



**Leading the way  
in  
Quantum & AI  
Innovations**



**QUANTUM AI  
GLOBAL**

## COMPANY SNAPSHOT

Quantum AI Global stands at the forefront of the AI and Quantum revolution, delivering the essential 'picks and shovels' of tomorrow's technology. With a legacy of pioneering research, breakthrough productization, and real-world commercial deployment, we are powering the infrastructure behind the next technological era.



**Founding** Nov 2019

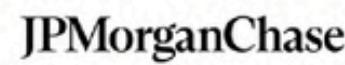
**Staff** 65+ across 3 offices

**Strengths**

- Market Ready Products
- 8 PhDs, 7 Research scholar pursuing PHD as employees
- In Revenue Mode

**Geographies** INDIA, US, UAE

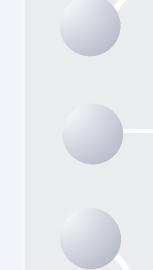
## Trusted By

GOVERNMENT	INDUSTRY	ACADEMIA
         	        	            

# What we DO

## RESEARCH to APPLICATION

***"Discovery is designed to translate"***



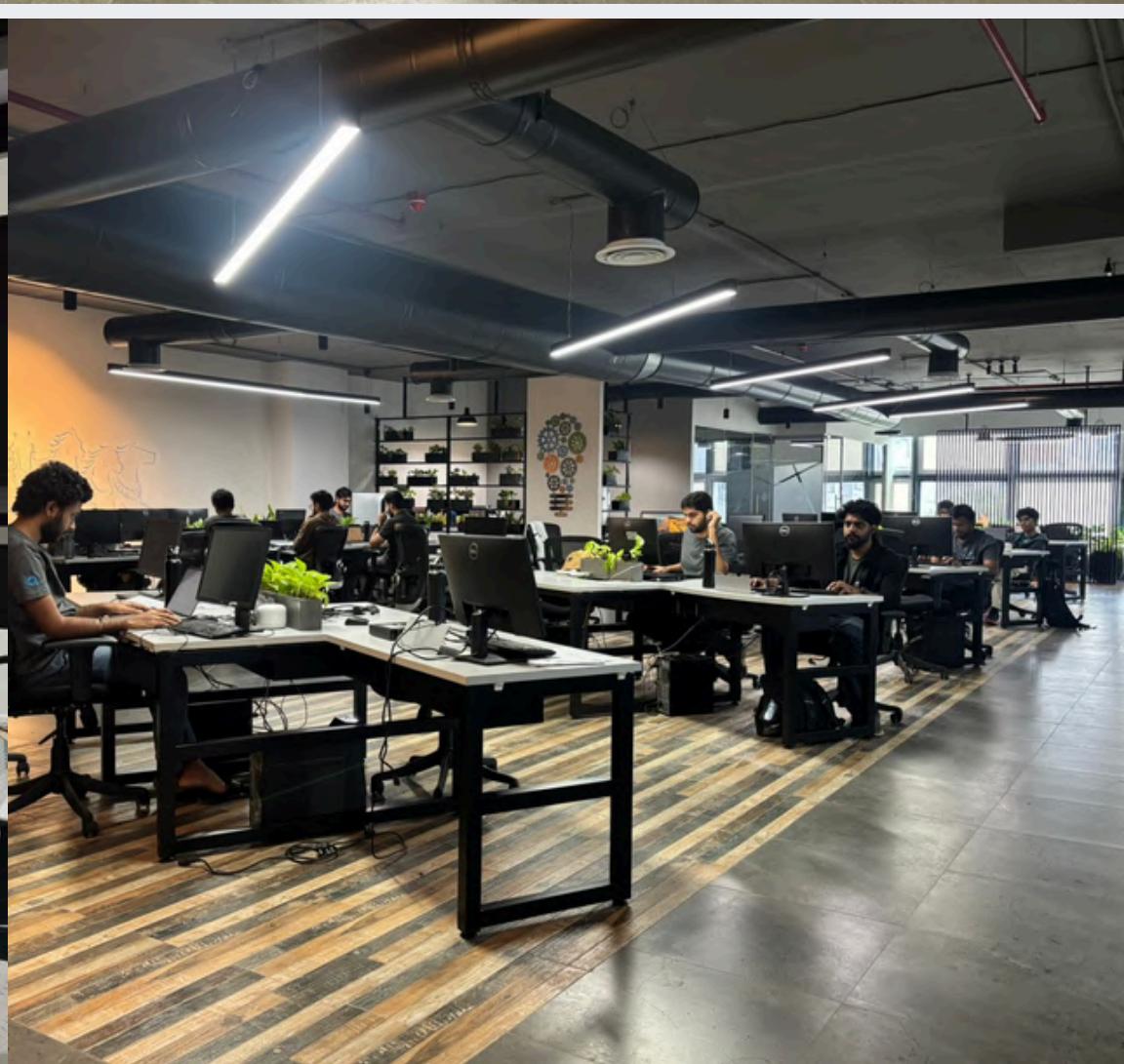
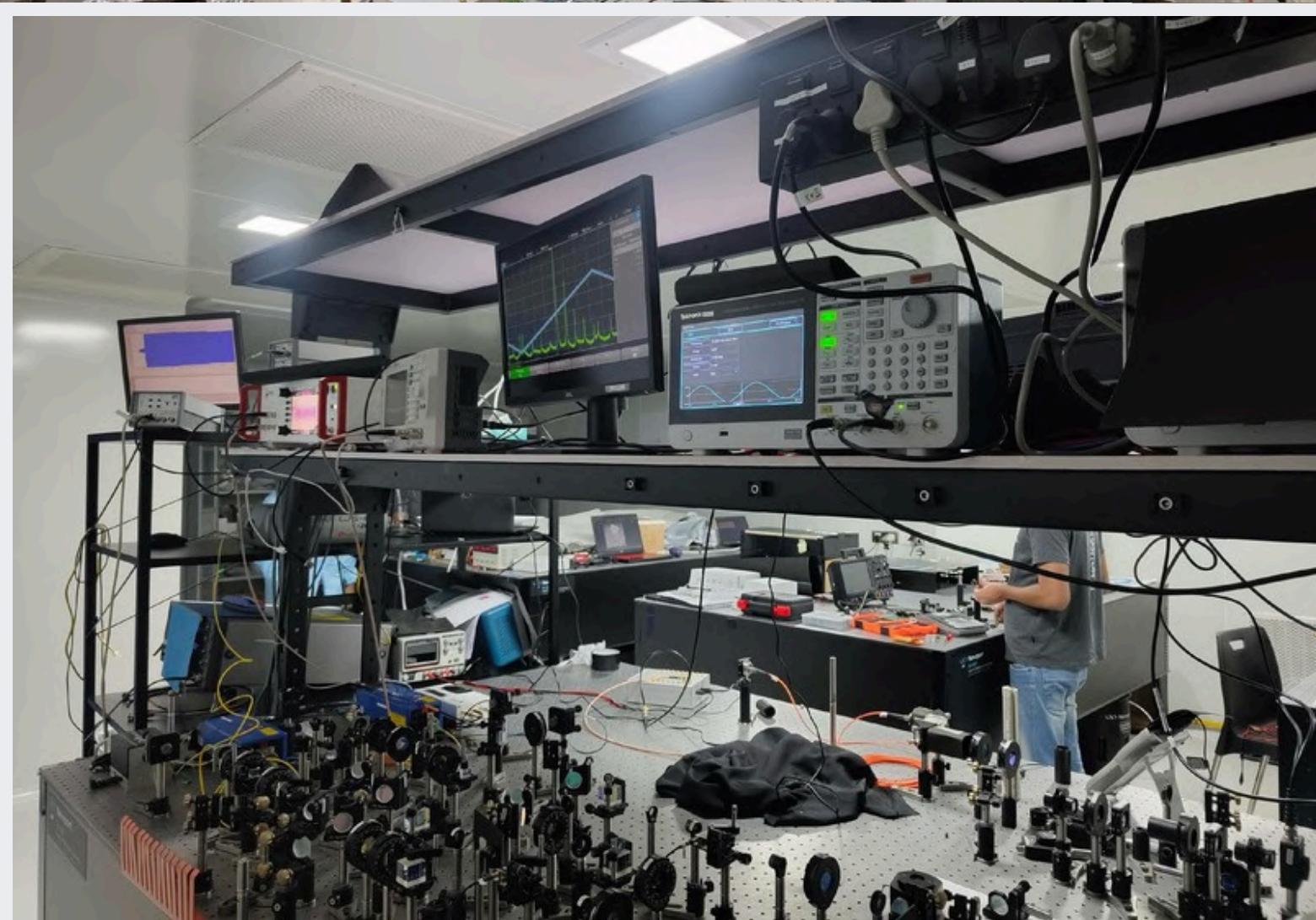
## APPLICATION to PRODUCTIZATION

***"High-powered product factory, where solutions are forged for impact"***

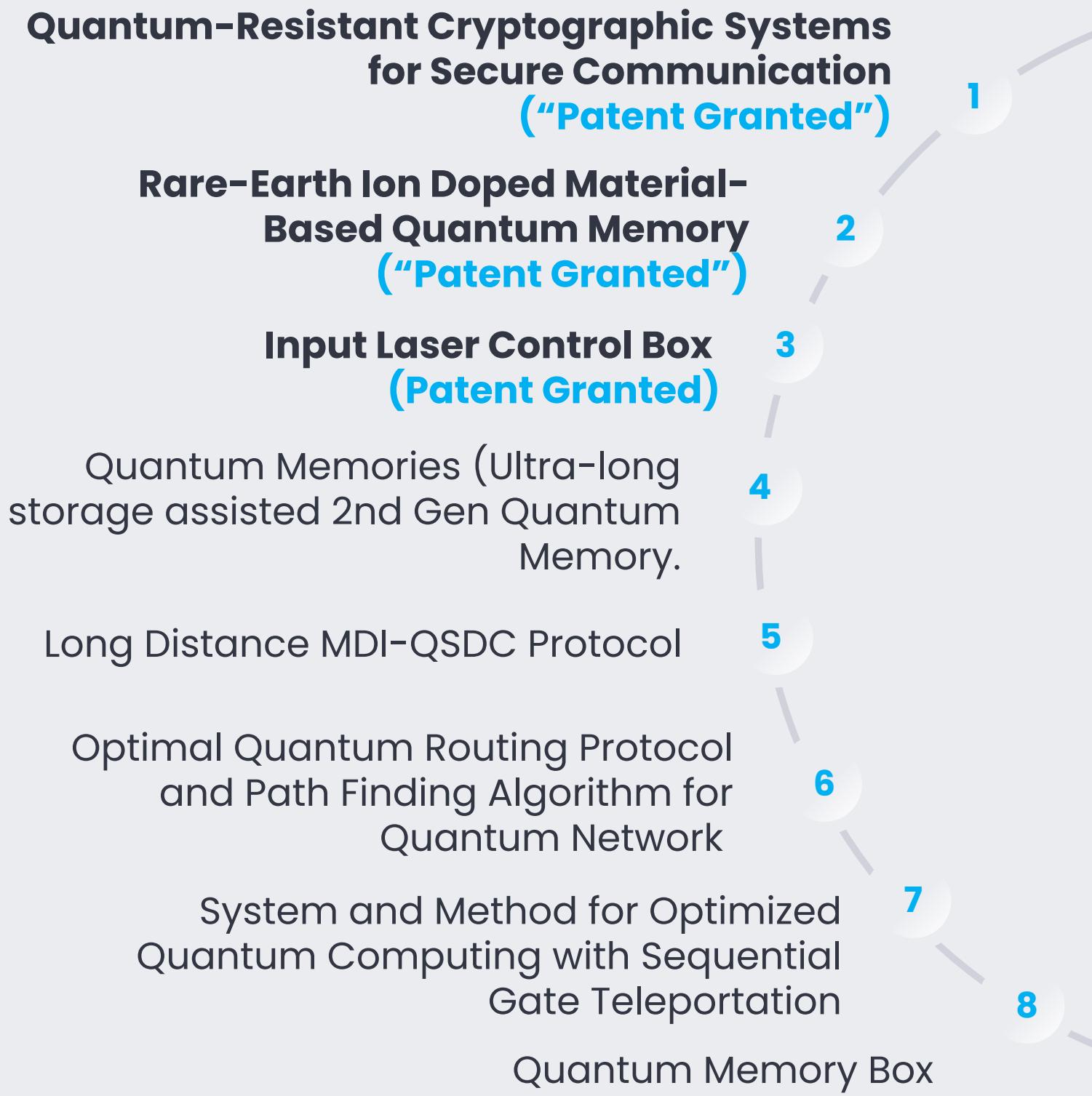
## PRODUCTIZATION to COMMERCIALIZATION

***"Change industries and shape a Quantum and AI powered future"***

## OUR RESEARCH LAB AND CORPORATE OFFICE



## OUR IP's



8 Quantum Random Number Generation QRNG with Digital Quantum Simulation

9 QubitIQ: An Intelligent System for Quantum Encoding Templates Recommendations

10 Long Distance MDI-QSDC protocol.

11 Software Platform for Modelling and Simulation of Quantum Network Communication

12 Rubidium-based Magnetometer For Bio-Sensing Application

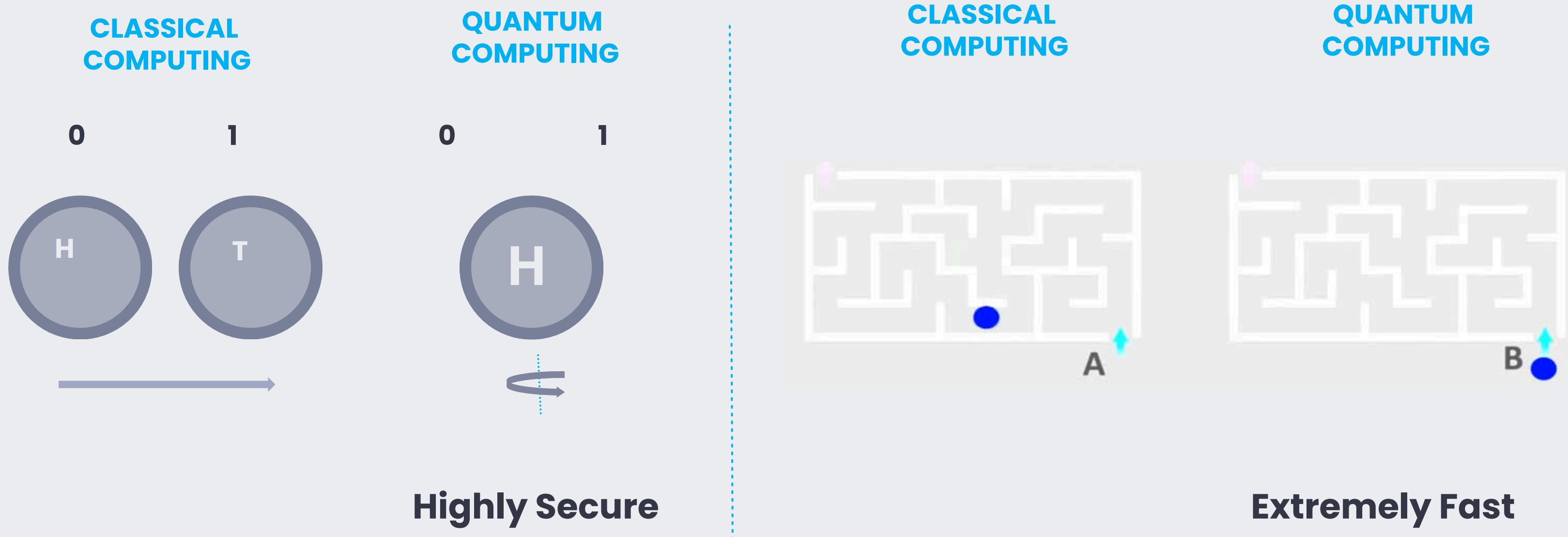
13 Measurement Device Independent-QSDC

14 Secure Quantum Multiparty XOR Protocol

15 Adaptive AI-Driven Hybrid Laser Locking for Quantum Sensing and Precision Applications.

# WHAT IS QUANTUM TECHNOLOGY?

# Quantum Technology



# Quantum Superposition

## "The Spinning Coin"

Imagine flipping a coin and freezing it mid-air whilst it's spinning. Until it lands, it's neither heads nor tails – it's **both at the same time!**

In the quantum world, particles can exist in multiple states simultaneously, just like our spinning coin. A quantum particle can be in two places at once, spinning both clockwise and anticlockwise, or have multiple properties simultaneously.

**Key Point: The "coin" only "decides" its state when we observe it – this is called "wavefunction collapse."**



# Quantum Entanglement

## "The Synchronised Dancers"



### Perfect Connection

Picture two dancers who have practised together so perfectly that even when separated by vast distances, they perform identical moves instantaneously.

### Instant Response

When one spins left, the other automatically spins right – no matter how far apart they are! This is quantum entanglement in action.

### Spooky Science

Einstein called this "spooky action at a distance" - measuring one particle instantly determines its entangled partner's state.

# Quantum Teleportation

**"The Ultimate Magic Trick"**

## The Setup

Imagine a magician who can make an object completely disappear from one box and instantly appear in another box across the room.

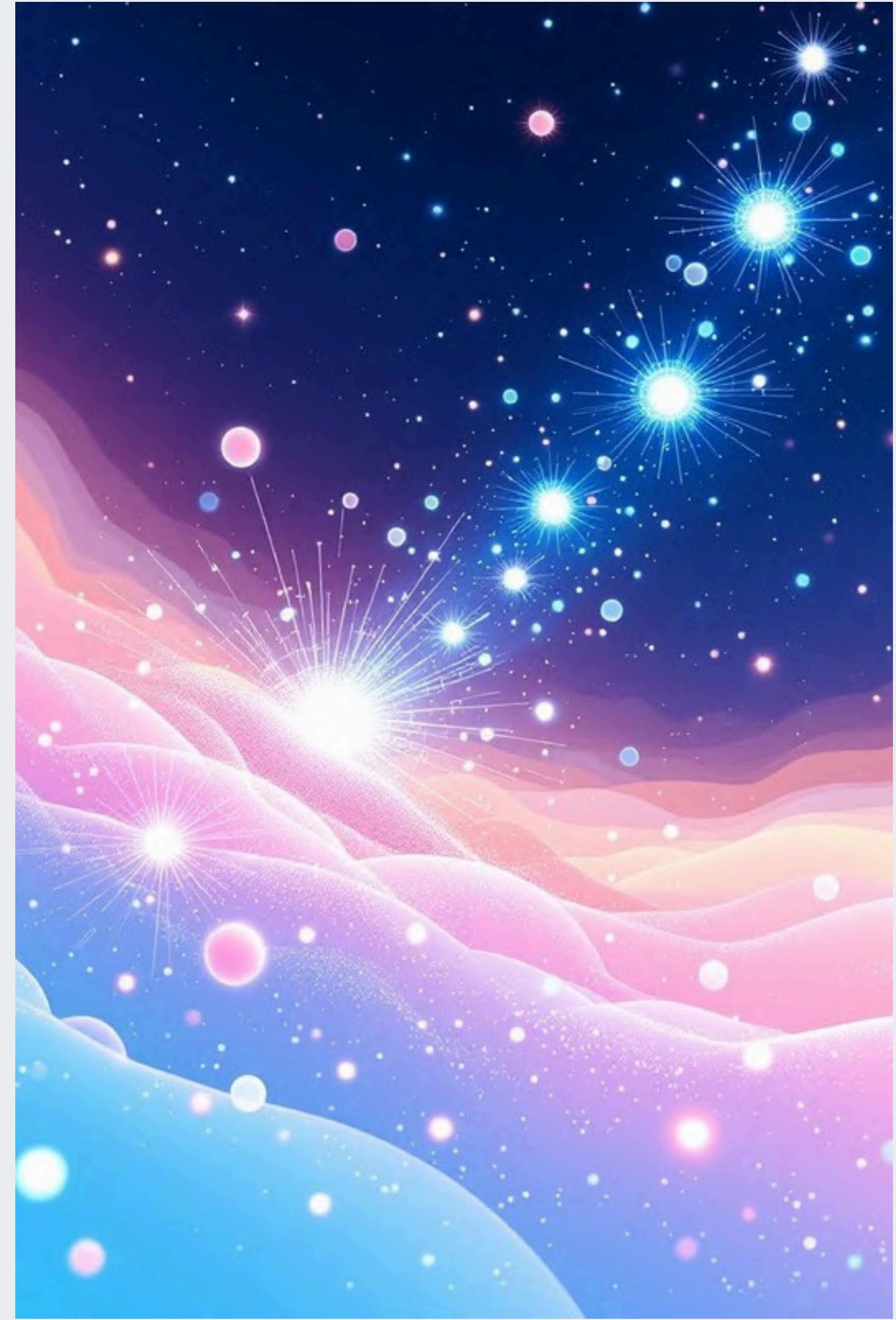
## The Twist

Here's the remarkable part: it's not the object itself that travels, but all its properties and information!

## The Reality

Quantum teleportation transfers all the quantum information of one particle to another particle far away, using entanglement as the connection.

**Key Point:** The original particle is destroyed in the process, but its exact quantum state is perfectly recreated elsewhere. It's like faxing the particle's blueprint!





## Why Does This Matter?

These strange quantum behaviours are the foundation for revolutionary technologies



### Quantum Computers

Using superposition to process multiple calculations simultaneously, solving problems impossible for classical computers.



### Ultra-Secure Communications

Using entanglement for unbreakable encryption that detects any attempt at eavesdropping.



### Precise Sensors

Using quantum effects for incredibly accurate measurements in medicine, navigation, and scientific research.

**The quantum world may seem bizarre, but it's the key to tomorrow's revolutionary technologies!**

# Quantum Technologies: Four Pillars



## Quantum Computing

Uses qubits (superposition + entanglement) to solve problems classical computers can't  
Applications: cryptography, optimization, drug discovery



## Quantum Communication

Enables ultra-secure data transfer using quantum entanglement & quantum key distribution (QKD)

•



## Quantum Sensing

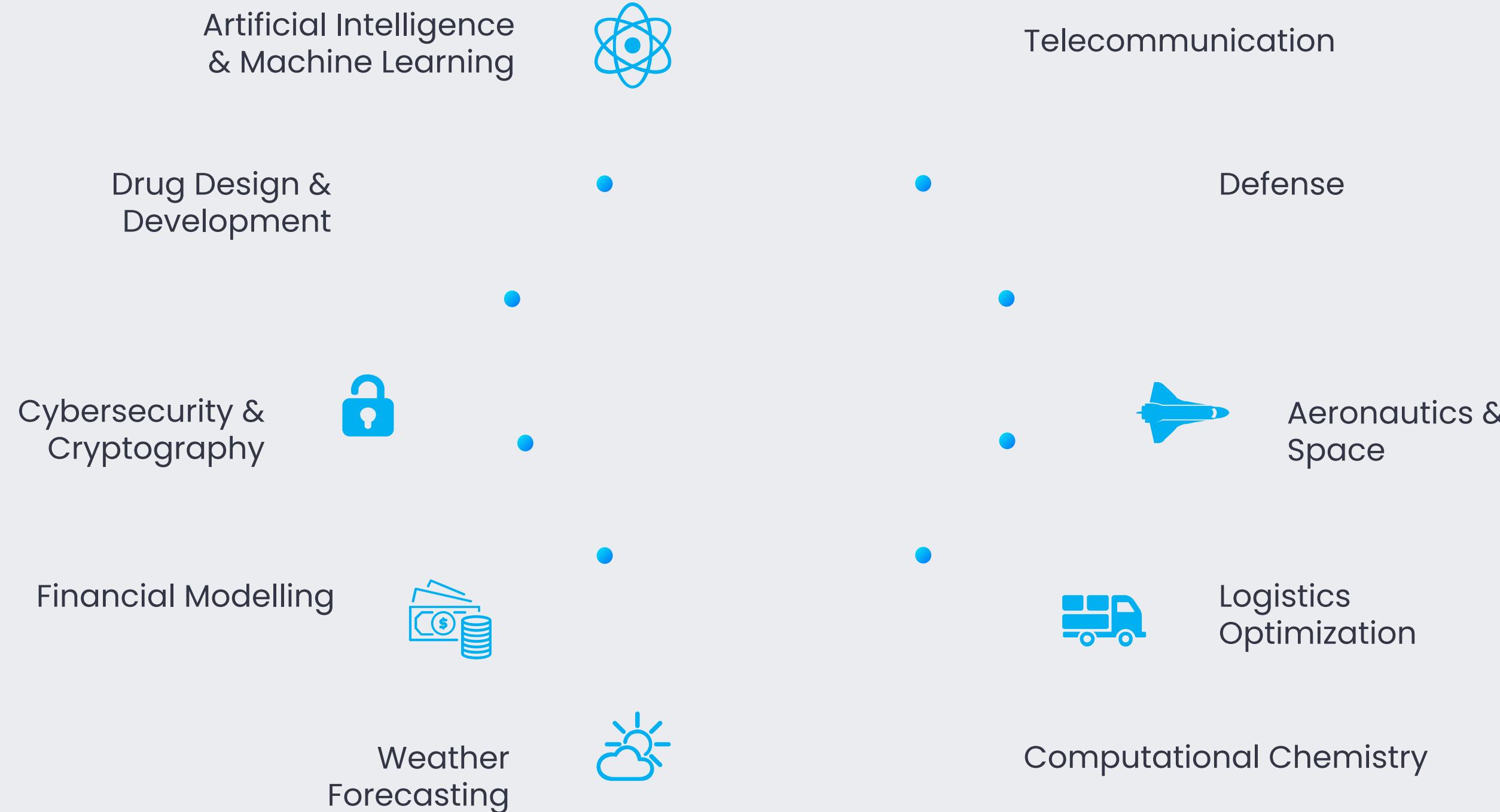
Exploits quantum states to measure time, magnetic fields, gravity, or position with extreme precision  
Better than classical sensors

•

## Quantum Materials

Novel materials: superconductors, topological insulators, NV centres in diamond, 2D materials  
Engineered to harness quantum effects for devices and applications

# Applications Of Quantum Technologies



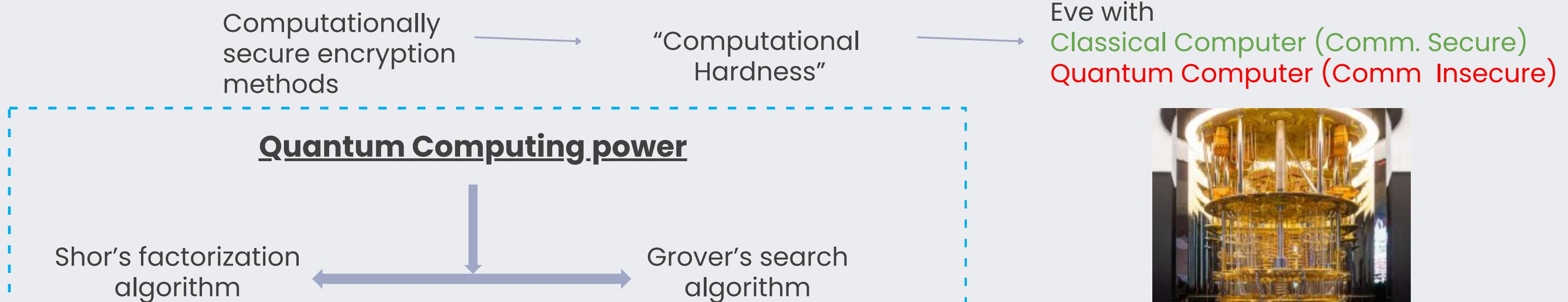
# Quantum Threat

<b>Current cryptographic standards</b>	<b>Type</b>	<b>Purpose</b>	<b>Impact from large scale quantum computer</b>
AES	Symmetric	Encryption	Larger key sizes needed (128-256 bits)
SHA-3	Hash function	Hashing	Larger output needed (128-284 bits)
RSA	Asymmetric	Signatures, key establishment	No longer secure
ECDSA, ECDH (elliptic curve cryptography)	Asymmetric	Signatures, Key exchanges	No longer secure
DSA (finite field cryptography)	Asymmetric	Signatures, key exchanges	No longer secure

Note: AES = advanced encryption standard; SHA-3 = secure hash algorithm 3;  
 RSA = Rivest-Shamir-Adleman cryptosystem;  
 ECDSA = Elliptic Curve Digital Signature Algorithm;  
 ECDH = Elliptic-curve Diffie-Hellman; DSA = Digital Signature Algorithm.

# Why security infrastructure been questioned in Quantum Era!

## **“Harvest Now, Decrypt Later”**



### ***Worldwide accepted Encryption and Hashing Standards***

Public key (RSA, ECC) cryptography, Private key (AES) cryptography, Hash signatures (MD5, SHA256) are worldwide accepted primitives in cybersecurity.

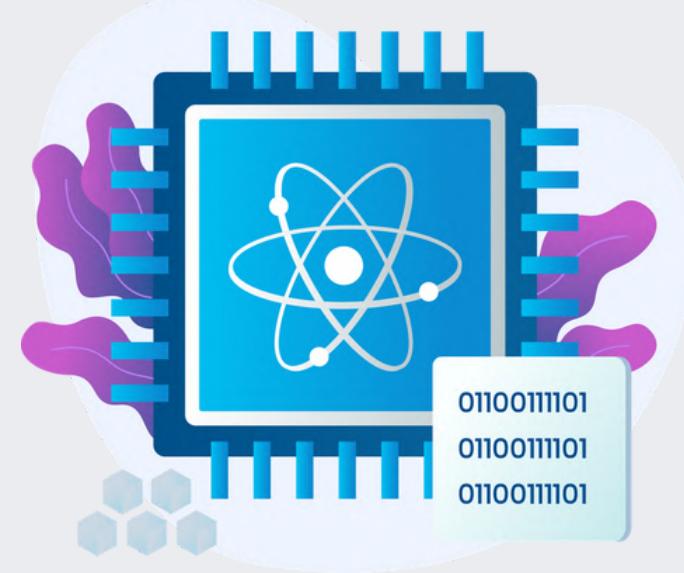
**Shor's attack:** Death sentence to potentially all existing public key schemes.

**Grover's attack:** Reduces search space of all symmetric keys and hash functions to half.



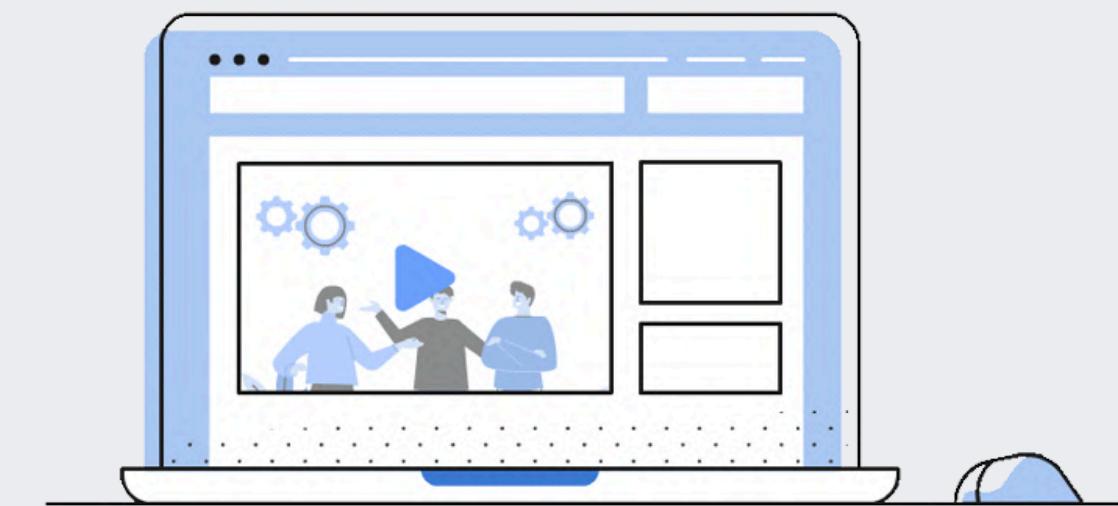
***“Cryptographically Relevant Quantum Computer (CRQC) is a quantum computer powerful enough and equipped with the software necessary to break the cipher keys used today in encryption.”***

# Y2Q—Year to Quantum



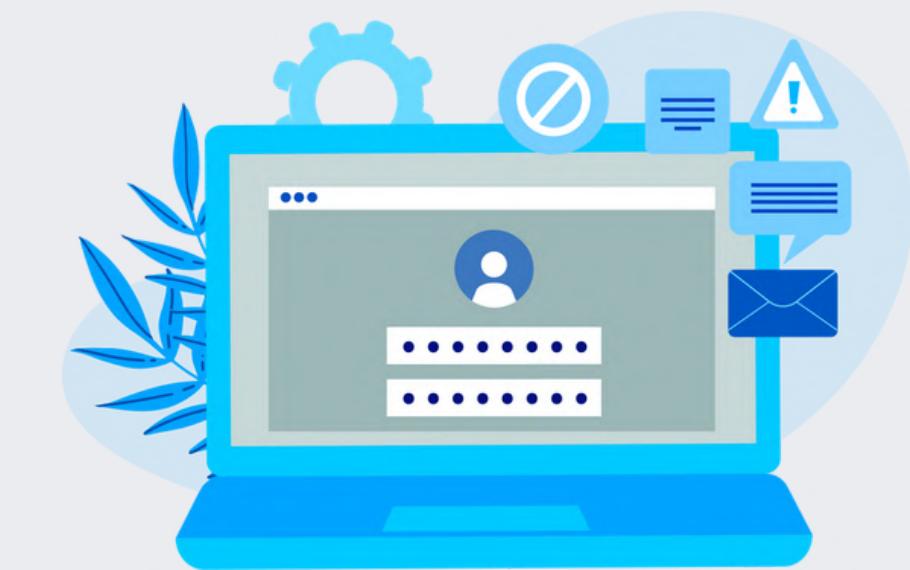
## What is Y2Q?

Y2Q refers to the time when quantum computers will be powerful enough to break traditional forms of encryption.



## Who is at Risk?

Any organization that stores and transacts sensitive information, from banks to government agencies are at risk from Y2Q.



## Solutions for Y2Q

One solution is the development of **quantum-safe cryptography**, which uses quantum mechanics to protect against quantum attacks & QKD.

Quantum Computing threat  
is knocking the doors!!

Submitted on 25 Mar 2016 (v1), last revised 31 Jan 2017 (this version: v3)

**Using Simon's Algorithm to Attack RSA**

Thomas Santoli, Christian Schaffner

We present new connections between quantum information and the field of classical cryptography. In particular, we provide examples where Simon's algorithm can be used to show insecurity of commonly used cryptographic symmetric-key primitives. Specifically, these examples consist of a quantum distinguisher for the 3-round Feistel network and a forgery attack on CBC-MAC which forges a tag for a chosen-prefix message querying only other messages (of the same length). We assume that an adversary has quantum-oracle access to the respective classical primitives. Similar results have been achieved recently in independent work by Kaplan et al. Our findings shed new light on the post-quantum security of cryptographic schemes and underline that classical security proofs of cryptographic constructions need to be revisited in light of quantum attackers.

Comments: 14 pages, 2 figures, v3: final polished version, more formal definitions added

Mar 2021

[arXiv:1603.09344 \[cs.CR\]](https://arxiv.org/abs/1603.09344) [pdf](https://arxiv.org/pdf/1603.09344.pdf)

**International Conference on the Theory and Application of Cryptology and Information Security**

↳ ASIACRYPT 2017: [Advances in Cryptology – ASIACRYPT 2017](#) pp 161–178 | [Cite as](#)

**Grover Meets Simon – Quantumly Attacking the FX-construction**

Gregor Leander & Alexander May

Conference paper | [First Online: 18 November 2017](#)

2390 Accesses | 50 Citations

Part of the [Lecture Notes in Computer Science](#) book series (LNCS, volume 10621)

**Abstract**

**Breaking Weak 1024-bit RSA Keys with CUDA**

Publisher: IEEE | [Cite This](#) | [PDF](#)

Kerry Scharfglass ; Darrin Weng ; Joseph White ; Christopher Lupo | [All Authors](#)

6 302

# Y2Q a Global Threat

memory Interesting paper.. I thought Mostaf and you may be interested in this paper! Factoring 2048 RSA integers in 177 days with 13436 qubits and a multimode memory Élie

Forbes

INNOVATION

**The Quantum Threat To Cryptography: Don't Panic, But Prepare Now**

Mike Brown Forbes Councils Member  
Forbes Technology Council  
COUNCIL POST | Membership (Fee-Based)

Jan 11, 2022, 09:30am EST

ADVERTISEMENT

CTO and co-founder at ISARA Corporation. Focused on technology for crypto agility and quantum safety.

in

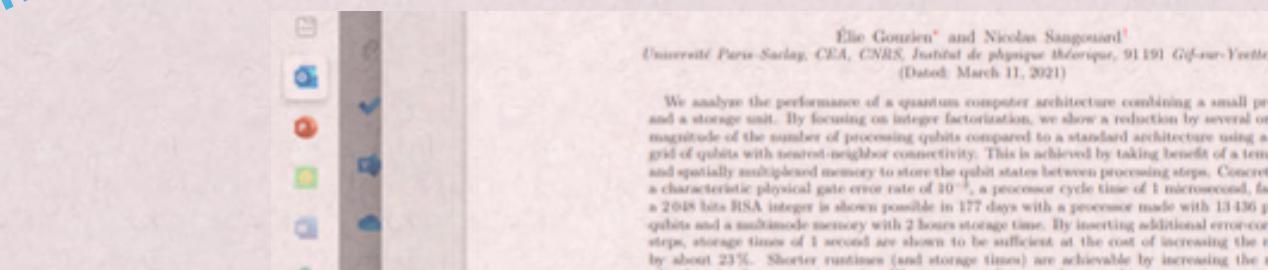
QUANTUM COMPUTING

**Organizations should make these 3 changes now to protect against the quantum computing threat**

Sep 13, 2022

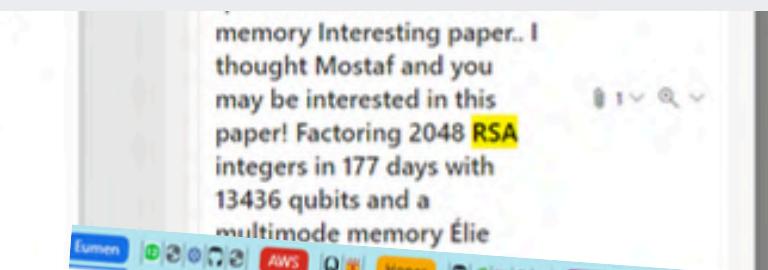
Quantum Computing threat  
is knocking the doors!!

# Y2Q a Global Threat



Élie Gouzien\* and Nicolas Sangouard\*  
Université Paris-Saclay, CEA, CNRS, Institut de physique théorique, 91191 Gif-sur-Yvette, France  
(Dated: March 11, 2021)

We analyze the performance of a quantum computer architecture combining a small processor and a storage unit. By focusing on integer factorization, we show a reduction by several orders of magnitude of the number of processing qubits compared to a standard architecture using a planar grid of qubits with nearest-neighbor connectivity. This is achieved by taking benefit of a temporally and spatially multiplexed memory to store the qubit states between processing steps. Concretely, for a characteristic physical gate error rate of  $10^{-4}$ , a processor cycle time of 1 microsecond, factoring a 2048 bits RSA integer is shown possible in 177 days with a processor made with 13 436 physical qubits and a multimode memory with 2 hours storage time. By inserting additional error-correction steps, storage times of 1 second are shown to be sufficient at the cost of increasing the runtime by about 23%. Shorter runtimes (and storage times) are achievable by increasing the number



memory Interesting paper.. I thought Mostaf and you may be interested in this paper! Factoring 2048 RSA integers in 177 days with 13436 qubits and a multimode memory Élie

Submitted on 25 Mar 2016  
Using Simon's algorithm to show insecurity of quantum-oracle access on the post-quantum attackers.

Thomas Santoli, Christophe Texier-Bonnieux, and Sébastien Tisserand

We present new constructions to show insecurity of quantum-oracle access on the post-quantum attackers.

Comments 14 pages

PC MAG

## Chinese Researchers Reportedly Crack Encryption With Quantum Computer

PC Mag

October 14, 2024 · 2 min read

Grover Meets Simon – Quantumly attacking the RSA construction

Gregor Leander & Alexander May

Conference paper | First Online: 18 November 2017

2390 Accesses | 50 Citations

Part of the *Lecture Notes in Computer Science* book series (LNCS, volume 10626)

Abstract

Conferences > 2012 13th International Conference on Cryptology in India

Breaking Weak 1024-bit RSA Keys with CUDA

Publisher: IEEE Cite This PDF

Kerry Scharfglass ; Darrin Weng ; Joseph White ; Christopher Lupo All Authors

6 302

FORUM

1

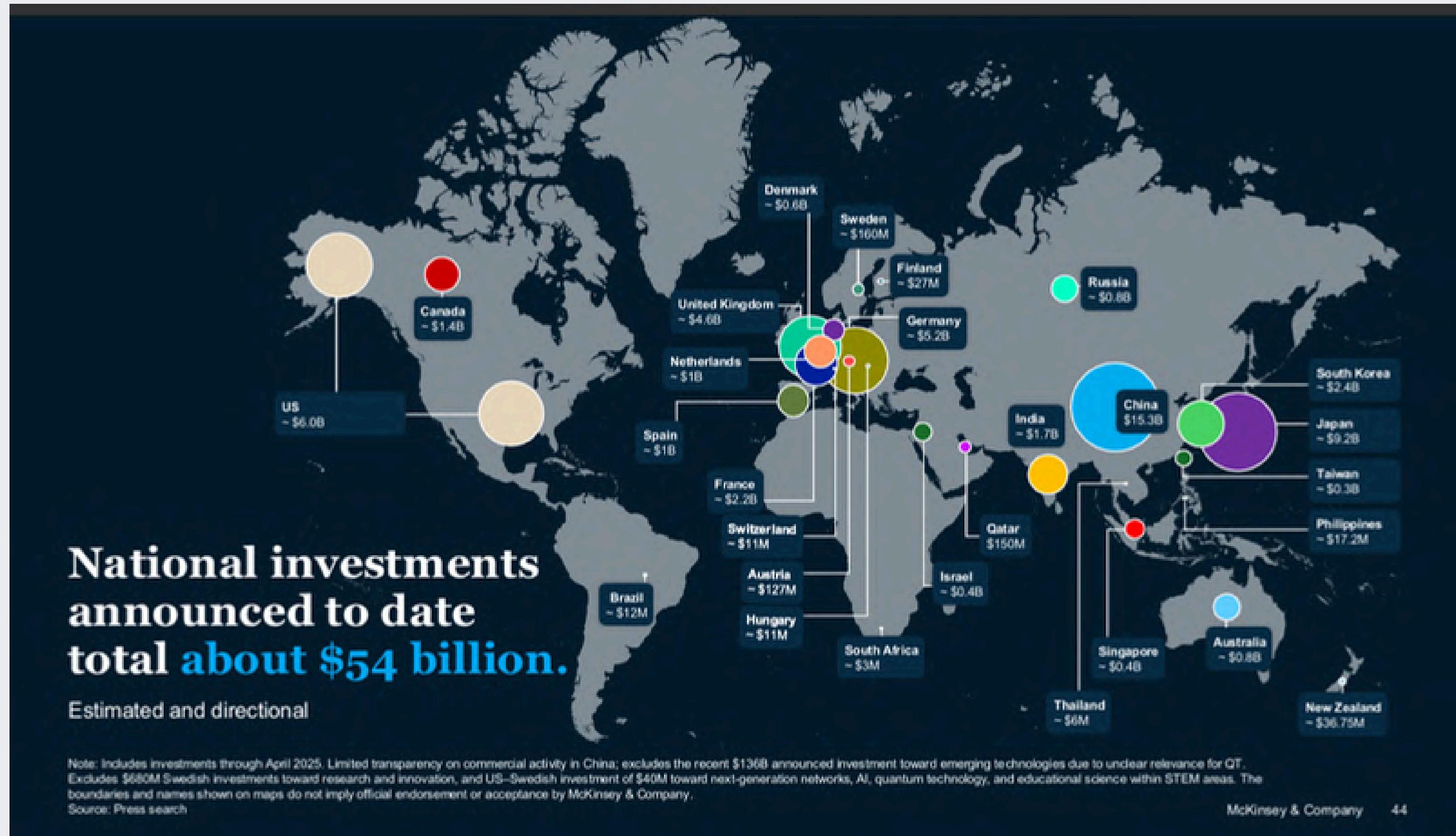
QUANTUM COMPUTING

Organizations should make these 3 changes now to protect against the quantum computing threat

Sep 13, 2022

New Features for you

# Global Quantum Investments By Country



LONG-TERM SOLUTION

## QUANTUM KEY DISTRIBUTION (QKD) NETWORK NATIONWIDE



# IMMEDIATE SOLUTION

## QUANTUM SAFE NETWORK FOR INDIVIDUAL ORGANIZATIONS



# Q-Forte: Quantum Assured InfoSec Platform



## OUR PRODUCTS

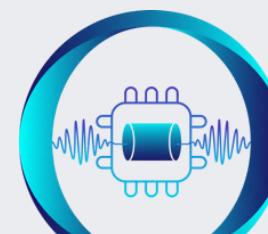
### QUANTUM CRYPTOGRAPHY



Q-FORTE

Quantum Assured information Security Platform

### QUANTUM COMMUNICATION



QUANTUM MEMORY



EPS QKD

Quantum Hardware  
Building the future of  
Quantum Internet

### QUANTUM SENSING

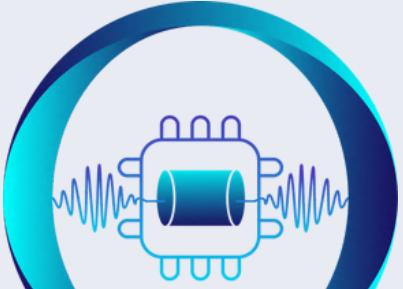


QUANTUM MAGNETO-METER

Quantum Biosensor Healthcare for

# Quantum Experimentation Kits for Academia

## Proposed solution for National Quantum Mission (NQM)



### Quantum Memory

**Quantum Storage Demonstrator Toolkit**  
An educational toolkit to explore Quantum Memory, highlighting its role in Quantum Storage, long-distance entanglement, and secure Quantum Key Distribution.



### EPS QKD

**Entanglement-based Quantum Key Distribution Experimentation kit**  
An interactive toolkit for exploring entanglement-based Quantum Key Distribution, Bell's Inequality, single-photon sources, and more — all in one system.



### Quantum Sensing

**Quantum Sensing and Atomic Physics**  
A hands-on kit for frequency and length metrology using atomic spectroscopy. Enables experiments in interferometry, Zeeman effect, ECDL, laser locking, and quantum magnetic sensing with Rb — ideal for learning atom-based precision measurement.



### QNTSim

**Quantum Network Simulator**  
India's first interactive quantum network simulator for academia to explore entanglement and secure communication through hands-on protocol demos and realistic network scenarios.



### Quantum Cluster

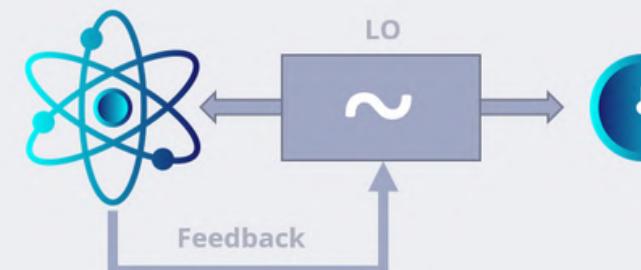
**Quantum Cluster**  
Accelerate Quantum Learning, Algorithm Development and Quantum Processing Unit (QPU) performance approximation.

# RESEARCH & POC DEVELOPMENT IN PROGRESS

01

## Atomic Clock

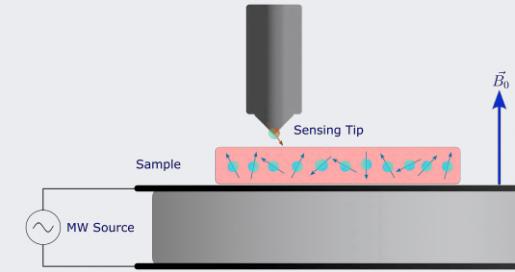
Unlocking the secrets of time, ultra-precise atomic clocks offer unmatched accuracy for critical applications in navigation and communication, with unmatched precision.



02

## Quantum Magnetometry for MRI

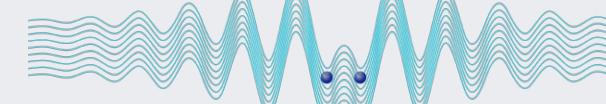
To design highly sensitive, compact, and miniaturized magnetic field sensors for magnetic resonance imaging.



03

## Quantum Gravimeter

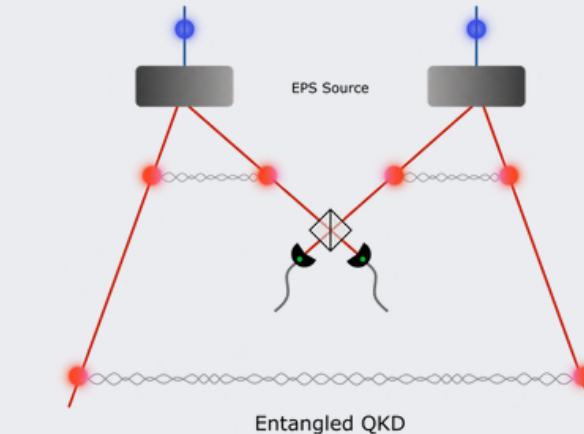
High precision gravitational field sensor for petroleum and mineral prospecting, geophysical surveys, seismology, and metrology.



04

## Quantum Repeater

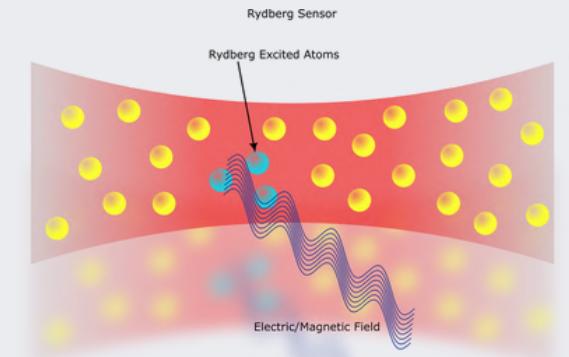
Quantum repeaters employ a process known as entanglement swapping. This involves creating entangled pairs of photons, sending them to intermediary nodes, and performing entanglement swapping operations to generate new entangled pairs.



05

## Rydberg Sensor

Rydberg sensors leverage the extreme sensitivity of Rydberg atoms to electric and magnetic fields to detect and measure these fields with high precision. Their unparalleled sensitivity allows for the detection of very weak signals.



# CORE TEAM



**Sanjay Chittore, Founder & CEO  
Entrepreneur**

deep understanding of the challenges and opportunities facing these industries



**Col Kapil Jaiswal (Retd), CTO  
Adjunct Prof, Cyber, Amrita VV, Ex-Director (InfoSec), MoD, GOI**

Lead national level Info Security and Cryptography Research team of 100+ domain specialists and Cyber Operations team of 50+ Red Team members



**Dr. Sachin Barthwal, Head of Quantum Technology  
PhD in Physics from University of Hyderabad**

Experimental Atomic Physicist with extensive experience of in Laser cooled Atomic Spectroscopy research including Quantum Sensor Technology



**Dr. Diksha Sharma, Quantum Research Scientist  
Research scholar in Quantum Machine Learning, IIT Jodhpur**

Experienced in quantum machine learning models for real-world tasks, developing interpretable, scalable, and resource-efficient quantum models.



**Dr. Monika, Quantum Sensing Lead  
PhD in Physical Science from AcSIR-NPL**

Experimental quantum optics physicist specializing in Rydberg atom based RF E-field sensing, quantum memory and atomic spectroscopy.



**Dr. Avinash Kumar, Quantum Optics Scientist  
PhD in Physics , Tata Institute of Fundamental Research**

Experimental physicist specialized in designing and building narrow linewidth laser cavities with expertise in optics and high-resolution spectroscopy.



**Dr. Dhanshre Thulkar, Head of Product Management  
PhD in Engineering from University of Mumbai**

Researcher in machine learning and image processing and experience in working with industry and academia



**Diana Dsouza, Head of Sales and Business Development**

Business Development leader with 18 years expertise in end-to-end product commercialization. Adept at ensuring successful market entry and driving robust sales performance.



**Rikteem Bhowmick, Quantum Communications Lead  
Research scholar pursuing PhD in Quantum Communication**

Experienced in developing entangled photon sources and designing quantum key distribution systems.



**Devendra Mishra, Quantum Hardware Lead  
Research scholar pursuing PhD in Quantum Optics IITB**

Experienced in Quantum Optics experimentation and Quantum communication Hardware (Quantum memory, Quantum Repeater, Etc.)



**Rama Theja, Opto Electronics Lead  
Masters in Quantum computing from DIAT Pune**

Quantum engineer with expertise in setting up quantum sources, QKD testbeds, and quantum memory hardware with integrated control electronics.



**Neelesh Singh Katoch, Quantum Software Engineer  
Masters in Cybersecurity from DIAT Pune**

Experienced engineer and researcher working on quantum-safe cryptography and cybersecurity, designing and implementing scalable, standards-compliant production solutions.

# SCAN THIS

**About QAIG**



**About Me**

