Quantal Technology LLC

Emergent quantum technology and applications

David Farley
Quantal Technology

Quantal Technology LLC

Quantum Truisms

- Quantum technologies *can potentially* be better than classical

- Quantum Computing & Software longest time horizon

- Quantum Sensing & Encryption here now

- Quantum states are fragile

- Expertise and suppliers are few

Quantum Computing – Entangled “Qubits”

- Qubit = “Quantum Bit” = atom with two states, or photon with two modes
- Entangled qubits allow for massively parallel computing
- Fundamental Problem: Environment quickly destroys entanglement
- Secondary Problem: Expertise and supplies

Quantum Algorithms - using a quantum computer

- Only a handful of quantum algorithms proven to enhance computing
- Requires programmers who understand quantum
- In the future, could enhance pharmaceutical development, etc.

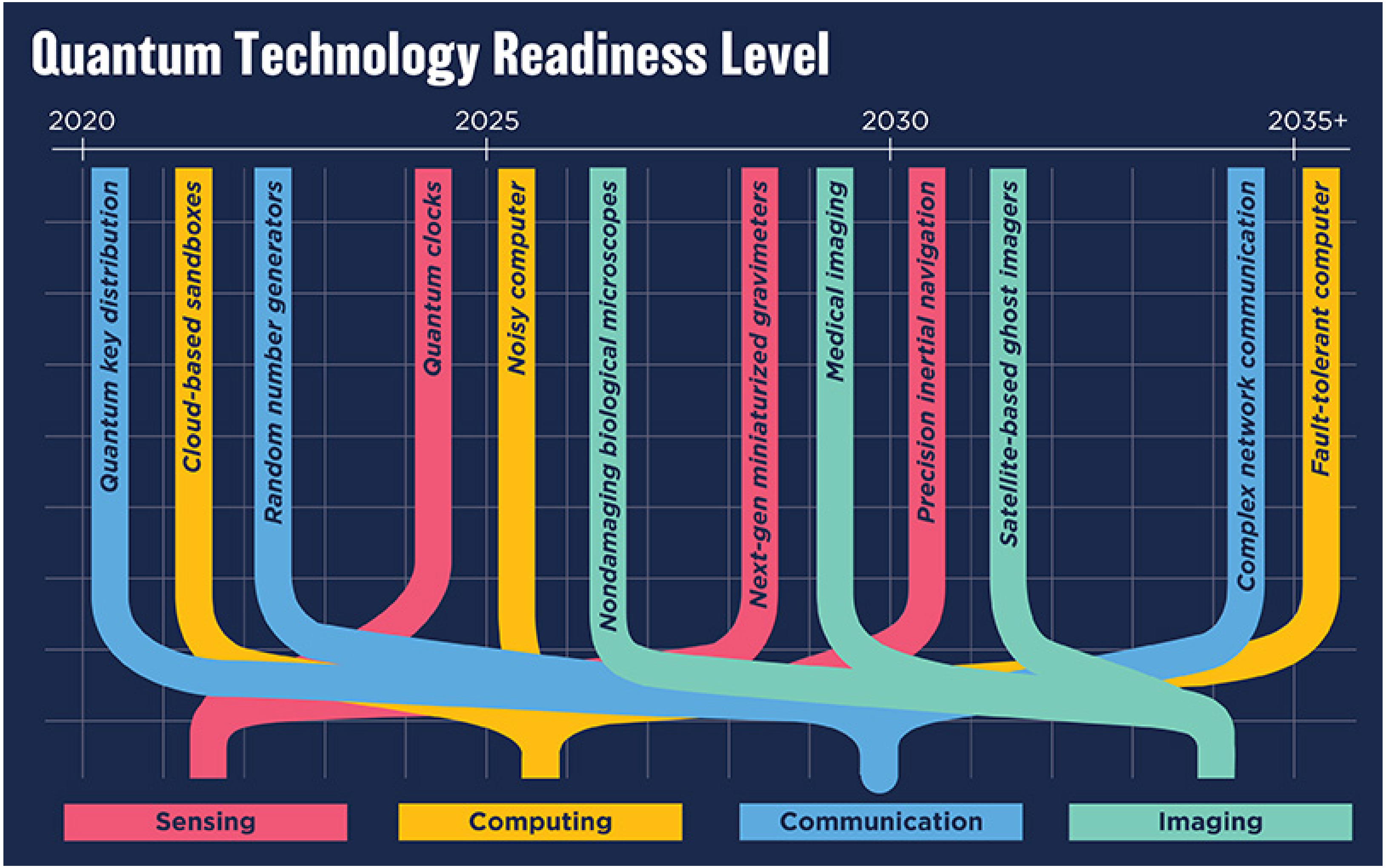
Quantum Sensing – ultrasensitive measurements

- Quantum states are fragile
- Quantum sensing leverages quantum sensitivity to environmental perturbations
- Opposite situation for quantum computing, where need to isolate from the environment

Quantum Encryption – Unbreakable (in theory)

- Quantum Key Distribution (QKD) – relies on non-cloning of quantum wave functions
- Shares random numbers between parties
- Random numbers for One-Time Pad (OTP) encryption protocol (unbreakable)

Quantal Technology LLC



Basic Quantum Theory (“spooky physics”)

Put a “state” into a “ket”: |vertical polarization> = $|V\rangle$

Now make a “superposition” of pure states: $|\psi\rangle = c_V|V\rangle + c_H|H\rangle$

This wave function is in both the horizontal and vertical states, until measured

Now consider <u>two</u> “entangled” particles (photons): $|\psi\rangle = c_1|HV\rangle + c_2|VH\rangle$

There is no way to factor out vertical or horizontal states

Quantum computers seek to leverage the entanglement of many particles

"Qubit" versus "Bit"

A classical computer uses "bits", which are <u>either</u> a "zero" (0 Volts) or a "one" (5 Volts)

In quantum, we have the "qubit", which is <u>both</u> a "zero" <u>and</u> a "one" $|\psi\rangle = |0\rangle + |1\rangle$

Until we measure it

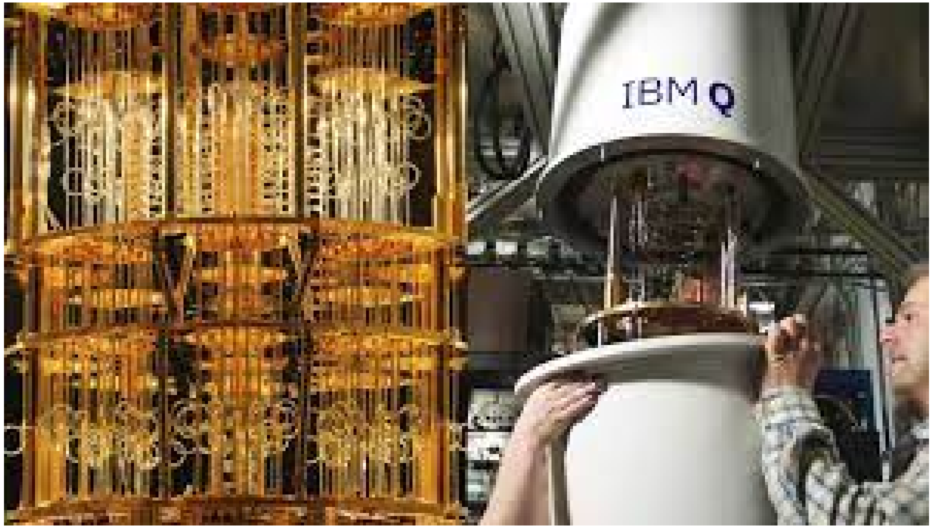
We can entangle two (or more) qubits: $|\psi\rangle = |10\rangle + |01\rangle$

This is the idea of a quantum computer

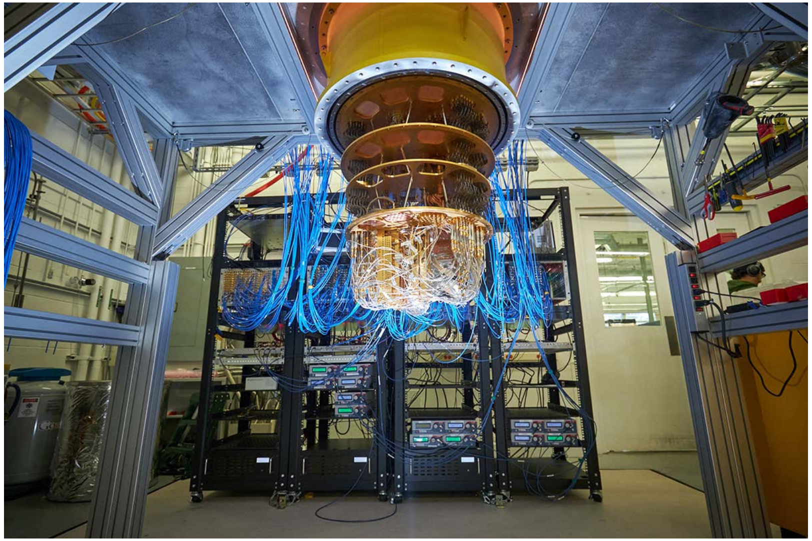
<u>Quantum Advantage Example: Li-3</u>

To simulate the electron wave function for Lithium (N=3 electrons) using a computational grid divided into 3*m* regions requires a classical computer able to store 2^{3mN} amplitudes. To achieve a precision of 10% requires m=3, so <u>2^{27} bytes needed (500 petabytes!)</u>. *A quantum computer needs just 27 entangled qubits.*

Quantum Computing



IBM

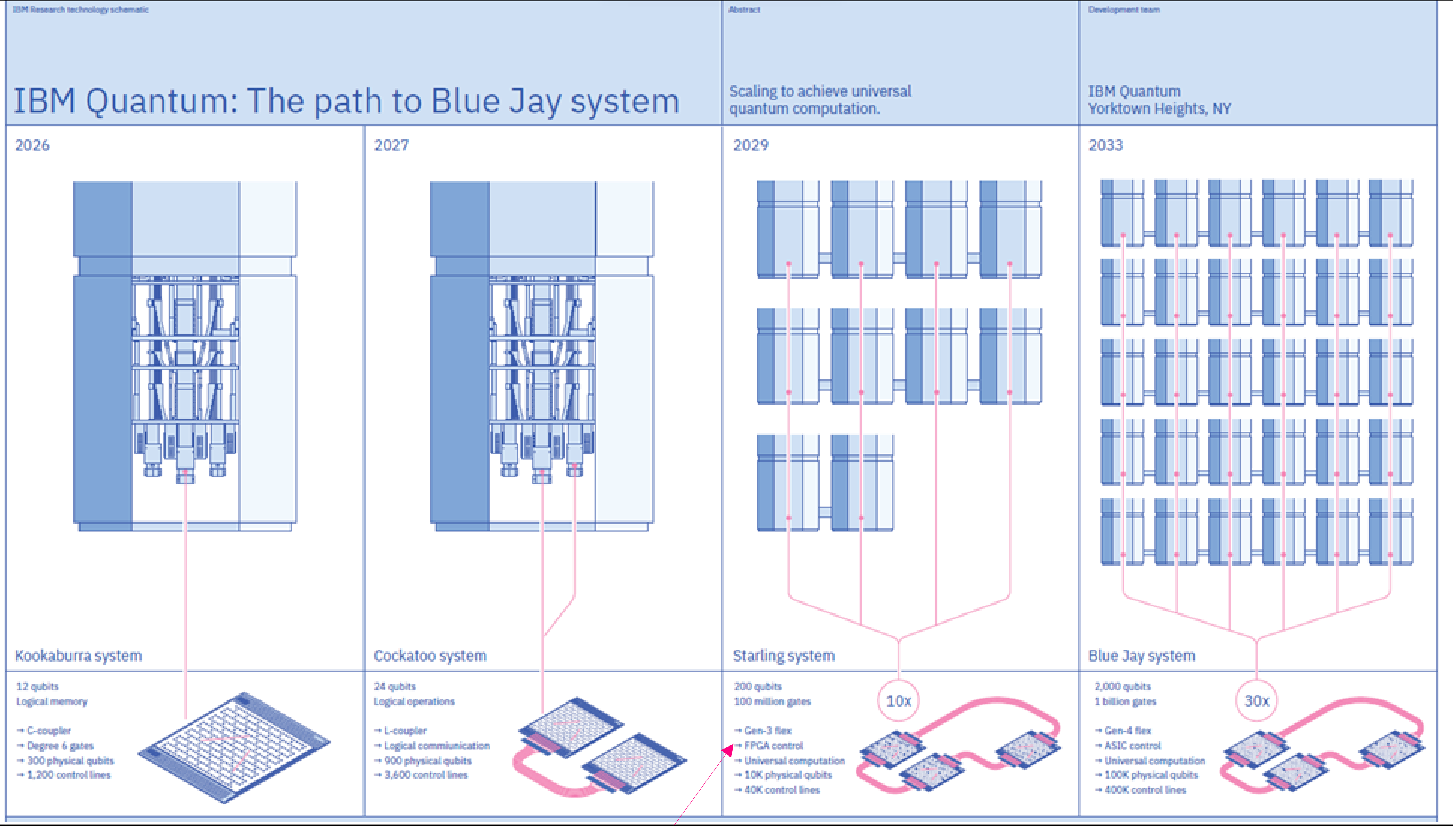


Google

<u>Different Approaches:</u>

- Superconducting qubits (pics)
- Trapped Ions
- Quantum dots
- Photons
- Others

Quantal Technology LLC



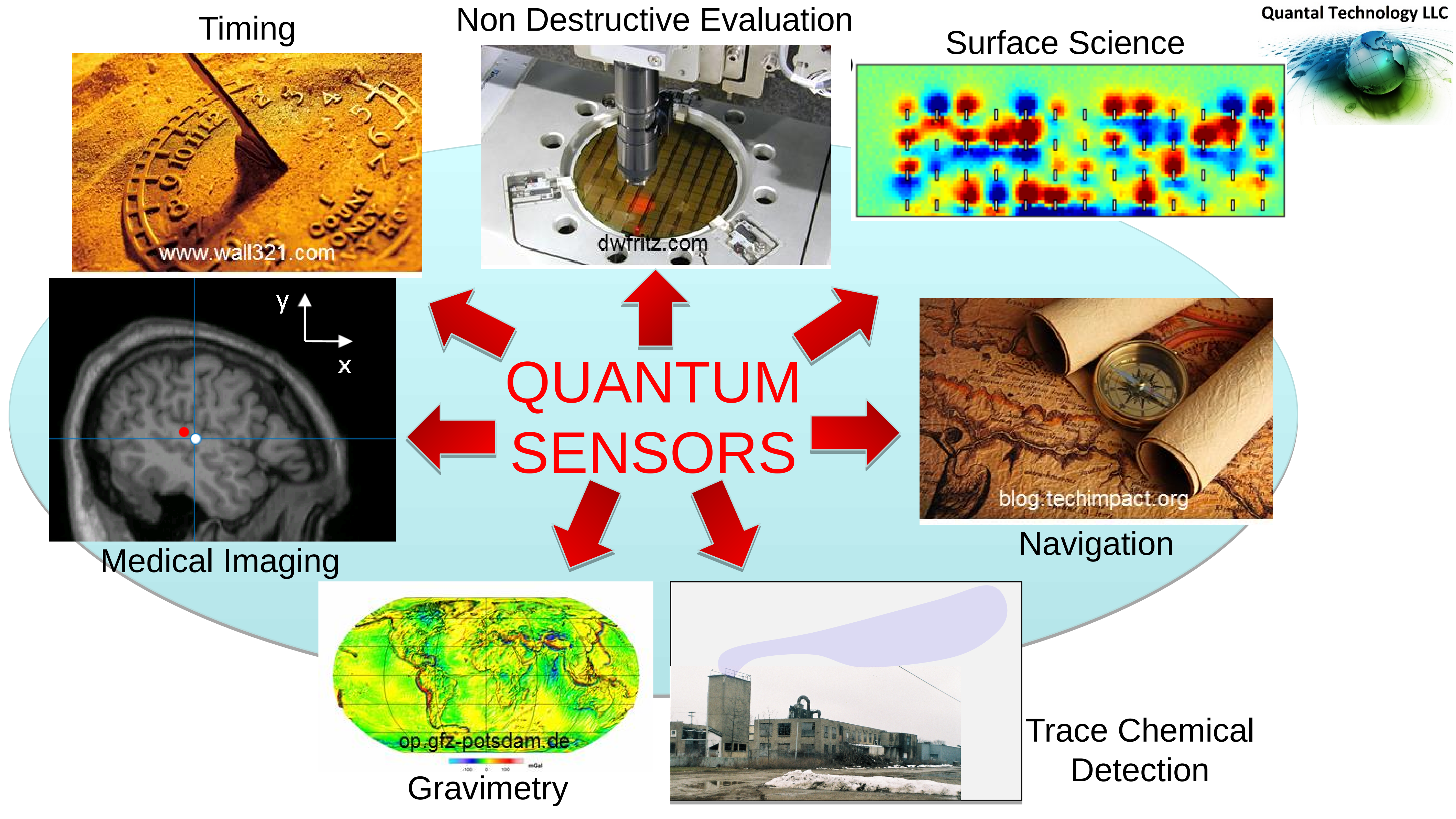
“FPGA control”

Quantum Algorithms

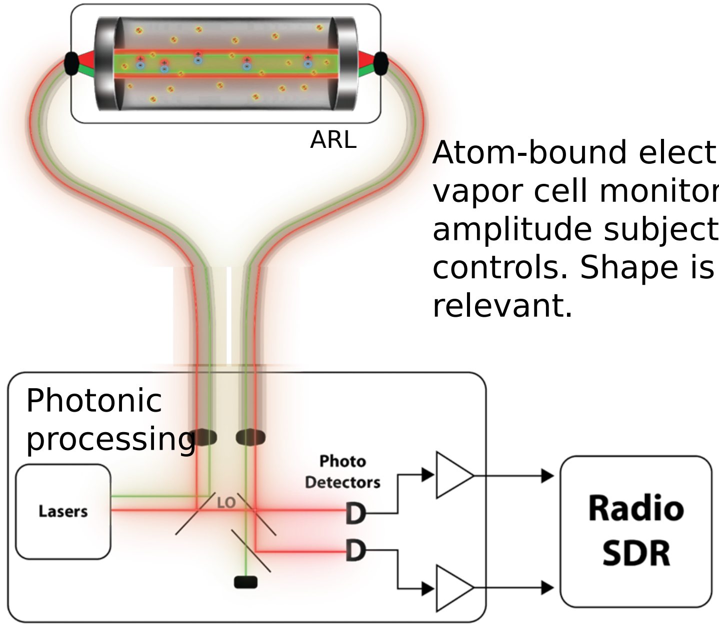
Quantum computers are useless without quantum algorithms (software):

- Currently requires expert knowledge in quantum mechanics and applications
- Only a handful of algorithms have been developed that would make a QC better than a classical computer
  - Shor’s Algorithm (breaks public-key encryption)
  - Grover’s Algorithm (sort a large database faster)

Company	Quantum Software Development Kit (QSDK)	Language	License
Microsoft	Microsoft Quantum Development Kit	Q#	MIT
Google	Cirq	Python	Apache 2
IBM	Qiskit	Python	Apache 2
Rigetti	Forest	Python	Apache 2


Quantal Technology LLC
Timing
www.wall321.com
Non Destructive Evaluation
dwfritz.com
Surface Science
QUANTUM
SENSORS
y
x
Medical Imaging
blog.techimpact.org
Navigation
op.gfz-potsdam.de
Gravimetry
Trace Chemical
Detection

Quantum "Antenna" or Aperture Established circa 2010



Atom-bound electrons in a vapor cell monitor RF amplitude subject to laser controls. Shape is not relevant.

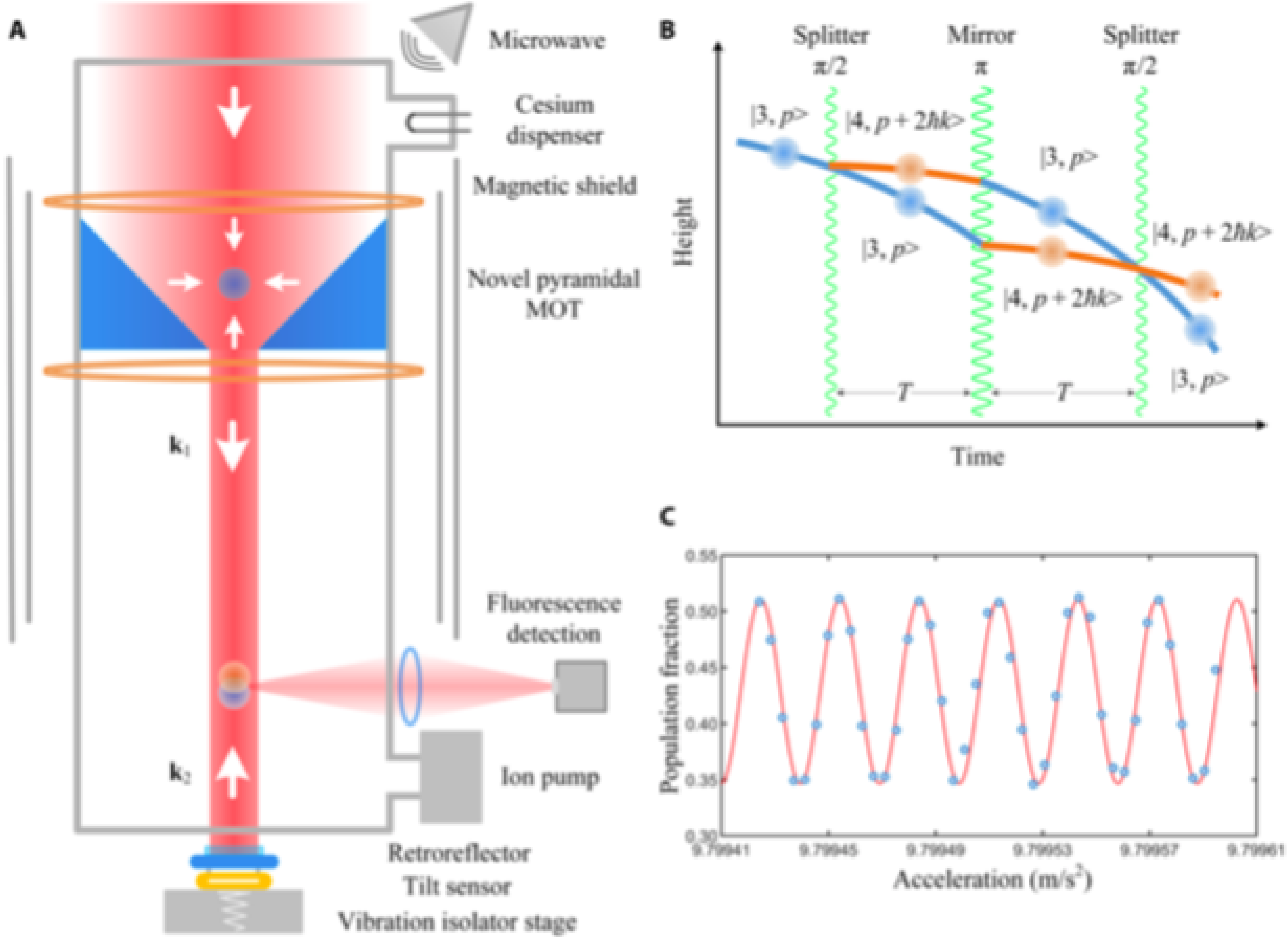
Receive only without inherent "gain"

DARPA Envisioned Program End State

Different Physics and Different Limits = Large Opportunity

DARPA *Quantum Apertures* Program

Atom Interferometry ("Quantum Gravity Sensor")

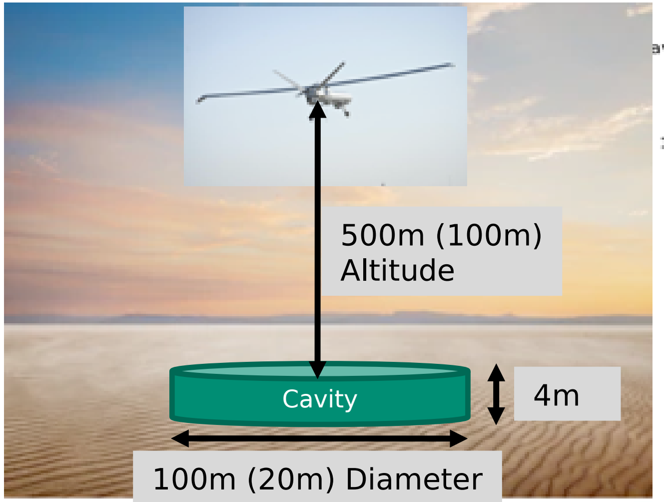


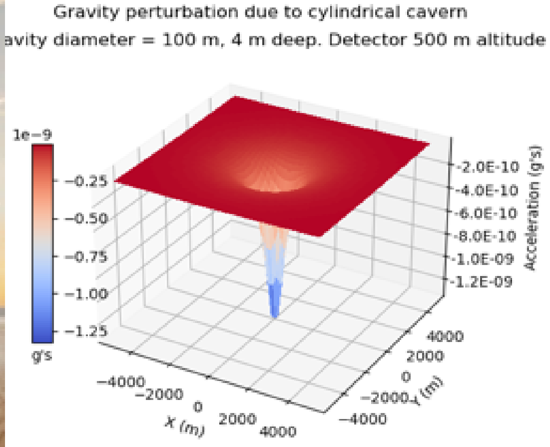
Quantum Gravimetry

Quantal Technology LLC

Detect Underground Structures

- Gravimetric signatures are always present as mass cannot be shielded
- Gravimetric methods based on atom interferometry may offer a solution for rapid, sensitive detection of buried structures



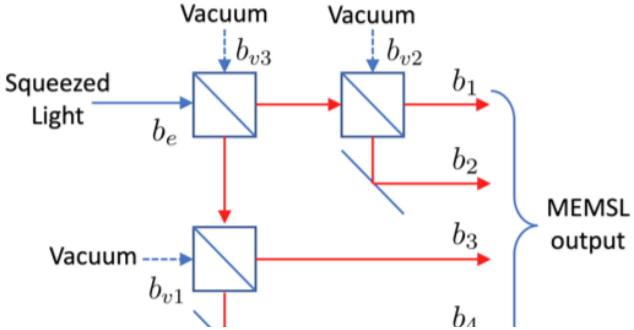


Muquans Instrument

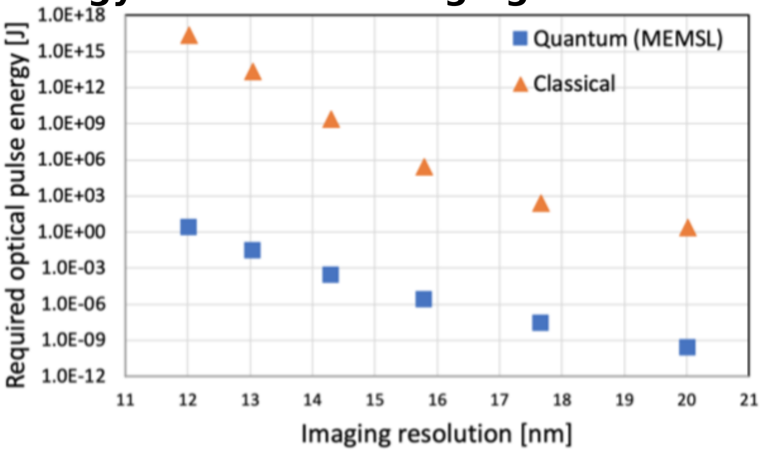
Quantal Technology LLC

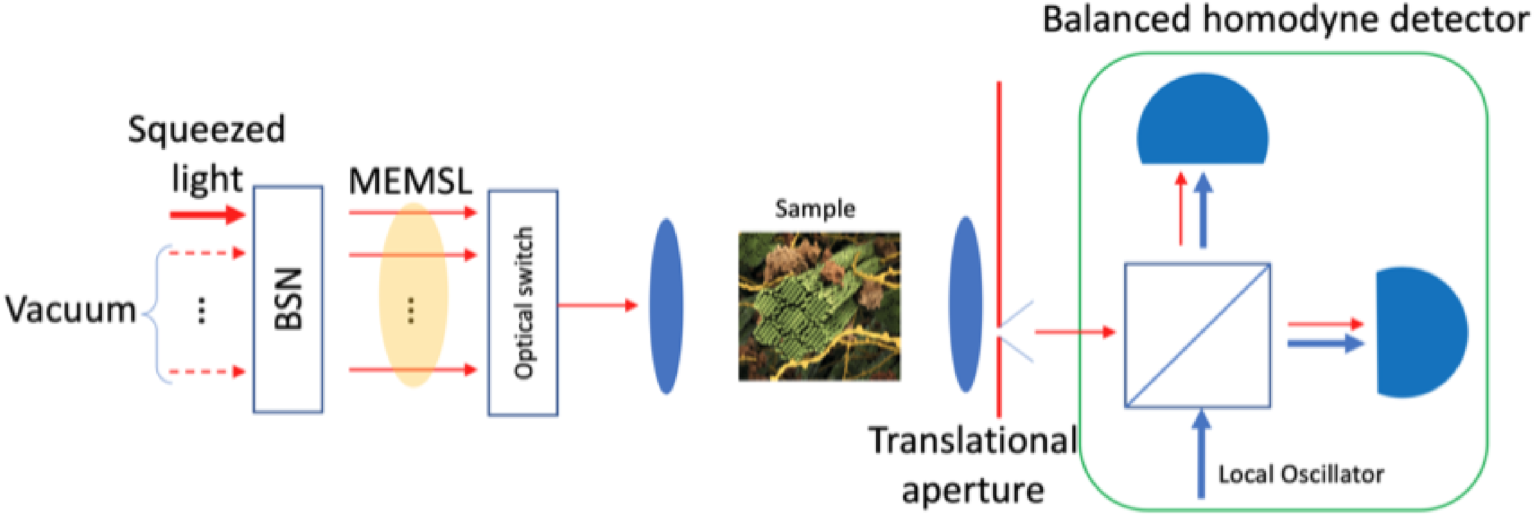
Quantum Imaging using Massively Entangled Multimode Squeezed Light (MEMSL)

Generation of a MEMSL source using a Beam Splitter Network



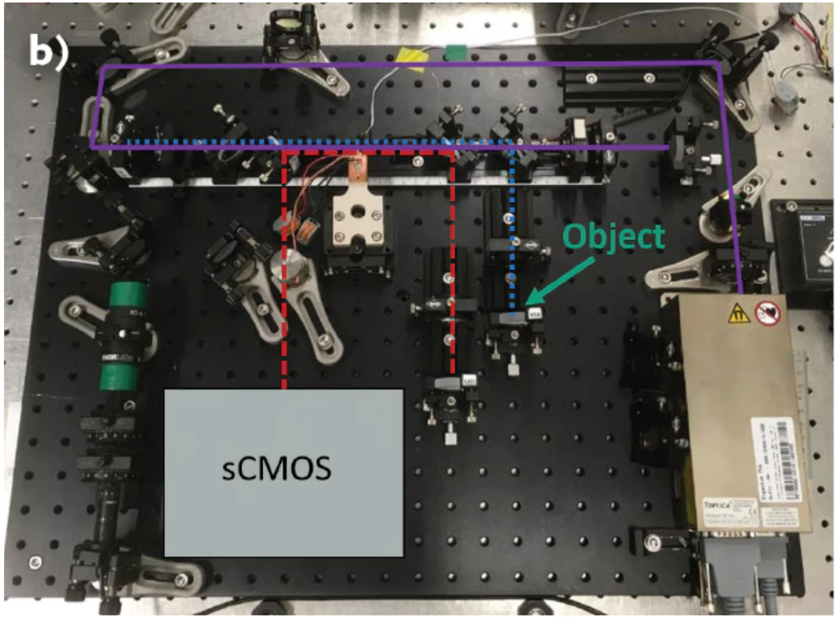
Calculated required optical pulse energy vs. desired imaging resolution

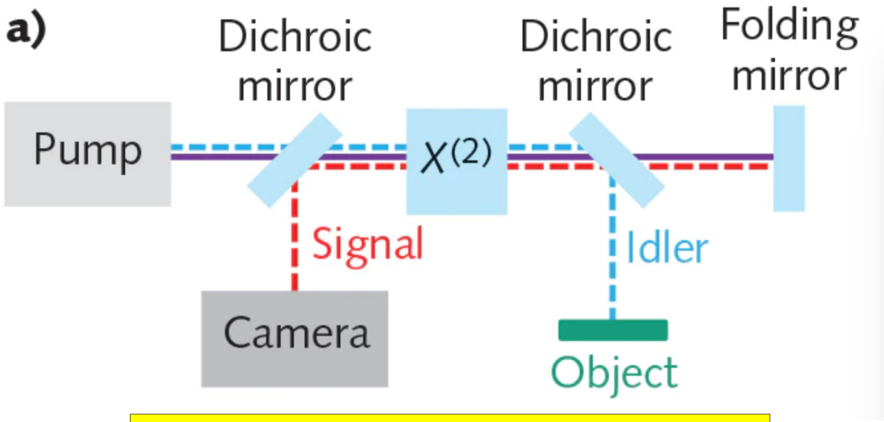




Quantum “Ghost” imaging

Quantal Technology LLC



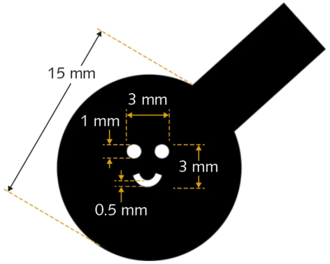


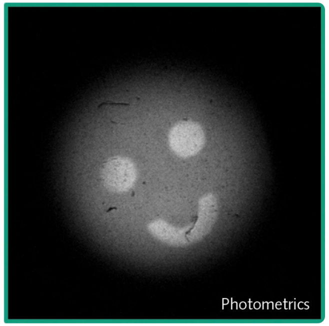
Entangled photon source

Quantum imaging with undetected photons

Gabriela Barreto Lemos, Victoria Borish, Garrett D. Cole, Sven Ramelow, Radek Lapkiewicz & Anton Zeilinger

Nature **512**, 409–412(2014) | Cite this article



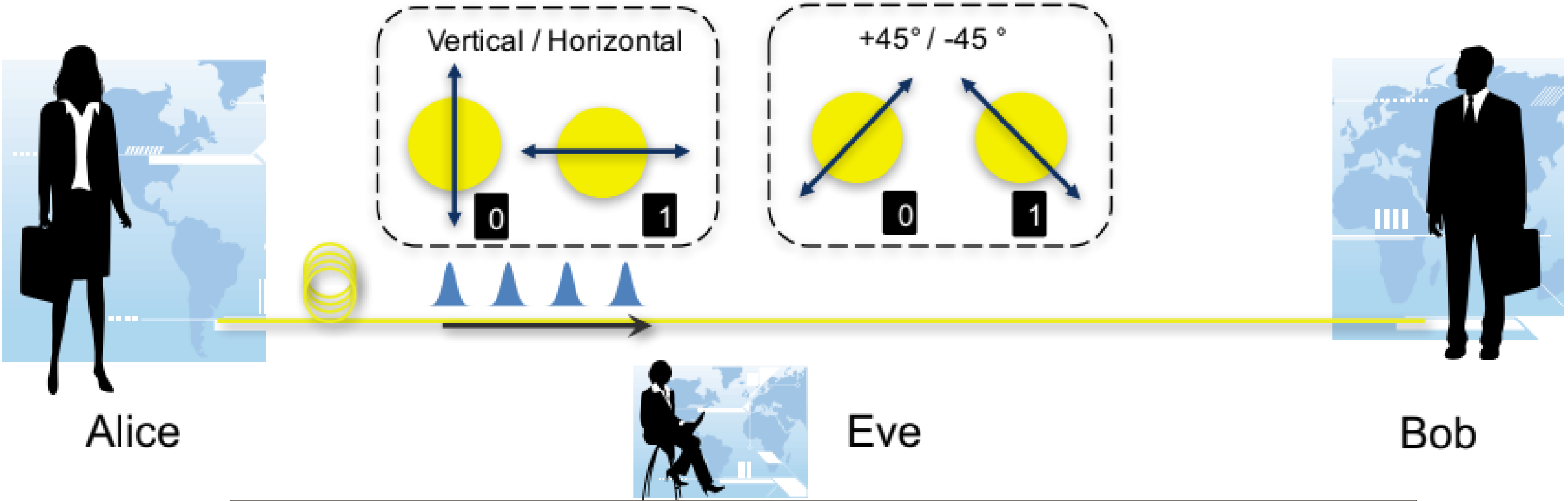


Target

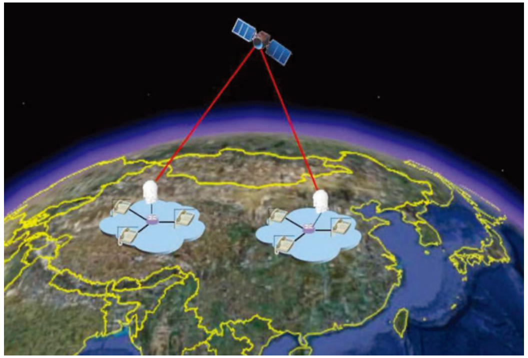
Image of target
in other spectral region

Quantal Technology LLC

Quantum Key Distribution (QKD) – “Quantum Encryption”



Secure because can detect Eavesdropper ”Eve”, who disrupts the quantum state



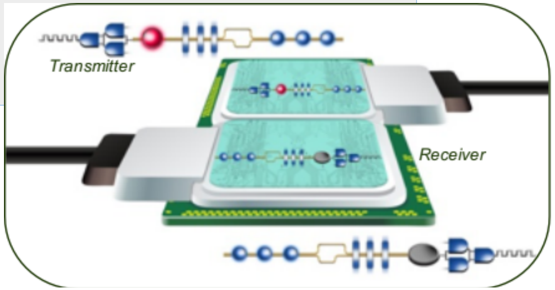
China’s Micius satellite sets distance record for quantum entanglement in space

Part of ambitious Chinese program: Quantum Experiments at Space Scale (QUESS; Chinese: 量子科学实验卫星)

QKD requires hardware unlike Public Keys, but significant software processing needed

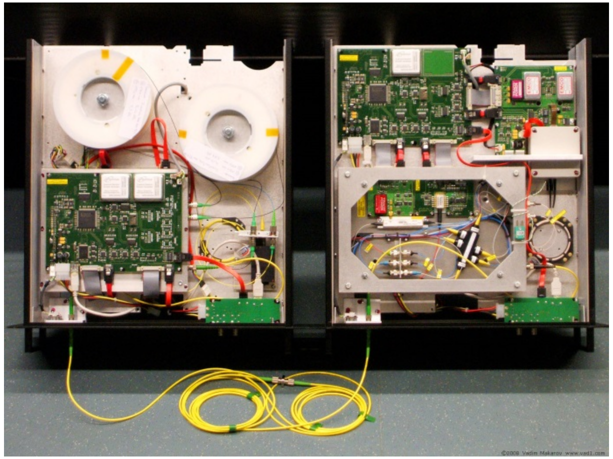
Unlike current data encryptions standards, which are software-based (e.g. RSA, AES, SHA), QKD relies on hardware:

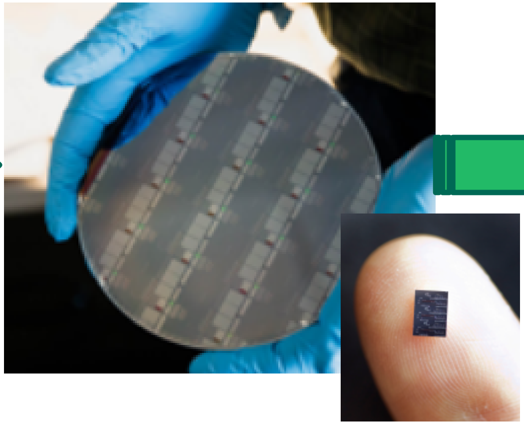
- Lasers (single photon or traditional laser)
- Detectors (single photon or homodyne)
- Fiber optics
- High-speed modulators

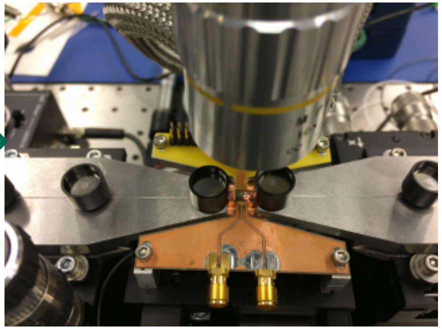


Trend is to put all components on a photonic chip

ID Quantique Clavis QKD System (Swiss)

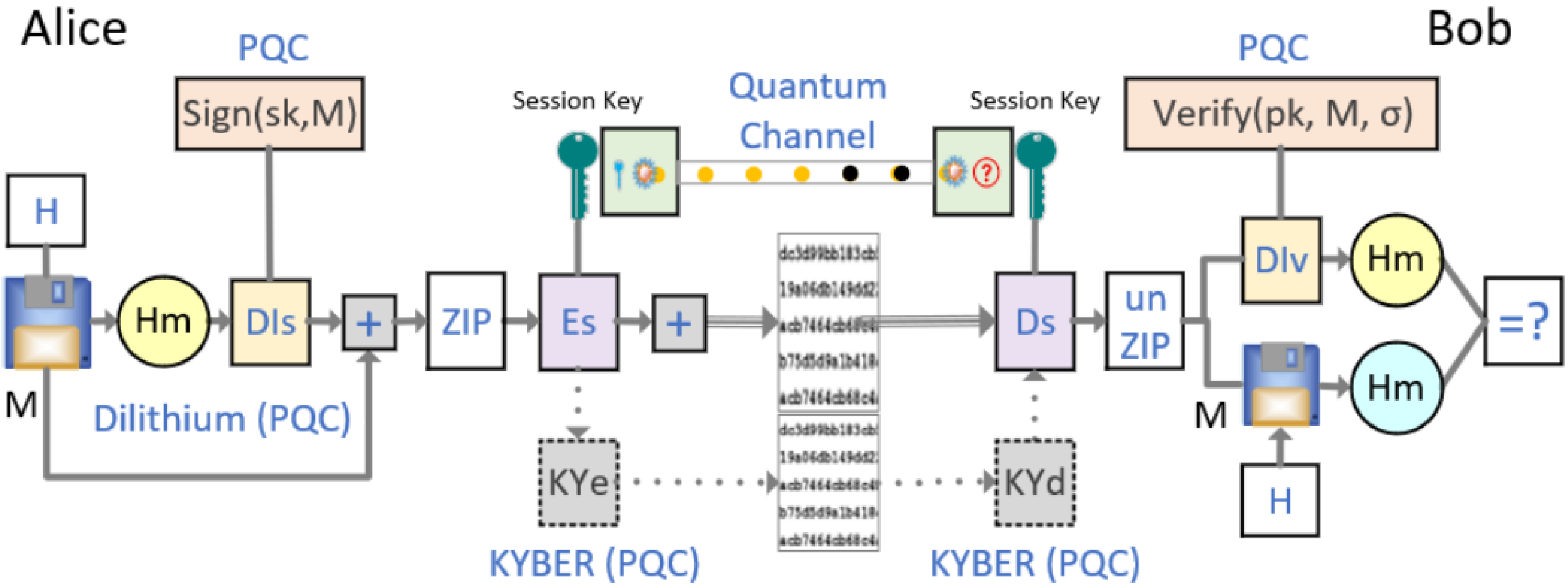






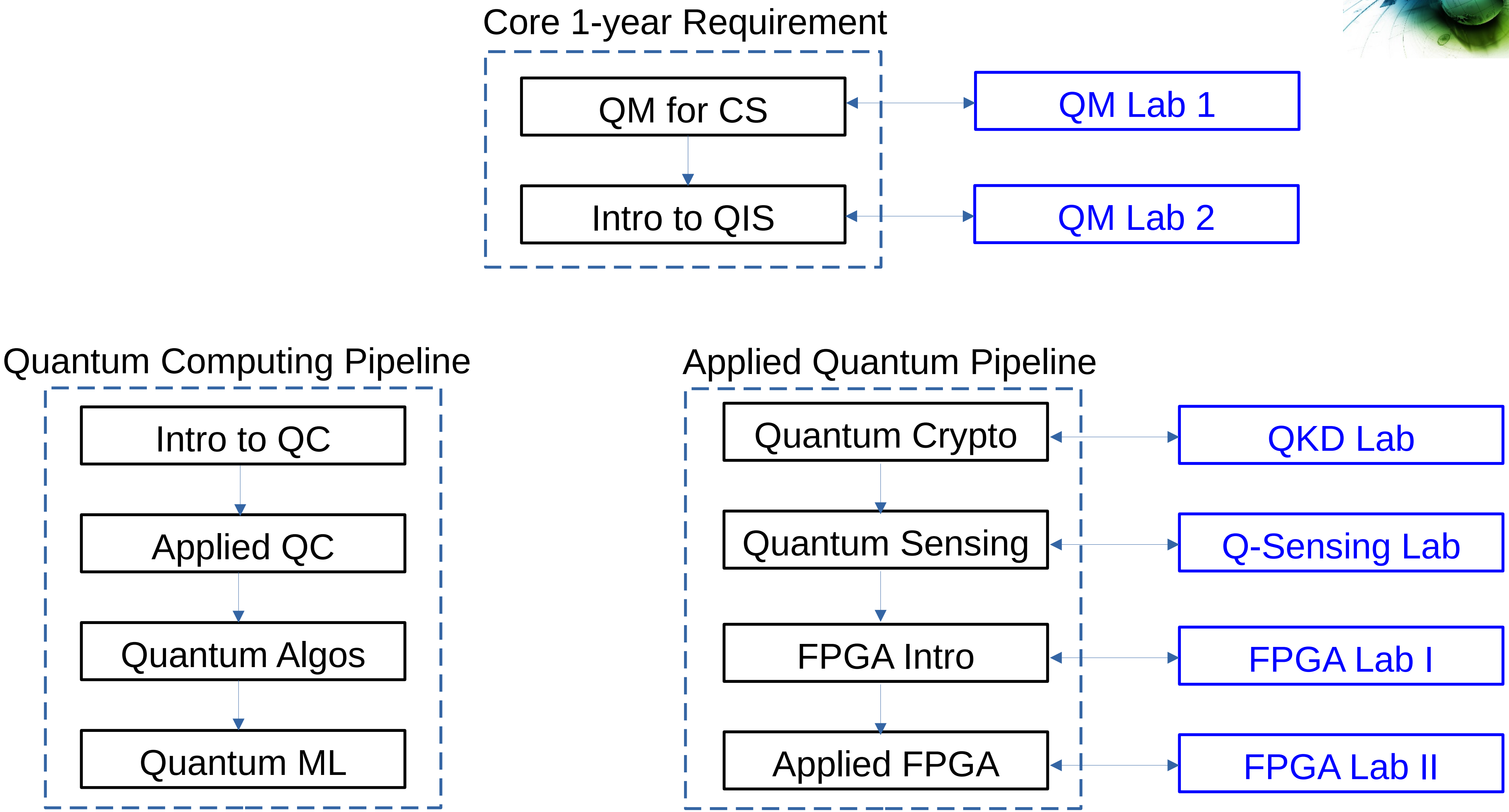
Quantal Technology LLC

Quantum Good Privacy at Morgan State University



QGP Authentication Protocol Diagram. M: Message, H: Hash Functions (SHA 2/3), Hm: Hashed message, Dis/Div: Dilithius Sign/Verify (PQC), ZIP/unZIP: Compression/Decompression, Es/Ds: Symmetric Key Encryption/Decroption, KYe/KYd: KYBER Encryption/Decryption (PQC)

Quantum Courses Progression



Extras