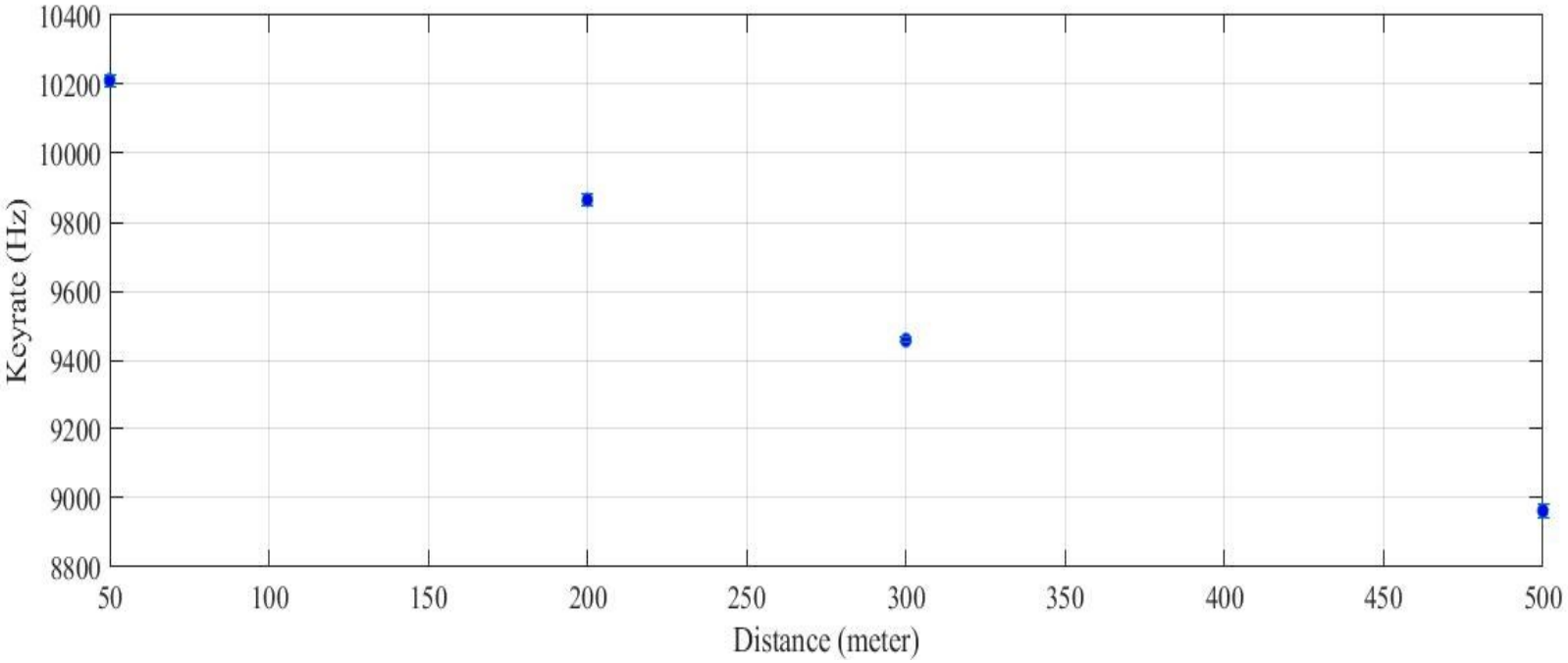
Losses for different humidity and temperature



≈ 0.97 ≈ 0.92 ≈ 0.87

Table for losses, in terms of attenuation factor, at different distances. The rows represent relative humidity and the columns represent temperature in Kelvin. We observe that the losses are almost independent of the relative humidity and temperature.

Distance vs Keyrate



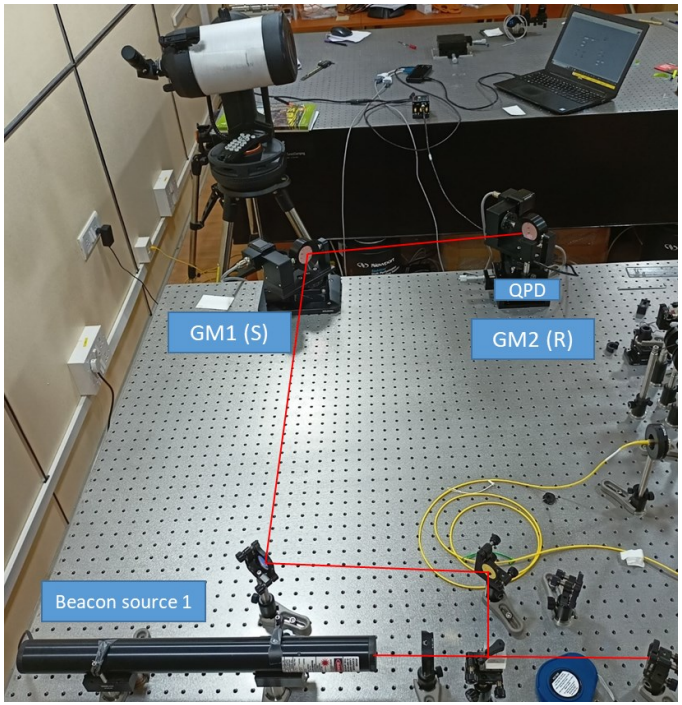
Experimentally, we put ND filters to induce attenuation in the photons. The resulting time stamps will generate diminished key rates proportional to the attenuation by ND filter.

QuIC

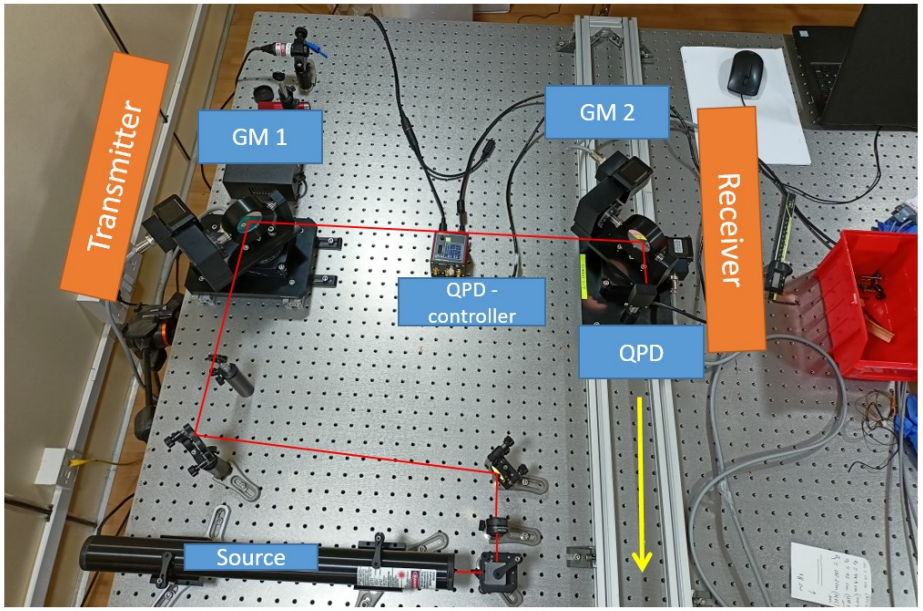
RRI

Experimental setup

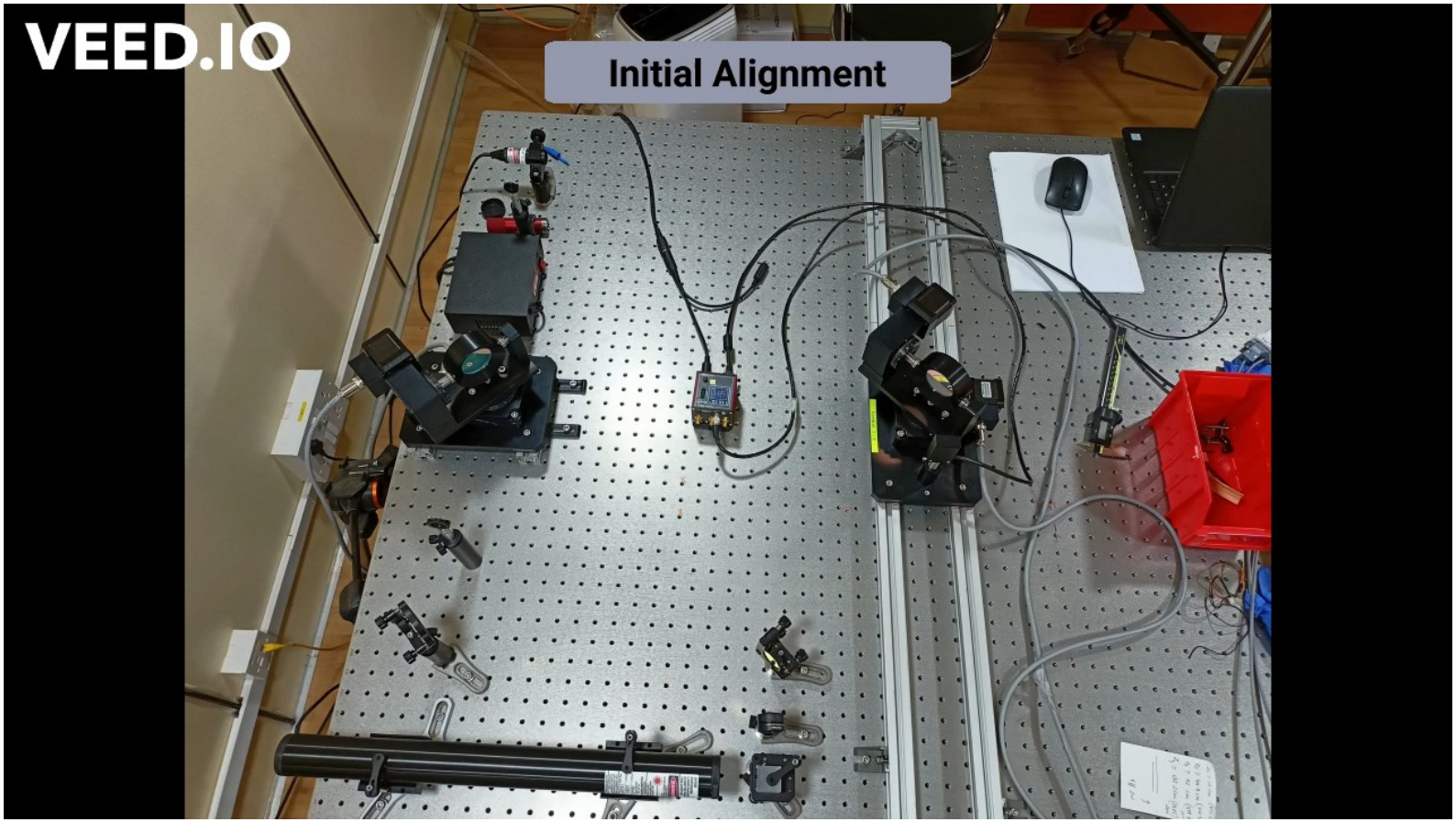
- **Using two gimbal mirror on a translational stage and single beacon in a closed loop setup**



- **Transmitter gimbal stationed and receiver gimbal moved on rail of length 1 meter.**

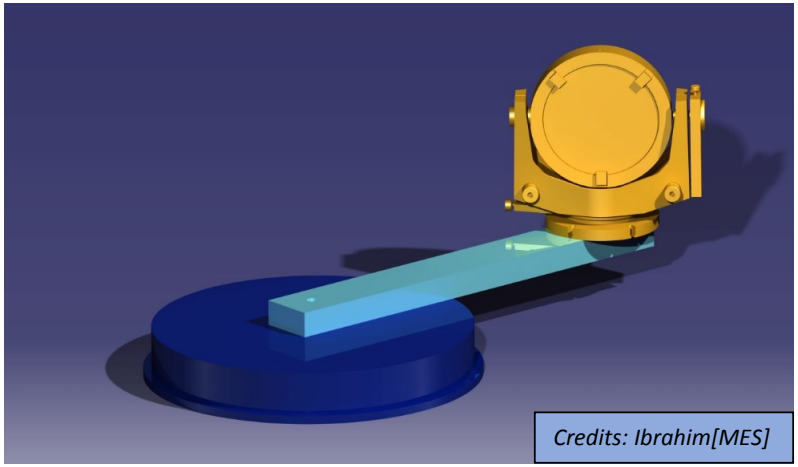


- GM 2 is mounted on a translational stage and displacement is introduced using the micrometer drive.
- Pointing and tracking is observed up to a displacement of 25mm

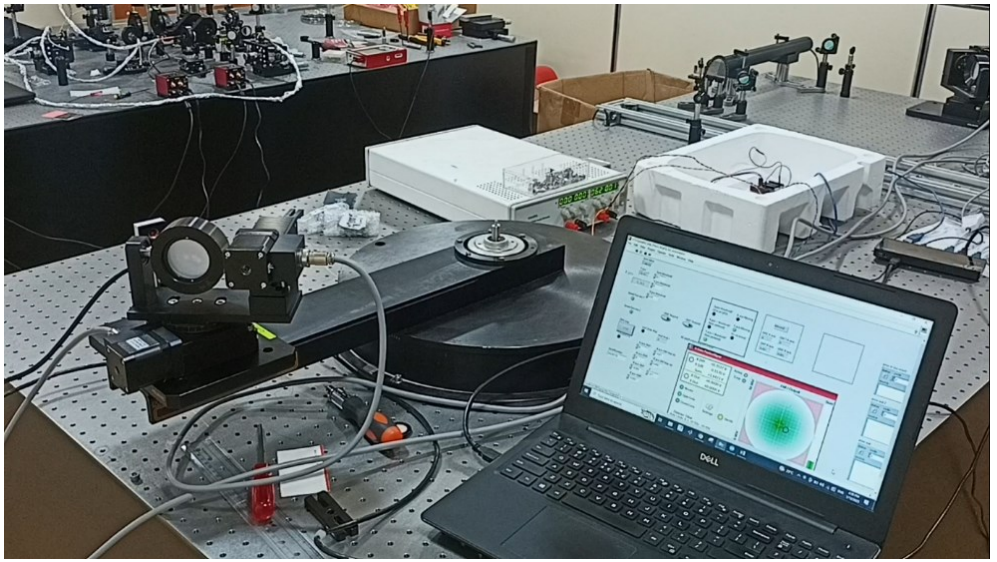

VEED.IO
Initial Alignment

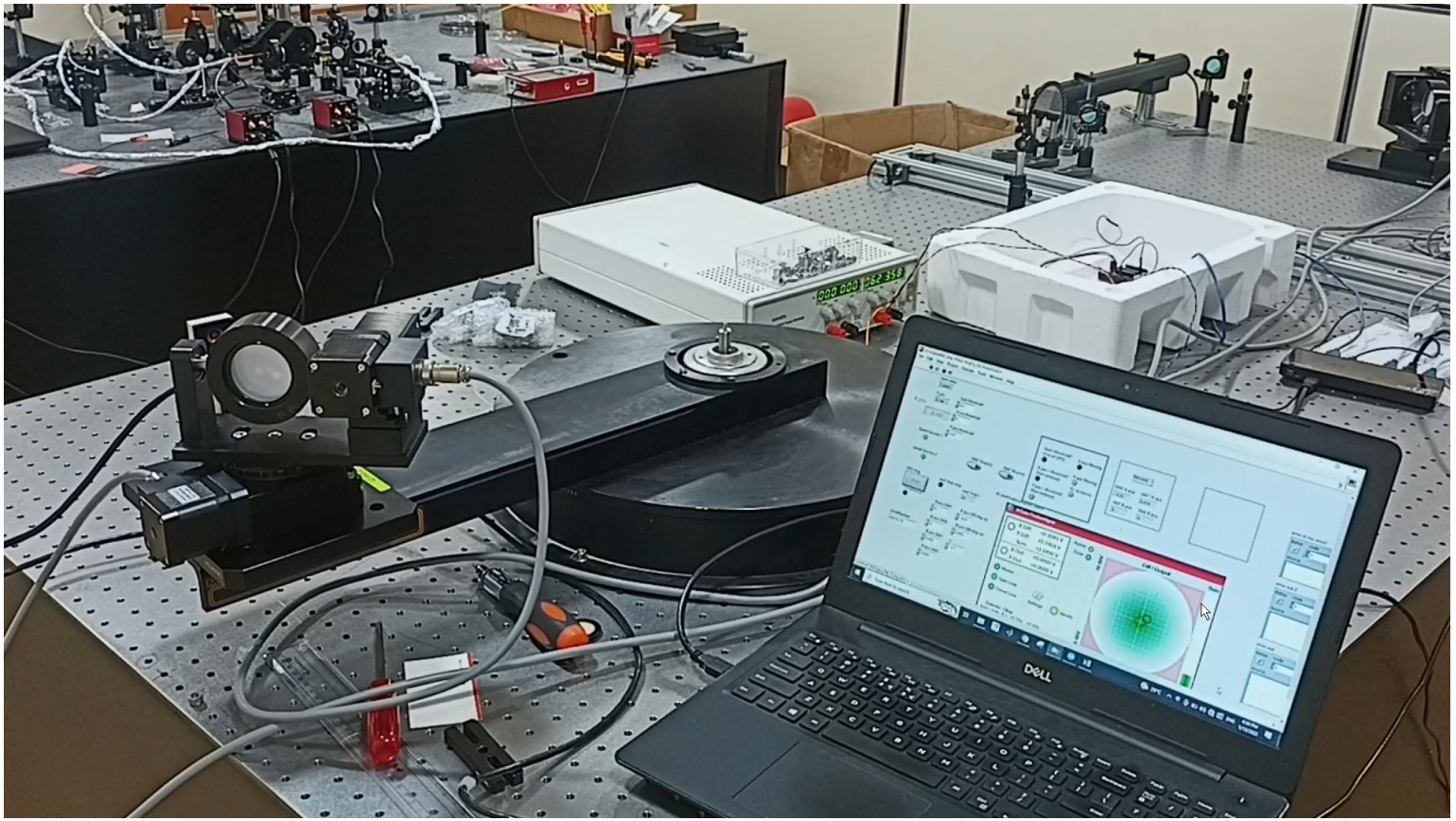
Feedback demonstration of moving receiver on circular motorized arm

Schematic



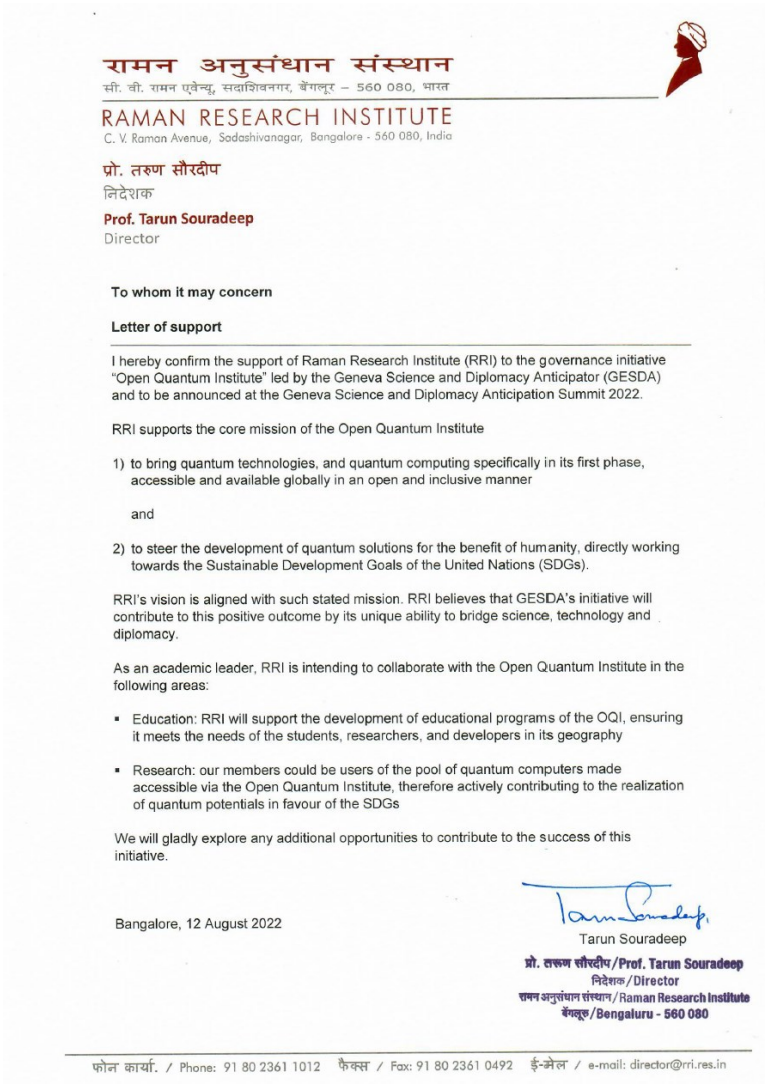
Experimental setup




DELL

More exciting news coming soon!

Stay tuned!



रामन अनुसंधान संस्थान
सी. वी. रामन एवेन्यू, सदाशिवनगर, बेंगलूर – 560 080, भारत
RAMAN RESEARCH INSTITUTE
C. V. Raman Avenue, Sadashivanagar, Bangalore - 560 080, India

प्रो. तरुण सौरदीप
निदेशक
Prof. Tarun Souradeep
Director

To whom it may concern

Letter of support

I hereby confirm the support of Raman Research Institute (RRI) to the governance initiative "Open Quantum Institute" led by the Geneva Science and Diplomacy Anticipator (GESDA) and to be announced at the Geneva Science and Diplomacy Anticipation Summit 2022.

RRI supports the core mission of the Open Quantum Institute

1) to bring quantum technologies, and quantum computing specifically in its first phase, accessible and available globally in an open and inclusive manner

   and

2) to steer the development of quantum solutions for the benefit of humanity, directly working towards the Sustainable Development Goals of the United Nations (SDGs).

RRI's vision is aligned with such stated mission. RRI believes that GESDA's initiative will contribute to this positive outcome by its unique ability to bridge science, technology and diplomacy.

As an academic leader, RRI is intending to collaborate with the Open Quantum Institute in the following areas:

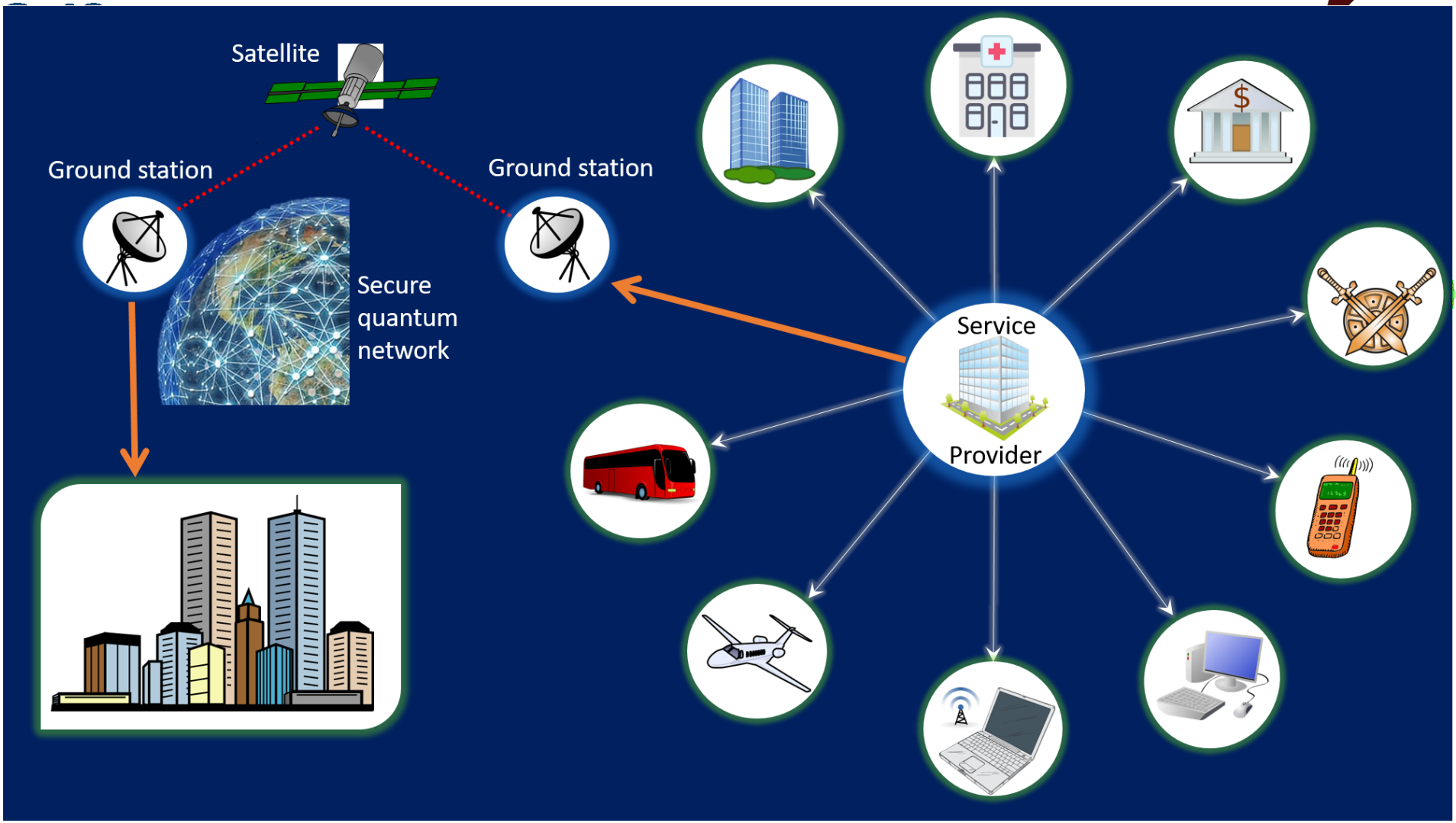
- Education: RRI will support the development of educational programs of the OQI, ensuring it meets the needs of the students, researchers, and developers in its geography
- Research: our members could be users of the pool of quantum computers made accessible via the Open Quantum Institute, therefore actively contributing to the realization of quantum potentials in favour of the SDGs

We will gladly explore any additional opportunities to contribute to the success of this initiative.

Bangalore, 12 August 2022

Tarun Souradeep
प्रो. तरुण सौरदीप / Prof. Tarun Souradeep
निदेशक / Director
रामन अनुसंधान संस्थान / Raman Research Institute
बेंगलूर / Bengaluru - 560 080

फोन कार्या. / Phone: 91 80 2361 1012 फैक्स / Fax: 91 80 2361 0492 ई-मेल / e-mail: director@rri.res.in


Satellite
Ground station
Ground station
Secure
quantum
network
Service
Provider