quantum technologies

turning a threat into an opportunity

radu ionicioiu

plan

I. quantum: the threat

II. quantum: the opportunity

III. quantum: a revolution in imaging

digitalisation: the next frontier

- digital Europe

- government cloud

cybersecurity is paramount

crypto: we use it every day

crypto: we use it every day

the problem

quantum computers will break internet security

- secure communications
- digital signatures
- mobile networks/5G
- financial transactions
  mobile banking, POS, e-commerce
- authentication
- critical infrastructure
- secure voting
- software updating
  cars, computers

$\Rightarrow$ *need to avoid the Q-Day (quantum apocalypse)* *how serious is the threat?*

Mosca equation

”store now, decrypt later” (SNDL) attack

Migration time
The number of years needed to properly and safely migrate the system to a quantum-safe solution

Shelf-life time
The number of years the information must be protected by the cyber-system

Threat timeline
The number of years before the relevant threat actors will be able to break the quantum-vulnerable systems

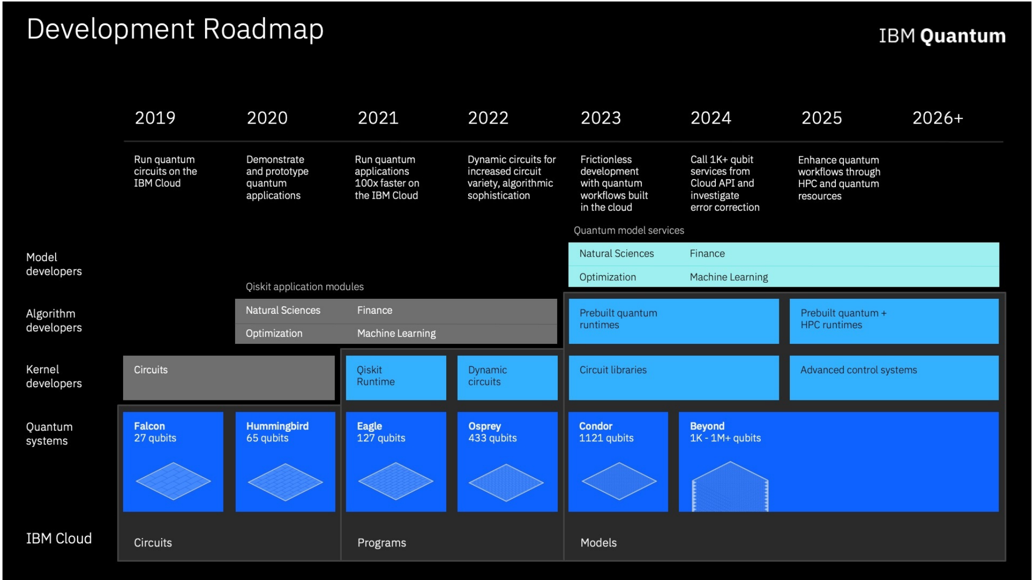
Danger zone

Source: Michele Mosca, University of Waterloo, Canada[13]

quantum computing

a $65 billion industry by 2030

IBM roadmap


Development Roadmap
IBM Quantum
2019
2020
2021
2022
2023
2024
2025
2026+
Run quantum circuits on the IBM Cloud
Demonstrate and prototype quantum applications
Run quantum applications 100x faster on the IBM Cloud
Dynamic circuits for increased circuit variety, algorithmic sophistication
Frictionless development with quantum workflows built in the cloud
Call 1K+ qubit services from Cloud API and investigate error correction
Enhance quantum workflows through HPC and quantum resources
Model developers
Quantum model services
Natural Sciences
Finance
Optimization
Machine Learning
Algorithm developers
Qiskit application modules
Natural Sciences
Finance
Optimization
Machine Learning
Prebuilt quantum runtimes
Prebuilt quantum + HPC runtimes
Kernel developers
Circuits
Qiskit Runtime
Dynamic circuits
Circuit libraries
Advanced control systems
Quantum systems
Falcon 27 qubits
Hummingbird 65 qubits
Eagle 127 qubits
Osprey 433 qubits
Condor 1121 qubits
Beyond 1K - 1M+ qubits
IBM Cloud
Circuits
Programs
Models

... any solutions?

Q-Day

two ways out

1. the classical way: post-quantum crypto (PQC)

   find quantum-resistant, public-key classical algorithms $\Rightarrow$ *NIST PQC*

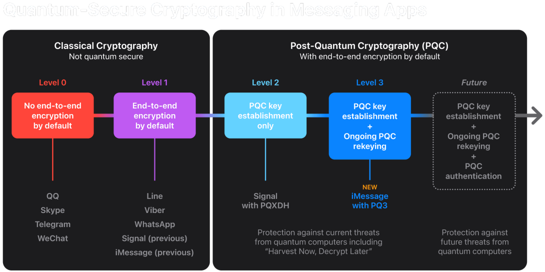
2. the quantum way: quantum key distribution (QKD)

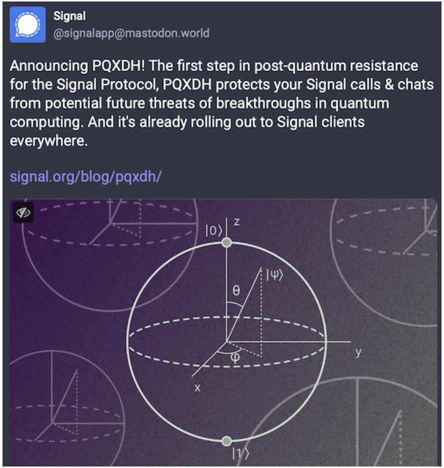
   use the power of quantum + symmetric crypto (AES, OTP)

the classical way: PQC

already deployed

- signal protocol: enhanced by PQC
- protects from future threats of quantum computers
- : iMessages with PQ3




Signal
@signalapp@mastodon.world

Announcing PQXDH! The first step in post-quantum resistance for the Signal Protocol, PQXDH protects your Signal calls & chats from potential future threats of breakthroughs in quantum computing. And it's already rolling out to Signal clients everywhere.

signal.org/blog/pqxdh/

the quantum way: QKD

1. use quantum resources to securely distribute keys
2. use keys in symmetric crypto (OTP, AES etc)

quantum solves 2 problems:

- true (quantum) randomness
- secure key distribution
  eavesdropper detected

the quantum way: QKD

why does it work?

- no-cloning theorem $\Rightarrow$ Eve cannot clone an unknown quantum state
- measurement changes a quantum state $\Rightarrow$ higher QBER, detectable

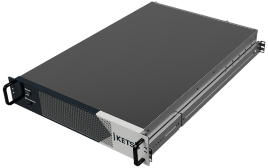
Eve will be detected !

classically impossible

QKD

commercial

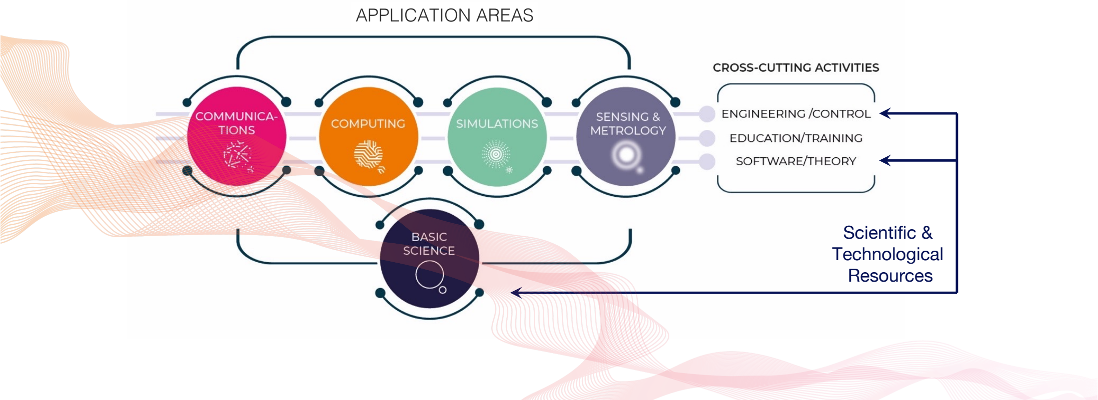
- providers: IDQ, ThinkQuantum, Toshiba, QTI, KeeQuant, Kets Quantum, QO Jena, LuxQuanta . . .
- € 150-300 k/pair



quantum: the opportunity

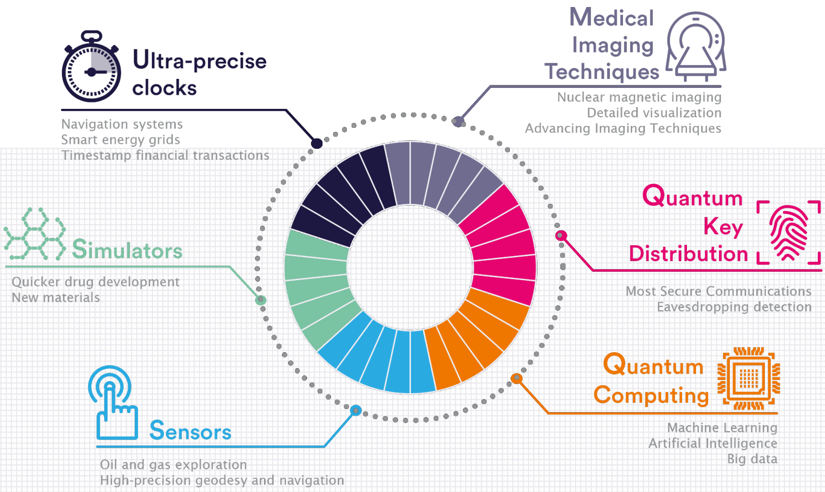
The Quantum Flagship

Structuring activities & efforts



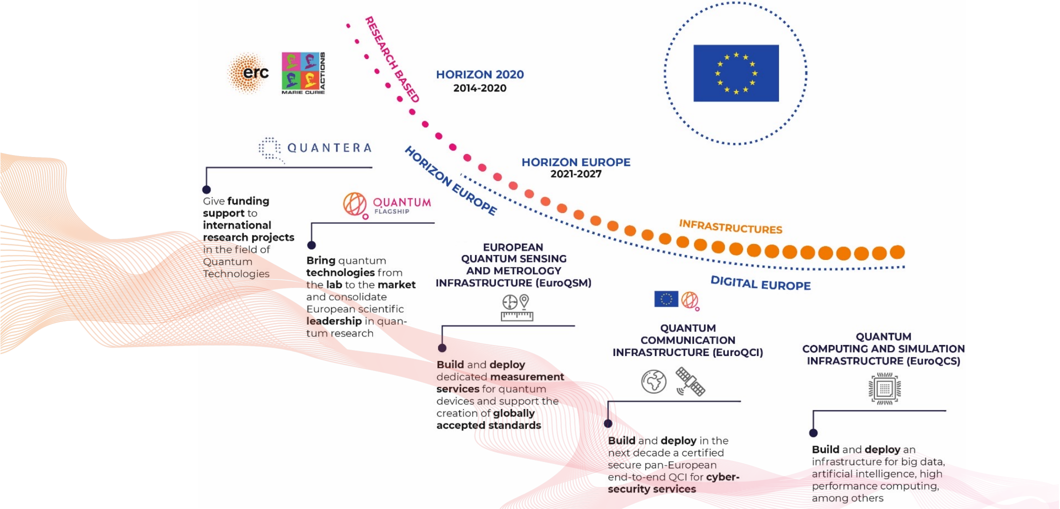
roqnet.ro

Quantum Technology Applications



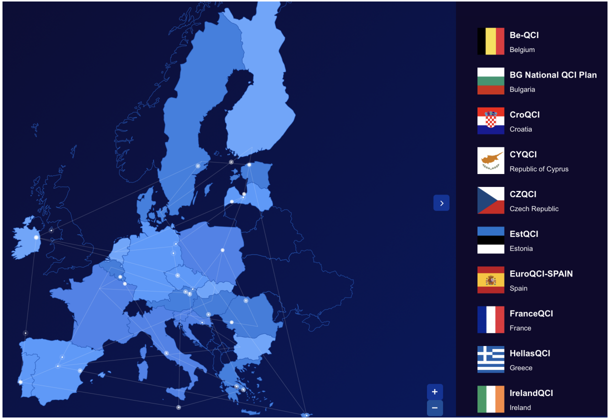
European Commission

From Flagship to Fleet



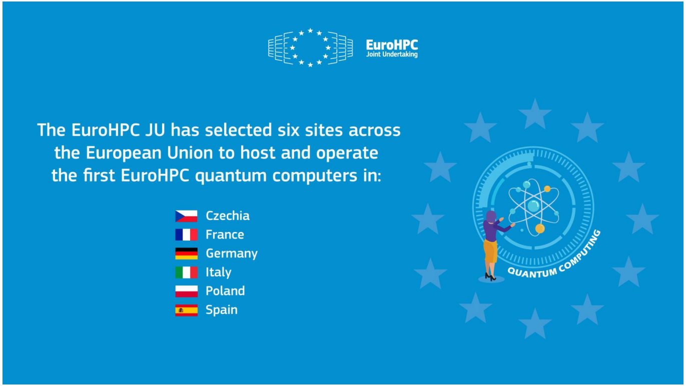
Petrus: building EuroQCI

- network of 27 national QCIs
- fiber + free-space links
- cross-border links



EuroQCS

- 6 sites across EU
- applications
  - molecular simulations: new medicines
  - new materials: batteries
  - traffic optimisation: maps
  - logistics: eMAG
  - scheduling: Bolt Glovo
- R&D, industry need quantum computers



quantum @RO

Romanian Quantum Network

2017 –

roqnet

www.roqnet.ro

Vision

quantum: the driving technology in 21st century

Mission

develop quantum technologies in Romania

Strategic objectives

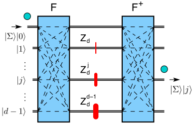
- *research*
- *education*
- *dissemination*

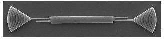
QUTECH-RO

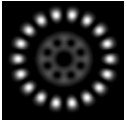
2018 – 2021

- €1.14 Mil
- 5 partners, 5 projects
- grant: UEFISCDI (PCCDI)
- https://roqnet.ro/qutech-ro/

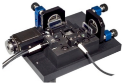
P1: Q-INFO	P2: Q-CHIP	P3: Q-VORTEX
IFIN-HH	INFLPR	IMT
quantum information quantum simulation quantum protocols	integrated quantum photonics 3D laser *fabrication*	optical vortices lithography

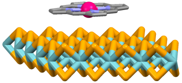






P4: Q-LAB	P5: Q-FERMI
UPB	ITIM-Cluj
Applied quantum optics Lab IBM-Q Lab quantum source	quantum computation with Majorana Fermions





play our strengths

use existing expertise/infrastructure

$\Downarrow$

theory, photonics/lasers, nanotechnologies

$\Downarrow$

bootstrap a national program in quantum technologies

quantum source

UPB + IFIN-HH

the first entangled-photons source build in RO

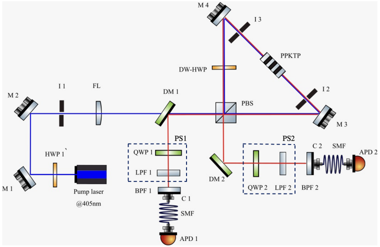
state-of-the-art

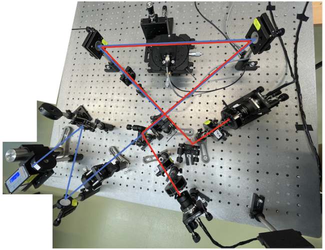
visibility: $\mathcal{V} = 98.9\%$

fidelity: $\mathcal{F} = 97\%$

$|S| = 2.684 \pm 0.03$

violates Bell-CHSH by $n_{\Delta} = 22$ standard deviations



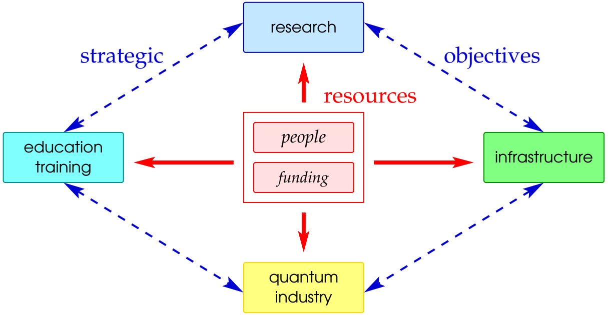


L.Dosan, A.Nazîru, M.Mihăilescu, R.I., Rom. Rep. Phys. **74**, 119 (2022)

QTSTRAT

RO national strategy in quantum communications

- **Q1. research**
  quantum research hubs
- **Q2. education and training**
  quantum specialists
- **Q3. infrastructure**
  intra-city q. networks, national quantum backbone, cross-border links
- **Q4. quantum industry**
  components, applications, services



https://qtstrat.granturi.ubbcluj.ro

a quantum revolution in imaging

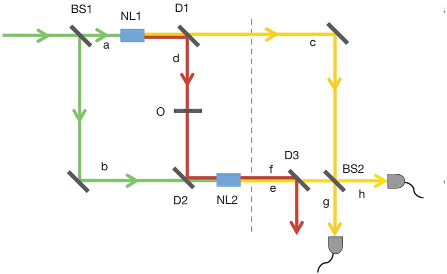
spooky imaging

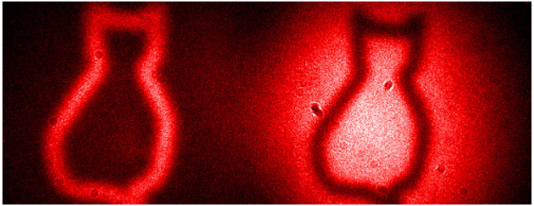
LETTER

doi:10.1038/nature13586

Quantum imaging with undetected photons

Gabriela Barreto Lemos[1,2], Victoria Borish[1,3], Garrett D. Cole[2,3], Sven Ramelow[1,3]†, Radek Lapkiewicz[1,3] & Anton Zeilinger[1,2,3]





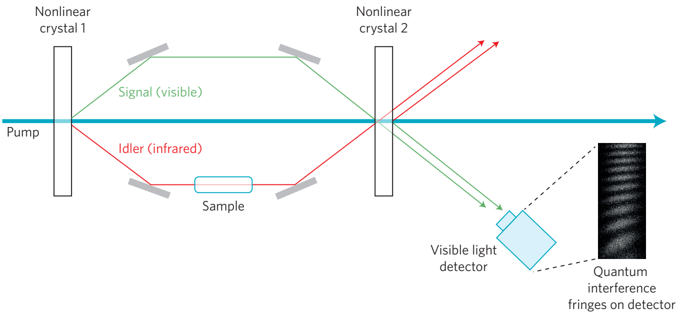
Nature **512**, 409 (2014)

spooky spectroscopy

LETTERS
PUBLISHED ONLINE: 4 JANUARY 2016 | DOI: 10.1038/NPHOTON.2015.252
nature photonics

Infrared spectroscopy with visible light

Dmitry A. Kalashnikov[1], Anna V. Paterova[1], Sergei P. Kulik[2] and Leonid A. Krivitsky[1]*



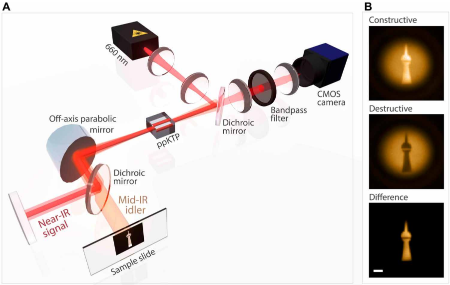
Nature Photonics **10**, 98 (2016); **10**, 77 (2016)

IR microscopy with visible light

OPTICS

Microscopy with undetected photons in the mid-infrared

Inna Kviatkovsky[1]*, Helen M. Chrzanowski[1], Ellen G. Avery[2,3,4,5,6,7], Hendrik Bartolomaeus[2,3,4,5,6], Sven Ramelow[1,8]

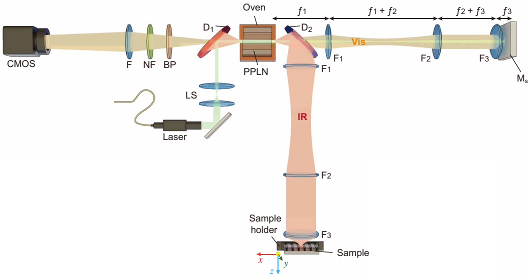


Sci.Adv. **6**, eabd0264 (2020)

OPTICS

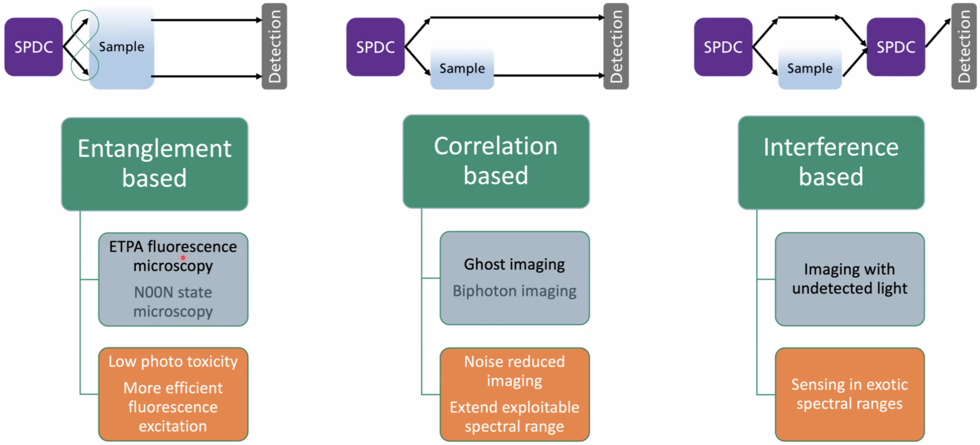
Hyperspectral infrared microscopy with visible light

Anna V. Paterova[1], Sivakumar M. Maniam[2,3], Hongzhi Yang[1], Gianluca Grenci[2,4]*, Leonid A. Krivitsky[1]*



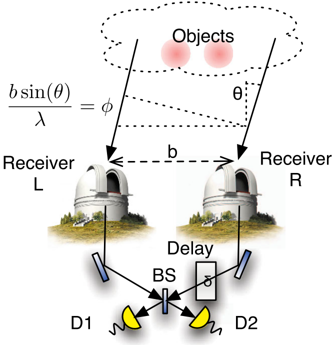
Sci.Adv. **6**, eabd0460 (2020)

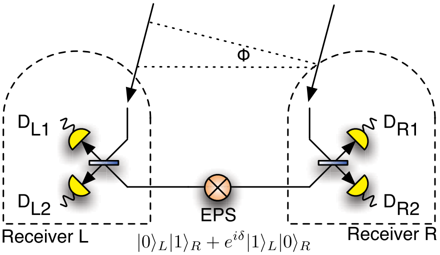
quantum imaging: 3 ways



Gilaberte Basset *et al.*, https://doi.org/10.1002/lpor.201900097

quantum-enhanced VLBI



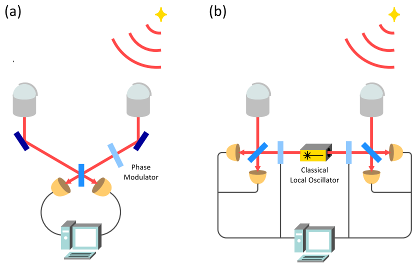


P. Riaud, Eur. Phys. J. D **66**, 8 (2012)

D. Gottesman *et al.*, PRL **109**, 070503 (2012)

quantum-enhanced VLBI

M. Tsang, PRL **107**, 270402 (2011)



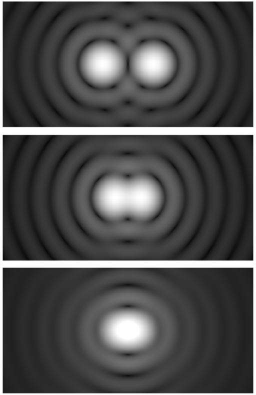
Fisher information, $\langle a^\dagger a \rangle = \langle b^\dagger b \rangle = \epsilon/2$, # measurements $M \sim T\Delta\nu$

direct (non-local)	local
$\|\|F^{(M)}\|\| \geqslant M\epsilon$	$\|\|F^{(M)}\|\| \leqslant M[\epsilon^2 + \mathcal{O}(\epsilon^3)]$

non-local measurements are better

beating the Rayleigh curse

- Rayleigh criterion: artefact of the imaging system
- info is contained in the phase, but imaging is done in intensity
- parameter estimation: Cramér-Rao bound



$$MSE(\theta) \geqslant \frac{1}{F(\theta)}$$

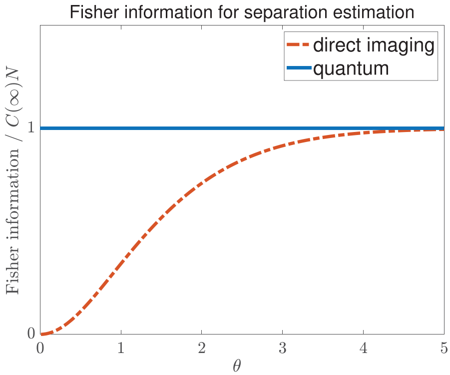
MSE: mean-square error

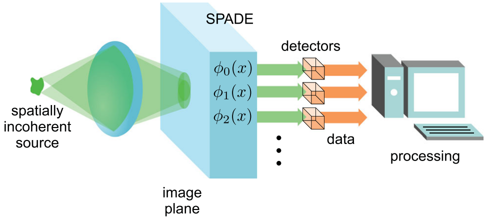
F: Fisher information

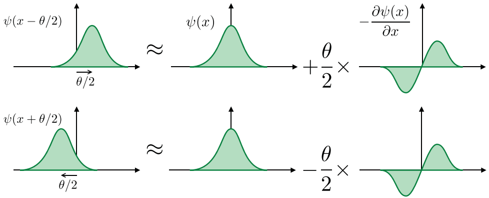
Tsang *et al.*, PRX **6**, 031033 (2016); Bojer *et al.*, New J. Phys. **24**, 043026 (2022)

Nair & Tsang, PRL **117**, 190801 (2016); Lupo & Pirandola, PRL **117**, 190802 (2016)

beating the Rayleigh curse

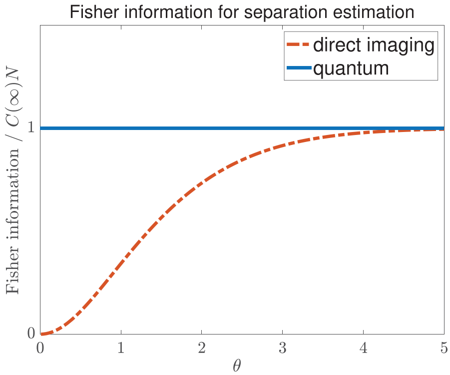


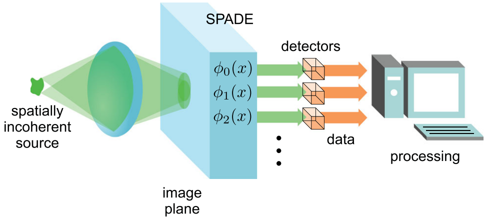


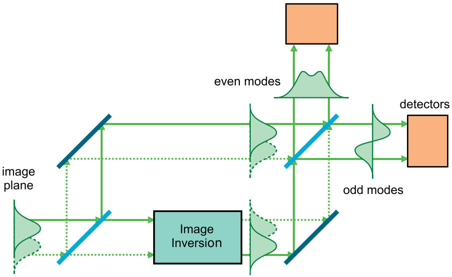


Tsang, *Resolving starlight: a quantum perspective*, Contemp. Phys. **60**, 279 (2020)

beating the Rayleigh curse







Tsang, *Resolving starlight: a quantum perspective*, Contemp. Phys. **60**, 279 (2020)

take home message

quantum technologies

not if, but when

- secure communications
- faster computers
- better imaging for astronomy (and not only)

any sufficiently advanced technology is indistinguishable from magic

Arthur Clarke

quantum mechanics is magic

Daniel Greenberger

Thank you!