The Scope and Prospects of Application of Quantum Computing in Pakistan

Jibran Rashid

August 28, 2021

IBA SMCS
School of Mathematics and Computer Science

QWORLD

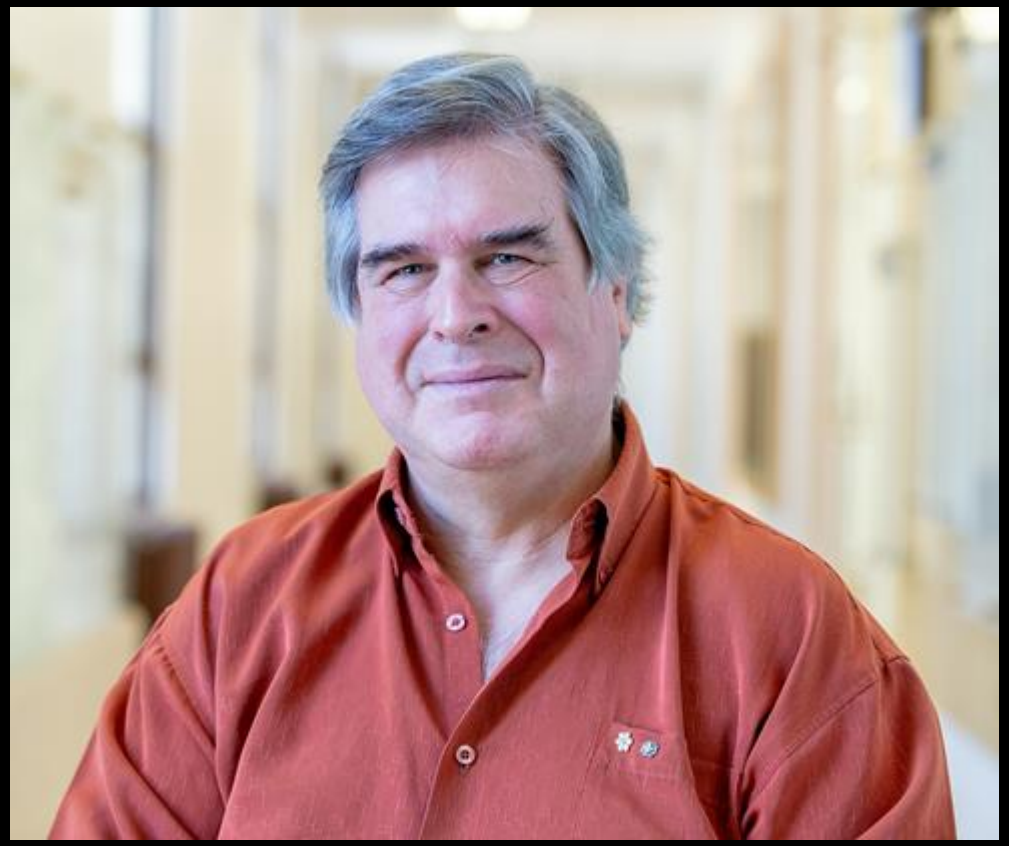
QPAKISTAN

Quantum Money

Stephen Wiesner (1942-2021)

Quantum Key Distribution – BB84

Charles Bennett



Gilles Brassard

Simulate Quantum Systems

Now I explicitly go to the question of how we can simulate with a computer

. . . ***the quantum mechanical effects*** . . .

But the full description of quantum mechanics for a large system with R particles is given by a function which we call the amplitude to find the particles at x1, x2, . . . xR, and therefore because it has too many variables,

it cannot be simulated with a normal computer.

Richard Feynman

Simulate Quantum Systems

Can you do it with a new kind of computer

— a quantum computer?

Now it turns out, as far as I can tell, that you can simulate this with a quantum system,

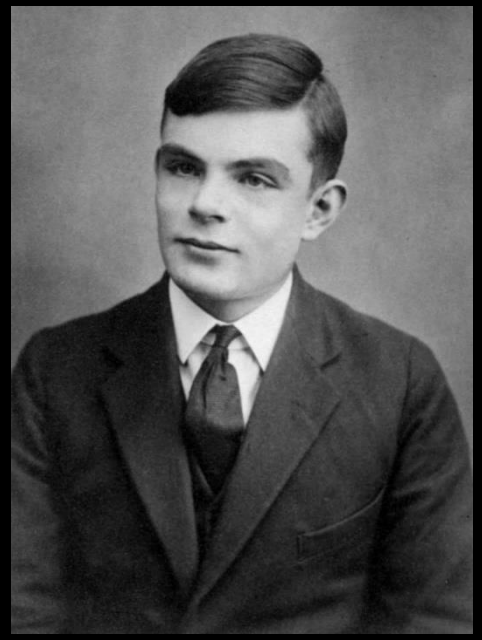
with quantum computer elements.

It's not a Turing machine, but a machine of a different kind.

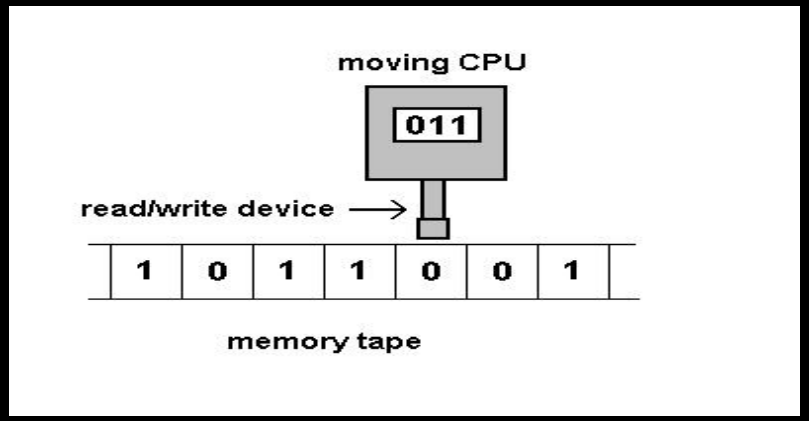
Richard Feynman

The Church-Turing Thesis

“Computable” = Turing-Computable



Alan Turing



Alonzo Church

Fundamental principle linking Computer Science to the real world!

Extended Church-Turing Thesis

Feasibly computable in the physical world
=
Efficiently computable by a Turing machine

Problem: Modeled as a set of binary strings, $L \subseteq \{0,1\}^*$.
Given an **input** $x \in \{0,1\}^*$, the task is to decide if $x \in L$

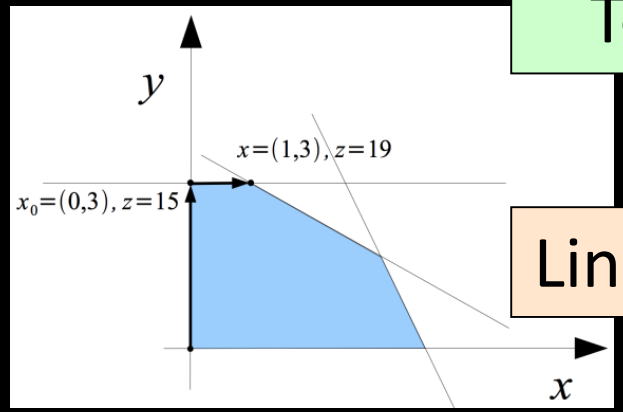
P

The class of problems for which there's an algorithm, for a deterministic digital computer, that always correctly decides if $x \in L$, after a number of steps upper-bounded by some polynomial in $|x|$ (the length of x)

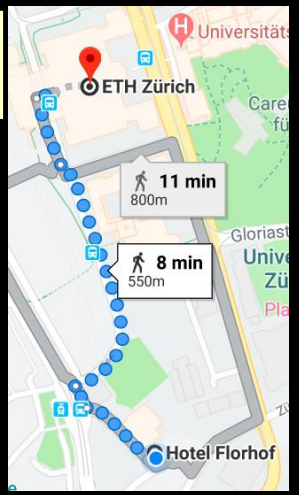
Examples:

Primality Testing

Connectivity



Linear Programming

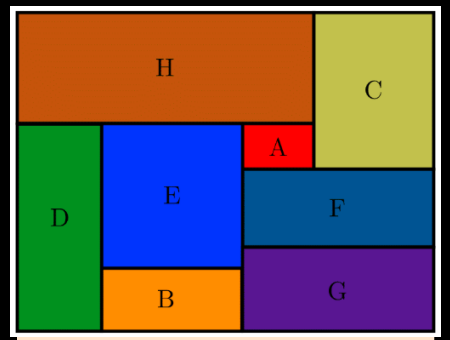


NP (Nondeterministic Polynomial-Time)

Informally, the class of problems for which there's a polynomial-time algorithm to **recognize** valid solutions (but the solutions might be exponentially hard to **find**)

Examples:

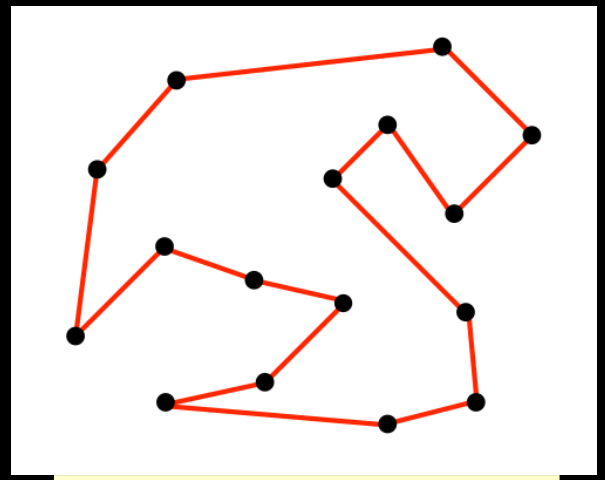
Factoring



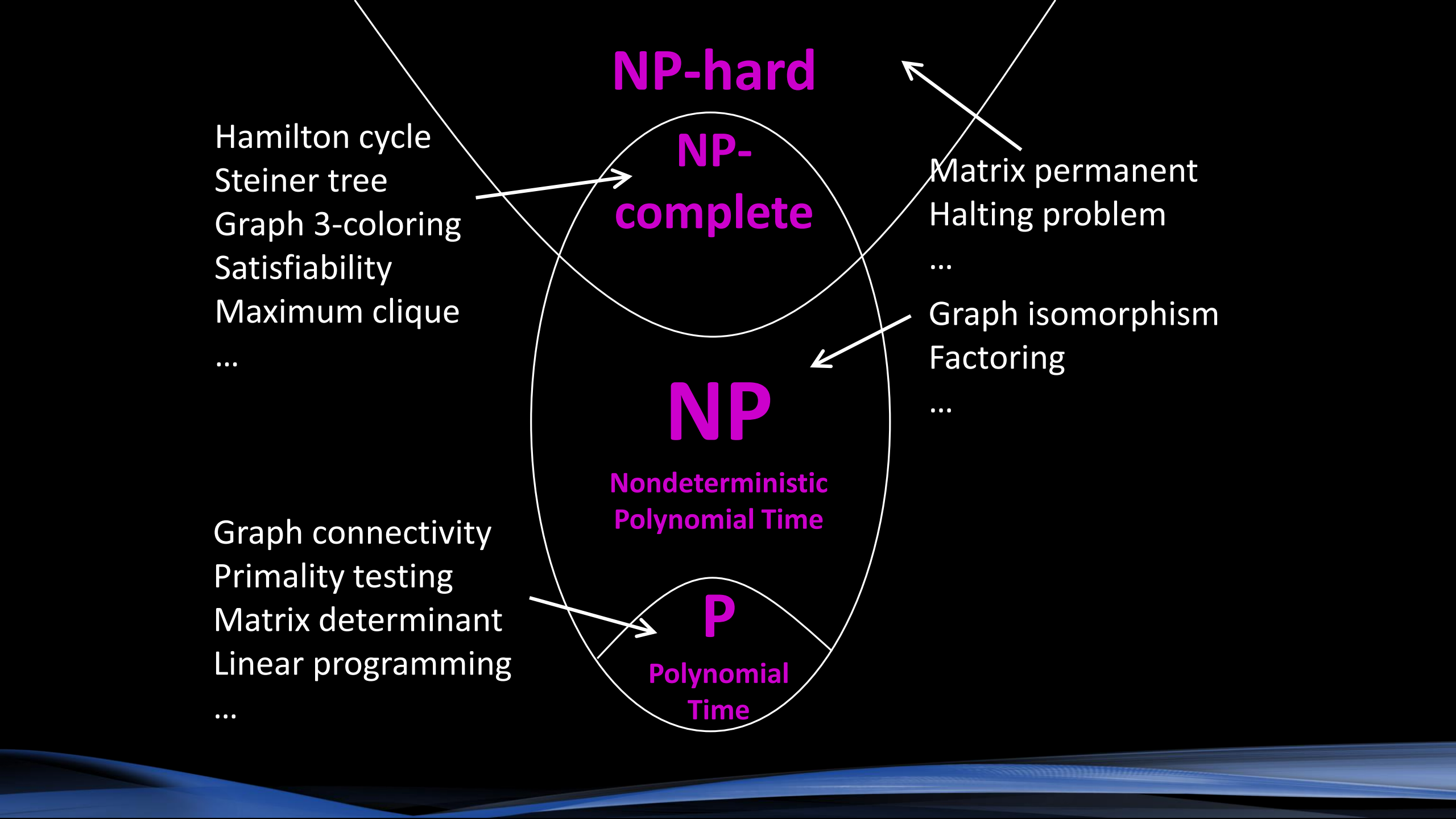
Bin Packing

Step	Hyp	Ref	Expression
1		efipi 21825	$\vdash (\exp(i \cdot \pi)) = -1$
2	1	oveq1i 6095	$\vdash ((\exp(i \cdot \pi)) + 1) = (-1 + 1)$
3		ax-1cn 9333	$\vdash 1 \in \mathbb{C}$
4		neg1cn 10418	$\vdash -1 \in \mathbb{C}$
5		1pneg1e0 10423	$\vdash (1 + -1) = 0$
6	3, 4, 5	addcomli 9554	$\vdash (-1 + 1) = 0$
7	2, 6	eqtri 2458	$\vdash ((\exp(i \cdot \pi)) + 1) = 0$

Theorem Proving



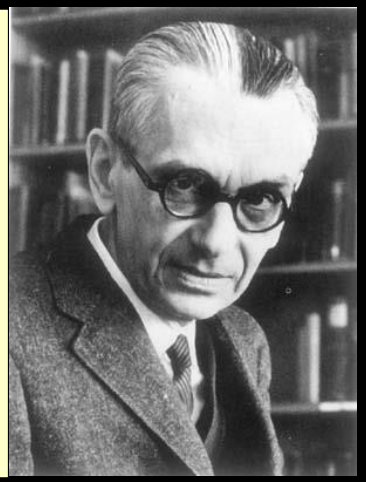
Traveling Salesperson


NP-hard
NP-complete
NP
Nondeterministic Polynomial Time
P
Polynomial Time
Hamilton cycle
Steiner tree
Graph 3-coloring
Satisfiability
Maximum clique
…
Matrix permanent
Halting problem
…
Graph isomorphism
Factoring
…
Graph connectivity
Primality testing
Matrix determinant
Linear programming
…

P=NP?

The (literally) $1,000,000 question

If there actually were a machine with [running time] ~Kn (or even only with ~Kn^2), this would have consequences of the greatest magnitude.
—Gödel to von Neumann, 1956



Integer Factorization is in BQP

Given an integer N, find its prime factors.

Consequently, we can break public-key cryptography systems such as RSA!

Peter Shor

Why Is Building A Quantum Computer So Hard?

Decoherence

Most re **rovides**

Scalable Quantum Computers
Are Not Possible

My Quantum Debate with Aram Harrow: Timeline, Non-technical Highlights, and Flashbacks I

Posted on March 16, 2013 by Gil Kalai

How the debate came about

(Email from Aram Harrow, June 4, 2011) Dear Gil Kalai, I am a quantum computing researcher, and was wondering about a few points in your paper...

(Aram's email was detailed and thoughtful and at the end he proposed to continue the discussion privately or as part of a public discussion.)

A Win-Win Situation

Scalable Quantum Computers Are Possible

Quantum Simulation

Quantum Chemistry

Factorization

Optimization and Machine Learning

...

A Win-Win Situation

Scalable Quantum Computers Are Not Possible

A Win-Win Situation

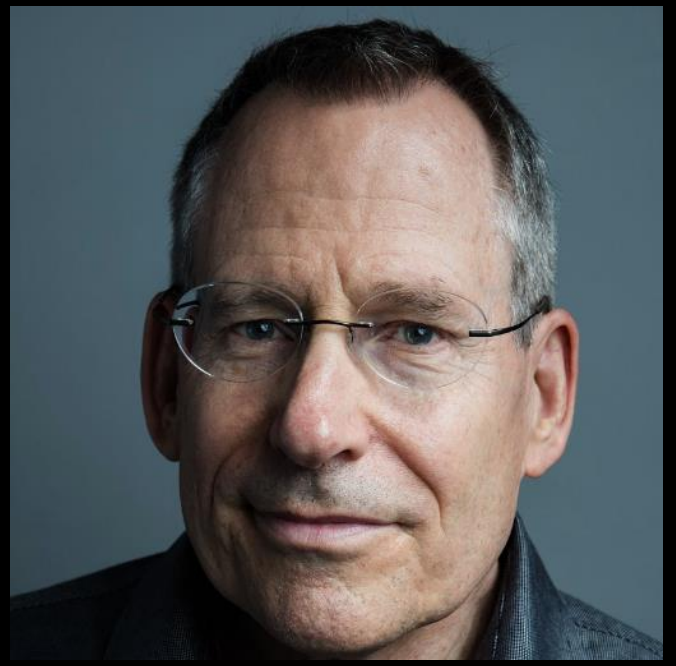
Scalable Quantum Computers Are Not Possible

New Physics!

NISQ Era

Noisy Intermediate-Scale Quantum: … size of quantum computers which will be available in the next few years, with a number of qubits ranging from **50** to a few hundred.

“Noisy” emphasizes that we’ll have imperfect control over those qubits; the noise will place serious limitations on what quantum devices can achieve in the near term.



John Preskill

Quantum Computational Supremacy

Use of a quantum computer to solve **some** well-defined problem much faster than **any** available classical computer running **any** known algorithm

Quantum technologies + Add to myFT

Google claims to have reached quantum supremacy

MOTHERBOARD
TECH BY VICE

OK, WTF Is Google's 'Quantum Supremacy'?

Google may have just ushered in an era of 'quantum supremacy'

'The first computation that can only be performed on a quantum processor'

By Jon Porter | @JonPorty | Sep 23, 2019, 7:06am EDT

SHARE

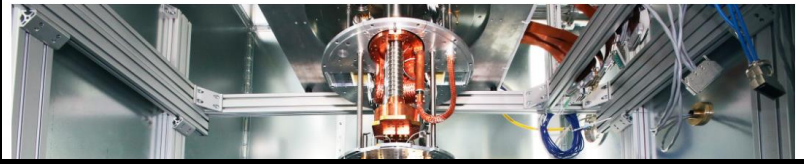
Google has reached quantum supremacy – here's what it should do next

TECHNOLOGY | ANALYSIS 26 September 2019

By Chelsea Whyte

Google's 'Quantum Supremacy' Isn't the End of Encryption

Google said its quantum computer outperformed conventional models. But it will s anything practical.



NEWS QUANTUM PHYSICS

Rumors hint that Google has accomplished quantum supremacy

Reports suggest a quantum computer has surpassed standard computers on a specific type of calculation

IBM's Response

Using Summit, the largest supercomputer currently on earth—which fills 2 basketball courts and has 250 petabytes of hard disk—it should be possible to simulate Google's 3-minute calculation in ~2.5 days, rather than the 10,000 years Google estimated

SCIENTIFIC AMERICAN®

QUANTUM COMPUTING

Light-Based Quantum Computer Exceeds Fastest Classical Supercomputers

The setup of lasers and mirrors effectively “solved” a problem far too complicated for even the largest traditional computer system

SCIENTIFIC AMERICAN®

QUANTUM COMPUTING

Light-Based Quantum Computer Exceeds Fastest Classical Supercomputers

The setup c

Quantum supremacy, now with BosonSampling

for even the

A group led by Jianwei Pan and Chao-Yang Lu, based mainly at USTC in Hefei, China, announced today that it achieved BosonSampling with 40-70 detected photons—up to and beyond the limit where a classical supercomputer could feasibly verify the results. (Technically, they achieved a variant called Gaussian

This manifesto is a call to launch an ambitious European initiative in quantum technologies, needed to ensure Europe's leading role in a technological revolution now under way.

President Trump has signed a $1.2 billion law to boost US quantum tech

The new National Quantum Initiative Act will give America a national master plan for advancing quantum technologies.

This manifesto is a call to launch an ambitious European initiative in quantum technologies, needed to ensure Europe's leading role in a technological revolution now under way.

Quantum Manifesto

A New Era of Technology

May 2016

SCIENTIFIC AMERICAN®

QUANTUM COMPUTING

China Is Pulling Ahead in Global Quantum Race, New Studies Suggest

The competition between the U.S. and China over development of quantum technology has implications for both the future of science and the two countries' political relations

now under way.

Quantum Manifesto

A New Era of Technology

May 2016

China

Quan

Global

udies

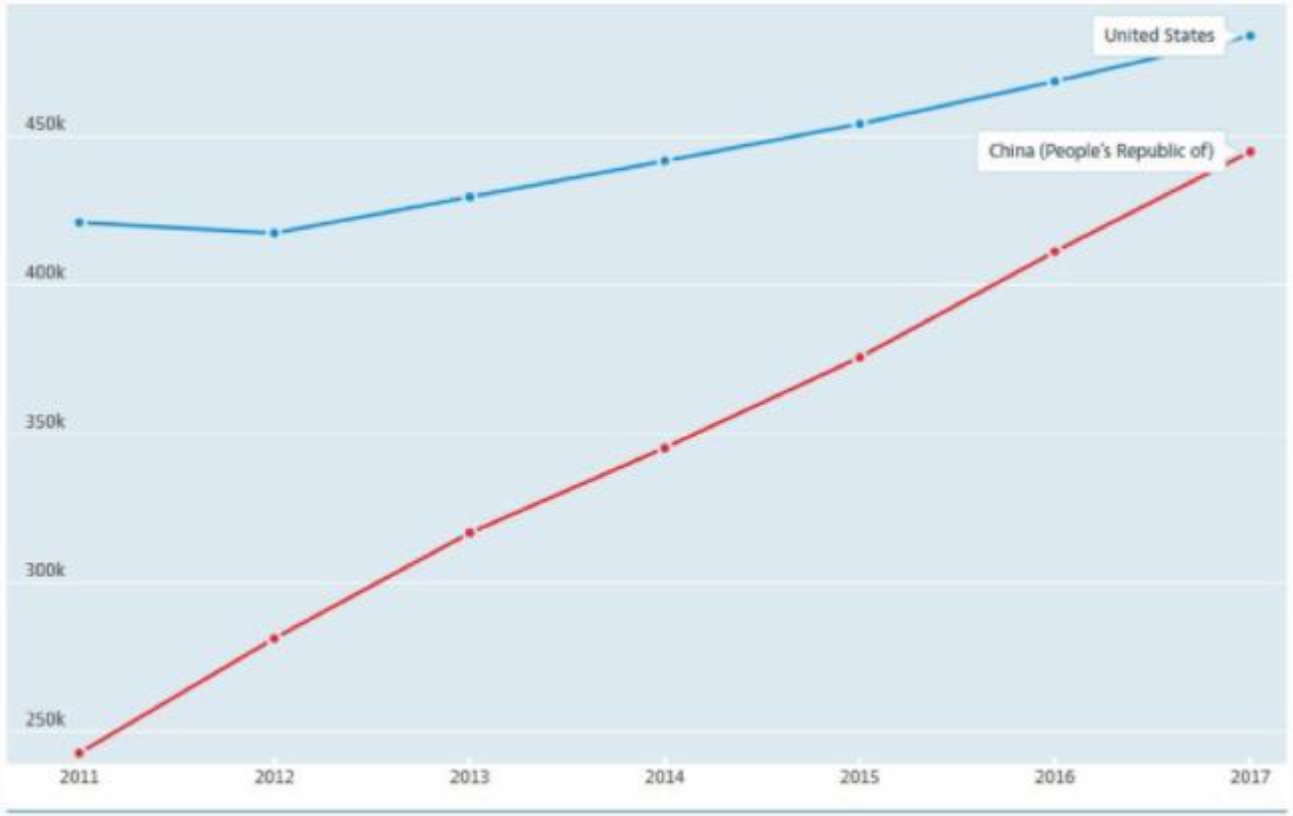
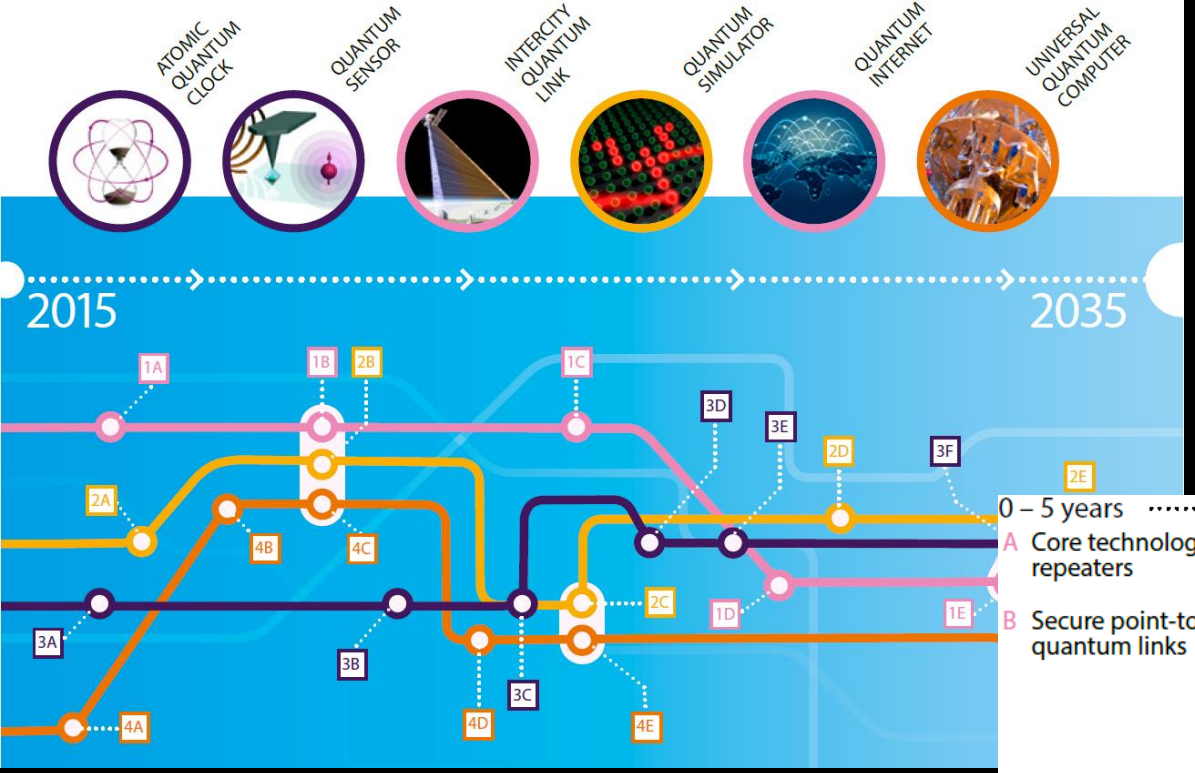


Figure 1: USA vs. China total annual R&D expenditure (millions of dollars) OECD SCIENCE, TECHNOLOGY & R&D STATISTICS

The competition bet
implications for

tum technology has
olitical relations
now under way.



0 – 5 years

- A Core technology of quantum repeaters
- B Secure point-to-point quantum links
- A Simulator of motion of electrons in materials
- B New algorithms for quantum simulators and networks
- A Quantum sensors for niche applications (incl. gravity and magnetic sensors for health care, geosurvey and security)
- B More precise atomic clocks for synchronisation of future smart networks, incl. energy grids
- A Operation of a logical qubit protected by error correction or topologically
- B New algorithms for quantum computers
- C Small quantum processor executing technologically relevant algorithms

5 – 10 years

- C Quantum networks between distant cities
- D Quantum credit cards
- C Development and design of new complex materials
- D Versatile simulator of quantum magnetism and electricity
- C Quantum sensors for larger volume applications including automotive, construction
- D Handheld quantum navigation devices
- D Solving chemistry and materials science problems with special purpose quantum computer > 100 physical qubit

> 10 years

- E Quantum repeaters with cryptography and eavesdropping detection
- F Secure Europe-wide internet merging quantum and classical communication
- E Simulators of quantum dynamics and chemical reaction mechanisms to support drug design
- E Gravity imaging devices based on gravity sensors
- F Integrate quantum sensors with consumer applications including mobile devices
- E Integration of quantum circuit and cryogenic classical control hardware
- F General purpose quantum computers exceed computational power of classical computers

Potential Applications of Quantum Computers

- **Probably**
  - Cryptography
  - Optimization
  - Simulation
  - **Science**
  - **Philosophy**

Potential Applications of Quantum Computers

- **Probably**
  - Cryptography
  - Optimization
  - Simulation
  - Science
  - Philosophy
- **Maybe**
  - Machine Learning
    - Dequantization

Potential Applications of Quantum Computers

- **Probably**
  - Cryptography
  - Optimization
  - Simulation
  - Science
  - Philosophy
- **Maybe**
  - Machine Learning
    - Dequantization
- **Not Really:**
  - Efficiently solving NP-Complete problems

Potential Applications of Quantum Computers

- **Probably**
  - Cryptography
  - Optimization
  - Simulation
  - Science
  - Philosophy
- **Maybe**
  - Machine Learning
    - Dequantization
  - *Contribute towards ending world hunger, ending climate change, finding aliens…*
- **Not Really:**
  - Efficiently solving NP-Complete problems

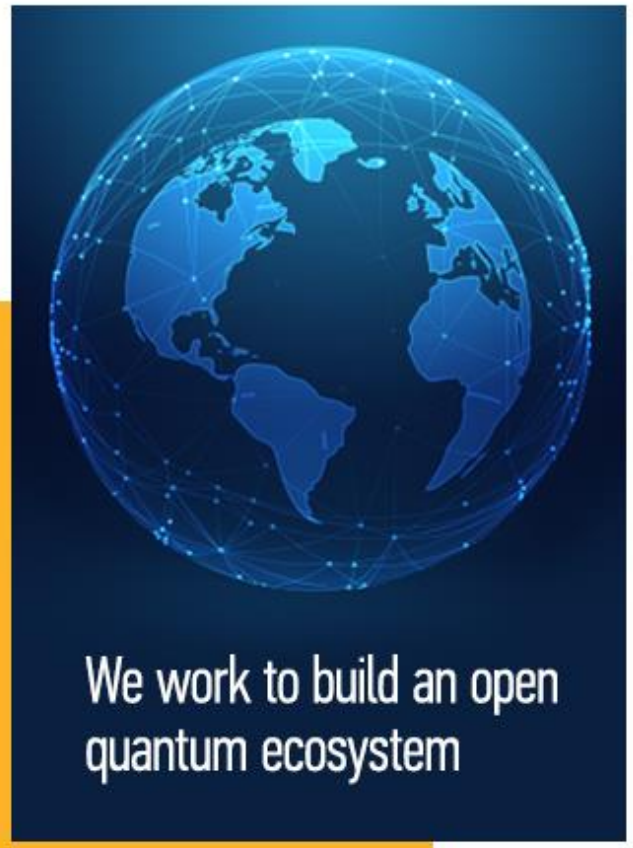
Challenges

- Quantum Compiler Design
- Benchmarking Quantum Software
- Error Mitigation Versus Error Correction
- New Ideas…

Challenges

- Quantum Compiler Design
- Benchmarking Quantum Software
- Error Mitigation Versus Error Correction
- New Ideas…

Need Interdisciplinary Education Initiatives!

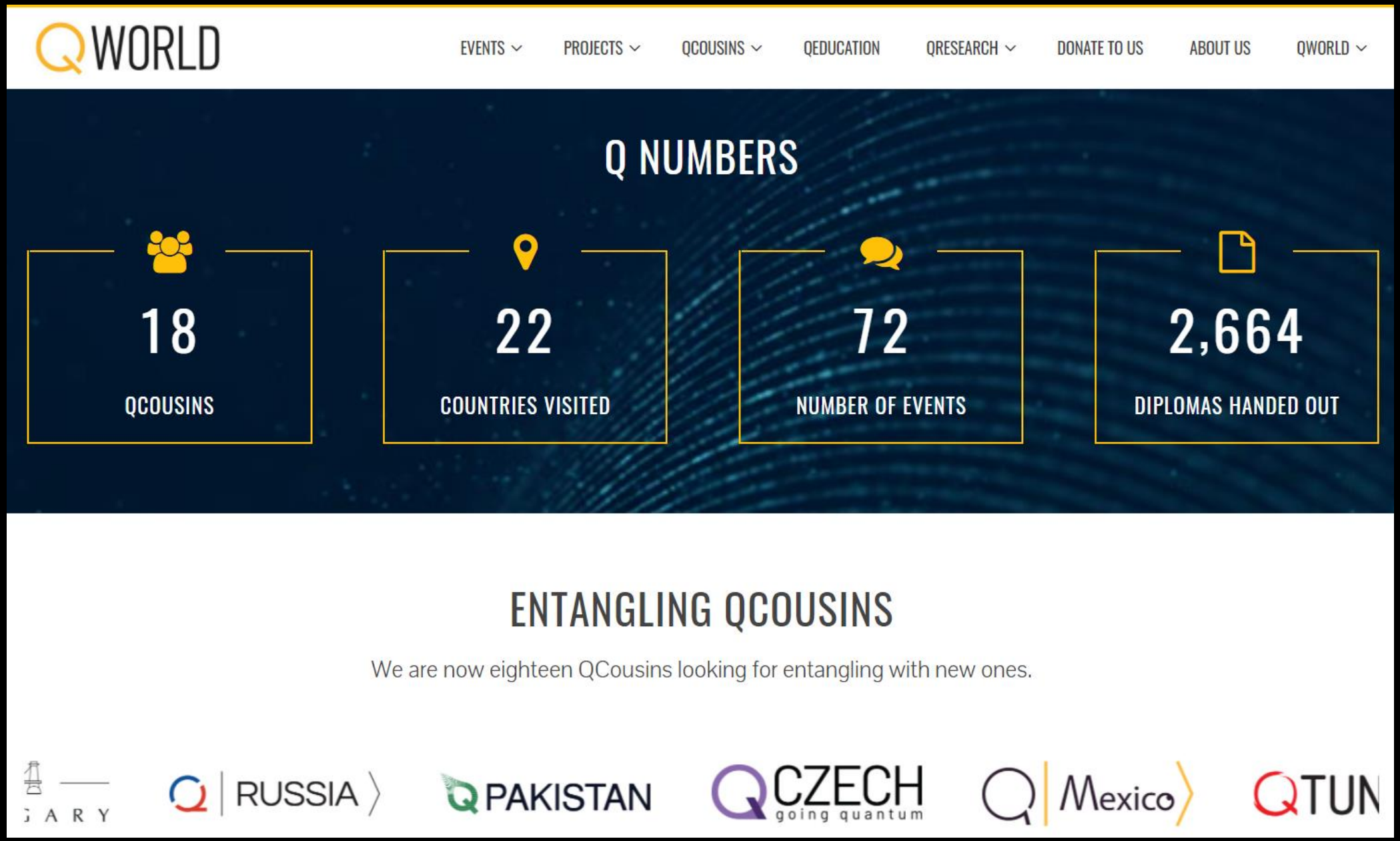


QWORLD

QWorld is a non-profit global organization that brings quantum computing researchers and enthusiasts together.

Its main goal is to popularize quantum technologies and software. Also, through education and skill development opportunities, QWorld is training the next generation of quantum scientists.

Join us in the second quantum revolution!


QWORLD
EVENTS
PROJECTS
QCOUSINS
QEDUCATION
QRESEARCH
DONATE TO US
ABOUT US
QWORLD
Q NUMBERS
18
QCOUSINS
22
COUNTRIES VISITED
72
NUMBER OF EVENTS
2,664
DIPLOMAS HANDED OUT
ENTANGLING QCOUSINS
We are now eighteen QCousins looking for entangling with new ones.
RUSSIA
PAKISTAN
CZECH
going quantum
Mexico
QTUN

Thank You

QWorld Discord Server Invite

https://discord.gg/vx7AQDYB

Contact: jrashid@iba.edu.pk