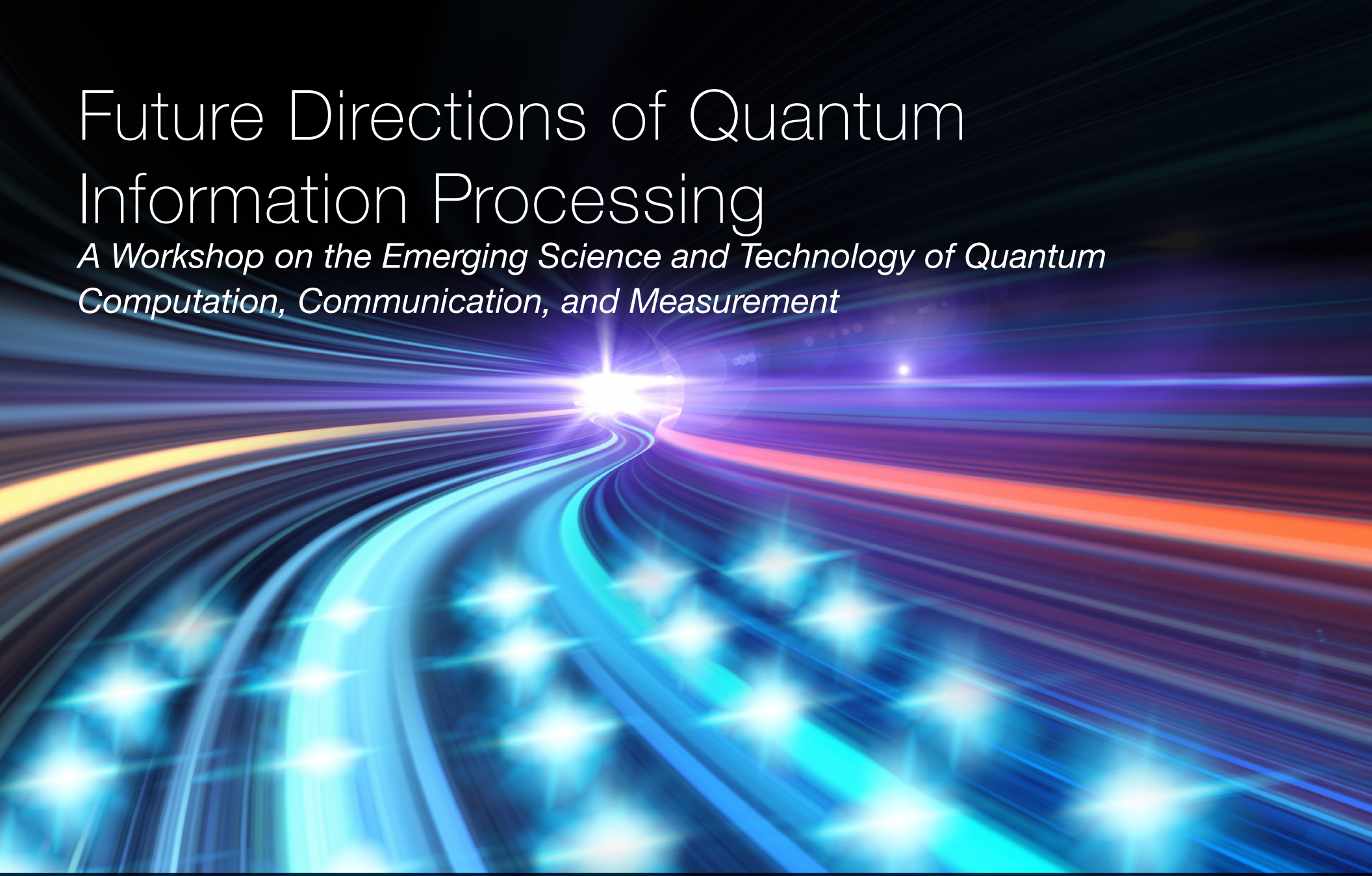
Future Directions of Quantum Information Processing

A Workshop on the Emerging Science and Technology of Quantum Computation, Communication, and Measurement



Seth Lloyd, *Massachusetts Institute of Technology*
Dirk Englund, *Massachusetts Institute of Technology*
Prepared by Kate Klemic Ph.D. and Jeremy Zeigler
Virginia Tech Applied Research Corporation

Workshop funded by the Basic Research Office, Office of the Assistant Secretary of Defense for Research & Engineering. This report does not necessarily reflect the policies or positions of the US Department of Defense

VT-ARC
Virginia Tech
Applied Research Corporation

Innovation is the key to the future, but basic research is the key to future innovation.

–Jerome Isaac Friedman,
Nobel Prize Recipient (1990)

Preface

Over the past century, science and technology have brought remarkable new capabilities to all sectors of the economy; from telecommunications, energy, and electronics to medicine, transportation and defense. Technologies that were fantasy decades ago, such as the internet and mobile devices, now inform the way we live, work, and interact with our environment. Key to this technological progress is the capacity of the global basic research community to create new knowledge and to develop new insights in science, technology, and engineering. Understanding the trajectories of this fundamental research, within the context of global challenges, empowers stakeholders to identify and seize potential opportunities.

The Future Directions Workshop series, sponsored by the Basic Research Office of the Office of the Assistant Secretary of Defense for Research and Engineering, seeks to examine emerging research and engineering areas that are most likely to transform future technology capabilities.

These workshops gather distinguished academic and industry researchers from the world's top research institutions to engage in an interactive dialogue about the promises and challenges of these emerging basic research areas and how they could impact future capabilities. Chaired by leaders in the field, these workshops encourage unfettered considerations of the prospects of fundamental science areas from the most talented minds in the research community.

Reports from the Future Direction Workshop series capture these discussions and therefore play a vital role in the discussion of basic research priorities. In each report, participants are challenged to address the following important questions:

- How might the research impact science and technology capabilities of the future?
- What is the possible trajectory of scientific achievement over the next 10–15 years?
- What are the most fundamental challenges to progress?

This report is the product of a workshop held August 25-26, 2016, 2016 at the Basic Research Innovation and Collaboration Center in Arlington, VA on the Future Directions of Quantum Information Processing. It is intended as a resource to the S&T community including the broader federal funding community, federal laboratories, domestic industrial base, and academia.

Executive Summary

At the most microscopic level, all physical systems are governed by the laws of quantum mechanics. Quantum information processing is the study of how information is gathered, transformed, and transmitted at the quantum level—in atoms, ions, photons, elementary particles, and microscopic solid state systems, which obey fundamentally quantum mechanical laws. Quantum computers, quantum communication channels, and quantum sensors are devices that can attain the ultimate limits of information processing.

The laws of quantum mechanics give rise to counterintuitive effects. Quantum information processors use "*quantum weirdness*" to perform tasks that classical information processors cannot. Quantum computers are being conceived that will process information stored on atomic, optical, and solid-state systems: they aim to use counterintuitive effects such as quantum superposition and entanglement to perform tasks such as quantum simulation, quantum search, and factoring/code breaking to solve problems that are hard or impossible on conventional classical computers. Quantum communication systems transmit information encoded in individual photons: they exploit the fact that quantum measurement is inevitably stochastic and destructive to enact quantum encrypted communication whose security is guaranteed by the laws of physics. Quantum sensors and measurement devices operate at the greatest possible sensitivity and precision allowed by physical law: from magnetometers, to quantum clocks, to advanced gravitational interferometers (e.g., LIGO), quantum metrology supplies the techniques required to push measurement to its ultimate limits.

On August 25-26, 2016, 25 distinguished experts in quantum information processing from academia, industry and government gathered in Arlington, VA for the "Future Directions in Quantum Information Processing" workshop to discuss and debate the current state-of-the-art of this important emerging field and to identify challenges and opportunities for the next 5, 10 and 20 years.

The workshop was organized to encourage lively discussion and debate through a series of small breakout sessions that focused on the three sub-fields of quantum information processing: quantum computing, quantum communication, and quantum sensing and metrology. After each breakout session, the whole group reconvened in plenary sessions to discuss common themes and technological requirements.

The participants reviewed the rapid advances made in quantum information theory and experiment over the past few decades that will shortly produce quantum computers that exceed the capabilities of classical computers; quantum communication systems that supply secure cryptography and push towards the fundamental physical limits of optical communication; quantum sensors and measurement devices representing the world's most accurate atomic clocks and positioning devices. Driven by the rapid development of quantum technologies, the expectation is that the next several decades will give rise to dramatic advances in quantum information processing.

The participants discussed the challenges and opportunities for quantum information processing and mapped the research trajectory over the next 5, 10, and 20 years:

5-year goals:

- The construction of small-scale quantum computers with 50-100 qubits capable of performing 10^4 coherent quantum logic operations.
- The development of highly coherent special purpose quantum information processors such as quantum simulators, quantum annealers, and integrated quantum optical circuits with hundreds or thousands of qubits.
- The demonstration of quantum repeaters to extend the range of quantum communication channels.
- The development of quantum sensing and metrology systems that use entanglement and squeezing to surpass the performance of semi-classical devices which are limited by the standard quantum limit.

10-year goals

- The construction of general purpose quantum computers with 100-1000 qubits, combined with the ability to perform 10^5 quantum logical operations on multiple qubits
- The demonstration of long-distance quantum communication channels consisting of multiple quantum repeaters, surpassing repeaterless quantum cryptography bounds
- Demonstration of long-distance networked quantum metrology.

20-year goals

- Large-scale general purpose quantum computers operating in a fully fault tolerant fashion and capable of factoring large numbers.
- Large-scale special purpose quantum simulators and annealers; and quantum transducers to photonic communication channels.
- Global quantum internet
- Space-based quantum GPS and global quantum clocks to provide universal sub-millimeter positioning accuracy.

To realize these ambitious goals will require a concerted effort to develop novel theoretical understandings of quantum information processing, to create tools for quantum Characterization, Validation, and Verification (qCVV), and to train a new generation of quantum technologists and engineers.

In addition to discussing important research challenges, the participants considered the importance of advances in infrastructure, including facilities in national and other government laboratories. Industrial development of quantum information processing technologies has recently expanded dramatically, with companies such as Google, Microsoft, and Intel joining in the long-term investment pioneered by IBM. Multiple quantum startups have also come into existence in the last few years. Nonetheless, the greatest support for the fundamental science of quantum information processing has come from governments. The United States government was an early supporter, but support outside of the U.S. has picked up pace. The UK, the European Union, Canada, Australia, and China recently embarked on high-profile research efforts in quantum information processing, with total commitments of over $2 billion over the next 5-10 years.

The participants were in unanimous agreement on their vision of the future of quantum information processing: Quantum technologies will play a dominant role in the development of powerful computers, secure and high-rate communication, and hyper-accurate sensors and imaging systems. The interplay between quantum information theory and experiment will create powerful new tools for understanding and harnessing fundamental phenomena, ranging from solid-state physics, to elementary particles and quantum gravity, to quantum chemistry and biology.

Introduction

One of the most remarkable scientific developments of the last few decades is the recognition that quantum information theory is a universal language for the behavior of quantum systems. Quantum information theory and technology represent the bold attempt to construct systems that gather, process, and transmit information at the fundamental limits posed by the laws of physics. At bottom, all current technologies for classical computation, communication, sensing and measurement are governed by the laws of quantum mechanics. Quantum mechanics determines the properties of semiconductors, the dynamics of lasers and amplifiers, and the accuracy of *interferometers* and clocks. For the developers of current technologies, quantum effects are often a nuisance: quantum tunneling induces leakage current in transistors, quantum noise adds uncertainty to signals, and quantum effects limit the precision of measurements of time, space, and magnetic fields. The theory and practice of quantum information processing show that such quantum effects are not bugs, but rather features that can be taken advantage of: quantum mechanics can be used to tune the properties of electron transport in solid state systems, to attain the quantum limits of communication and amplification, and to surpass the standard quantum limits to measurement.

By understanding the properties of counterintuitive quantum effects such as entanglement—Einstein's "spooky action at a distance"—quantum information opens up the road to performing computations such as Shor's factoring algorithm that accomplish tasks for which no efficient classical algorithms are known, to communications whose security is guaranteed by the laws of quantum mechanics (*quantum cryptography*), and to measurement devices such as Wineland's quantum logic clock and NV-based nanoscale sensors that use *entanglement* to attain unprecedented accuracy and precision. Realizing the full power of quantum information processing technologies to construct large scale *quantum computers*, a quantum internet, and globally linked quantum clocks (*quantum GPS*), will dramatically transform the ways in which information is gathered, processed, and communicated. **Achieving the full potential of quantum information processing would result in unhackable computer systems, quantum machine learning techniques that can find patterns that are inaccessible to any classical learning method, GPS that determines position at the sub-millimeter scale, inertial guidance and navigation systems that maintain the precision of GPS over weeks, and detection and imaging systems that surpass the Rayleigh diffraction limit by orders of magnitude.**

Historical development of quantum information science

The study of quantum mechanics began in 1900, when Max Planck showed that light came in discrete chunks, or 'quanta'. Planck's discovery implies that, at bottom, nature is digital: only a discrete and finite set of elementary particles, atoms, and molecules exists. However, while the building blocks are discrete, nature is not only digital. Planck showed that phenomena that we think of as continuous, such as waves, were actually composed of particles. But quantum mechanics also implies that discrete objects—particles—are associated with continuous waves. This wave-particle duality means that quantum information possesses a richer structure than classical information. In the mid-1920s, Schrödinger and Heisenberg developed the formal mathematical structure of quantum mechanics, and the subsequent half century witnessed a tremendous explosion of understanding of the fundamental quantum properties of matter, including the development of solid-state physics, the invention of the laser based on quantum properties of light, and the completion of the Standard Model for elementary particles in 1972.

Quantum mechanics is the universal theory for the behavior of matter at its most fundamental scales, and it also governs the behavior of information at those scales. The most recent half-century of quantum investigations have revealed fundamental limits on the accuracy and precision with which measurement devices can obtain information about nature—the Standard Quantum Limit, which governs the accuracy of clocks and interferometers in the absence of counter-intuitive

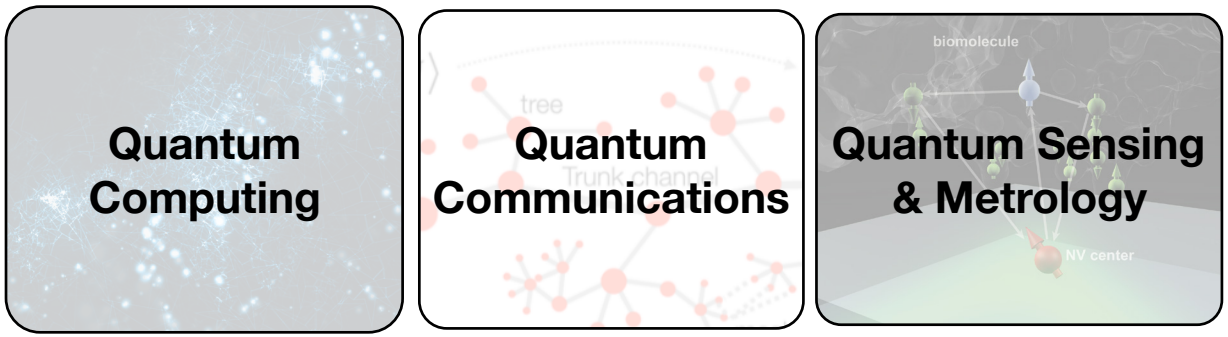


Figure 1. This report is organized around three key areas of quantum information processing: Quantum Computing (including Simulation); Quantum Communications; and Quantum Sensing & Metrology.

quantum effects such as squeezing and entanglement, and the *Heisenberg limit*, which sets the ultimate quantum limits to metrology. The quantum properties of light have revealed the ultimate capacities of communication channels such as free-space communication using radio, microwaves, and light, and of fiber optic communication channels. The fact that measurement inevitably disturbs quantum systems enables quantum cryptography: *quantum communication channels* can be used to distribute secret keys whose security is guaranteed by the laws of physics. Quantum mechanics governs not only the number of bits that can be stored in physical systems, but also the rate at which those bits can flip: quantum mechanics governs the power of computation.

Despite early work by Richard Feynman and David Deutsch, in the early 1990s, only a handful of researchers around the world were working on problems of quantum information; the abstract and esoteric nature of the field, and its apparent lack of practical "applications", generated limited interest in the scientific community. This situation changed dramatically in 1994 when Peter Shor showed that a quantum computer with a few tens of thousands of quantum bits and capable of performing a few million quantum logic operations could factor large numbers and so break the ubiquitous RSA public key cryptosystem. This "killer quantum app" rightly generated huge interest. At the same time, practical designs for building quantum computers were created: arrays of spins, atoms, or *quantum dots* were shown, in principle, to be capable of universal quantum computation via electromagnetic resonance, and models for ion-trap quantum computing were developed. The theoretical physics and computer science communities turned their attention to quantum information, developing a detailed and interlocking set of theories of quantum computation, quantum communication, and quantum metrology. By 2000, it had become clear that quantum information theory provides a universal language for understanding the behavior of quantum systems and for designing and implementing quantum technologies.

The development of quantum technology: To understand the rapid development of quantum information processing technologies over the last quarter century, it is instructive to consider the development of classical information processing technology over the last half century. The progress of classical computation has famously followed 'Moore's law', which can be phrased as the observation that the number of transistors per chip doubles every two years, with individual transistors quickly approaching the fundamental limit of size, single atoms. Moore's law is not a law of nature, but an empirical law of technological development. The semiconductor industry has invested trillions of dollars to maintain this exponential progress. The results are stunning: a smartphone is a more powerful computer than most supercomputers of the 1990s.

The driving forces behind Moore's law are a whole series of 'mini-Moore's laws' operating at the level of improvements in material science, control, precision measurement, and nanomanufacturing techniques enabled by a series of exponential improvements in the understanding of the microscopic properties of matter and energy and our abilities to control them. For example, the manipulation of the band-structures of semiconductors and the fabrication of devices that operate by *quantum tunneling* rely on purely quantum effects; atomic force microscopes allow the imaging of individual atoms; light sources and amplifiers for optical communication operate within fundamentally quantum mechanical constraints; and precision interferometer operate at the standard quantum limit, such as the **L**aser **I**nterferometer **G**ravitational-Wave **O**bservatory (LIGO). The development of quantum technologies for information processing and metrology has piggy-backed on the exponential progress of these quantum mini-Moore's laws. Wineland's quantum logic atomic clock is many orders of magnitude more precise than the atomic clocks of a few decades ago. Superconducting quantum bits are more than three orders of magnitude more coherent than when they were introduced in 2000. Integrated photonic circuits and sources developed for telecommunications have allowed the construction of multi-photon quantum interferometer arrays which, had they been implemented with the technologies of the 1990s, would have required an optical table the size of a football field. The injection of *squeezed light* into LIGO holds the promise of increasing the sensitivity of the huge interferometer by up to an order of magnitude.

Although driven by exponential advances in quantum technologies, the density of quantum bits in general-purpose quantum computers has not doubled every two years over the past two decades. Quantum computers already store and process information at the level of individual atoms and photons, so you can't make these components smaller than they already are! (Interestingly, many of the advances in the *coherence* of superconducting *qubits* have occurred

"Quantum error correction, quantum communication, and the development of coherent quantum interfaces between light and matter are required to construct large scale quantum computers and a quantum internet."

by making them larger rather than smaller, to take advantage of the self-averaging processes of noise.) To make larger quantum computers, we must solve the problems of modularity and integration of highly precise quantum systems. Quantum error correction, quantum communication, and the development of coherent quantum interfaces between light and matter are required to construct large scale quantum computers and a *quantum internet*. **The current moment represents a turning point for the development of larger and larger-scale quantum computing.**

US government support for fundamental research has played a crucial role in the past development of quantum information technologies, and will play a crucial role in the future. Industry has also played a key role. IBM was one of the initial innovators in quantum cryptography and quantum computation, and continues to play a strong role today. Microsoft has invested significant resources in the development of *topological quantum computing*. Over the last decade, BBN has made strong contributions to quantum computing and quantum communications. Google has recently made a strong investment in quantum information technologies, and Intel has started a large program in the field. Multiple quantum information start-ups have entered the field. However, the development of quantum information technologies cannot be supported by industry alone. To make the next leap in quantum information processing requires the development of quantum devices and techniques that are specific to quantum information processing. Highly coherent quantum bits, techniques for constructing and manipulating large-scale entangled states, quantum communication channels and quantum repeaters, and the development of quantum error correction are all essential to the quantum information technologies of the future.

In recognition of the importance of the development of quantum information theory and technology, 25 researchers from around the globe gathered in Arlington, VA on August 25-26, 2016, to discuss the current state of the art of the field and to identify challenges and opportunities for quantum information processing over the next 5, 10, and 20 years. The two-day workshop was organized to encourage lively discussion and debate and to maximize the interaction of participants. The first day began with short, introductory presentations that framed the workshop goals. The remainder of the first day was spent in small group discussions according to three areas of quantum information processing: quantum computing, quantum communication and quantum sensing and metrology. Each session was chaired by an academic expert of the field. The second day was spent as a whole group in white-space discussions. Although there were differences in predictions of the time scales for the development of future quantum technologies, the researchers came to almost unanimous consensus on the present state and on the future promises of quantum information processing. This report documents their conclusions.

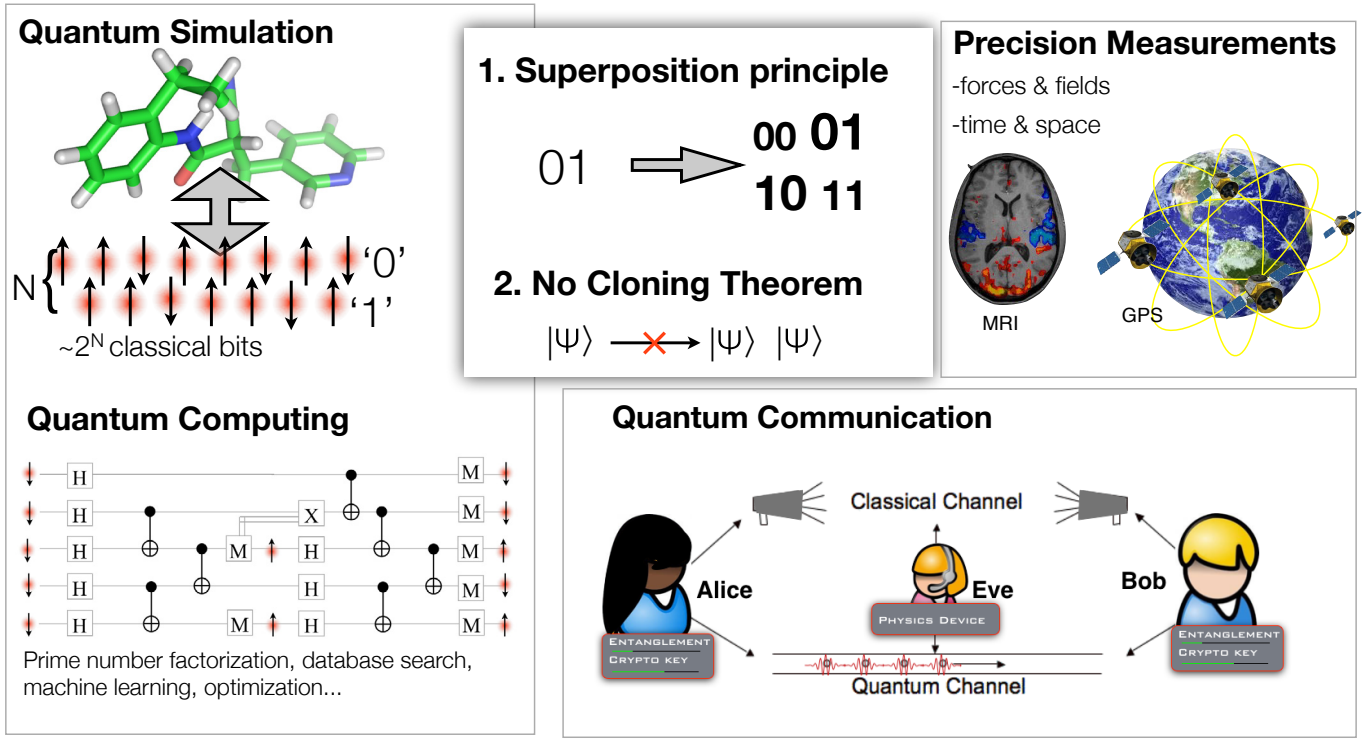


Figure 2. Three key areas of quantum technologies: Quantum Simulation and Computing; Precision Measurements and Metrology; and Quantum Communications. These technologies are enabled by the laws of quantum mechanics. Two essential underlying principles are the superposition principle (quantum states can be in multiple distinct observables states simultaneously, even when these states are delocalized) and the no-cloning theorem (quantum mechanics doesn't allow an unknown state to be copied).

Recent Advances and Current Prospects in Quantum Information Processing

Progress in quantum computing, quantum communication, and quantum sensing and metrology has accelerated markedly over the last decade. As mentioned in the introduction, one of the primary drivers of this advance has been the development of exponentially more precise technologies for fabrication, sensing, and control: the same technologies that drive Moore's law for classical computation. Just as important, however, is the ongoing progress in quantum information theory to develop new quantum algorithms, more powerful error correcting codes, novel methods for quantum secured communications, and *entanglement* and squeezing-based techniques for quantum measurement. It is the interplay between theory and experiment that has driven quantum information processing technologies forward at an accelerating pace.

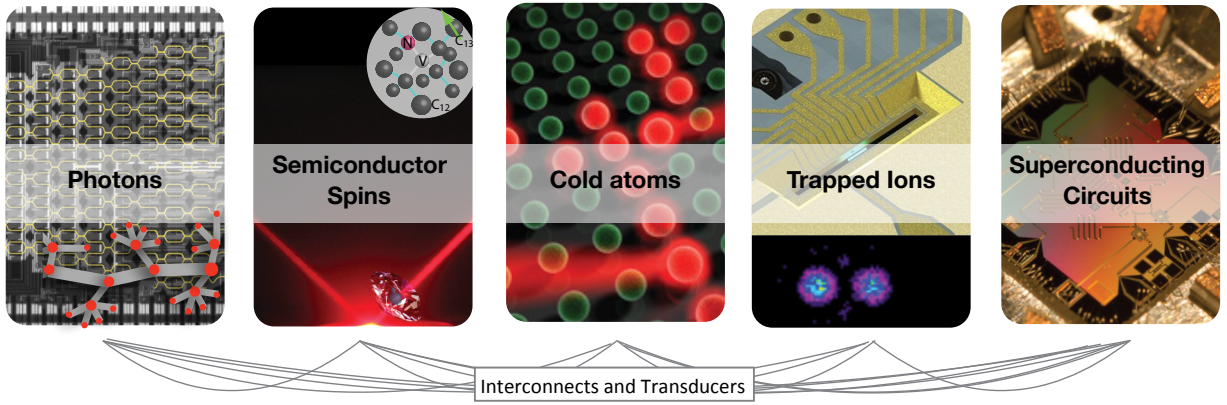


Figure 3. Leading physical platforms for quantum information processing include photons, spins in semiconductors, ultracold atoms, trapped ions, and superconducting circuits. A major area of research also focuses on connecting these platforms, which often requires the development of transducers to photonic states, which can travel long distances with little *decoherence*.

Quantum computation

Quantum computers stand on the cusp of an exciting transition. For the last several decades, quantum computation has been performed on relatively small scale quantum systems containing up to a dozen or so qubits. The very first proof of principle quantum computations were performed using room temperature nuclear magnetic resonance (NMR). These were followed by simple demonstrations of quantum computation on *ion traps*, superconducting systems, and quantum optics. Multiple technologies have been developed to demonstrate quantum bits and operations, including atom-optical systems, solid-state atom or atom-like systems such as phosphorus atoms embedded in silicon, *quantum dots*, or nitrogen vacancies in diamond (*NV-diamond*). Few-qubit devices using semiconductor quantum dots have been demonstrated. A particularly promising, but difficult to implement, method for quantum information processing is based on topological systems.

At the time of this workshop, several quantum computing technologies stand out for their ability to perform extended quantum information processing and—most important—for their promise of scalability: semiconductor spins, ultracold neutral atoms and trapped ions, superconducting circuits, and optical photons, see Figure 3.

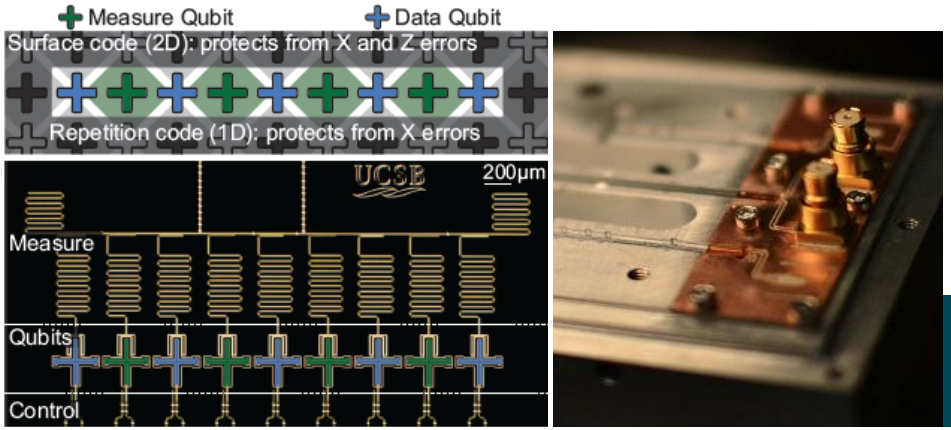


Figure 4. Superconducting quantum computing approaches. *(left)* **Circuit-model computing approach with 9 qubits for error correction** *(Martinis group, Google).* *(right)* **3D cavities have enable record coherence times and error correction** *(Yale).*

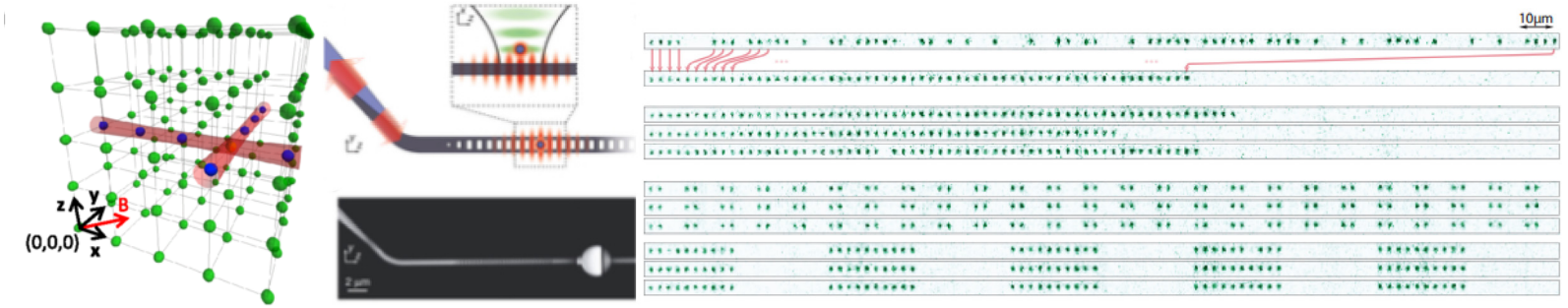


Figure 5. *(left)* **Ultracold atoms can now be assembled in 3D lattices where they can be addressed by laser beams, as shown here as a 5x5x5 array of neutral atoms** *(Credit: D.S. Weiss group, Penn State). (center)* **An alternative approach consists of nanophotonic device interfaces. Shown here is a photonic crystal nanocavity whose evanescent field can be coupled to an individual ^{87}Rb atom (blue circle). A tapered fiber connected to the cavity allows efficient coupling to fiber optics.** *(right)* **Regular 1D and 2D arrays of individually controlled atoms were recently assembled using optical tweezers with real-time feedback.** *(Credit for b and c: Lukin, Greiner, and Vuletic groups at Harvard and MIT).*

Ion traps (Fig. 7) are a tested quantum information processing platform that has recently been used to demonstrate a variety of technically difficult quantum information processing tasks at the level of tens of ions and hundreds of quantum logic operations. There is a relatively clear technological path over the next few years to extending such ion-trap based systems to around fifty qubits and to performing thousands of coherent quantum logic operations.

Similarly, superconducting quantum information processing has made great strides in the last decade (Fig. 4). Clever design of the underlying qubits and superconducting microwave cavities has led to the construction of superconducting quantum information processors with qubits that are orders of magnitude more coherent than the initial superconducting qubits of the early 2000s. Individual gate fidelities in superconducting qubits have been demonstrated at one part in 10^3-10^4. Moreover, because they can be implemented lithographically, superconducting circuits have a clear path for scalability. The next few years are also likely to see superconducting quantum information processors with around fifty qubits and capable of performing thousands of coherent operations.

Other quantum information processing technologies have also made great progress in the last decade. Atom-optical systems allow large numbers of atoms to be trapped and individually addressed (Fig. 5). Such systems exhibit high levels of *coherence* and in principle can be used to perform large numbers of coherent quantum logic operations.

Semiconductor systems, including quantum dots (Fig. 6), atom-like semiconductor systems (Fig. 10), and semiconductor dopants, also show great promise for performing large numbers of quantum logic operations on large numbers of qubits. Because they are manufactured lithographically, including processes similar to classical silicon-based microprocessor chips, semiconductor quantum information processors may offer a high degree of scalability and architectural flexibility.

A *quantum computer* with fifty qubits, capable of performing thousands of coherent operations, might still seem a pretty small device. Nonetheless, a mid-scale quantum computer with these capabilities crosses an important threshold, for it is at this scale that it becomes effectively impossible to characterize and simulate the behavior of such a quantum computer using even the most powerful classical computers. A quantum computer with fifty qubits requires $2^{50} \approx 10^{15}$ memory sites on a classical computer merely to record the state of the quantum device. To simulate the dynamics of such a quantum computer on a classical computer requires the ability to exponentiate 10^{15} by 10^{15} matrices. These requirements will lie outside of the capability of classical computers for many years to come. If we can construct quantum computers with one hundred qubits, which is a reasonable 5-10 year goal, simulating such devices would require classical computers with around 10^{30} memory sites and capable of exponentiating 10^{30} by 10^{30} matrices, which is unlikely to happen for decades, if ever. Quantum computers are on the verge of breaking the barrier of classical computation.

The scale at which classical computation becomes impossible is also the scale at which quantum computers can begin to simulate the behavior of other quantum systems to an accuracy that classical computers cannot attain. Simulating condensed-matter and particle physics models, including models of *quantum gravity*, represents the most powerful near-term application of quantum computation. The last decade has seen rapid progress in demonstrations of quantum simulation, including the development of a variety of novel techniques for simulating quantum chemistry. Up until now, however, these simulations

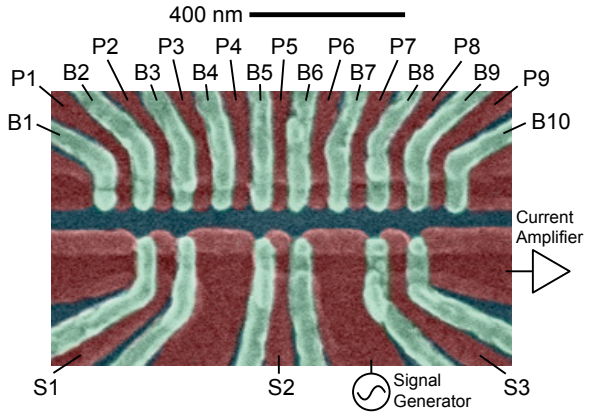


Figure 6. Nanoscale device to control 12 semiconductor quantum dots in an undoped Si/SiGe heterostructure. *(Credit: David Zajac, Petta Group, Princeton University)*

can still also be performed classically using very large, sometimes special-purpose, classical computers. We are about to cross over the barrier at which quantum computers become the most powerful tool available for the characterization of quantum behavior across a wide variety of naturally occurring quantum systems.

The last decade has also witnessed a large number of experimental advances in the demonstration of quantum algorithms, from improved versions of Shor's algorithms, to matrix inversion, to *quantum machine learning* protocols. To attain the initial promised advantage of quantum computation will require quantum computers with 100-1000 *qubits* capable of performing around 10^4 coherent operations in the case of linear algebra methods and topological quantum machine learning, a reasonable five to ten year goal. To perform Shor's algorithm and to break public-key cryptography for current code standards requires fault tolerant quantum computation over tens of thousands of logical qubits, and millions of physical qubits, which represents a grand challenge twenty year goal. Nonetheless, performing quantum algorithms on the mid-scale quantum computers available over the next few years will make up an important benchmarking process. An essential ingredient of this benchmarking will be the ongoing development of procedures for Quantum Characterization, Validation, and Verification (*qCVV*), a toolkit of methods for analyzing the design and implementation of quantum information processors, validating the coherence and integrity of their components, and validating their performance.

The quantum computers described above are general-purpose systems capable of performing arbitrary quantum algorithms within their memory and coherence restrictions. The last decade has also seen tremendous progress in the construction of special purpose quantum information processors which, while not (or not yet) capable of universal quantum computation, nonetheless provide powerful paradigms for quantum simulation and for demonstrating and exploring large-scale entanglement. Because they face less stringent performance requirements than general purpose quantum computers, such special purpose quantum information processors have attained impressive results. *Ion traps* represent a powerful technology for quantum computation, by entangling multiple ions into so-called 'Schrödinger's cat' states (Fig. 7). Quantum clocks can attain unprecedented precision. *Cold atoms* in optical lattices allow the demonstration and characterization of entanglement over hundreds of atoms. Integrated quantum optical circuits allow the implementation of hundreds of coupled, tunable *interferometers*, enabling the construction of large-scale linear optical devices 'on-chip' which could not be implemented on a conventional optical table. Large-scale quantum annealers implemented using superconducting circuits allow the simulation of tunable transverse Ising models over thousands of qubits. Solid-state quantum information processing devices using nitrogen vacancies in diamond, semiconductor quantum dots, and atomic spins in solids can use entanglement to function as highly sensitive detectors of electric and magnetic fields. Special purpose quantum information processors have already allowed the simulation of highly complex quantum systems whose behavior lies far beyond the reach of any classical computer.

Such special purpose, large scale, controllable quantum systems have generated great interest recently. The D-Wave quantum annealer currently contains more than a thousand qubits in an integrated superconducting quantum circuit and implements a programmable transverse Ising model. While in some cases such models are amenable to classical simulation (e.g., via a quantum Monte Carlo algorithm), the commercial availability of D-Wave devices has fostered a broad experimental and theoretical effort to uncover their underlying capabilities. The next generation of *quantum annealers* will exhibit tunable couplings that go beyond the transverse Ising model and that are difficult or impossible to simulate classically.

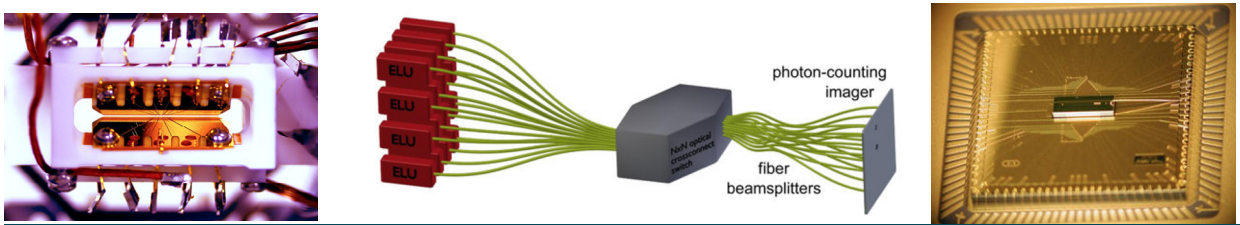


Figure 7. *(left)* **A small programmable (5-qubit) trapped ion quantum computer. (Monroe group, University of Maryland and Joint Quantum Institute).** *(center)* **Photonic interconnects to connect quantum memory modules (***Credit: Kenneth R Brown, Jungsang Kim & Christopher Monroe). (right)* **Advanced microfabricated ion traps from Sandia National Laboratories** *(Image courtesy of Duke University).*

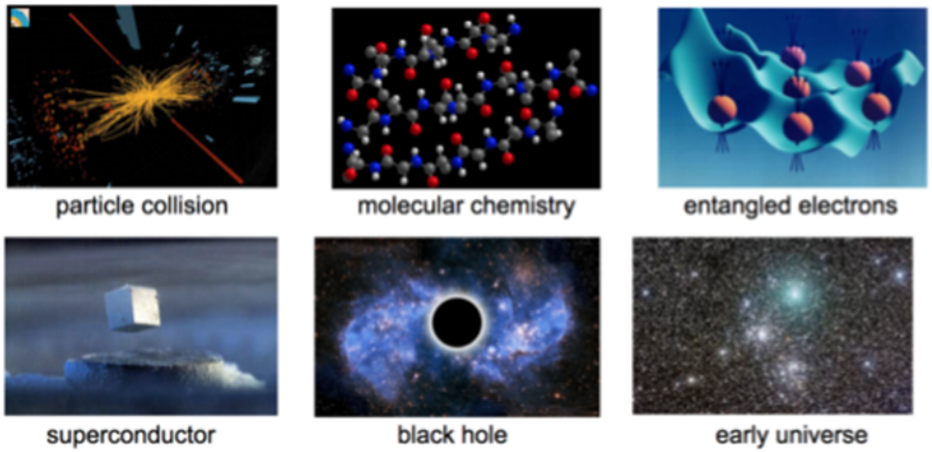


Figure 8. "A quantum computer can simulate efficiently any physical process that occurs in Nature, maybe—We don't actually know for sure."—John Preskill, Caltech

Theory of quantum computation

The last two decades have seen a huge explosion in the theory of quantum computation. The 1990s saw the invention of fundamental quantum algorithms for factoring, finding eigenvectors and eigenvalues, quantum simulation, and quantum search. The theory of *quantum error correcting codes* and of robust, scalable quantum computation was also developed during this time. The late 1990s offered up the concept of adiabatic quantum computation and of quantum annealing, techniques which try to find the solutions to hard optimization problems by mapping those solutions to the lowest energy state—the ground state—of a quantum system, and by using tunable *Hamiltonian dynamics* and *quantum tunneling* to find that ground state.

Interestingly, despite intensive efforts, novel quantum algorithms have proved largely elusive. The last ten years have seen the development of quantum algorithms for matrix inversion/solving linear equations that are exponentially faster than their classical counterparts, and their application to problems of machine learning, but these methods, like Shor's algorithm, are fundamentally based on quantum Fourier transforms and on finding eigenvalues/eigenvectors. Part of the difficulty in finding new quantum algorithms lies in the fact that there are not many problems such as factoring that are thought to be exponentially hard but not NP-complete. Since quantum computers seem unlikely to be able to solve *NP-complete* problems in polynomial time, this leaves few truly novel problems to attack. Nonetheless, existing methods such as quantum simulation have been widely extended over the last decade, showing as noted above that even small quantum computers with fifty to a hundred qubits could do much better than classical computers for simulating a wide variety of quantum systems.

Despite the paucity of novel quantum algorithms, quantum computer science has explored large swatches of previously unknown territory over the last twenty years, with great progress in the last ten. The development of the theory of QMA completeness—the quantum analogue of NP completeness—has spurred multiple investigations in the feasibility of constructing quantum computers by engineering their Hamiltonian dynamics. More recently, the notion of '*quantum supremacy*'—the concept that even simple quantum systems can generate data with statistics that could not be generated by any classical computer—has inspired investigations into the power of simple quantum circuits of the sort that experiment is likely to make available over the next few years (Fig. 9).

Over the last two decades, advances in the theory of error correcting codes have had profound effect on the viability of constructing large scale quantum computers—devices of the sort that could factor large numbers require quantum error correction to function reliably. Improvements in the thresholds of quantum error correcting codes over the last decade have made it clear that the construction of such large scale quantum computers is at least possible in principle, although in practice building them remains a grand challenge with a time frame of twenty years or more.

The field of quantum information processing is marked by tight connections between theory and experiment. It is this strong and fast feedback between theorists and experimentalists that has generated the accelerated progress in quantum information processing technologies over the past two decades.

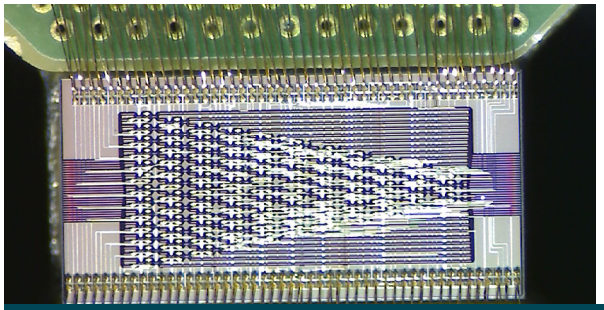


Figure 9. Programmable Photonic Integrated Circuits (PICs) allow precision control of tens to hundreds of photonic waveguides with near-perfect phase stability, building on modern silicon electronics processing. Programmable PICs are being used for quantum communications, machine learning, and have been proposed as an early system to demonstrate "quantum supremacy" by boson sampling. *(Image Credit: MIT, AFRL, OPSIS)*

Quantum communication

Quantum communication is a field with multiple applications and wide-reaching implications. First, quantum mechanics governs the capacity of communication channels such as fiber optic cables or free-space optical and electromagnetic channels, to transmit classical information. Second, quantum mechanics enables communication protocols such as quantum key distribution and other forms of *quantum cryptography*, quantum secret sharing and quantum data locking, whose security is guaranteed by the laws of physics. Third, *quantum communication channels* can be used to transmit quantum information between quantum computers, enabling the construction of a *quantum internet*. The last decade has witnessed great progress in all three of these applications of quantum communication theory and technology. For many decades, the ultimate communication capacity of bosonic channels such as optical communication channels in the presence of loss, noise, and amplification, was unknown. The theoretical limit of such channels was finally uncovered in the last two years: although we do not yet know how to attain this limit in practice, at least we know what the target is. These limits are important because existing fiber optic and free space communications are already pushing down to within a few orders of magnitude of the ultimate physical limits. To advance communication capacity requires a thorough understanding of the theory and practice of communication using fundamentally quantum systems such as photons.

Quantum cryptography and *quantum key distribution* systems—including commercially available systems—have been in place for almost two decades now. Advances in photonics have pushed the current technologies up to secure bit rates of 10^5-10^6 bits per second in the lab. The near term goal is to push up such secure communication rates to 10^7-10^8 bits per second over metropolitan distances up to 100 km or so. Recent theoretical developments in the theory of quantum communication imply that to go to much longer distances requires the construction of *quantum repeaters*—devices that extend short-range distribution of quantum information to longer range by combinations of *quantum entanglement* and quantum error correction. The construction of long distance quantum repeaters is an active field of research in quantum technologies.

One of the primary applications of quantum cryptography is secure communications with satellites. Satellites require secret keys to allow secure communication with their operators, but secret keys are consumed over time, making such communication less secure the longer the satellites have to operate. Quantum key distribution from earth to space provides a potential solution to this problem. Fortunately, because the primary impediment to quantum key distribution between ground and satellite is absorption and turbulence in the atmosphere, direct quantum cryptographic links with satellites are possible without the use of quantum repeaters, and active programs to establish such links are underway in China, Canada, and Europe.

The long term goal of quantum communication systems is a quantum internet, quantum computers connected via quantum communication channels. Quantum communication channels distribute quantum bits and entanglement while maintaining *quantum coherence*. Quantum bits can either be sent directly by encoding them on photons and sending them from sender to receiver, or by quantum teleportation, which operates by distributing quantum entanglement between the parties who wish to send quantum information. Quantum teleportation can then be accomplished by local measurements and classical communication. The feasibility of networked quantum computers has recently been demonstrated experimentally using ions, *cold atoms*, superconducting devices, and *color centers* in diamond (Fig. 10). Spins in semiconductors quantum dots can be efficiently entangled with photons, and these photons can be directly embedded in the telecom spectrum. Quantum teleportation demonstrations were recently reported in metro-scale fiber networks. Despite

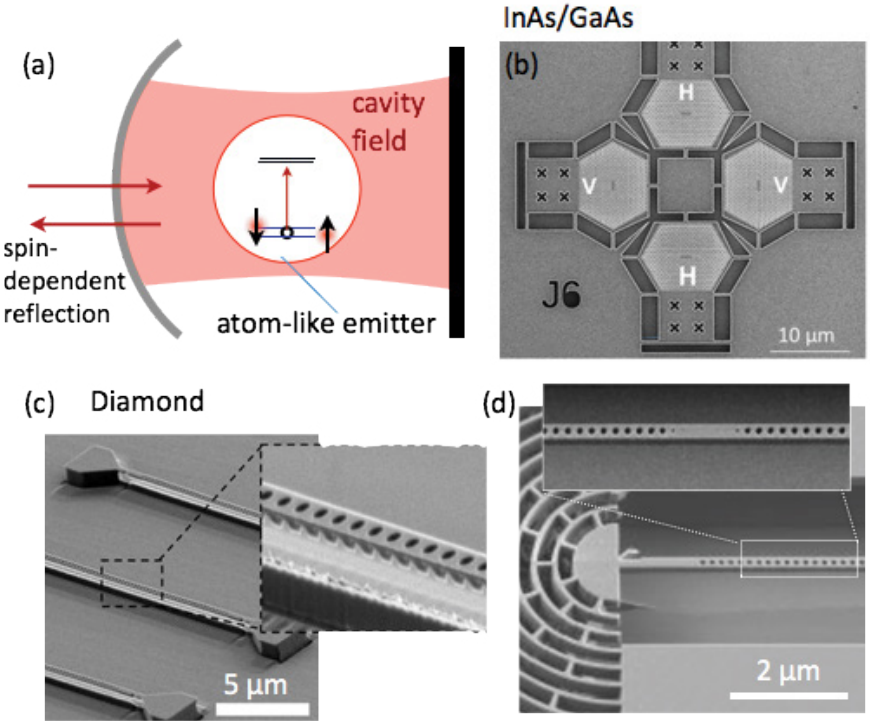


Figure 10. Optical cavities can act as efficient interfaces between incident photons and atom-like quantum memories *(a)*. **Such interfaces based on photonic crystal cavities are being used to link quantum memories in photonic circuits.** *(b)* **Cavity-waveguide networks for InAs/GaAs quantum dots.** *(Credit: Waks group, University of Maryland).* *(c)* **Diamond cavity-waveguide systems with triangular** *(bottom left)* **and** *(d)* **rectangular** *(bottom right)* **nanobeams for NV and SiV memories.** *(MIT and Harvard)*

these advances, a functional quantum repeater node, has not yet been demonstrated. After rapid progress, such repeaters appear to be attainable within a 5-year time horizon. The theory of quantum computation combined with quantum communications has shown that the construction of a quantum internet would have profound implications for quantum computation and for secure communications. Quantum computers linked via quantum communication channels offer disruptive solutions to computer security: by using the laws of quantum mechanics to protect stored information and to render the operation of a quantum computer inaccessible to outside operators, quantum data locking and so-called 'blind' quantum computation render quantum computers linked together in a quantum internet much less susceptible to hacking than conventional computers. The theory of distributed quantum computation over a quantum internet shows that linked quantum computers could allow users to share joint information in a trusted way, ranging from quantum secret sharing and quantum decision making to fraud-free quantum voting. **Just as the conventional classical internet has enabled a wide variety of applications that go beyond the use of a single classical computer, the quantum internet has the potential to change the way people and organizations collaborate and compete, establishing trust while protecting privacy.**

Quantum sensing and metrology

Quantum sensors and measurement devices are the most established applications of quantum information technology. At bottom, the fundamental limits to all precision measurement are set by quantum mechanics. For example, the precision limits to optical interferometers and conventional atomic clocks are determined by quantum fluctuations—the so-called "shot noise" or "*standard quantum limit*." Quantum noise sets the fundamental limits to measurement accuracy and precision. The standard quantum limit is indeed standard, and quantum, but it is not a limit. Over the past several decades, the application of quantum information theory to metrology has shown that the use of counterintuitive quantum effects such as coherence, entanglement, and squeezing can attain measurement accuracy and precision that go beyond the standard quantum limit. The '*Heisenberg limit*' to measurement is attained by using quantum coherence and entanglement to reach the actual bounds to accuracy and precision allowed by quantum mechanics. Quantum information theory has elucidated the fundamental bounds to measurement for systems ranging from atomic clocks, to interferometers such as LIGO, to magnetometers, to gyroscopes, to positioning, to time of arrival measurements, and more.

Reaching those limits requires attention to the ways in which '*quantum weirdness*' plays out in the context of sensing and measurement. For example, quantum information theory has shown that the ultimate limits to interferometry can be reached by injecting exotic quantum states such as squeezed vacuum states into ports of the interferometer. The plans for attaining the full capabilities of advanced LIGO require exactly such injection of squeezed vacuum into the 4-km long arms of the interferometer. The ultimate limits to measuring time are realized using exotic squeezed and entangled states of atoms and light: as noted above, Wineland's quantum logic quantum clock, which for many years represented the sine qua non standard for optical frequency atomic clocks, operates by entangling optical and microwave frequency qubits within the atoms of the clock.

The development of novel materials and systems for quantum information processing has dramatically expanded the scope of precision measurement over the last few decades. For example, nitrogen vacancy centers in diamond consist of defects in the otherwise pure carbon diamond crystal, i.e. a nitrogen atom is substituted for a carbon atom and produces an adjacent lattice vacancy. Such NV-centers behave like trapped atoms in the diamond crystal, with two electron spins that can be precisely controlled by optical and microwave fields. Moreover, the NV's electron spins can couple strongly to the nuclear spins of nearby carbon 13 atoms. As a result, an NV-center is effectively a quantum microprocessor with several controllable electron and nuclear spins. The exquisite quantum control afforded by NV-centers makes them highly sensitive probes of the local magnetic field. NV-centers can therefore be used as nanoscale magnetometers to measure magnetic fields in their vicinity. The sensitivity is remarkable as it allows individual nuclear spins to be measured on a surface, a 'holy grail' experiment in magnetic resonance imaging. While some applications of NV-center magnetometry are semi-classical and obey the standard quantum limit, the ability to put the electron of the NV-center into an entangled state with nearby nuclear spins translates into the potential to operate as Heisenberg-limited magnetometers that probe the local magnetic field to the ultimate accuracy allowed by quantum mechanics. Their quantum limited sensitivity allows them to also measure the local temperature and electric field. NV-centers can not only operate as quantum limited magnetometers, electrometers, and thermometers, they have also been proposed for applications such as gyroscopes and precision clocks. NV-centers are not the only 'solid-state' atomic system that allow the construction of precision measurement devices that rely on squeezing and entanglement: semiconductor quantum dots, and defects in silicon carbide (SiC), while at an earlier stage of development also hold considerable promise. Semiconductor quantum dot systems based on electrons and electron spin could give rise to similar quantum based sensors and detectors.

A remarkable development in precision quantum measurement over the last several decades has been the construction of quantum-limited vibrational sensors and accelerometers. Nanofabricated mechanical cantilevers can be fabricated and instrumented to operate at the standard quantum limit. While individual quantum cantilevers can operate at the standard quantum limit, theoretical proposals exist to entangle such cantilevers with light and with each other, holding out the promise to construct nanomechanical systems that operate at the Heisenberg limit for metrology and could be used to detect effects of *quantum gravity*.

Superconducting devices are already used for precision measurements of electrical conductivity. Superconducting Quantum Interference Devices (SQUIDs) uses superconducting interferometry to make highly precise measurements of magnetic flux. SQUIDs are commonly combined in integrated quantum circuits with superconducting qubits. The ability to entangle such qubits holds the potential to use superconducting quantum microprocessors to attain Heisenberg limits of conductivity and flux. The use of entanglement and squeezing in atomic clocks to enhance accuracy and precision was one of the very first proposed applications of quantum information theory to precision measurement. So-called 'Schrödinger's cat' states, a quantum superposition of the most energetic (live) state of a set of neutral atoms or ions, and the least energetic (dead) state, give the highest precision of any quantum state for marking out time, surpassing the standard quantum limit and attaining the Heisenberg limit. Such cat states can now be produced with exquisite precision in superconducting microwave cavities. Quantum information theory sets out the applications and uses of entanglement for precision measurement of time, and ion trap quantum information processors can be used as entangled quantum clocks for attaining unprecedented precision in temporal measurement. As noted above, entanglement in the quantum logic atomic clock is the key to attaining accurate optical frequency clocks. A quantum network of atomic clocks connected by quantum communication channels would allow the benefits of squeezing and entanglement in measurements to be extended to a quantum sensor network. The resulting network could use entanglement for highly accurate measurements of position and acceleration, producing, among other things, secure and accurate '*quantum GPS*'. Optical frequency atomic clocks already function as sensitive detectors of the earth's gravitational field via the gravitational redshift. Extended networks of entangled quantum clocks could function as highly accurate gravitometers to probe the structure of seismic faults.

A network of quantum clocks could also prove highly effective in applications of detection and imaging. One of the important quantum developments of the last two decades has been the construction of quantum theories and of proof of principle experiments that exhibit quantum enhancements in the optical detection and resolution/imaging of objects both close up (quantum microscopy) and far away (quantum illumination; sub-Rayleigh limit quantum imaging). Quantum imagers connected with a network of quantum clocks have the potential to exhibit strong enhancements in detection and imaging.

Measurement devices tailored for different applications may rely on very different types of qubits. Connecting these coherently into a sensor network requires quantum transducers—devices that transform quantum information from one form into another, see Fig.3. For example, a quantum transducer may transform a stationary qubit stored on an atom into a flying qubit stored on a photon, or a qubit stored in an optical cavity into a qubit stored on a superconducting qubit. The design and implementation of accurate, coherent quantum transducers lie at the heart of quantum sensing. The remarkable success of existing quantum sensors and measurement devices arises from the quantum technologies that allow the construction of quantum transducers. The future development of even more accurate and precise quantum sensors will hinge on the development of more effective quantum interfaces and transducers.

"The development of novel materials and systems for quantum information processing have dramatically expanded the scope of precision measurement over the last few decades."

Conceptual and Technical Challenges

To realize the promise of quantum information processing technologies, we must overcome multiple challenges. The close interplay between theory and experiment in quantum information processing implies that the technical challenges are intimately bound up with conceptual challenges. Here we present the primary challenges for each of the three sub-fields of quantum information processing. These challenges are intimately linked from field to field. For example, novel methods of quantum sensing and control must be developed to enable advanced quantum computers and quantum communication systems. There is a need for highly coherent and efficient quantum interfaces and transducers that connect all three sub-fields. Finally, all fields share the common challenge of quantum characterization, validation, and verification.

The workshop participants framed important technical challenges for the three research areas within the context of:

- The development of highly coherent, highly controllable quantum bits and quantum logic operations.
- The integration of such qubits and quantum logic operations into large-scale quantum computers that operate reliably via quantum error correction.
- The construction of long-distance quantum communication channels based on quantum repeaters.
- The linking together of quantum computers via quantum communication channels to construct a quantum internet.
- The development of novel quantum algorithms for quantum simulation, quantum networks, and quantum machine learning.
- The construction of quantum sensors and measurement devices that use entanglement and squeezing to attain the ultimate physical limits of precision and sensitivity.
- The linking together of quantum sensors in quantum networks via quantum GPS, and the global quantum clock to attain unprecedented accuracy for detection and imaging.

All of these topics are linked by the common need for reliable quantum transducers, devices that transform quantum information, from photons to cold atoms to ions to quantum dots to spins to superconducting systems.

1. Challenges for quantum computing

Both trapped-ion and superconducting quantum computers exhibit the ability to put together ten to twenty qubits and to perform individual quantum logic operations with high fidelity. The primary challenges for attaining the 5-10 year goals are to scale up such devices and to perform large numbers of quantum logic operations with similarly high fidelity. Scalability and fidelity challenges are different for ion traps and for superconducting systems. For ion traps, scalability requires the capacity to transfer quantum information reliably between multiple ion traps, either by moving ions coherently from one trap to another, or by quantum teleportation. However cross-talk in controlling individual ions is a significant problem. Because superconducting quantum computers are integrated, on-chip devices, the problem of scaling up the number of qubits on chip is not so severe, but the challenges of controlling individual qubits without cross talk while maintaining high individual and collective gate fidelities remain difficult. A strong combined theoretical and experimental effort will be required to characterize, verify, and validate the behavior of large-scale superconducting circuits.

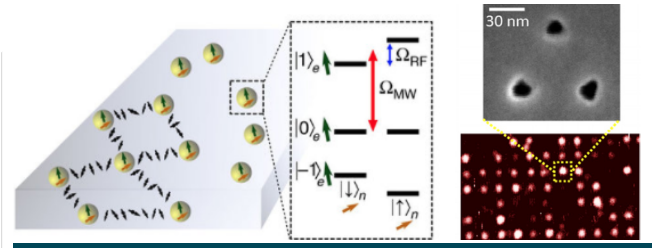


Figure 11. Arrays of NV-centers in diamond, closely enough spaced so that electron spins interact magnetically, are promising for mid-scale quantum computers that could even function at room temperature. The image on the left shows a schematic of the required architecture *(Image credit: N. Yao, NComm, 2012)***; it is now becoming possible to reach the required length scales experimentally** *(D. Scarabelli, Nano Letters, 2016).*

Ion traps and superconducting quantum circuits have strong underlying fabrication support. Sandia Laboratories has developed a successful ion trap foundry, whose products are used by many of the world's leading ion trap groups. The early days of superconducting qubits (ca. 2000) saw many problems with fabrication and materials, but there has been steady progress in reducing the ubiquitous 1/f noise in superconducting circuits, and design principles have been developed for constructing superconducting qubits whose coherence properties are largely immune to such noise. Consequently, the fidelities of superconducting qubits and quantum logic gates have increased more than three orders of magnitude in the last decade, to the point where superconducting circuits represent a highly promising quantum technology for the implementation of mid-scale quantum computers.

While ion-trap and superconducting quantum computers are currently the most promising platforms for developing mid-scale quantum computers, it is too early to focus basic science of these technologies alone. Atom-optical systems and semiconductor systems afford high degrees of coherence and scalability (Fig. 11). Because of their intrinsic resistance to noise and errors, topological systems also hold great promise. While topological methods for quantum information processing are still in their early stage of technological development, breakthroughs in system design and material fabrication could make such systems strong candidates for constructing both mid- and large-scale quantum computers.

The development of mid-scale quantum computers with the desired reliability faces a wide range of technical challenges both at the design and build stage, and at the level of quantum scalability (Fig. 12). Research is needed to understand and combat the sources of noise and errors. Novel fabrication and design techniques for reducing noise in ion traps and superconducting quantum circuits will have to be developed, and novel quantum control techniques to reduce errors will have to be implemented. The first line of defense in any experimental implementation of quantum logic is at the design phase: individual qubits should be constructed to naturally resist *decoherence* and errors; couplings between qubits should be designed to allow high fidelity quantum logic gates while minimizing cross-talk; input-output ports should be implemented in a way that allows high accuracy preparation and measurement, and the coupling of quantum information to quantum communication channels. The second line of defense against noise and errors relies on active quantum control—the implementation of error reduction techniques such as dynamical decoupling and more sophisticated quantum control techniques to reduce noise and errors at the single qubit level, and to ensure that quantum logic operations are performed with high fidelity. The third level of defense against noise and errors consists of *quantum error correcting codes*.

Quantum error correction

The most significant advances in quantum error correction over the past decade have come from the theoretical side, refining existing coding schemes and coming up with novel schemes, such as surface codes, with better error correction thresholds. **Continuing this progress in devising better quantum error correction methods is one of the primary challenges for quantum information theory.**

A promising approach to fault tolerant quantum computation is the implementation of topological schemes. Topological systems exhibit intrinsic quantum error resistance: local errors do not disrupt the computation. The problem of developing fault tolerant topological quantum computers is a joint theory/experiment question of designing and building effectively two-dimensional topological systems. Considerable progress has been made in identifying materials and systems with the proper topological features, but much more progress needs to be made if topological quantum computation is to become a reality. The demonstration of fault tolerant topological quantum logic represents one of the significant challenges for quantum information processing over the 5-10 year timeframe.

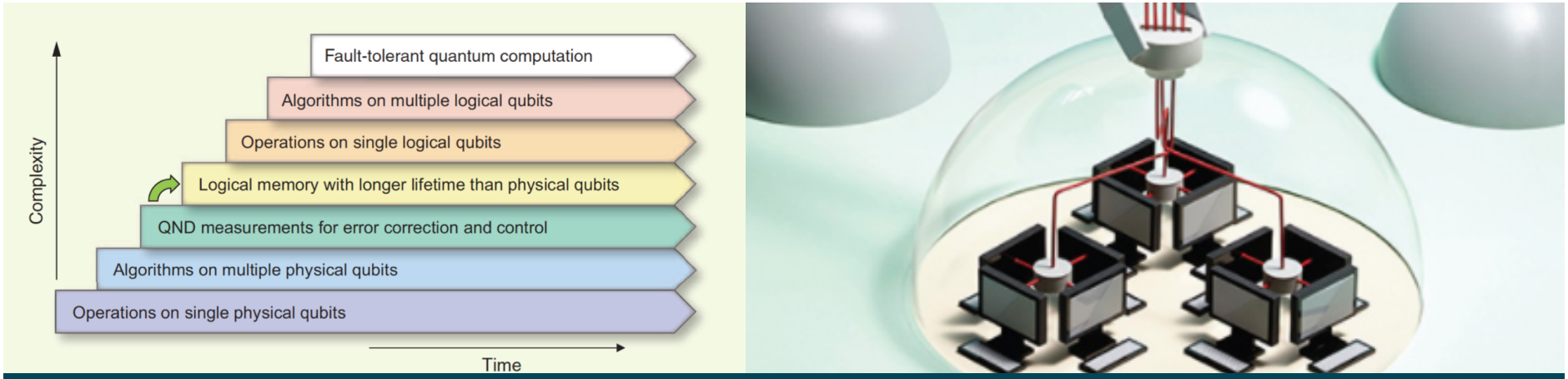


Figure 12. *(left)* **To develop fault-tolerant quantum computation requires mastery of increasingly sophisticated technologies. Quantum algorithms and quantum nondemolition measurements on few qubits are possible today. Logical qubit encoding with performance better than the physical constituent qubits will likely be accomplished in the next five years.** *(Credit: Devoret and Schoelkopf, Science 339, 1169 (2013)) (Right)* **A focus is on the architectures that will efficiently link quantum memories into networks and modular quantum computers.** *(Image credit: C. Monroe, R. Schoelkopf, and M. Lukin / Scientific American, 2016)*

"Perhaps most important, as quantum computers grow in size, quantum simulators will be essential for simulating their components and subcircuits as part of the ongoing process of quantum characterization, validation, and verification that is essential for the development of quantum technology."

Algorithms for mid-scale quantum computers

This path towards building mid-scale quantum computers must also address what we will do with these mid-scale devices when we have them. They are too small to factor large numbers, but mid-scale quantum computers could prove to be powerful devices for quantum simulation. To realize this potential, novel quantum algorithms for quantum simulation must be developed and benchmarked against classical algorithms. Such algorithms include quantum simulations of solid-state systems, quantum field theory and elementary particles, and the recent demonstration of the connection between quantum error correction and the AdS-CFT correspondence of quantum gravity. Perhaps most important, as quantum computers grow in size, *quantum simulators* will be essential for simulating their components and subcircuits as part of the ongoing process of quantum characterization, validation, and verification that is essential for the development of quantum technology.

Mid-scale quantum computers will also be capable of exhibiting *quantum supremacy*: they can produce outputs with probabilities that apparently can't be produced by classical computers. At the moment, the nearest-term demonstrations of quantum supremacy do not necessarily have practical application (except, of course, for demonstrating that quantum computers can do things classical computers can't). An important challenge for mid-scale quantum computation is to develop new and useful forms of quantum supremacy.

A particularly promising application of mid-scale quantum computation is *quantum machine learning*. Classical machine learning is a broad set of techniques that allow computers to find patterns in data. Because of the ubiquity of big data, classical machine learning represents a widely applicable and socially relevant application of computation. Quantum machine learning represents the application of quantum computers to the same set of tasks. It has been shown that if data can be represented in a quantum mechanical form, e.g., as states of qubits, then quantum computers provide exponential speed ups over their classical counterparts for a variety of important machine learning problems. To represent data in quantum form requires a quantum random access memory (*qRAM*), which can translate classical data into quantum mechanical states. Although constructing a large scale qRAM is a difficult technical problem, such a device does not in principle require quantum error correction, so it is potentially less daunting than constructing a large-scale, fault tolerant quantum computer. Even without large-scale qRAM, quantum algorithms have been shown to provide exponential speed-ups over the best available classical algorithms, e.g. algorithms for learning the topological structure of data.

Special purpose quantum information processors

Quantum annealers containing thousands of qubits are now commercially available. Existing transverse Ising model quantum annealers can often be simulated efficiently on a classical computer using quantum Monte Carlo methods. If quantum annealers can be constructed with additional so-called 'non-stoquastic' couplings, however, then they are in principle capable of universal quantum computation. A quantum annealer is an artificial quantum system with a programmable *Hamiltonian dynamics*. Such systems represent an alternative approach to universal quantum computation and allow novel methods for quantum error correction. A significant technological challenge for the 5-10 year timeframe is the construction, characterization, validation, and verification (*qCVV*) of highly coherent quantum annealers with tunable non-stoquastic couplings. The complementary theoretical challenge is the development of novel methods for fault-tolerant Hamiltonian quantum computation.

Quantum annealers have a variety of near-term applications. They can be used to simulate interesting models in condensed matter physics, e.g., various transverse field Ising models and their quantum phase transitions. As open quantum systems operating at non-zero temperature, they also allow us to simulate such models in the presence of coupling to a well characterized environment. One of the most promising applications of quantum annealers is deep quantum learning. Deep learning is a powerful classical learning technique in which many-layered ('deep') artificial neural networks are used to identify complex patterns in data. Quantum annealers are currently being used to implement deep quantum networks for machine learning. Highly coherent *quantum annealers* with tunable non-stoquastic couplings have the potential both to generate patterns that can't be generated classically—i.e., to implement quantum supremacy—and to recognize patterns that can't be recognized classically. The implementation and characterization of deep quantum learning networks is a significant challenge for the 5-10 year timeframe.

In addition to being a potentially powerful platform for general-purpose quantum computing, atoms trapped in *optical lattices* can be used for analog quantum simulation. They can model a wide range of systems that are difficult to model on classical computers, including widely studied condensed matter Hamiltonians, like Hubbard models and quantum magnetism, and novel Hamiltonians that have never been applied to condensed matter. They can be used to study a variety of lattice structures and systems in reduced dimensions, all with very accurately known potentials and interactions. Both the spatial and momentum distributions of cold atoms can be measured, along with band structures, interparticle correlation functions, and signatures of many particle entanglement. Furthermore, since the time-scales in these systems are relatively long, out-of-equilibrium phenomena can be studied in ways that are well beyond what can be observed in real condensed matter systems or with classical computers.

Integrated quantum optical systems—dense, tunable interferometric arrays etched into a silicon chip—are one of the most remarkable recent developments in quantum information processing technology. Derived from the technologies for constructing classical optical switching arrays, integrated photonic systems have proved to be powerful tools for performing quantum information processing. They have been used to demonstrate quantum walks and boson sampling (a particular form of quantum supremacy being developed in linear optical systems). The nonlinearities necessary for interacting photonic qubits can be realized using atomic or material nonlinearities, or through the act of measurement. Supplemented with efficient photon counting detectors and nonclassical light sources, integrated linear optical systems represent a potentially scalable alternative path to the construction of universal quantum computers. In the context of quantum information processing, loss remains a significant challenge for such integrated photonics. Implementing low-loss integrated photonics and the development of theoretical and experimental tools for compensating for loss is an important 5-10 year goal for quantum information processing.

Other promising quantum platforms such as *NV-diamond*, atoms doped in semiconductors, and semiconductor quantum dots, share with the quantum technologies discussed above the need for comprehensive qCVV.

"A significant technological challenge for the 5-10 year timeframe is the construction, characterization, validation, and verification (qCVV) of highly coherent quantum annealers with tunable non-stoquastic couplings."

QUANTUM COMPUTING 5-YEAR OUTLOOK

Mid-scale quantum computers with 50–100 qubits capable of performing 10^4 quantum logic operations without quantum error correction.

High-fidelity logical qubits that function better than their physical constituents.

Fault-tolerant quantum logic operations on 1–2 logical qubits.

Special-purpose quantum information processors such as *quantum simulators* and quantum annealers with hundreds or thousands of qubits & applications to quantum chemistry or the demonstration of fundamental quantum effects such as entanglement over hundreds to thousands of qubits.

Quantum Random Access Memory (*qRAM*) prototypes.

Applications of 'mid-scale' quantum computers to quantum simulation, quantum machine learning, and demonstration of quantum supremacy.

Quantum Characterization, Verification, and Validation (qCVV) of mid-scale quantum circuits with quantum error correction.

QUANTUM COMPUTING 10-YEAR OUTLOOK

General-purpose quantum computers with 100-1000 qubits, with the ability to perform 10^5 quantum logical operations on multiple qubits with individual gate fidelities of 0.9999.

Fault-tolerant quantum logic operations on 10-100 logical qubits.

Special-purpose quantum computers such as quantum simulators and quantum annealers with hundreds or thousands of qubits & applications to quantum chemistry or the demonstration of fundamental quantum effects such as entanglement over hundreds to thousands of qubits.

Development of special-purpose deep quantum learning circuits.

Large-scale qRAM & quantum machine learning on medium-scale quantum computers.

Mid-scale, error corrected quantum computers.

Application of special-purpose quantum information processors to problems in elementary particle physics and quantum gravity.

QUANTUM COMPUTING 20-YEAR OUTLOOK

Large-scale universal, fault-tolerant quantum computers to factor, to solve hard linear algebra problems, to perform quantum simulation, and to perform machine learning. Such quantum computers will be able to perform a wide variety of computations that could not be performed classically.

Large-scale special purpose quantum simulators, annealers, integrated quantum optical circuits networked with general purpose quantum computers.

Quantum simulators established as a universal tool for the characterization of fundamental quantum effects and the design of novel quantum technologies and materials.

Strong experimental and theory connections between quantum information science and other fields, such as high energy physics, quantum gravity, chemistry, and computational biology.

2. Challenges for quantum communications

The Internet is among the most important inventions of the 20th Century. We are now poised for the development of a *quantum internet* to exchange quantum information and distribute entanglement among quantum computers. A quantum internet promising new capabilities that would be impossible in a classical world, including long-distance unconditionally-secure communication, precision sensing and navigation, and distributed quantum information processing. Such a quantum internet will likely consist of different types of quantum memories and quantum information processors connected by optical links, as shown in figure 13. It will include many types of quantum memories and sensors, including cold atoms, solid-state, and photonic and superconducting, as mentioned above. This heterogeneity parallels an essential aspect of today's "classical internet of things", as it interconnects different information processing systems with individual advantages and shortcomings.

Some essential components of the quantum internet have already been deployed, including *quantum key distribution* links over fiber, free-space, and initial satellite links; *quantum teleportation* in deployed fiber; and the first optical links between entangled NV spin systems. However, there are several important challenges to be met.

Quantum key distribution (QKD)

Virtually all of today's encrypted internet traffic uses asymmetric public-key cryptography. However, asymmetric encryption schemes, such as the widely used RSA algorithm, are not inherently secure; their security relies on the unproven assumption that an eavesdropper does not possess the computational resources or algorithms to break a ciphertext. By contrast, symmetric encryption schemes, such as the one-time pad, provide perfect secrecy but require the users to hold secret, identical keys. The only provably secure way to amplify secret information at a distance uses the properties of quantum mechanics.

Theoretical bounds were recently demonstrated on the rate at which secret keys can be generated as a function of the distance between the communicating parties. When comparing today's experimental demonstrations to the theoretical rate limits, one still finds that at a given loss, a two-order-of magnitude gain is still possible with better experimental hardware and improved protocol implementations. However, even with the best possible protocols, the rate will eventually approach zero after a few hundred kilometers, as photon transmission practically vanishes.

Major challenges in quantum key distribution in the near-term are focused on practical implementations to approach fundamental channel capacity limits, and on building deployed QKD networks in fiber and free-space/atmospherics. The demanding and specialized hardware requirements for many forms of QKD make the deployment costly. These include single photon detectors for discrete-variable (DV) QKD, complex coherent networks for continuous-variable QKD, and high-extinction ratio electro-optic modulators. Modern photonic integrated circuit technology can address many of these hardware challenges and also allows for operation over many spectral channels to multiply up key rates. With continued advances in protocols and a transition to advanced photonic integrated circuits hardware, it is likely that key rates will push into the regime of tens to hundreds of Mbit/s over optical fiber in metro-scale links. Another important aspect of QKD development are practical and extensible architectures fitting the need of the application, including different types of network topologies in fiber networks, atmospheric links between ground and air frames, as well as satellite-based optical links. These QKD deployments should also be extensible to memories, laying the groundwork for *quantum repeater* networks. QKD field deployments are important intermediate steps towards quantum networks, as they require many of the precision timing and networking properties that will be essential for quantum repeater links.

Another major challenge is to close side-channel attacks—attacks against practical QKD implementations—at the protocol level. Measurement device independent (MDI) QKD and decoy state QKD protocols have closed detection and photon number splitting side-channel attacks. Device-independent QKD will provide the ultimate protection against side-channel attacks, including in transmitter hardware.

Quantum repeater networks/ the quantum internet

The next phase in quantum networks is to link distant quantum memories. In a basic repeater network, atomic quantum memories along a link are pairwise-entangled and connected via free space or fiber links.

There is active research and development in deploying small quantum networks on the metro-scale. The first examples of entangled quantum memories between partial repeater nodes have been developed, but major challenges must still be overcome. Quantum channels must have very low phase noise (which degrades quantum interference), and long-distance quantum networks require exquisite synchronization of time, frequency, and phase. QKD field deployments mentioned above are important in developing this precision network technology. Additional qubits are needed for quantum error correction, entanglement distillation, and quantum repeater multiplexing. Auxiliary components including quantum frequency conversion and on-demand entangled photon pair sources will extend link distances, increase entanglement rates, and enable fault tolerance in the network. There has been great progress on both of these components, but further improvements are needed in efficiency and scalability.

There appears to be much room to reduce the technical hurdles for high-speed quantum repeater networks by improved quantum repeater protocols. Particularly promising are protocols that incorporate feed-forward error correction, eliminating most of the time-consuming two-way classical communication between repeater nodes. Developing such protocols requires methods for producing error-corrected, loss-protected photonic entangled states and small-scale photonic quantum logic processors. An ultimate goal would be the creation of loss-protected optical quantum channels that could maintain encoded photonic quantum states in the laboratory and across deployed optical channels longer than is possible in low-loss optical fiber. Here, too, improved on-demand photon pair sources and detectors are of great importance.

Quantum networks could allow for long-distance quantum cryptography, but also many other functions not possible on today's internet. For instance, a quantum network opens the possibility to generate multi-party entangled states that can be used for various quantum enhanced communication tasks such as sharing a common secret key for efficient cryptographic conferencing, anonymous communication, or boosting classical information transfer. Distributed logical operations will enable quantum information processing between the network nodes, which will allow secure and private 'quantum cloud computing' and secure multi-party computation.

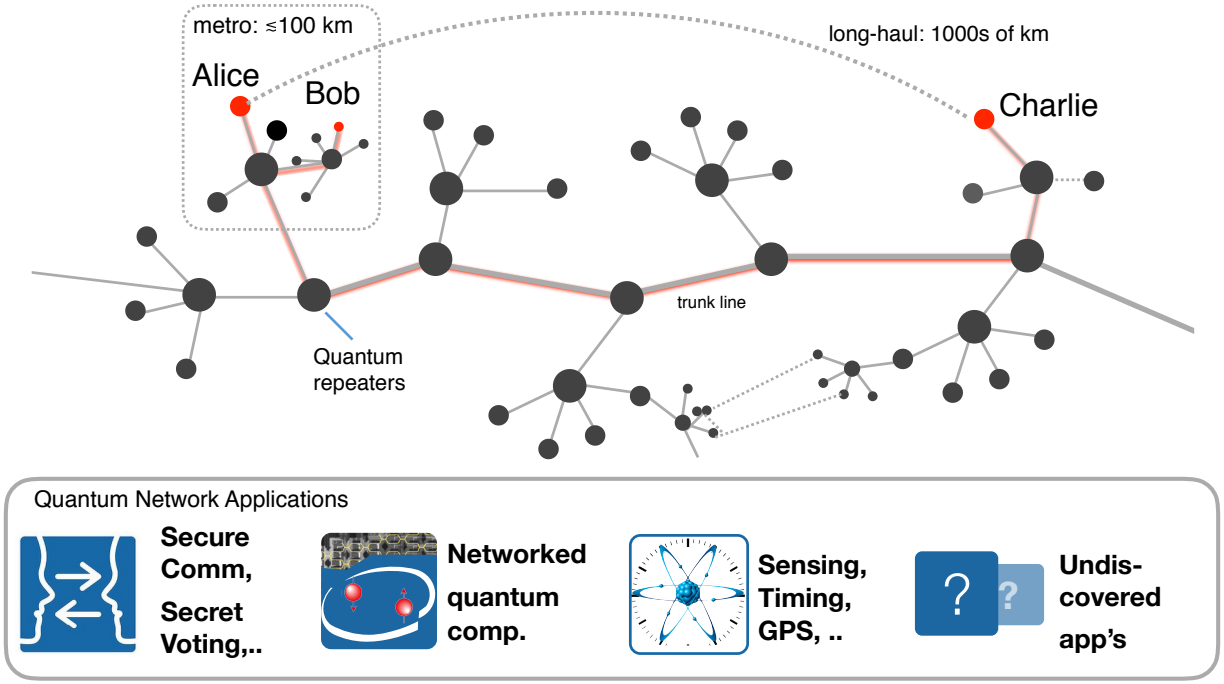


Figure 13. Quantum key distribution (QKD) allows unconditionally secure communication between two users, Alice and Bob, but its reach is limited to the metro-scale because of photon loss. Long-range quantum communications will become possible with the introduction of quantum repeater nodes in trunk lines that could span vast distances. These connected quantum memories will form a "quantum network" layer on top of today's classical internet. This "quantum internet" will allow a host of new proposed technologies beyond secure quantum communications, no doubt including many still undiscovered applications.

QUANTUM COMMUNICATION 5-YEAR OUTLOOK

Efficient on-demand sources of entangled photon pairs or larger entangled photonic micro-clusters; investigation of new photon source concepts to close the gap between system-level requirements on photon efficiency and experimental capability.

Optical communication systems operating near the quantum limit, for example using chip-based multi-mode optimal receivers to approach channel capacity limits.

Single photon detectors with >0.99 detection efficiency.

Quantum cryptography with secure bit transmission rates of more than 10^8 per second.

Efficient quantum interfaces between long-lived stationary memories (atomic and solid-state) and photons.

Prototype quantum repeaters and linking of two or more small-scale quantum computers via high-fidelity quantum communication channels.

Efficient quantum frequency conversion between telecom photons and atom-like memories as well as superconducting microwave cavities.

QUANTUM COMMUNICATION 10-YEAR OUTLOOK

Advanced photonic components and protocols for quantum key distribution at rates hundreds of Mbit/sec over metro-scale (~50km) distances in network topologies that are upgradable with quantum repeaters.

Development of on-demand single and entangled photon pair sources with sufficient purity, efficiency, and indistinguishability to produce large photonic cluster states.

The development of photon-loss-protected photonic states for forward error correction, allowing new forms of long-range quantum state transfer, cryptography, and mid-scale photonic quantum information processors.

Quantum repeater links beating repeaterless quantum cryptography rate-loss bounds

The demonstration of long-distance quantum communication channels consisting of multiple quantum repeaters, beating repeaterless quantum cryptography bounds.

High bit rate quantum cryptography over 1000s of kilometers. Construction of prototype quantum internet consisting of multiple medium scale quantum computers connected via high fidelity quantum communication channels.

QUANTUM COMMUNICATION 20-YEAR OUTLOOK

Networks capable of distributing entanglement at high rates over continental length scales, including efficient coherent interfaces to various types of quantum computers (atoms, solid-state, microwave...).

Quantum networks for efficient links between many quantum memories, high-speed quantum teleportation, cryptography, and modular quantum computing.

Small quantum networks are connected into global "quantum internet" whose functions, beyond secure communication and parallel computing, will include many other applications, including quantum digital signatures, quantum voting and secret sharing, anonymous transmission of classical information, and a host of sensing and metrology applications.

3. Challenges for quantum sensing and metrology

Quantum sensing and metrology represents perhaps the most mature and widely applied use of quantum information processing technology, with interferometers, atomic clocks, magnetometers, gyroscopes and accelerometers already operating at the *standard quantum limit*. **The primary challenge for quantum sensing and metrology is to surpass the standard quantum limit to attain the ultimate, Heisenberg-limited bounds to precision and accuracy.** To attain these bounds will require a concerted, joint theoretical/experimental effort over the next 5-10 years and beyond. Attaining strong quantum enhancements in detection (e.g., quantum illumination) and in sub-Rayleigh quantum imaging represent significant challenges. Equally important is the construction of compact and robust *quantum sensors*, detectors, and imagers that are suitable for deployment in extreme environments.

Here, we address the challenges for quantum sensing, metrology, and imaging via different platforms—interferometers, quantum clocks, NV-diamond quantum magnetometers, quantum gyroscopes, nanomechanical accelerometers, and networked quantum sensors (quantum GPS). Throughout, we emphasize the combination of theoretical and experimental challenges to be faced in attaining the ultimate quantum limits of precision measurement.

Interferometry

Optical interferometers represent one of the oldest precision quantum technologies and among the first to reach the standard quantum limit. To surpass the standard quantum limit requires the use of non-classical states such as squeezed states: e.g., the injection of squeezed vacuum into LIGO is a key part of the plan to gain the last order of magnitude in precision accessible for gravitational wave detection. While the plan to inject squeezed vacuum in LIGO has a long history, in just the last year it was shown that injection of squeezed vacuum is in fact the optimal strategy for attaining the ultimate quantum limits to precision of interferometry.

LIGO is a gigantic interferometer that maps out tiny changes in distance by interfering waves of light. One of the promising advances in quantum information processing technologies, described above, is the construction of integrated quantum optical chips containing hundreds of tunable interferometers in a square centimeter. Such devices have already demonstrated their power for performing quantum walks and boson sampling, and their tunable nature makes them natural candidates for implementing deep quantum learning using linear optics, integrated nonlinearities or measurement-induced nonlinearity, and methods to protect against or correct photon loss (culminating in fully loss-protected photonic channels). The ultimate quantum precision for measurement of changes in distance that such devices afford remains an open question. A challenge for the next 5-10 years is whether the use of non-classical states such as squeezed vacuum and multi-photon entangled states in integrated quantum optics provides a significant enhancement over semi-classical methods.

Quantum clocks

Atomic clocks represent one of the first applications of entangled states to enhance measurement accuracy and precision. Already in 1994, Dave Wineland's group at NIST had proposed using 'Schrödinger's cat' states of ions to enhance the precision of ion-trap atomic clocks beyond the standard quantum limit. Subsequent experimental demonstrations of such cat states in ion traps, combined with theoretical results on the ultimate capabilities of quantum clocks that use highly non-classical states, led to rapid advances in clock technology. Wineland's quantum logic atomic clock, which operates by entangling optical and microwave transitions within different atoms, represented for years the single most accurate measurement device on the planet.

The primary challenge for the demonstration of more accurate and precise quantum clocks is to combine the theory of precision quantum measurement with the practice to build quantum clocks that use quantum effects such as entanglement to continue

Figure 14. Quantum hardware is being deployed in space. In 2016, China launched a special-purpose satellite for quantum secure communications *(left).* **Space-based quantum networks could enable new forms of quantum global positioning systems and ultra-precise measurements** *(right).*

to implement the world's most precise measurement instruments. As will be seen below, if such quantum clocks can be linked by quantum communication channels to implement a global quantum GPS network (Fig. 14), the precision of global timekeeping can in principle be increased by orders of magnitude.

NV-diamond sensors

Nitrogen vacancy diamond (NV-diamond) combines in a single system (an NV-center) the precision control and readout of atom-optical systems with the robustness of solid-state systems. Nitrogen vacancies behave like 'super atoms' embedded in a diamond lattice. They afford exquisite control of their interactions with their surrounding nuclear spins, allowing the creation of large-scale entangled states between electrons and nuclei. Such states have the potential to provide highly precise measurements of the electromagnetic field at the nanoscale level. Current use of NV-centers for magnetometry and electric field sensing operates largely at the semi-classical standard quantum limit. A significant challenge for NV-diamond magnetometry over the next 5-10 years is to harness the effects of entanglement to attain Heisenberg limited magnetic field measurements.

Their ability to sense electromagnetic fields at distances of angstroms to nanometers make NV-centers into quantum probes with the potential to detect and image single molecules on the diamond surface (Fig. 15, left). They can also function as precise thermometers to measure the temperature in their local nanoscale environment. Spin-orbit couplings allow NV-centers to function as single-atom gyroscopes to measure changes in rotation and orientation. NVs or similar semiconductor spin systems may also produce new types of precision oscillators. Entangled NV-centers located a mile apart formed the basis for recent experimental demonstrations of loop-hole free Bell inequalities—an experimental test of Einstein's spooky action at a distance. Finally, if coupled by photons, NV-centers have the potential for modular universal quantum computation and quantum repeaters.

Their ubiquitous utility render NV-centers one of the most promising substrates for quantum sensing, imaging, and information processing. Much work remains to be done, however. The current quantum applications of NV-centers arose out of advances in fabrication technology for NV-diamond, by allowing the relatively precise implantation of NV-centers in ultra-pure and isotopically enhanced diamond. An important challenge to the development of NV- diamond quantum technologies is the ability to implant NV-centers with atomic precision. If this were possible, crystalline arrays of NV-centers could allow improved error corrected logical qubits or could be used for room-temperature solid state quantum computation.

Nitrogen vacancies are not the only type of atom-like defect that is available for quantum information processing. Silicon vacancy centers are significantly more stable optically, and there is promise that they, too, will feature long spin *coherence times*. SiC di-vacancies, though less studied than NV-diamond, represent a highly promising system for quantum information processing, including metrology and computation. A key challenge over the next 20 years is the ongoing development of material and fabrication techniques to put to use controllable, atom-like systems in solid state.

Nanomechanical resonators

The quantization of vibrational degrees of freedom—phonons—is an essential feature of matter. The recent construction of quantized mechanical resonating devices such as nanomechanical cantilevers (Fig. 15, right) holds great promise for the measurement of acceleration and of fundamental gravitational effects. The challenge over the next 5-10 years is to develop nanomechanical quantum devices that can exhibit the same counterintuitive phenomena such as squeezing and entanglement that have already been observed in atom-optical and solid-state devices. Such squeezed and entangled nanomechanical resonators

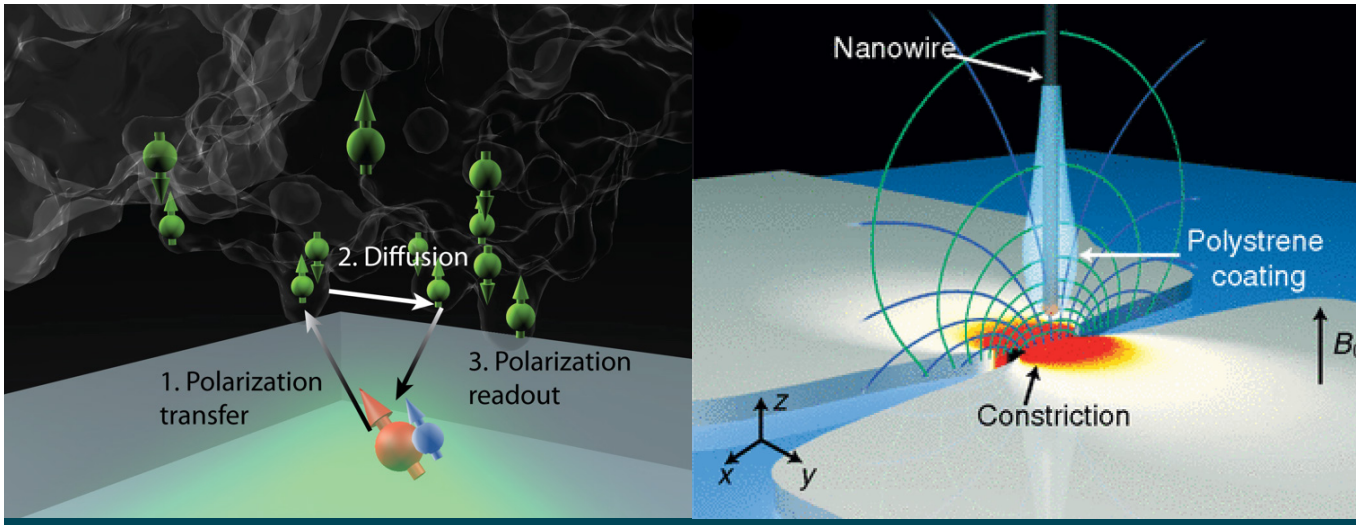


Figure 15. *(left)* **NV centers embedded a few nanometers under a diamond surface are being developed as ultra-sensitive magnetic field probes of external materials, including nuclear magnetic resonance detection of single proteins** *(Credit: P Cappellaro, MIT; R Walsworth, M Lukin, H Park, Harvard). (right)* **An alternative method, magnetic resonance force detection with nanoscale cantilevers, is being developed for nanometer-scale nuclear magnetic resonance imaging.** *(credit: Raffi Budakian, U. Waterloo)*

could serve as probes that measure acceleration and gravitational fields to beyond the standard quantum limit. Because they are relatively massive compared to individual atoms and electrons, quantized vibrational mechanical systems can also provide sensitive tests of the predictions of various theories of quantum gravity.

Just as the ability to link up quantum computers via quantum communication lines into a quantum internet opens up a host of applications for extended quantum computation, the ability to link up quantum sensors and measurement devices via quantum communication channels opens up a host of potential applications for quantum sensing and imaging. The classical global positioning system (GPS) consists of clocks mounted on satellites able to exchange temporal signals with each other and with observers on the ground. If the clocks on the satellites are quantum clocks operating beyond the standard quantum limit, and if the signals that they exchange encode time in a way that protects *quantum coherence*, the resulting quantum GPS (qGPS) has the potential to provide unprecedented accuracy in temporal and spatial resolution. The technical challenges to creating such a quantum GPS system are great, but are perhaps not so great as they first might seem. First, GPS clocks are already quantum clocks operating at the standard quantum limit: entangled clocks that surpass this limit have been constructed on the ground, and might soon make their way into orbit. Second, the fact that GPS satellites are in space greatly simplifies quantum communications, as free-space optical communication between satellites suffers no atmospheric attenuation or turbulence.

Clearly, the implementation of quantum GPS is a grand challenge, to be achieved on a 10-20 year timeframe. In the meanwhile, quantum information theory faces the challenge of determining the ultimate precision of networked quantum clocks. While the last two decades have seen multiple advances in the theory of quantum precision measurement, including the establishment of the Heisenberg limit for measurements made with a single quantum device, much less is known about the precision of measurements made by quantum sensors linked by quantum communication channels. The Heisenberg limit provides a $\sqrt{N}$ enhancement over the standard quantum limit, where N is the number of individual measurements made. However, in the case of positioning by reference to a network of quantum sensors—quantum GPS— it is not known whether this limit still applies. For example, it is possible—even if unlikely—that the precision of quantum positioning might grow exponentially with the number of quantum clocks in the network. **One of the primary challenges to quantum information theory is to determine the ultimate limits to precision measurement allowed by an internet of quantum clocks or quantum GPS.**

QUANTUM SENSING & METROLOGY 5-YEAR OUTLOOK

Quantum sensing and metrology systems that use entanglement and squeezing to surpass the performance of semiclassical devices that operate at or above the standard quantum limit.

Best-of-class sensors based on NV-diamond (magentometers), atom/ion traps (entangled quantum clocks), *squeezed light* (interferometers), engineered multi-photon quantum states (spectrometers), atom interferometers (gyroscopes, gravitometers).

Diamond quantum sensors for precision detection of spins, molecules, and biological processes.

QUANTUM SENSING & METROLOGY 10-YEAR OUTLOOK

Long-distance networked quantum metrology: quantum GPS and global quantum clocks.

Mapping the atomic structure of individual small biomolecules under native conditions using quantum magnetometers.

Noninvasive, real-time mapping of individual neurons using quantum magnetometers.

The development of quantum sensor networks.

QUANTUM SENSING & METROLOGY 20-YEAR OUTLOOK

Quantum sensing as an established tool for brain and neuroscience, including real-time recording and imaging of action potentials.

Quantum sensing using solid-state spins established for mapping biomolecules under native conditions; applications in life sciences, chemistry, batteries...

Space-based quantum GPS and global quantum clocks to provide universal sub-millimeter positioning accuracy.

Detection of gravitational waves and dark matter with a space-based network of quantum sensors (e.g., clocks, atom interferometers).

How to get there

To attain these specific and ambitious goals for quantum computation, communication, and sensing/measurement in the timeframes envisaged, the participants identified a set of continuing goals that need to be pursued over the full twenty-year period.

- Continual improvement of precision quantum control, including coherent quantum feedback
- Continued reduction of decoherence and noise
- Identification and testing of novel quantum platforms and materials
- Continued research into topological quantum materials for fault-tolerant quantum computation
- Understanding the computational power of analog and digital quantum simulators
- Creation and characterization of large, controllable entangled quantum states
- Development of methods for qCVV—quantum certification, verification, and validation
- Development of improved quantum error correction and fault tolerance
- Understanding the physical limits of quantum metrology
- Improved light sources, photonics, and detectors
- Development of novel quantum algorithms
- A combined theoretical and experimental effort on scalability and modularity for quantum systems

National resources for quantum information processing

The United States government has initiated and supported a variety of powerful and effective resources for quantum information processing research.

The DOD was the first government agency worldwide to recognize the promise of quantum information technologies and to provide funding. Beginning in 1994, immediately after Shor's algorithm, DOD funding agencies, including DARPA, ARO, AFOSR, and ONR, began supporting research into quantum information theory and quantum information technology that resulted in a host of remarkable advances. The first ion-trap quantum computers, the first optical quantum logic gates, and the first experimental realizations of quantum algorithms, were all created in the US in the 1990s. More recently, DOD investment in superconducting quantum information processing has supported the development of superconducting qubits that hold the world records for coherence and controllability. Over the last few decades, DOD-supported theoretical investigations have given rise to novel quantum algorithms, quantum error correction techniques, and advances in secure quantum communications and networked quantum computers.

The National Institute of Standards and Technology (NIST), another original founder of the field, has continued at the forefront of the field over the last two decades. NIST supports two joint centers in quantum information science at the University of Maryland (UMD). The Joint Quantum Institute (JQI), established in collaboration with UMD and the Laboratory for Physical Sciences (LPS), has played an important role in developing a variety of quantum technologies and has become a global leader in quantum information processing theory and technology. More recently, NIST and UMD established the Joint Center for Quantum Information and Computer Science to complement JQI with a focus on the computational aspects of quantum information processing.

The National Laboratories have also played an important part in the development of the field. Los Alamos National Laboratory (LANL) supplied many early innovations in quantum information dating back to the 1980s and continues to maintain a powerful theoretical group. The recent acquisition of a D-Wave quantum annealer adds a strong experimental component to this effort. MIT Lincoln Laboratory has played a crucial role in the development of lithographic technologies for superconducting quantum circuits, dating back to 2000, and remains at the forefront of this effort to this day, with the capacity to supply highly coherent networked qubits for multiple purposes. In the last decade Sandia National Laboratory has developed a broad program in quantum information technologies, including a strong theoretical effort in quantum information processing, and support for a foundry that supplies many US research groups with powerful ion traps.

It was the unanimous sense of the researchers at the workshop that the government assets in quantum information should continue to be supported, and that further efforts should be made to coordinate the efforts of these assets with research programs in academia and in industry, for example by fostering industry-academia collaborations. Many of the experimental systems have reached a level where engineering is becoming too difficult to manage within traditional university research groups. This gap could be addressed through centers of excellence focused on quantum engineering; support for concentrated centers with the required expertise and/or research staff in quantum engineering, electronics design, etc.; and a push to encourage quantum engineering at university undergraduate and graduate programs. Many other systems are highly promising, but require continued support to reach the point at which they could reasonably be scaled.

A National Initiative in Quantum Information Science and Technology

For the first two decades of development of the field of quantum information, the United States was the world leader, with particular emphasis on the development of novel quantum technologies. Now there is competition. Other countries have built strong programs in quantum information science and technology and are expanding their support. Canada and Australia have for a decade and a half featured quantum information as one of their primary national research foci. Great Britain has begun a £500 million effort in quantum technologies and the European Union recently announced a €1 billion Flagship Program in quantum information. China is investing similar amounts in the development of quantum cryptography networks, earth-to-satellite quantum communication links, quantum repeaters, and quantum computation.

One of the questions debated at the workshop was whether the United States should have a single, unified, large-scale program in quantum information science and technology. The sense of the considerable majority of researchers was that the historical strength of the US effort arose in part from its 'bottom up' approach, as compared with the 'top down' approach of other nations. The rapid progress of research on quantum information in the US came about because different funding agencies and institutions mounted strong and successful efforts aimed at specific problems. Participants largely agreed that a National Initiative in Quantum Information Processing could provide the greater degree of coordination between funding efforts that is necessary to attain the grand challenges facing the field, but that the creation of such an initiative should not be at the expense of the highly successful bottom-up approach in which agencies and institutions pursue the goals that are most important for their individual mandates.

Conclusions

In its early beginnings, results for quantum information processing were purely theoretical, and fundamental limits were not yet known. Since then, the field has exploded to provide a host of novel quantum technologies for computation, communication, and precision measurement and sensing. This technological development was made possible by, and in turn inspired the development of a comprehensive theory of quantum information.

The accelerating pace of technological and theoretical development in quantum information has brought the field to a crucial phase. At this moment, there is a clear path to developing mid-scale quantum computers that can solve problems that are difficult or impossible for classical computers to solve; quantum cryptography is a reality, and development of quantum repeaters holds the promise for global quantum-secured communications and a host of new applications; the possibility of constructing measurement devices that attain the Heisenberg limit has been demonstrated, and methods have been developed that should allow a host of measurement, sensing, and imaging technologies to reach their fundamental quantum limits. As noted in the last section, there is a clear roadmap with well-defined milestones for attaining the goals of quantum information processing technologies over the next 5-10 years. To attain the final grand challenges over a 20 year time frame will require the close coordination of experimental and technological efforts with theoretical investigations into quantum error correcting codes, methods for quantum communication, and quantum sensing and imaging. Continuing fundamental research beyond 'quantum engineering' applications is mandatory if we are to realize the power of quantum information processing technologies. It is too early to focus on a limited set of physical quantum architectures. Similarly, new techniques for channel encoding are required to attain the capacities of quantum channels. With continued research into the fundamental theory and experimental practice of quantum information processing, we anticipate the development of novel computational platforms (e.g., topological quantum computers), and of experimentally realizable methods to attain the physically dictated bounds to communication and sensing. US Government support for basic research in quantum information processing over the past two decades has seeded an entire new field of science and technology. Continued research into the fundamental science of quantum information processing over the next two decades will allow us to reap the quantum harvest.

"To attain the final grand challenges over a 20 year time frame will require the close coordination of experimental and technological efforts with theoretical investigations into quantum error correcting codes, methods for quantum communication, and quantum sensing and imaging."

Glossary

Coherence: A coherent quantum state maintains a deterministic phase within a superposition. 6, 9

Cold atoms or ultracold atoms: Gas-phase atoms, typically in a vacuum, that are cooled to near 0 Kelvin by laser cooling and other related methods. 10, 12

Color Center: A fluorescent defect in a crystal, such as the nitrogen vacancy center in diamond. 12

Decoherence: Environmental effects that destroy quantum coherence (q.v.). 8, 16

Entanglement: A counterintuitive form of quantum correlation that Einstein characterized as 'spooky action at a distance'. 5, 8

Hamiltonian dynamics: The dynamics of a quantum system governed by physics described by a Hamiltonian operator. 11, 18

Heisenberg limit: The ultimate limit to precision sensing, detection, and measurement that can be attained using counterintuitive quantum effects such as entanglement and squeezing. 6, 13

Interferometer: A device that uses interference between waves to perform precision measurement. 5, 10

Ion trap: A device that uses static and oscillatory electromagnetic fields to trap ions in a regular array. Ion traps allow a high degree of quantum coherence and quantum control and are promising systems for quantum computation and for precision measurement. 8, 10

Nitrogen-Vacancy diamond (NV-diamond): An 'artificial atom' in diamond composed of a nitrogen atom coupled with a vacant space in the diamond lattice. NV-diamond exhibit high levels of quantum coherence and addressability which render them promising systems for quantum information processing. 8, 18

NP-completeness: A complexity class in theoretical computer science for problems that have no efficient (polynomial-time) algorithm to solve, but whose solution is efficient to verify. 11

Optical lattice: A lattice formed by intersecting laser beams that can be used to trap and address arrays of atoms. Atom-optical lattices allow high levels of coherence and scalability and are promising systems for quantum computation. 18

Quantum annealer: A special-purpose quantum information processor whose goal is to find the solutions to hard optimization problems via a coherent quantum analog to the classical process of simulated annealing. 10, 18

Quantum bit or 'qubit': The quantum analog of a classical bit. A two-state quantum system that can exhibit quantum effects such as coherence, superposition, and entanglement with other qubits. 7, 10

Quantum Characterization Validation and Verification (qCVV): The set of techniques required to characterize the ability of quantum systems to acquire, transmit, and process information, and to validate and verify their efficient operation. 10, 18

Quantum coherence: The effect of the wave-like nature of quantum mechanics. 12, 25

Quantum coherence time: The duration over which a quantum superposition is preserved. 8, 24

Quantum communication channel: A communication channel such as a fiber optic cable that allows quantum bits to be transmitted while preserving quantum coherence. 6, 12

Quantum computer: A device that processes information exploiting the quantum properties of individual elementary particles, atoms, quantized solid-state systems, and the like. 5, 9

Quantum cryptography: A set of theoretical and experimental techniques that use the properties of quantum mechanics to transmit information securely. 5, 12

Quantum dot: An artificial atom consisting of a nanoscale semiconductor crystal. 6, 8

Quantum error correcting code: A quantum analog of a classical error correcting code, which encodes quantum information in a redundant form that allows errors to be detected and corrected. 11, 16

Quantum GPS: A network of quantum clocks connected by quantum communication channels. 14, 23

Quantum gravity: A physical theory that reconciles quantum physics with gravity. 9, 14

Quantum internet: A network of quantum computers connected by quantum communication channels. 7, 12

Quantum key distribution: A quantum cryptographic technique for distributing a secret key whose privacy is guaranteed by the laws of quantum mechanics. 12, 20

Quantum machine learning: A set of quantum information processing techniques for finding and classifying patterns in data. *10*, *17*

Quantum random access memory (qRAM): The quantum analog of classical random access memory (RAM). qRAM allows information to be stored and retrieved while retaining quantum coherence. *17*, *19*

Quantum repeater: A device that can act as an effective amplifier of quantum coherence and entanglement. Quantum repeaters are necessary for establishing long-range quantum communication channels. *12*, *21*

Quantum sensor: A device that uses quantum effects to detect and measure. *13*, *23*

Quantum simulator: A special-purpose 'quantum analog computer' that is used to simulate the behavior of other quantum systems. *17*, *19*

Quantum supremacy: The demonstration that a quantum system can perform a task that no classical computer can do in a reasonable time, i.e., a duration that grows polynomially with the size of the problem. *11*, *17*

Quantum teleportation: The process by which all of the information contained in one quantum state (such as a photon) is perfectly transferred to another location. Successful quantum teleportation also requires the exchange of classical information between the two sites, so it does not allow for superluminal transmission of information. *12*, *20*

Quantum tunneling: The process by which a quantum system can jump—or "tunnel"—through an energetic barrier. For example, classically, a tennis ball cannot tunnel through a wall, but in quantum mechanics, an electron could tunnel through a region of space where it is not energetically allowed. *6*, *11*

Quantum weirdness: The notion that physics at the quantum scale behaves in counter-intuitive ways. *3*, *13*

Squeezed light: Light whose quantum fluctuations in electric or magnetic field have been reduced below the Standard Quantum Limit. *6*, *25*

Standard Quantum Limit: The limit to precision measurement that can be attained by semi-classical methods that do not use quantum coherence, entanglement, or squeezing. For photons, this is known as the "shot noise limit." *13*, *23*

Topological quantum computing: An idea for quantum computing in which the quantum memories are not composed of particles—such as electrons—but of quantum braids in 3D space-time, whose topological order could be more stable to interactions with the environment. *7*

Appendix I
Quantum Workshop Attendees

David Cory
https://uwaterloo.ca/institute-nanotechnology/people-profiles/david-g-cory
University of Waterloo, dcory@uwaterloo.ca
Department of Chemistry
PhD (1987), Physical Chemistry, Case Western Reserve University

David Cory is a Professor in the Department of Chemistry and the Canada Excellence Research Chair in Quantum Information at the University of Waterloo. He is also a visiting researcher at Canada's Perimeter Institute for Theoretical Physics, and chair of the advisory committee for the Canadian Institute for Advanced Research. Dr. Cory is an experimentalist working to develop solid-state quantum devices based on spins and superconductors. His group also aims to contribute new ideas for control and benchmarking quantum devices.

Ivan Deutsch
http://cquic.unm.edu
University of New Mexico, ideutsch@unm.edu
Department of Physics and Astronomy
PhD (1992), Physics, University of California, Berkeley

Ivan H. Deutsch is Regents' Professor of Physics and Astronomy at the University of New Mexico and a Project Director at the Center for Quantum Information and Control (CQuIC). He receved his BS in physics from MIT in 1987, his physics PhD from UC Berkeley in 1992, was a postdoc at France Tel/ecom in 1993, and an NRC postdoc at NIST from 1993-1995. He joined the UNM faculty in 1995 and together with Carlton M. Caves, established CQuIC in 2008. He is the founder of Southwest Quantum Information and Technology (SQuInT), a leading interdisciplinary workshop in quantum information science, now in its 18th year. His research expertise is in quantum information theory, quantum optics, and atomic-molecular-optical (AMO) physics. He studies the physical implements of quantum information processing in AMO systems with particular emphasis on quantum control, measurement, and tomography. A current interest is in the power and limitations of analog quantum information processors.

Jonathan P. Dowling
http://quantum.phys.lsu.edu
Louisiana State University, jdowling@lsu.edu
Department of Theoretical Physics, Hearne Institute for Theoretical Physics
PhD (1988), Mathematical Physics, University of Colorado at Boulder

Jonathan P. Dowling is the Hearne Chair Professor of Theoretical Physics and Co-Director of the Hearne Institute for Theoretical Physics, Department of Physics and Astronomy at Louisiana State University, Baton Rouge, Louisiana. He was a Visiting Research Scientist at the International Center for Theoretical Physics in Trieste, Italy (1986-1987); a Visiting Research Scientist at the Max Planck Institute for Quantum Optics in Garching, Germany (1989-1990); and a National Research Council Research Associate in the Optical Science & Technology group at Army Aviation and Missile Command (AMCOM), Huntsville, Alabama (1990-1994). He then took a post as Research Physicist at AMCOM (1994-1998), before leaving to take a position as Research Scientist at the Senior Level in the Quantum Computing Technologies Group at JPL, where he was eventually promoted to Group Supervisor & Principal Scientist (1998-2004), before taking his current posts at LSU in 2004. Prof. Dowling has over 130 published articles, with an h-index of over 37, and he holds eight US patents in the fields of nonlinear and quantum optics. He is a Fellow of the American Association for the Advancement of Science, a Fellow of the American Physical Society, a Fellow of the Institute of Physics, and a Fellow of Optical Society of America, and has served on the editorial board of Physical Review, the Journal of the European Optical Society, Concepts of Physics and Crystals. He has been awarded the Willis E. Lamb Medal for Laser Science and Quantum Optics (2002), the US Army Research and Development Achievement Award (1996), the NASA Space Act Award (2002), and was runner up for the Discover Magazine Technology of the Year Award (2001).

Dirk Englund
http://qplab.mit.edu
Massachussetts Insitute of Technology, englund@mit.edu
Department of Electrical Engineering & Computer Science
PhD (2008), Applied Physics, Stanford University

Dirk Englund is Jamieson Career Development Professor of Electrical Engineering and Computer Science at MIT and is a member of the Research Laboratory of Electronics (RLE) and Micosystems Technology Laboratory (MTL). His research focuses on quantum technologies based on semiconductor and optical systems. Recent recognitions include the 2011 Young Faculty Award, the 2012 IBM Young Faculty Award, and an 2016 R&D100 Award.

Alexey Gorshkov
http://groups.jqi.umd.edu/gorshkov/
University of Maryland, NIST, *gorshkov@jqi.umd.edu*
Department of Physics
PhD (2006), Physics, Harvard University

Alexey Gorshkov is an Adjunct Assistant Professor in the Department of Physics at the University of Maryland, a fellow at the National Institute of Standards and Technology and a fellow at the Joint Quantum Institute (JQI) and Joint Center for Quantum Information and Computer Science (QuICS) at the University of Maryland. Dr. Gorshkov leads a theoretical research group working at the interface of quantum optics, atomic and molecular physics, condensed matter physics, and quantum information science.

Saikat Guha
https://sites.google.com/site/saikatguha/
Raytheon BBN Technologies, *sguha@bbn.com*
Quantum Information Processing Group
PhD (2008), Electrical Engineering and Computer Science, MIT

Saikat Guha is a Lead Scientist with the Quantum Information Processing group at BBN Technologies in Cambridge, MA. Dr. Saikat represented India at the International Physics Olympiad in 1998, where he was awarded the European Physical Society award. He was awarded the Raymie Stata Award for Outstanding Teaching for his role as teaching assistant for the MIT course Signals and Systems in Fall 2005. A DARPA Information in a Photon program team he led won the Raytheon 2011 Excellence in Engineering and Technology Award, Raytheon's highest technical honor. Saikat's research interests include investigating fundamental quantum limits on optics-based information processing with applications to communications, imaging and computation, and structured realizations of optical systems that can approach those performance limits. He is also interested in network science and network communication theory. He currently leads several research projects funded by DARPA, ONR, NSF, and DoE, on various topics spanning quantum-limited optical information processing.

Kai Hudek
http://iontrap.umd.edu
University of Maryland, *khudek@gmail.com*
Department of Physics
PhD (2013), Physics, University of Colorado at Boulder

Kai Hudek is a Research Scientist in the laboratory of Chris Monroe at the University of Maryland. His research aims to construct and use ion-trap-based quantum computer hardware at a scale that will be able to perform computational tasks that are hard or impossible using conventional information technology.

Liang Jiang
http://jianggroup.yale.edu/
Yale University, *liang.jiang@yale.edu*
Department of Applied Physics
PhD (2009), Physics, Harvard University

Liang Jiang is an Assistant Professor of Applied Physics and Physics at Yale University. His research interests are AMO physics, condensed matter physics, and quantum information science. Prof. Liang has made important contributions to secure quantum communication over long distances, including quantum repeater with encoding, optimization of quantum repeaters, and network based quantum computation. Liang has also worked on room-temperature diamond-based quantum information processing, including ultra-long nuclear spin quantum memories, perfect quantum state transfer via thermal spin chains, and nano-magnetometer using color defects in diamond. Recently, Liang has been investigating quantum information processing with electro-opto-mechanical systems and superconducting circuits that have ultra-strong couplings and unprecedented non-linearity of microwave photons. Liang has been awarded the Alfred P. Sloan Research Fellowship and the David and Lucile Packard Foundation Fellowship in 2013.

Mark Kasevich
https://web.stanford.edu/group/kasevich/cgi-bin/wordpress/
Stanford University, *kasevich@stanford.edu*
Department of Physics
PhD (1992), Applied Physics, Stanford University

Mark Kasevich is Professor of Physics and Applied Physics, Stanford University and co-founder and consulting Chief Scientist of AOSense, Inc. His research interests are centered on the development of quantum sensors of rotation and acceleration based on cold atoms (quantum metrology), the application of these sensors to the tests of General Relativity, the investigation of many-body quantum effects in Bose-condensed vapors (including quantum simulation), and the investigation of ultra-fast laser-induced phenomena.

Wolfgang Ketterle
http://cua.mit.edu/ketterle_group/
MIT, *ketterle@mit.edu*
Department of Physics
Cambridge, MA

Wolfgang Ketterle has been the John D. MacArthur professor of physics at MIT since 1998. He received a diploma (equivalent to master's degree) from the Technical University of Munich (1982), and the Ph.D. in physics from the University of Munich (1986). He did postdoctoral work at the Max-Planck Institute for Quantum Optics in Garching and at the University of Heidelberg in molecular spectroscopy and combustion diagnostics. In 1990, he came to MIT as a postdoc and joined the physics faculty in 1993. Since 2006, he is the director of the Center of Ultracold Atoms, an NSF funded research center, and Associate Director of the Research Laboratory of Electronics. His research group studies properties of ultracold atomic matter. For his observation of Bose-Einstein condensation in a gas in 1995, he received the Nobel Prize in Physics in 2001. Other honors include the Gustav-Hertz Prize of the German Physical Society (1997), the Rabi Prize of the American Physical Society (1997), the Fritz London Prize in Low Temperature Physics (1999), the Benjamin Franklin Medal in Physics (2000), and a Humboldt research award (2009).

Raymond Laflamme
https://services.iqc.uwaterloo.ca/people/profile/laflamme/
University of Waterloo, *iqc-dtr@uwaterloo.ca*
Department of Physics and Astronomy, Institute of Quantum Computing
PhD (1988), Applied Mathematics and Theoretical Physics, Cambridge University

Raymond Laflamme is a Professor in the Department of Physics and Astronomy and the Director of the Institute for Quantum Computing at the University of Waterloo and is also a the Director of the Quantum Information Program at the Canadian Institute for Advanced Research (CIFAR). His pioneering research in quantum information processing work includes theoretical approaches to quantum error correction, novel uses of linear optics to make quantum information processors and new methods to make quantum information robust against corruption in both cryptographic and computational settings. He has received a Fellowship from the American Association for the Advancement of Science, the American Physical Society and the Royal Society of Canada.

Andrew Landahl
www.sandia.gov
Sandia National Laboratories, *alandahl@sandia.gov*
Center for Computing Research
PhD (2002), Physics, Caltech

Dr. Landahl is a Senior member of technical staff in the Quantum Information Science and Technology Center at Sandia National Laboratory. His research has spanned topics in quantum error correction, quantum algorithms, and quantum control. He has BS degrees in Math and Physics from Virginia Tech, MS and PhD degrees in Physics from Caltech, and post-doctoral experience from MIT. He is a Distinguished Scientist at Sandia National Laboratories and a Research Professor at the University of New Mexico. He recently chaired the American Physical Society's Topical Group on Quantum information, helping it to grow to over 1600 members.

Daniel Lidar
http://qserver.usc.edu/
University of Southern California, *lidar@usc.edu*
Department of Electrical Engineering, Chemistry and Physics
PhD (2000), Physics, Hebrew University of Jerusalem

Daniel Lidar is a Professor of Electrical Engineering, Chemistry, and Physics, and holds a Ph.D. in physics from the Hebrew University of Jerusalem. He did his postdoctoral work at UC Berkeley. Prior to joining USC in 2005 he was a faculty member at the University of Toronto. His main research interest is quantum information processing, where he works on quantum control, quantum error correction, the theory of open quantum systems, quantum algorithms, and theoretical as well as experimental adiabatic quantum computation. He is the Director of the USC Center for Quantum Information Science and Technology and is the Scientific Director of the USC-Lockheed Martin Center for Quantum Computing. Lidar is a recipient of a Sloan Research Fellowship and is a Fellow of the AAAS, APS, and IEEE.

Seth Lloyd
http://meche.mit.edu/people/faculty/SLLOYD@MIT.EDU
MIT, slloyd@mit.edu
Department of Mechanical Engineering
PhD (1988), Physics, Rockefeller University

Seth Lloyd is Nam P. Suh Professor of Mechanical Engineering and Professor of Physics at MIT. Dr. Lloyd's research focuses on problems on information and complexity in the universe. He was the first person to develop a realizable model for quantum computation and is working with a variety of groups to construct and operate quantum computers and quantum communication systems. Dr. Lloyd has worked to establish fundamental physical limits to precision measurement and to develop algorithms for quantum computers for pattern recognition and machine learning. Dr. Lloyd's work on complex systems currently focuses transitions between stability and instability in complex dynamical systems.

Mikhail Lukin
http://lukin.physics.harvard.edu/
Harvard University, lukin@physics.harvard.edu
Department of Physics
PhD (1998), Physics, Texas A&M University

Mikhail Lukin is Professor of Physics at Harvard University. His research is in the areas of quantum optics and atomic physics. The emphasis is on studies of quantum systems consisting of interacting photons, atoms, molecules and electrons coupled to realistic environments. His group is developing new techniques for controlling the quantum dynamics of such systems, and studying fundamental physical phenomena associated with them. These techniques are used to explore new physics, as well as to facilitate implementation of potential applications in emerging areas such as quantum information science and in more traditional fields such as nonlinear optics. In the course of this work we are also exploring the emerging interfaces between quantum optics and atomic physics on the one hand, and condensed matter and mesoscopic physics on the other.

Trey Porto
http://groups.jqi.umd.edu/porto/
NIST and University of Maryland, porto@jqi.umd.edu
Joint Quantum Institute and PML
PhD (1996), Physics, Cornell University

Trey Porto is a NIST researcher and Adjunct Professor at the University of Maryland studying ultra-cold atoms in optical lattices as a platform for quantum simulation and information.

John Preskill
www.theory.caltech.edu/~preskill
California Institute of Technology, preskill@caltech.edu
Department of Physics
PhD (1980), Physics, Harvard University

John Preskill is the Richard P. Feynman Professor of Theoretical Physics at the California Institute of Technology, and Director of the Institute for Quantum Information and Matter at Caltech. Preskill received his Ph.D. in physics in 1980 from Harvard, and joined the Caltech faculty in 1983. Preskill began his career in particle physics and cosmology, but in the 1990s he got excited about the possibility of solving otherwise intractable problems by exploiting quantum physics; he is especially intrigued by the ways our deepening understanding of quantum information and quantum computing can be applied to other fundamental issues in physics, such as the quantum structure of space and time.

Barry Sanders
http://iqst.ca/people/peoplepage.php?id=4
University of Calgary, sandersb@ucalgary.ca
Institute for Quantum Science and Technology
PhD (1987), Physics, Imperial College

Dr Barry Sanders is AITF iCORE Strategic Chair in Quantum Information Science and Director of the Institute for Quantum Science and Technology at the University of Calgary. He is especially well known for seminal contributions to theories of quantum-limited measurement, highly nonclassical light, practical quantum cryptography and optical implementations of quantum information tasks. His current research interests include quantum resources & algorithms, optical, atomic and solid-state implementations of quantum information processing, quantum processes in biological systems, and machine learning for quantum control. His achievements are recognized through Fellowships with the Institute of Physics (U.K.), the Optical Society of America, and the American Physical Society, and Senior Fellowship with the Canadian Institute for Advanced Research. Sanders is Editor-in-Chief of New Journal of Physics, a former Associate Editor of Physical Review A, a former Editor of Optics Communications and a former editor of Mathematical Structures of Computer Science.

Peter Shor
http://math.mit.edu/~shor/
Massachussetts Institute of Technology, *shor@mat.mit.edu*
Department of Mathematics
PhD (1985), Applied Mathematics, MIT

Peter Shor is Professor of Applied Mathematics as Massachussetts Institute of Technology. He received his B.S. in Mathematics from Caltech in 1981 and his a Ph.D. in Applied Mathematics from M.I.T. in 1985. After a one-year postdoctoral fellowship at the Mathematical Sciences Research Institute in Berkeley, he moved to AT&T Bell Laboratories. In 2003, he became Professor of Applied Mathematics at MIT. Until 1994, his research focused on algorithms for conventional computers and research in probability and combinatorics. In 1994, he discovered an algorithm for factoring large integers into primes on a (still hypothetical) quantum computer. Since then, his research has focused on investigating quantum computing and quantum information theory.

Jake Taylor
http://groups.jqi.umd.edu/taylor
QuICS/JQI/NIST, *jmtaylor@umd.edu*
Quantum Measurement Division
PhD (2006), Physics, Harvard University

Jake Taylor is a Physicist at the National Institute of Standards and Technology, co-director of the Joint Center for Quantum Information and Computer Science at the University of Maryland, and a Joint Quantum Institute Fellow. His research group investigates the fundamental limits to quantum devices for computation and communication. He received an AB in Astronomy & Astrophysics and Physics at Harvard in 2000 and then spent a year as a Luce Scholar at the University of Tokyo. Taylor returned to Harvard for his PhD in the group of Mikhail Lukin in 2006, and went on to a Pappalardo Fellowship at MIT. In 2009 Taylor joined the Joint Quantum Institute and NIST. He is the recipient of the Newcomb Cleveland Prize of the AAAS, the Samuel J. Heyman Service to American “Call to Service” medal, the Silver Medal of the Commerce Department, the Presidential Early Career Award for Science and Engineering, and the IUPAP C15 Young Scientist prize.

Lorenza Viola
http://www.dartmouth.edu/~viola/
Dartmouth College, *Lorenza.Viola@Dartmouth.edu*
Department of Physics and Astronomy
PhD (1996), Theoretical Physics, University of Padua

Lorenza Viola is a theoretical physicist specializing in quantum information science. Following a Laurea (Master) degree in Physics from the University of Trento, Italy (1991), and a Ph.D. in Theoretical Physics from the University of Padua, Italy (1996), she has been a postdoctoral fellow at the Massachusetts Institute of Technology and a J. R. Oppenheimer Fellow at Los Alamos National Laboratory. She joined the faculty of Dartmouth College in 2004. Her research encompasses a broad range of topics in theoretical quantum information science, with emphasis on open quantum systems and quantum control, quantum correlations, and quantum matter.

Edo Waks
www.ireap.umd.edu/NanoPhotonics
University of Maryland, *edowaks@umd.edu*
Department of Electrical and Computer Engineering
PhD(2003), Electrical Engineering, Stanford University

Edo Waks is a professor in the Department of Electrical and Computer Engineering at the University of Maryland, College Park. He is also a member of the Joint Quantum Institute (JQI), a collaborative effort between the University of Maryland and NIST, Gaithersburg, dedicated to the study of quantum coherence. Waks received his B.S. and M.S. from Johns Hopkins University, and his Ph.D. from Stanford University. He is a recipient of a Presidential Early Career Award for Scientists and Engineers (PECASE), an NSF CAREER award, and ARO Young Investigator Award for the investigation of interactions between quantum dots and nanophotonic structures. His current work focuses coherent control and manipulation semiconductor quantum dots, and their interactions with photonic crystal devices for creating strong atom-photon interactions.

Ian Walmsley
http://www2.physics.ox.ac.uk/research/ultrafast-quantum-optics-and-optical-metrology
University of Oxford, ian.walmsley@physics.oc.ac.uk
Department of Physics
PhD (1986), Physics, Imperial College London

Ian Walmsley is the Hooke Professor of Experimental Physics at the University of Oxford, where he is also the Pro-Vice-Chancellor for Research and Innovation. His group's research covers a broad range of optical science and engineering, especially in the areas of ultrafast, nonlinear and quantum optics. In these areas the group has contributed to the development of methods for characterizing quantum states and ultrafast optical fields, and applied these to the study of the generation and utilization of nonclassical light and to the control of the interaction of quantum light and matter. These are used to investigate fundamental phenomena in quantum physics and toward realising quantum information processing protocols. He is the Director of the Networked Quantum Information Technologies Hub, a £38M centrefunded by the UK Research Councils to develop next-generation quantum technologies, and leads the QUTE European Consortium Virtual Institute for Quantum Sensing, Metrology and Imaging.

Ronald Walsworth
http://walsworth.physics.harvard.edu/index.html
Harvard University, rwalsworth@cfa.harvard.edu
Department of Physics
PhD (1991), Physics, Harvard University

Ronald Walsworth is a Senior Lecturer on Physics at Harvard University. He leads an interdisciplinary research group with a focus on developing precision measurement tools and applying them to important problems in both the physical and life sciences: from quantum physics, astrophysics, and nanoscience to bioimaging, brain science, and medical diagnostics. Current areas of research include: nanoscale magnetometry and spin physics with Nitrogen Vacancy (NV) centers in diamond; the use of laser frequency combs as improved optical wavelength calibrators for astrophysics, with applications to the search for Earth-like exoplanets; precision tests of fundamental physical laws and symmetries using atomic clocks; super-resolution optical imaging and functionalized electron microscopy for brain science and other bioimaging applications; and the development of novel NMR and MRI tools, with applications to basic spin physics and medical imaging.

David Weiss
http://www.phys.psu.edu/people/dsw13
Penn State University, dsweiss@phys.psu.edu
Department of Physics
PhD (1993), Physics, Stanford University

David Weiss is a Professor of Physics and Associate Head for Research at Penn State University. His research uses ultracold atoms and optical lattices to make precise measuremnts of fundamental constants and to test fundamental symmetries. His group is currently studying 1D gases - the foundations of quantum statistical mechanics, attempting to build a neutral atom quantum computer, and searching for the electron dipole moment.

Birgitta Whaley
http://www.cchem.berkeley.edu/kbwgrp/
University of California - Berkeley, whaley@berkeley.edu
Department of Chemistry
PhD (1984), Chemistry, University of Chicago

Birgitta Whaley is Professor of Chemistry, Founder and co-Director of the Berkeley Quantum Information and Computation Center at the University of California, Berkeley, and Faculty Scientist at the Lawrence Berkeley National Laboratory. Her research focuses on quantum information, quantum computation, macroscopic quantum systems, quantum control and simulation of complex quantum systems. Whaley is a Fellow of the American Physical Society, has served as chair of the APS Division of Chemical Physics and is currently Program Chair of the APS Topical Group in Quantum Information. Professional honors include awards from Bergmann, Sloan, and Alexander von Humboldt Foundations, as well as senior Fellowships from the Miller Institute (Berkeley) and the WIKO, Institute of Advanced Studies (Berlin). She has served on advisory committees for the National Academy of Sciences, Los Alamos and Lawrence Livermore National Laboratories, two Australian Centers in Quantum Information Science and Technology, and on Advisory Boards for the Perimeter Institute for Theoretical Physics, the Kavli Institute for Theoretical Physics. Whaley is author of over 220 scientific publications and co-author of the book "Controlling the Quantum World: The Science of Atoms, Molecules and Photons", published by the National Academies Press, Washington DC (2007).

Appendix II

Workshop Co-chairs

Seth Lloyd, *MIT*

Dirk Englund, *MIT*

Observers

Jiwei Lu, *OASDR&E (Basic Research Office)*

Robin Staffin, *OASDR&E (Basic Research Office)*

Dale Ormond, *OASDR&E*

Paul Alsing, *AFRL*

Tof Carim, *OSTP*

Claire Cramer, *DOE*

Tatjan Curcic, *AFOSR*

Michael Hayduk, *AFRL*

Mark Heiligman, *IARPA*

Prem Kumar, *DARPA*

Tristan Nguyen, *AFOSR*

Tim Polk, *OSTP*

Peter Reynolds, *ARO*

Charles Tahan, *LPS*

Claire Vitti, *UK MOD*

Jamie Watson, *Australian Embassy*

Carl Williams, *NIST*

Wojciech Zurek, *Los Alamos National Laboratory*

Rapporteurs

Kate Klemic, Research Scientist
Virginia Tech Applied Research Corporation

Tom Hussey, Senior Consultant
Virginia Tech Applied Research Corporation

Matt Bigman, Research Analyst
Virginia Tech Applied Research Corporation