Potential Quantum Networking Applications

Panagiotis Spentzouris

Quantum Internet Blueprint Workshop

February 5-6, 2020

The Quantum Internet

- What will it do
  - Connect any 2 points on earth via quantum communications
- How will it do it
  - Interconnect nodes based on heterogeneous set of technologies
  - Enable the realization of a diverse set of quantum protocols that will allow quantum resources (sensors, processors, …) to form networks to achieve capabilities beyond what is achievable through classical means
    - A network of quantum networks (over arbitrarily long distances)
    - Most likely operating in parallel with the classical internet
- Why build it (what are these capabilities/applications that could go beyond what is classically achievable)
  - We discuss these applications in the context of specific networks that enable some function, with specific requirements on technology, fidelity, and operations

Evaluating/establishing application requirements

- Understand fundamental physics motivation (e.g. does quantum entanglement provide an advantage)
- Requirements of quantum protocols (in the ideal case)
- Technological constraints due to quantum hardware (and incremental path to utilize near-term hardware)
- Characterize and chart evolution of networks based on tolerance to loss and errors
  - needed minimum rate probability of loss, inaccuracy of transmission and measurement
- Most application protocols have only been analyzed for perfect parameters.
  - exact requirements of real-world application of these protocols need to be determined
    - Investigations to study/understand real vs ideal operations possibly needs a co-design approach utilizing testbeds and possibly simulation

Secure Quantum Communications

- Potential applications include banking, national security, energy delivery infrastructure, securing PID and other sensitive data, VoIP, …
- Quantum Key Distribution is the main research area in this domain
  - only existing method that allows establishment of cryptographic keys with proven security through an insecure communication channel
  - Many protocols (for a range of applications) with different requirements
- Some classes of use cases have less stringent requirements than those of a fully developed Quantum Internet and have already being deployed (fiber –metropolitan, and via satellite)
  - Requiring standard optical components and sources, with some protocols also incorporating Bell State Measurements

Secure Quantum Communications

- Trusted repeater (node) network applications (digital signature authentication for e.g. VoIP, teleconferencing, already demonstrated)
  - Point-to-point communication using short-distance intermediate nodes that utilize QKD pairwise to generate key
  - Does not require end-to-end transmission of qubits or generation of entanglement
  - Relies on trust in the intermediary nodes (assumes they are secure for eavesdropping)
- Does not address:
  - control issues in quantum networks for end-to-end qubit delivery
  - generation of long-lived entanglement.

Tokyo QKD network

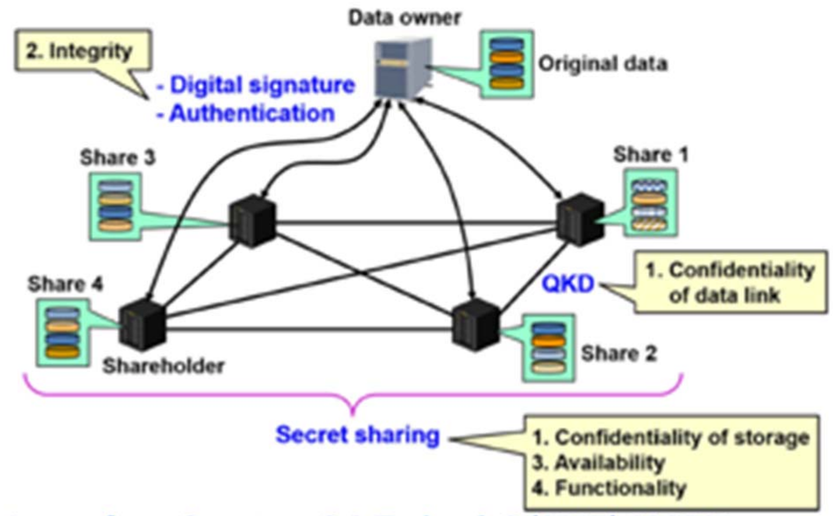


Image from Quantum Sci. Technol. 2 (2017) 020501

Fermilab

Secure Quantum Communications

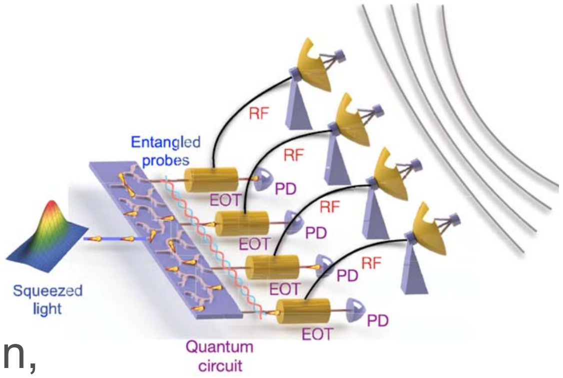
- Applications in prepare and measure schemes: QKD, two-party cryptography, …
  - Secure encryption key, transactions between non-trusted nodes
- Prepare and measure networks are the first building block for a general purpose quantum internet
  - Providing (or, requiring) end-to-end quantum functionality for their operations
- Transmission and measurement could be post-selected
- Qubits are immediately measured to produce classical correlations.
  - no quantum memory is needed at the nodes
  - nodes required to be able to act on single qubits only
- Requires generation of many qubits (sequentially)
- Applications making use of this network can tolerate timing fluctuations, qubit loss, and errors
  - With requirements depending on the specifics of the application

Blind Quantum Computing

- Compute on encrypted data without the compute resource gaining any information on the data or the operations on them. Data that require such security include medical records, credit card information, trade secrets, and sensitive government information
  - Cloud security affects virtually anyone who uses computing resources today
- Requires a simple quantum node capable of preparing and measuring single qubits and a quantum network that allows a (remote) client to communicate with the quantum computing server
  - The network has to support entanglement generation for any 2 end-nodes, qubit measurements at the node, qubit operations at the node, qubit storage at the node for at least the amount of time necessary to ensure quantum link establishment and processing of the information on the computer
    - Quantum memory and repeater nodes, entanglement distribution and swapping, routing

Quantum Sensor Networks

- A sensor network exploits the correlations across the sensors to enhance the sensitivity and measurement capabilities of the system, with potential applications measurements that require
  - estimating many parameters at once (or a function of those parameters), e.g. nanoscale nuclear magnetic resonance imaging
  - measuring global parameters e.g. mapping magnetic fields, phase imaging, precision clocks
- In general, sensor networks require end nodes with local memory and controls that allow implementation of complex protocols, multipartite entangled states, entanglement distillation, and deterministic teleportation
- Both discrete-variable (DV) and continuous-variable (CV) multipartite entanglement protocols have been developed
- Demonstration using entangled radiofrequency (rf) photonic sensor network with multipartite CV entanglement to enhance precision of measuring the rf wave's properties.
  - A concept demonstrator, not a general sensor network use case (no repeater or memory employed)



Networks of atomic clocks

- A network of atomic clocks could achieve transformational improvements in precision and security over conventional classical solutions
  - Standalone atomic clocks already perform close to the SQL
  - quantum-correlated states of remote clocks yield the best possible clock signal allowed by quantum theory for the combined resources
- Applications of such networks enable
  - a world platform for time and frequency metrology
  - improved gravity models for earth sciences
  - investigations of fundamental laws of nature, such as relativity, the connection between quantum and gravitational physics
  - Searches for macroscopic dark matter objects
- Realization of such a quantum network requires a number of advances in quantum network technology
  - quantum links with high repetition rate and fidelity capability for entanglement distribution
  - quantum repeaters and entanglement purification approaches.
  - Applications could involve space flight capable nodes, generating additional technology development requirements.

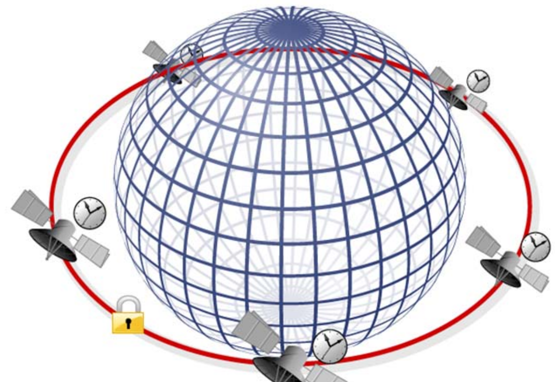


Image from *Nat. Phys.* **10**, 582–587 (2014)

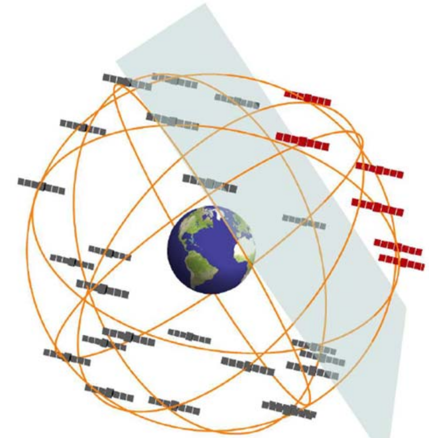


Image from Nat Commun **8,** 1195 (2017).

Networks enabling sensor phase information transfer

- Applications take advantage of improved baseline for interference measurements of optical and IR interferometric telescope arrays
  - studies of active galactic nuclei, improved sensitivity parallax measurements to enhance knowledge of stellar distances, and imaging of extra-solar planets.
- Initial concept involved long-baseline optical telescopes, requiring
  - quantum teleportation and quantum repeaters
  - entanglement distillation and repeater protocols to control noise and losses.
- A more recent approach employs quantum memories allowing for
  - relaxation of the entanglement rate requirements
  - also extending applicability to more than two sites.
- Fundamental physics applications: assuming discovery of dark matter waves, determine instantaneous wave fronts and directions of propagation to map their distribution in the galaxy.
  - spatially extended wave front manifests as non-local correlations in the field displacements at distributed detector sites

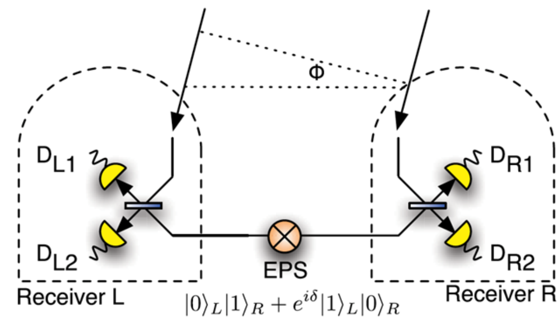


Image from PRL 109, 070503 (2012)

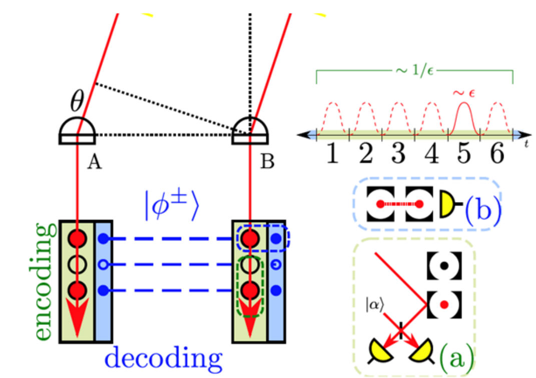


Image from Phys. Rev. A 100, 022316

Fermilab

Distributed Quantum Computing

- Distributed memory many-computer architecture
  - Memories, repeaters supporting necessary depth of operations at each node
  - Local operations have to be performed fault-tolerantly
- Quantum computers that can arbitrarily exchange quantum communication at any distance
- At this stage of the network any protocol should run, enabling any quantum computing application
  - Creating a market for quantum computing services
  - Both science and quality-of-life transformational applications possible
- What are appropriate test beds? Error tolerances for early application deployment (e.g. NISQ processors in close proximity)?

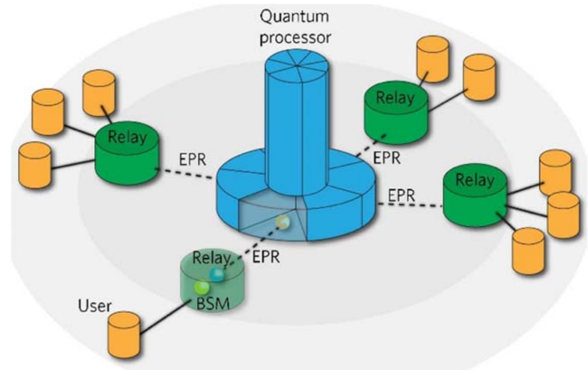
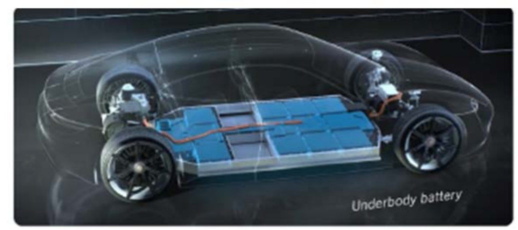
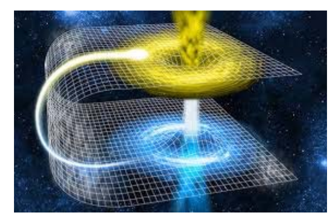


Image from *Nature Photon* **10,** 671–675 (2016). https://doi.org/10.1038/nphoton.2016.179





Quantum Network evolution timeline

- Define stages of quantum internet development based on the requirements for the specific network functionality
- For each stage incorporate R&D for optimizing performance
  - Including deployment specifics (distance, scale)

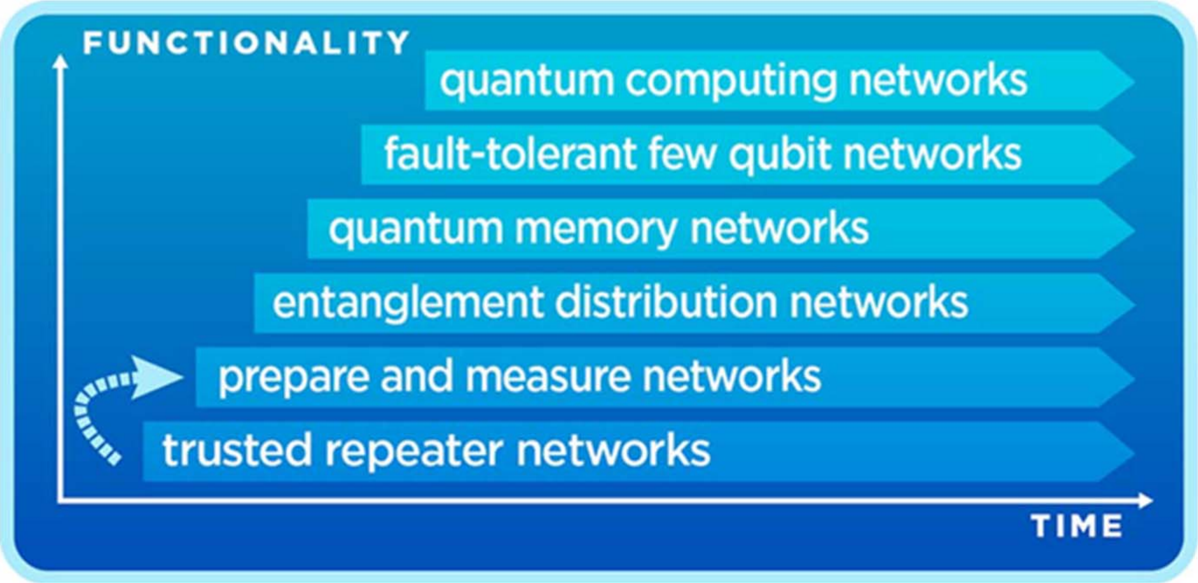


Image from Science 19 Oct 2018: Vol. 362, Issue 6412, eaam9288

- Goal to transform time ordered stack to a timeline with milestones, including R&D, testbeds, and demonstrators

Outlook

- Many exciting, potentially transformative quantum network applications that will be enabled by the quantum internet
  - Underpinned by quantum network technologies
- The ultimate goal is to deploy infrastructure with the flexibility to serve all use cases, including supporting multiple applications at the same time.
- Since no (generic) quantum network has been realized to date, we cannot study actual usage behavior
  - resort to studying properties of application protocols and insights from experiments and technology demonstrators
- To fill the gaps, the Quantum Internet Blueprint could include deployment of testbeds to co-develop technology and application protocol
  - testbeds that could evolve as the seeds for the Quantum Internet