



**KSEA Technical Monograph
KSEA-TM-2006-02**

An Assessment of Quantum Computation Research

April, 2006

Yong Wook Kim

**Department of Physics
Lehigh University
Bethlehem, Pennsylvania 18015
USA**

This is a report from the study project conducted by KSEA,

“An Assessment of Quantum Computation Research”

Part 2 of ‘Assessment of U.S. R&D Trends in Advanced Technology Areas’.

**Project Sponsor: KOFST
(Korean Federation of Science and Technology
Societies)**

**Performer: KSEA
(Korean-American Scientists and Engineers
Association)**

Performance Period: October 2005 – March 2006

Project Director: Kwang-Hae (Kane) Kim, 34th President of KSEA

Investigator and Report Author:

Yong Wook Kim

**Department of Physics
Lehigh University
Bethlehem, Pennsylvania 18015
USA**

610-758-3922; FAX 610-7585730

Email: ywk0@lehigh.edu

**© KSEA (Korean-American Scientists and Engineers Association)
1952 Gallows Rd., Suite 300, Vienna, VA 22182
<https://www.ksea.org/index.asp>**

PREFACE

Under the support of KOFST (Korean Federation of Science and Technology Societies), KSEA (Korea American Scientists and Engineers Association) conducted a study of R&D trends on Information Technology and interfacing technology areas. The study is part of the KOFST project, "Overseas Science and Technology Policy, Organization and Trends."

A two-volume report was produced. The first volume covers core computer science and engineering and networking branches of the IT research and development field. It was produced by a study team led by Dr. Se June Hong and consisting of 9 researchers who were not only members of KSEA but also members of a sister organization of KSEA, KOCSEA (Korean Computer Scientists and Engineers Association in America). The first volume became KSEA Technical Monograph KSEA-TM-2006-01.

The second volume became this technical monograph, KSEA-TM-2006-02. It was produced by Professor Yong Wook Kim and deals with the quantum computation branch of the IT research field.

All of us involved in this study project wish to thank KOFST. As the project director, I gratefully acknowledge this significant contribution of Professor Yong Wook Kim to KSEA and all professionals interested in the quantum computation research.

April, 2006

Kwang-Hae (Kane) Kim
Project Director and 34th President of KSEA

Table of contents

	page
Executive Summary	ES-1 – ES-4
Executive Summary in Korean	ESK-1 – ESK-3
Abstract	1
1. General Properties of Quantum Systems	1
A. Quantum Entanglement	1
B. Exploiting Entanglement – Quantum Teleportation	4
C. Quantum Information	5
D. Quantum Cryptography	7
E. Quantum Computation	8
2. Introduction to Quantum Computation Algorithm	10
3. Quantum Computation Roadmap, Version 2.0	15
A. An Overview	15
B. Background on Quantum Computation	18
C. Purpose and Methodology of the Roadmap	20
D. High-Level Goals of the Quantum Computation Roadmap	24
E. Mid-Level View of the Quantum Computation Roadmap	26
4. Experimental Subfields of Approaches to Quantum Computation	28
A. Nuclear Magnetic Resonance (NMR) Approaches	28
B. Ion Trap Quantum Approaches	30
C. Neutral Atom Approaches	30
D. Cavity Quantum Electro-dynamic (QED) Approaches	32
E. Optical Approaches	34
F. Solid State Approaches	36
G. Superconducting Approaches	39
H. “Unique” Qubit Approaches	40
5. Concluding Remarks	43
Acknowledgment	44
References and Bibliography	45
Author’s Short Narrative Vita	58

Executive Summary

An Assessment of Quantum Computation Research

Yong W. Kim
Department of Physics, Lehigh University
Bethlehem, Pennsylvania 18015, USA

The interest in quantum computation is driven by three basic reasons: (a) the expectation that the progress with device miniaturization predicts atomic-dimension features in integrated micro-circuits within the next decade; (b) the realization that it is possible to visualize computational algorithms built on quantum mechanical states of a one or more particles or photons; and (c) a quantum bit (a qubit) makes it possible to impart intrinsic information securely and facilitates computation algorithms that would be impossible to encode in classical computing algorithms. These reasons are considered fundamental, and while it may be conceivable to slow the movements but it does not appear possible to stop or slow the rise of intrinsic interest among scientists and engineers. Aside from applications based on quantum mechanical construct of a piece of information, continuing reduction of device features to atomic dimensions necessitates consideration of extraneous quantum mechanical effects in the nature of a state of a building block system that are required to define a single information bit.

The research activities remain largely in the science of realizing quantum computation, rather than in fashioning a computing device, and this means wide-open opportunity for new entries into the field. The field is extremely active, consistent with the high expectations among disparate parties ranging from the science policy makers, research funding agencies, business of new technology, defense strategists to lay public. New textbooks are being introduced into the graduate-level course offerings as experimental offerings in many universities. Aside from the what-if imaginations, the movement is providing new ways to think about the quantum mechanical nature of physical states in small scales and high-resolution inspection of quantum systems in highly magnified ways. Clearer and more simplified understandings emerge. For instance, quantum computation must clarify a qubit and prescribe its stability in the presence of

microscopic fluctuations due to thermodynamic characteristics of a physical system that defines the qubit. Unplanned modifications by thermal fluctuation lead to loss of the information represented by the qubit, or the so-called decoherence phenomenon, which any successful computational algorithm must be prepared to accommodate. Peter Shor has shown the algorithm and the requisite preservation of the integrity of the qubits used in the algorithm, namely, the error correction procedure to overcome the thermal or mechanical events of decoherence.

The challenges and the success of Shor's algorithm reside in the fact that the quantum mechanical specification of a state of the building block system includes quantum entanglement of more than one pure states of the system. A qubit may be represented by a pure state or an entangled state in the form of a linear combination of the pure states. The makeup of such an entangled state cannot be pinpointed until a measurement has been made. Such a measurement destroys the entangle state, and this feature makes it a secure way of encoding a piece of information from eavesdropping. It also makes it feasible to realize secure transmission of a photon or a particle over a large distance, i.e., the so-called quantum teleportation, if a particle pair or a photon pair is produced in an entangled way. Such entangled states can be constructed with a set of entities that number two or more; this enlarges the dynamic range of a qubit beyond two.

The rush of research is centered about two foci: one, theoretical development of new quantum computing algorithms; and two, devising of realistic laboratory systems, in which qubits may be created, localized and triggered into computational transformation according to a given quantum mechanical algorithm. Shor's algorithm is for factorization of a large number, for which a large gain in speed by the quantum mechanical algorithm has been demonstrated over classical computational algorithms, and remains the only known application of quantum computation. It is also generally agreed that classical counterpart simply cannot accomplish the task. Conversion of all classical computation to quantum computation is not only undesirable but also appears not feasible. However, it is widely understood that continued investigation would identify a significant class of problems appropriate to quantum computation.

Experimental realization of quantum computation is being explored in many different fronts. Qubits may be composed of entangled photons, different spin states of a single particle, or motional eigenstates of a single particle in a trap. There are a number of approaches identified as follows:

- nuclear magnetic resonance (NMR) quantum computation,
- ion trap quantum computation,
- neutral atom quantum computation,
- cavity quantum electro-dynamic (QED) computation
- optical quantum computation,
- solid state (spin-based and quantum-dot-based) quantum computation,
- superconducting quantum computation, and
- “unique” qubits quantum computation (e.g., electrons on liquid helium, spectral hole burning, etc.).

Currently, progress within each of these approaches is monitored and tested by the criteria, known as the DiVincenzo criteria. It quantifies a number of threshold issues, and necessary conditions for any viable quantum computation technology are stated as follows:

- i) a scalable physical system of well-characterized qubits;
- ii) the ability to initialize the state of the qubits to a simple fiducial state;
- iii) long (relative) decoherence times, much longer than the gate-operation time;
- iv) a universal set of quantum gates;
- v) a qubit-specific measurement capability;
- vi) the ability to interconvert stationary and flying qubits; and
- vii) the ability to faithfully transmit flying qubits between specified locations.

The last two criteria address the necessary conditions for quantum computer networkability.

These criteria address many concurrent considerations. The physical properties, such as decoherence rates of the two-level qubits used to represent quantum information must be well understood. The physical resource requirements must scale linearly in the number of qubits, not exponentially, if the approach is to be a candidate for a large-scale quantum computation technology. It must be possible to initialize a register of qubits to some state from which

quantum computation can be performed. The time to perform a quantum logic operation must be much smaller than the time-scales over which the system's quantum information decoheres. There must be a procedure identified for implementing at least one set of universal quantum logic operations. In order to read out the result of a quantum computation there must be a mechanism for measuring the final state of individual qubits in a quantum register. The two networking criteria are necessary if it is desired to transfer quantum information from one location to another, (e.g., between different registers or between different processors in a distributed computing situation).

It is most likely that a single photon or electron source will play a prominent role as a timing means for initiating computational gate operation to be applied to the qubits. A source capable of producing a single photon or an electron, no more or no less, at a time under a command remains a critical capability for quantum computation. Any one of the above lines of investigation will be worthy of the intellectual investment because they will provide a platform on which to advance new understanding of the state of a physical system at small distances, and to develop tools and working systems based on the new knowledge. The general view is that the successful quantum computational system may not be any one of these approaches but based on new syntheses of the relevant physics. The central workhorse system will require many basic tools of experimental physics, now at hand as well as those yet to be developed. Accumulation of the body of expertise will serve well the eventual participation in the new enterprise of quantum computation.

This assessment investigation was carried out at the request of the Korean Federation of Science and Technology Societies (KOFST) through the Korean Scientists and Engineers in America (KSEA). The author acknowledges partial support by the KOFST and by Lehigh University.

Executive Summary in Korean

Quantum Computation

Yong W. Kim
Department of Physics, Lehigh University
Bethlehem, Pennsylvania 18015, USA

Quantum Computation . ()
device integrated micro-
circuit ; () algorithm
; ()
algorithm
, qubit ,
quantum computation .
device
device
, device
quantum computation quantum computation
strategist , quantum computation
Quantum computation
,
qubit , quantum computation
decoherence , algorithm
Peter Shor factorization quantum
computation algorithm decoherence
quantum computation

Shor quantum computation algorithm

eigenfunction eigenfunction quantum entanglement
qubit wavefunction

wavefunction
entangled state wavefunction entangled
wavefunction

, entangled wavefunction wavefunction
qubit
, qubit dynamic range digital bit

quantum computation algorithm
qubit

algorithm
Shor algorithm factorization Shor quantum
computation algorithm algorithm
factorization quantum computation algorithm
algorithm
quantum algorithm

Quantum computation
Qubit entangled photon eigenstate
spin
entangled state

- NMR quantum computation
- quantum computation
- quantum computation
- matter wave resonant cavity quantum computation
- quantum computation
- spin quantum dot quantum computation
- quantum computation
- helium spectral hole burning qubit
- quantum computation

group DiVincenzo

-) qubit
-) qubit
-) Decoherence logic gate
-) quantum logic gate
-) qubit
-) Qubit
-) Qubit

quantum computer network

DiVincenzo criteria

, two-level qubit
qubit

decoherence
quantum computation
qubit
quantum logic operation

decoherence
quantum logic operation

Quantum computation

quantum register
register register

Quantum computation
networking

Quantum computation

stochastic

quantum computation
quantum computation

gate logic operation

quantum computation
quantum computation

An Assessment of Quantum Computation Research

Abstract

The industry-wide drive to increase the computing speed continues to follow Moore's empirical scaling rule of feature size reductions in microelectronic devices with time. The current device sizes approach the mesoscopic regimes, forcing the consideration of quantum mechanical effects on the classical information bits. This report documents an assessment of the state-of-the-art of the research efforts to define and build a science and technology base for quantum computation. The quantum computation enterprise has been organized as a response to such an eventuality. It is comprised of construction of quantum mechanical information bit (a qubit) and algorithmic operations on a suite of such qubits to achieve quantum computation. The present consensus is that a quantum computation algorithm is superior to classical counterparts in that certain computational tasks, which cannot be encoded in classical computation, an example being factorization of large integers, can be executed at significantly higher speeds. Shor's algorithm presents a specific demonstration of such an intrinsic capability. The potential strength of quantum computation arises from a new understanding of entangled states as the basis of a qubit. Shor has also formulated a quantum-computing algorithm that is capable of effectively circumventing the losses of the qubit-encoded information due to intrinsic fluctuations in the small physical systems (i.e., the decoherence problem). Construction of a qubit and its quantum mechanical peculiarities are reviewed in this report, together with an introduction to Shor's quantum computation algorithm. The so-called quantum computation roadmap, as maintained by a loose group of investigators in the field, is also reviewed. Specific research efforts to realize rudimentary quantum computing systems, implemented with quantum computation algorithms, are described. Conclusions, together with recommendations given in the executive summary, are presented as a snapshot view of the current state of the research efforts.

1. General Properties of Quantum Systems

The interest in quantum computing is driven by three basic reasons: (a) the expectation that the progress with device miniaturization predicts atomic-dimension features in integrated micro-circuits within the next decade; (b) the realization that it is possible to visualize computational algorithms built on quantum mechanical states of a one or more particles or photons; and (c) a quantum bit (a qubit) makes it possible to impart intrinsic information securely and facilitates computation that would be impossible to encode in classical computing algorithms. These reasons are considered fundamental, and while it may be conceivable to slow the movements but it does not appear possible to stop or slow the rise of intrinsic interest among scientists and engineers. Aside from applications based on quantum mechanical construct of a piece of information, continuing reduction of device features to atomic dimensions necessitates consideration of extraneous quantum mechanical effects in the nature of a state of a building block system that are required to define a single information bit.

A. Quantum Entanglement

In the mid thirties, Schrödinger discussed the argument by Einstein, Podolsky, and Rosen (“EPR”) that the theory of quantum mechanics is incomplete. In classical mechanics the state of a system is essentially a list of the system's properties — namely, the positions and momenta of all the particles comprising the system. The theory specifies how properties change in terms of a law of evolution for the state, which Pauli characterized as a ‘detached observer’ idealization.[Pauli] According to the Copenhagen interpretation, such a description is not possible for quantum systems; the import of the state resides in the probabilities that can be inferred for the outcomes of possible future observations on the system. Einstein proposed arguments instead, showing that the quantum state is simply an incomplete characterization of the system, as a result of the missing parameters or “hidden variables.”

Einstein's definition of a complete theory entailed certain conditions of separability and locality for composite systems consisting of separated component systems: each component system separately should be characterized by its own properties, even though

such properties may emerge stochastically, and it should be impossible to alter the properties of a distant system by acting on a local system. In Bell's extension of the EPR argument made it apparent that these conditions, when suitably formulated as probability constraints, are equivalent to the requirement that statistical correlations between separated systems should be reducible to probability distributions over common causes, be it deterministic or stochastic.

Two particles that are prepared from a source in a certain quantum state and move apart retain matching correlations between both the positions of the two particles and their momenta. Any measurement of either position or momentum on a particular particle would allow with certainty the prediction of the outcome of a position measurement or momentum measurement on the other particle. These measurements are, however, mutually exclusive: either a position measurement can be performed, or a momentum measurement, but not both simultaneously. Furthermore, either correlation can be observed, but the subsequent measurement of momentum, say, after establishing a position correlation, will no longer yield any correlation in the momenta of the two particles. This is as if the position measurement disturbs the correlation between the momentum values, forcing a puzzling conclusion that the quantum state of the particle pair is inconsistent with the separate individual labeling of the particles that could be associated with appropriately correlated values for the outcomes of position and momentum measurements. EPR concluded that the quantum state was incomplete.

Schrödinger coined the term 'entanglement' to describe this peculiar connection between quantum systems.[Schroedinger] In the second part of the paper, Schrödinger showed that, in general, a sophisticated experimenter can, by a suitable choice of operations carried out on one system, 'steer' the second system into any chosen 'mixture' of quantum states. That is, the second system cannot be steered into any particular state at the whim of the experimenter, but the experimenter can constrain the state into which the second system evolves to lie in any chosen set of states, with a probability distribution fixed by the entangled state.

He found this conclusion sufficiently unsettling to suggest that the entanglement between two separating systems would persist only for distances small enough that the time taken by light to travel from one system to the other could be neglected, compared with the characteristic time periods associated with other changes in the composite system. Most physicists were swayed by this suggestion. This was unfortunate, because the study of entanglement was ignored for thirty years until John Bell's reconsideration and extension of the EPR argument.[Bell]

Bell looked at entanglement in simpler systems of matching correlations between two-valued dynamical quantities, such as polarization or spin, of two separated systems in an entangled state. He showed that the statistical correlations between the measurement outcomes of suitably chosen *different* quantities on the two systems are inconsistent with an inequality derivable from Einstein's separability and locality assumptions — in effect from the assumption that the correlations have a common cause. Bell's investigation generated an ongoing debate on the foundations of quantum mechanics. It led to confirmation that entanglement can persist over long distances, [Aspect, et al] thus disproving Schrödinger's supposition of the spontaneous decay of entanglement as two entangled particles separate. But it had to wait until the 1980s before wide acceptance of the non-local correlations of entangled quantum states was crytalized as a new kind of non-classical resource that could be exploited.[Lo, et al; Nielson and Chuang]

B. Exploiting Entanglement - Quantum Teleportation

Consider again Schrödinger's realization that an entangled state could be used to steer a distant particle into one of a set of states, with a certain probability. Suppose that two persons A and B share an entangled state of two photons in an entangled state of polarization. Person A has in her possession one of the entangled photons, and person B has the other. Imagine that A has an additional photon in an unknown state of polarization, u , and that it is possible for A to perform an operation on the two photons in her possession that will transform B's photon into one of four states, depending on the four possible (random) outcomes of A's operation: either the state u , or a state that is related to u in a definite way. A's operation entangles the two photons in her possession, and disentangles B's photon, steering it into a state u^* . Once A communicates the

outcome of her operation to B, B knows either that $u^* = u$, or how to transform u^* to u by a local operation. This phenomenon is known as “quantum teleportation.”

A and B have managed to use their shared entangled state as a quantum communication channel to destroy the state u of a photon in A's part of the universe and recreate it in B's part of the universe. Since the polarization state of a photon requires specifying the value of an angle that can vary continuously, without a shared entangled state A would have to convey an infinite amount of classical information to B in order for B to reconstruct the state u precisely. The binary expansion of an angle variable is represented by a potentially infinite sequence of 0's and 1's, or an arbitrary angle variable requires an infinite number of bits. To specify the outcome of A's operation having four possible outcomes with equal *a priori* probabilities, on the other hand, requires two bits of classical information, B can reconstruct the state u on the basis of just two bits of classical information communicated by A, apparently by exploiting the entangled state as a quantum communication channel to transfer the remaining information.[Nielsen and Chuang; Josza]

C. Quantum Information

The amount of classical information we gain when we learn the value of a random variable is represented by a quantity called the Shannon entropy, measured in bits.[Shannon and Weaver] A random variable is defined by a probability distribution over a set of values. In the case of a binary random variable, with equal probability for each of the two possibilities, the Shannon entropy is 1 bit, representing maximal uncertainty. For all other probabilities the Shannon entropy is less than 1. For the case of maximal knowledge or zero uncertainty about the alternatives, where the probabilities are 0 and 1, the Shannon entropy is zero.

Since information is always embodied in the state of a physical system, we can also think of the Shannon entropy as quantifying the physical resources required to store classical information. Suppose A wishes to communicate some classical information to B over a classical communication channel, say, in an email message. A relevant question concerns the extent to which the message can be compressed without loss of information, so that B

can reconstruct the original message accurately from the compressed version. According to Shannon's source coding theorem (noiseless coding theorem), the minimal physical resource required to represent the message is given by the Shannon entropy of the source.

The natural next question is, what happens if we use the quantum states of physical systems to store information, rather than classical states? It turns out that quantum information is radically different from classical information. The unit of quantum information is the 'qubit', representing the amount of quantum information that can be stored in the state of the simplest quantum system, such as the polarization state of a photon.[Schumacher] As we have noted earlier, an arbitrarily large amount of classical information can be encoded in a qubit. This information can be processed and communicated but, because of the peculiarities of quantum measurement, at most only one bit can be accessed.[Holevo]

While classical information can be copied or cloned, the quantum 'no cloning' theorem asserts the impossibility of cloning an unknown quantum state.[Dieks; Wootters and Zurek] To see why, consider how we might construct a classical copying device. A NOT gate is a device that takes a bit as input and produces as output either a 1 if the input is 0, or a 0 if the input is 1. In other words, a NOT gate is a 1-bit gate that flips the input bit. A controlled-NOT gate, or CNOT gate, takes two bits as inputs, a control bit and a target bit, and flips the target bit if and only if the control bit is 1, while reproducing the control bit. A CNOT gate functions as a copying device for the control bit if the target bit is set to 0, because the output of the target bit is then a copy of the control bit (i.e., the input 00 produces output 00, and the input 10 produces output 11). Insofar as we can think of a measurement as simply a copying operation, a CNOT gate is the paradigm of a classical measuring device.

Suppose we attempt to use our CNOT gate to copy an unknown qubit state. Since we are now proposing to regard the CNOT gate as a device for processing quantum states, the evolution from input states to output states must be effected by a physical quantum transformation. Now quantum transformations are linear on the linear state space of qubits. Linearity of the state space means that for any two qubit states that are orthogonal

in the space of qubit states, there are qubit states that are represented by linear superpositions or sums of 0 and 1, with certain coefficients. Such superpositions, say, a superposition with equal coefficients that could be represented symbolically as $0+1$, are non-orthogonal to 0 and to 1. Linearity of the transformation means that any transformation must take a qubit state represented by the sum of two orthogonal qubits to a new qubit state that is the sum of the transformed orthogonal qubits. If the CNOT gate succeeds in copying two orthogonal qubits, it cannot succeed in copying a linear superposition of these qubits. Since the gate functions linearly, it must instead produce a state that is a linear superposition of the outputs obtained for the two orthogonal qubits. That is to say, the output of the gate will be represented by a quantum state that is a sum of two terms, where the first term represents the output of the control and target for the first orthogonal qubit, and the second term represents the output of the control and target for the second orthogonal qubit. This could be written as $00+11$. This is an entangled state and not the output that would be required by a successful copying operation, where the control and target each outputs the superposed qubit (which could be written as $(0+1)(0+1)$).

D. Quantum Cryptography

Linearity prevents the possibility of cloning or measuring an unknown quantum state. Similarly, it can be shown that if A sends B one of two nonorthogonal qubits, B can obtain information about which of these qubits was sent only at the expense of disturbing the state. That is, for quantum information there is no information gain without the disturbance. The impossibility of copying an unknown quantum state is the basis of the application of quantum information to cryptography. There are quantum protocols involving the exchange of classical and quantum information that A and B can exploit to share a secret random key, which they can then use to communicate privately.[Lo] Any attempt by an eavesdropper to monitor the communication between A and B will be detectable because no quantum information can be gained without incurring some disturbance to the quantum communication channel.

E. Quantum Computation

Quantum information can be processed, but the accessibility of this information is limited by the Holevo bound as mentioned earlier. Deutsch first showed how to exploit quantum entanglement to perform a computational task that is impossible for a classical computer.[Deutsch] Suppose we have a black box that evaluates a function f . The arguments of f (inputs) are either 0 or 1. The values (outputs) of f are either the same for both arguments, i.e., f is constant, or different for the two arguments, i.e., f is said to be *balanced*. We are interested in determining whether f is *constant* or *balanced*. Now, classically, the only way to do this is to run the black box twice, for both arguments 0 and 1, and to pass the values (outputs of f) to a circuit that determines whether they are the same (for *constant*) or different (for *balanced*). Deutsch showed that if we use quantum states and quantum gates to store and process information, then we can determine whether f is *constant* or *balanced* in one evaluation of the function f . The task is to design the circuit in a sequence of gates to produce the answer to a global question about the function (*constant* or *balanced*) in an output qubit register that can then be read out or measured.

Recall the quantum CNOT gate, with two orthogonal qubits 0 and 1 as possible inputs for the control, and 0 as the input for the target. One can think of the input control and output target qubits, respectively, as the argument and associated value of a function. This CNOT function associates the value 0 with the argument 0 and the value 1 with the argument 1. For a linear superposition of the orthogonal qubits, say $0+1$, as input to the control, and the qubit representing 0 as the input to the target, the output is the entangled state $00+11$, a linear superposition in which the first term represents the argument 0 and associated value (0) of the CNOT function, and the second term represents the argument 1 and associated value (1) of the CNOT function. The entangled state represents all possible arguments and corresponding values of the function as a linear superposition, but this information is not accessible. What is accessible by a suitable choice of quantum gates is information about whether or not the function has certain global properties. This

information is obtainable without reading out the evaluation of any individual arguments and values.

The situation is analogous for Deutsch's function f . Here the output of f can be represented as either $00 + 10$ or $01 + 11$ (in the *constant* case), or $00 + 11$ or $01 + 10$ (in the *balanced* case). The two entangled states in the *constant* case are orthogonal in the 4-dimensional two-qubit state space and span a plane. We can label this the *constant* plane. Similarly, the two entangled states in the *balanced* case span a plane, the *balanced* plane. These planes are orthogonal in the 4-dimensional state space, except for an overlap: a line, representing a non-entangled two-qubit state. It is therefore possible to design a measurement to distinguish the two global properties of f , *constant* or *balanced*, with a certain probability (actually, $1/2$) of failure, when the measurement yields an outcome corresponding to the overlap state, which is common to the two cases. Nevertheless, only one query of the function is required when the measurement succeeds in identifying the global property. With a judicious choice of quantum gates, it is even possible to design a quantum circuit that always succeeds in distinguishing the two cases.

Deutsch's example shows how quantum information, and quantum entanglement, can be exploited to compute a global property of a function in one step that would take two steps classically. There are quantum algorithms that achieve an exponential speed-up over any known classical algorithm, and in some cases the speed-up can be shown to be exponential over any classical algorithm. Essentially, this is again due to the phenomenon of entanglement. Indeed, the amount of information required to describe a general entangled state of n qubits grows exponentially with n . The state space (i.e., Hilbert space) has 2^n dimensions, so a general entangled state is a superposition of 2^n n -qubit states. In classical mechanics there are no entangled states: a general n -bit composite system can be described with just n times the amount of information required to describe a single bit system. So the classical simulation of a quantum process would involve an exponential increase in the classical informational resource required to represent the quantum state, as the number of qubits that become entangled in the evolution grows linearly, and there would be a corresponding exponential slowdown in calculating the evolution, compared to the actual quantum computation performed naturally by the

system. However, there are still significant debates as to what exactly explains the speed-up. [Bub]

While Deutsch's problem has no interesting application, there now exist several quantum algorithms for non-trivial problems, notably Shor's factorization algorithm for factoring large composite integers in polynomial time and Grover's database search algorithm.[Lo, Popescu and Spiller; Bub; Barenco]

2. Introduction to Quantum Computation Algorithm

By the early nineties it was known that a quantum computer could be faster than any classical computer for certain problems. Nonetheless these observations were largely driven by academic curiosity. This changed when Shor devised a polynomial time algorithm for factoring large numbers on a quantum computer.[Shor]

The algorithm was viewed as important because the difficulty of factoring large numbers is relied upon for most cryptography systems. If an efficient method of factoring large numbers is implemented most of the current encryption schemes would be worthless. While it has not been proven that factoring large numbers can not be achieved on a classical computer in polynomial time, the fastest algorithm publicly available for factoring a large number n (whose representation has $\log n$ bits) runs in, or exponential time.

$$O(e^{c(\log n)^{1/3} + (\log \log n)^{2/3}})$$

In contrast Shor's algorithm runs in

$$O((\log n)^2 + \log \log n)$$

on a quantum computer, and then must perform $O(\log n)$ steps of post processing on a classical computer. Overall, this time is polynomial, and this discovery propelled the study of quantum computing forward.

Shor's algorithm hinges on a result from number theory: the function $F(a) = x^a \bmod n$ is a periodic function when x is an integer coprime to n . In the context of Shor's algorithm n will be the number we wish to factor. When two numbers are coprime it means that their greatest common divisor is 1.

Calculating this function for an exponential number of a 's would take exponential time on a classical computer. Shor's algorithm utilizes quantum parallelism to perform the exponential number of operations in one step. Since $F(a)$ is a periodic function, it has some period r . We know that $x^0 \bmod n = 1$, and therefore $x^r \bmod n = 1$, and $x^{2r} \bmod n = 1$, and so on.

Given this information and through the following algebraic manipulation:

$$x^r \equiv 1 \pmod{n}$$

$$(x^{r/2})^2 - 1 \equiv 0 \pmod{n}$$

and if r is an even number

$$(x^{r/2} - 1)(x^{r/2} + 1) \equiv 0 \pmod{n}$$

We can see that the product $(x^{r/2} - 1)(x^{r/2} + 1)$ is an integer multiple of n , i.e., the number to be factored. So long as $|x^{r/2}|$ is not 1, then at least one of $(x^{r/2} - 1)$ and

$(x^{r/2} + 1)$ must have a nontrivial factor in common with n . So by computing $\gcd(x^{r/2} - 1, n)$, and $\gcd(x^{r/2} + 1, n)$, we will obtain a factor of n , where \gcd is the greatest common denominator function.

Shor's algorithm tries to find r , the period of $x^a \bmod n$, where n is the number to be factored, and x is an integer coprime to n . To do this Shor's algorithm creates a quantum memory register with two parts. In the first part the algorithm places a superposition of the integers, which are to be a 's in the $x^a \bmod n$ function. We will choose our a 's to be the integers 0 through $q - 1$, where q is the power of two such that $n^3 \leq q < 2n^2$. Then the

algorithm calculates $x^a \bmod n$, where a is the superposition of the states, and places the result in the second part of the quantum memory register.

Remember, the number n is represented by a $\lceil \log n \rceil$ bit string. We must calculate $x^a \bmod n$ an exponential number of times, with respect to the length of the encoded input to the algorithm.

Next the algorithm measures the state of the second register, the one that contains the superposition of all possible outcomes for $x^a \bmod n$. Measuring this register has the effect of collapsing the state into some observed value, say k . It also has the side effect of projecting the first part of the quantum register into a state consistent with the value measured in the second part. Thus, measurement of the second part results in exactly one value, and causes the other partition to collapse into a superposition of the base states consistent with the value observed in the second part.

After this measurement the second part of the register contains the value k , and the first part of the register contains a superposition of the base states whose evaluation in $x^a \bmod n$ produces k . We know $x^a \bmod n$ is a periodic function, therefore the first part of the register will contain the values $c, c + r, c + 2r, \dots$, where c is the lowest integer such that $x^c \bmod n = k$. The next step is to perform a discrete Fourier transform on the contents of first part of the register. The application of the discrete Fourier transformation has the effect of peaking the probability amplitudes of the first part of the register at integer multiples of the quantity q/r .

Measuring the first part of the quantum register will yield an integer multiple of the inverse of the period with high probability. Once this number is retrieved from the quantum memory register, a classical computer can do analysis of this number, make a guess as to the actual value of r , and from that compute the possible factors of n . This post processing is treated in more detail below.[Shor]

Shor's algorithm for factoring a given integer n can be broken down into simple steps.

- a. Determine if the number n is a prime, an even number, or an integer power of a prime number. If it is, we will not use Shor's algorithm. There are efficient classical methods for determining if an integer n belongs to one of the above groups, and providing factors for it if it does. This step would be performed on a classical computer.
- b. Pick a integer q that is the power of 2 such that $n^3 \leq q < 2n^2$. This step would be done on a classical computer.
- c. Pick a random integer x that is coprime to n . When two numbers are coprime, it means that their greatest common divisor is 1. There are efficient classical methods for picking such an x . This step would be done on a classical computer.
- d. Create a quantum register and partition it into two sets, register one and register two. Thus the state of the quantum computer can be given by: $left|reg1, reg2\rangle$. Register one must have enough qubits to represent integers as large as $q - 1$. Register two must have enough qubits to represent integers as large as $n - 1$.
- e. Load register one with an equally weighted superposition of all integers from 0 to $q - 1$. Load register two with the 0 state. The quantum computer would perform this operation. The total state of the quantum memory register at this point is:

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle$$

- f. Apply the transformation $x^a \text{ mod } n$ to each number stored in register one and store the result in register two. Due to quantum parallelism this will take only one step, as the quantum computer will only calculate $x^{|a\rangle} \text{ mod } n$, where $|a\rangle$ is the superposition of states created in step 5. This step is performed on the quantum computer. The state of the quantum memory register at this point is:

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, x^a \text{ mod } n\rangle$$

- g. Measure the second register, and observe some value k . This has the side effect of collapsing register one into an equal superposition of each value a between 0 and $q - 1$ such that $x^a \bmod n = k$. This operation is performed by the quantum computer. The state of the quantum memory register after this step is:

$$\frac{1}{\sqrt{\|A\|}} \sum_{a \in A} |a, k\rangle$$

Here A is the set of a 's such that $x^a \bmod n = k$, and $\|A\|$ is the number of elements in that set.

- h. Compute the discrete Fourier transform on register one. The discrete Fourier transform when applied to a state $|a\rangle$ changes it in the following manner:

$$|a\rangle = \frac{1}{\sqrt{q}} \sum |c\rangle * e^{2\pi i a c / q}$$

This step is performed by the quantum computer in one step through quantum parallelism. After the discrete Fourier transform the register is in the state:

$$\frac{1}{\sqrt{\|A\|}} \sum_{a \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c, k\rangle * e^{2\pi i a c / q}$$

- i. Measure the state of register one, call this value m , this integer m has a very high probability of being a multiple of q/r , where r is the desired period. The quantum computer performs this step.
- j. Take the value m , and on a classical computer do some post processing which calculates r based on knowledge of m and q . There are many ways to do this post processing, and it is done on a classical computer.
- k. Once r is attained, a factor of n can be determined by taking $\gcd(x^{r/2} + 1, m)$ and $\gcd(x^{r/2} - 1, m)$. If a factor of n is found, then one stops, and if not, go to step 4. This final step is done on a classical computer.

Step k contains a provision for Shor's algorithm failing to produce the factors of n . Shor's algorithm can fail for many reasons; for example, the discrete Fourier transform could be measured to be 0 in step i, making the post processing in step j impossible. At other times the algorithm will sometimes find factors of 1 and n , which is correct but not useful.[Williams and Clearwater]

Shor's algorithm is not the only algorithm that seems to be better on a quantum computer than any classical computer for a problem, which is considered to be useful. Grover devised an algorithm to find an item in an unsorted list of N elements in operations. No classical algorithm can guarantee finding the item in less than N in $0.758\sqrt{N}$ operations, and in the average case it would take $N/2$ operations.[Feynman]

There are numerous references on quantum information and quantum computation, both in published and unpublished form. In particular, the author have found the lecture notes and monographs useful in developing his understanding of the basic issues as well as the challenges that lie ahead.[Preskill; Stoltz and Suter]

3. Quantum Computation Roadmap, Version 2.0 (2004) [QIST Roadmap]

A. An Overview

Quantum computation (QC) holds out tremendous promise for efficiently solving some of the most difficult problems in computational science, such as integer factorization, discrete logarithms, and quantum simulation and modeling that are intractable on any present or future conventional computer. New concepts for QC implementations, algorithms, and advances in the theoretical understanding of the physics requirements for QC appear almost weekly in the scientific literature. This rapidly evolving field is one of the most active research areas of modern science, attracting substantial funding that supports research groups at internationally leading academic institutions, national laboratories, and major industrial-research centers. Well-organized programs are underway in the United States, the European Union and its member nations, Australia, and in other major industrial nations. Start-up quantum-information companies are already in operation.

Wide ranged experimental approaches from a variety of scientific disciplines are being pursued to meet the fundamental quantum mechanical challenges involved. Yet experimental achievements in QC, although of unprecedented complexity in basic quantum physics, are only at the proof-of-principle stage in terms of their abilities to perform QC tasks. It will be necessary to develop significantly more complex quantum-information processing (QIP) capabilities before quantum computer-science issues can begin to be experimentally studied. To realize this potential will require the engineering and control of quantum-mechanical systems on a scale far beyond anything yet achieved in any physics laboratory. This required control runs counter to the tendency of the essential quantum properties of quantum systems to degrade with time (“decoherence”). Yet, it is known that it should be possible to reach the “quantum computer-science test-bed regime”—if challenging requirements for the precision of elementary quantum operations and physical scalability can be met. Although a considerable gap exists between these requirements and any of the experimental implementations today, this gap continues to close.

To facilitate the progress of QC research towards the quantum computer-science era, a two-day “Quantum Information Science and Technology Experts Panel Meeting” was held in La Jolla, California, USA, in late January 2002 with the objective of formulating a QC roadmap. The panel’s members decided that a desired future objective for QC should be “to develop by 2012 a suite of viable emerging-QC technologies of sufficient complexity to function as quantum computer-science test-beds in which architectural and algorithmic issues can be explored.” The panel’s members emphasize that although this is a desired outcome, not a prediction, they believe that it is attainable if the momentum in this field is maintained with focus on this objective. The intent of this roadmap is to set a path leading to the desired QC test-bed era by 2012 by providing some direction for the field with specific five- and ten-year technical goals. While remaining within the “basic science” regime, the five-year (2007) goal would project QC far enough in terms of the precision of elementary quantum operations and correction of quantum errors that the potential for further scalability could be reliably assessed. The ten-year (2012) goal

would extend QC into the “architectural/algorithmic” regime, involving a quantum system of such complexity that it is beyond the capability of classical computers to simulate. These high-level goals are ambitious but attainable as a collective effort with cooperative interactions between different experimental approaches and theory.

Within these overall goals, different scientific approaches to QC will play a variety of roles: it is expected that one or more approaches will emerge that will actually attain these goals. Other approaches may not—but will instead play other vitally important roles, such as offering better scalability potential in the post-2012 era or exploring different ways to implement quantum logic, that will be essential to the desired development of the field as a whole. It was the unanimous opinion of the Technology Experts Panel (TEP) that it is too soon to attempt to identify a smaller number of potential “winners;” the ultimate technology may not have even been invented yet. Considerable evolution of and hybridization between approaches has already taken place and should be expected to continue in the future, with existing approaches being superseded by even more promising ones.

A second function of the roadmap is to allow informed decisions about future directions to be made by tracking progress and elucidating interrelationships between approaches, which will assist researchers to develop synergistic solutions to obstacles within any one approach. To this end, the roadmap presents a “mid-level view” that segments the field into the different scientific approaches and provides a simple graphical representation using a common set of criteria and metrics to capture the promise and characterize progress towards the high-level goals within each approach. A “detailed-level view” incorporates summaries of the state-of-play within each approach, provides a timeline for likely progress, and attempts to capture its role in the overall development of the field. A summary provides some recommendations for moving toward the desired goals. The panel members developed the first version of the QC roadmap from the La Jolla meeting and five follow-up meetings held in conjunction with the annual ARO/ARDA/NSA/NRO Quantum Computing Program Review (QCPR) in Nashville, Tennessee, USA, in August 2002. The present (version 2.0) update was developed out of a further four meetings at

the August 2003 QCPR; the roadmap will continue to be updated annually. The quantum computer-science test-bed destination that we envision in this roadmap will open up fascinating, powerful new computational capabilities: for evaluating quantum-algorithm performance; allowing quantum simulations to be performed; and for investigating alternative architectures, such as networked quantum sub-processors. The journey to this destination will lead to many new scientific and technological developments with potential societal and economic benefits. Quantum systems of unprecedented complexity will be created and controlled, potentially leading to greater fundamental understanding of how classical physics emerges from a quantum world, which is as perplexing and as important a question today as it was when quantum mechanics was invented. We can foresee that these QC capabilities will lead into an era of “quantum machines” such as atomic clocks with increased precision with benefits to navigation, and “quantum enhanced” sensors. Quantum light sources will be developed that will be enabling technologies for other applications such as secure communications, and single atom doping techniques will be developed that will open up important applications in the semiconductor industry. We anticipate that there will be considerable synergy with nanotechnology and spintronics. The journey ahead will be challenging but it is one that will lead to unprecedented advances in both fundamental scientific understanding and practical new technologies.

B. Background on Quantum Computation

The representation of information by classical physical quantities such as the voltage levels in a microprocessor is familiar to everyone. But quantum information science (QIS) has been developed to describe binary information in the form of two-state quantum systems, such as: two distinct polarization states of a photon; two energy levels of an atomic electron; or the two spin directions of an electron or atomic nucleus in a magnetic field. A single bit of information in this form has come to be known as a “qubit.” With two or more qubits, it becomes possible to consider quantum logical-”gate” operations in which a controlled interaction between qubits produces a (coherent) change in the state of one qubit that is contingent upon the state of another. These gate operations are the building blocks of a quantum computer.

In principle, a quantum computer is a very much more powerful device than any existing or future classical computer because the superposition principle allows an extraordinarily large number of computations to be performed simultaneously. For certain problems, such as integer factorization and the discrete-logarithm problem, which are believed to be intractable on any present-day or future conventional computer, this “quantum parallelism” would permit their efficient solution. These are important problems as they form the foundation of nearly all publicly used encryption techniques. Another example of great potential impact, as first described by Feynman, is quantum modeling and simulation (e.g., for designing future nanoscale electronic components)—exact calculations of such systems can only be performed using a quantum computer. [Feynman] This simulation capability has the potential for discovering new phenomenology in mesoscopic/nanoscale physics, which in turn could lead to new devices and technologies. (It is not known if quantum computers will offer computational advantages over conventional computers for general-purpose computation.) To realize this potential will require the engineering and control of quantum-mechanical systems on a scale far beyond anything yet achieved in any physics laboratory. Many approaches to QC from diverse branches of science are being pursued. Needless to say, these present-day QC technologies are some orders of magnitude away in both numbers of qubits and numbers of quantum logic operations that can be performed from the sizes that would be required for solving interesting problems. A few experimental approaches are now capable of performing small numbers of quantum operations on small numbers of qubits, with realistic assessments of the challenges for scale-up, while the bulk of the field is at the single qubit stage with optimistic ideas for producing large-scale systems.

There are both fundamental and technical challenges to bridging this gap. A serious obstacle to practical QC is the propensity for qubit superpositions of 0 and 1 to “decohere” into either 0 or 1. (This phenomenon of decoherence is invoked to explain why macroscopic objects are not observed in quantum superposition states.) However, theoretical breakthroughs have been made in generalizing conventional error-correction concepts to correct decoherence in a quantum computer. A single logical bit would be

encoded as the state of several physical qubits and quantum logic operations used to correct decoherence errors. These quantum error-correction ideas have been shown to allow robust, or fault-tolerant QC with the encoded logical qubits, at the expense of introducing considerable overhead in the numbers of physical qubits and elementary quantum logic operations on them. (For example, one logical qubit may be encoded as a state of five physical qubits in one scheme, although the number of physical qubits constituting a logical qubit could well be different for different physical QC implementations.) It has been established, under certain assumptions, that if a threshold precision per gate operation could be achieved, quantum error correction would allow a quantum computer to compute indefinitely.

An essential ingredient of quantum error-correction techniques and QC in general, is the capability to create entangled states of multiple qubits on demand. In these peculiarly quantum mechanical states the joint properties of several qubits are uniquely defined, even though the individual qubits have no definite state. The strength of the correlations between qubits in entangled states is the most prominent feature distinguishing quantum physics from the familiar world of classical physics. The unusual properties of these states underlie the potential new capabilities of QC and other quantum technologies. Although present-day QC experiments are making rapid progress, demonstrations of on demand entanglement are few and the precision of gate operations is quite far from the fault tolerant thresholds. However, experimental capabilities will progress and the fault-tolerant requirements are likely to be relaxed once the underlying assumptions are adapted to specific approaches. The overall purpose of this roadmap is to help achieve these thresholds and to facilitate the progress of QC research towards the quantum computer-science era.

C. Purpose and Methodology of the Roadmap

This roadmap has been formulated and written by the members of a Technology Experts Panel (TEP or the “panel”), whose membership of internationally recognized researchers in quantum information science and technology (QIST) held a kick-off meeting in La

Jolla, California, USA, in late January 2002 to develop the underlying roadmap methodology. The TEP membership was as follows:

Chair: Dr. Richard Hughes – Los Alamos National Laboratory

Deputy Chair: Dr. Gary Doolen – Los Alamos National Laboratory

Prof. David Awschalom – University of California: Santa Barbara

Prof. Carlton Caves – University of New Mexico

Prof. Michael Chapman – Georgia Tech

Prof. Robert Clark – University of New South Wales

Prof. David Cory – Massachusetts Institute of Technology

Dr. David DiVincenzo – IBM: Thomas J. Watson Research Center

Prof. Artur Ekert – Cambridge University

Prof. P. Chris Hammel – Ohio State University

Prof. Paul Kwiat – University of Illinois: Urbana-Champaign

Prof. Seth Lloyd – Massachusetts Institute of Technology

Prof. Gerard Milburn – University of Queensland

Prof. Terry Orlando – Massachusetts Institute of Technology

Prof. Duncan Steel – University of Michigan

Prof. Umesh Vazirani – University of California: Berkeley

Prof. K. Birgitta Whaley – University of California: Berkeley

Dr. David Wineland – National Institute of Standards and Technology, Boulder

The TEP held a further five meetings in conjunction with the annual ARO/ARDA/NSA/NRO Quantum Computation Program Review (QCPR) meeting in Nashville, Tennessee, USA, in August 2002. The sheer diversity and rate of evolution of this field, which are two of its significant strengths, made this a particularly challenging exercise. To accommodate the rapid rate of new developments in this field, the roadmap will be a living document that will be updated annually, and at other times on an *ad hoc* basis if merited by significant developments. Certain topics will be revisited in future versions of the roadmap and additional ones added; it is expected that there will be significant changes in both content and structure. At the La Jolla meeting, TEP members

decided that the overall purpose of the roadmap should be to set as a desired future objective for QC

“to develop by 2012 a suite of viable emerging-QC technologies of sufficient complexity to function as quantum computer-science test-beds in which architectural and algorithmic issues can be explored.”

The roadmap is intended to function in several ways to aid this development. It has a prescriptive role by identifying what scientific, technology, skills, organizational, investment, and infrastructure developments will be necessary to achieve the desired goal, while providing options for how to get there. It also performs a descriptive function by capturing the status and likely progress of the field while elucidating the role that each aspect of the field is expected to play toward achieving the desired goal. The roadmap can identify gaps and opportunities, and places where strategic investments would be beneficial. It will provide a framework for coordinating research activities and a venue for experts to provide advice. The roadmap will therefore allow informed decisions about future directions to be made, while tracking progress, and elucidating interrelationships between approaches to assist researchers to develop synergistic solutions to obstacles within any one approach. The roadmap is intended to be an aid to researchers and to those managing or observing the field.

Underlying the overall objective for the QC roadmap, the panel members decided on a four level structure with a division into “high level goals,” “mid-level descriptions,” “detailed level summaries,” and a summary that includes the panel’s recommendations for optimizing the way forward.

The panel members decided on specific ambitious, but attainable five- and ten-year high-level technical goals for QC. These technical goals set a path for the field to follow that will lead to the desired QC test-bed era in 2012.

The mid-level roadmap view captures the breadth of approaches to QC on the international scale and uses a graphical format to describe in general terms how the

different research approaches are progressing towards these technical goals relative to common sets of criteria and metrics. The panel decided to first segment the field into a few broad categories, with multiple projects grouped together in each category according to their underlying similarities. The panel decided that two types of measures were necessary to adequately represent the status of each category: a set of criteria characterizes the “promise” of a class of approaches as a candidate QC technology; whereas a set of metrics captures the “status” of the approach in terms of technical advances along the way to achieving the high-level goals.

The “detailed summaries” provide more information on the essential concept of each approach, the breadth of projects involved, the advantages and challenges of the class of approaches, and a timeline for likely progress according to a common format. These summaries, written by subgroups of the panel members after soliciting input from their respective scientific communities, are intended to provide a brief, readable account that represents the status and potential of the entire approach from a world-wide perspective. The panel has endeavored to provide a complete, balanced, and inclusive picture of each research approach, but with the caveat that it is expected that additional content will need to be added to each summary in future versions of the roadmap, after further input from the scientific community. The panel members decided that it was not appropriate for the roadmap to attempt to describe the relative status of different individual projects within each approach.

The panel members found it especially challenging to adequately represent the status and role of theory in the roadmap. Clearly, theory has been pivotal in the development of QC to its present state, providing often-unanticipated advances that have stimulated experimental investigations. At the same time, it is difficult to schedule or define meaningful “metrics” for such future breakthroughs. For Version 1.0 of the roadmap the panel decided that the primary focus would be on experimental approaches to QC and limited the description of theory to its historical role. In the present Version 2.0 release all sections have been updated to reflect advances in the 14 months since release of Version 1.0. In addition new sections on cavity-QED approaches to QC and a full theory

section, with coverage of decoherence theory, quantum information theory, quantum algorithms and QC complexity, and quantum computer architectures, have been added. In addition, each detailed summary for the different experimental areas provides an overview of the specific areas in which additional theory work is needed.

D. High-Level Goals of the Quantum Computation Roadmap

Although QC is a basic-science endeavor today, it is realistic to predict that within a decade fault-tolerant QC could be achieved on a small scale. The overall objective of the roadmap can be accomplished by facilitating the development of QC to reach a point from which scalability into the fault-tolerant regime can be reliably inferred. It is essential to appreciate that “scalability” has two aspects: the ability to create registers of sufficiently many physical qubits to support logical encoding *and* the ability to perform qubit operations within the fault-tolerant precision thresholds. The desired 2007 and 2012 high-level goals of the roadmap for QC are therefore:

by the year 2007, to

- *encode a single qubit into the state of a logical qubit formed from several physical qubits,*
- *perform repetitive error correction of the logical qubit, and*
- *transfer the state of the logical qubit into the state of another set of physical qubits with high fidelity; and*

by the year 2012, to

- *implement a concatenated quantum error-correcting code.*

Meeting these goals will require both experimental and theoretical advances. While remaining within the basic-science regime, the 2007 high-level goal requires the achievement of four ingredients that are necessary for fault-tolerant scalability:

- creating deterministic, on-demand quantum entanglement;
- encoding quantum information into a logical qubit;
- extending the lifetime of quantum information; and

- communicating quantum information coherently from one part of a quantum computer to another.

This is a challenging 2007 goal—requiring something on the order of ten physical qubits and multiple logic operations between them, yet it is within reach of some present-day QC approaches and new approaches that may emerge from synergistic interactions between present approaches.

The 2012 high-level goals, which requires on the order of 50 physical qubits, are to:

- exercise multiple logical qubits through the full range of operations required for fault tolerant QC in order to perform a simple instance of a relevant quantum algorithm; and
- approach a natural experimental QC benchmark, i.e., the limits of fullscale simulation of a quantum computer by a conventional computer.

The 2012 goal would be within reach of approaches that attain the 2007 goal. It would extend QC into the quantum computer test-bed regime, in which architectural and algorithmic issues could be explored experimentally. Quantum computers of this size would also open up the possibilities of quantum simulation as originally envisioned by Feynman. New ways of using the computational capabilities of these small quantum computers could be explored, such as distributed QC and classically networked arrays (“type II” quantum computers), which recent work suggests may be advantageous for partial differential equation simulations, even though in contrast to other potential QC applications no exponential or polynomial speed-up would be possible.

Within these overall goals, different scientific approaches will play a variety of roles; it is expected that one or more approaches will emerge that will actually attain these goals, while others will not, but will instead play vitally important supporting roles (by exploring different ways to implement quantum logic, for instance) that will be essential to the desired development of the field as a whole. It was the unanimous opinion of the

TEP that it is too soon to attempt to identify a smaller number of potential “winners;” the ultimate technology may not have even been invented yet. Considerable evolution of and hybridization between the various approaches has already taken place and should be expected to continue in the future, with some existing approaches being superseded by even more promising ones.

E. Mid-Level View of the Quantum Computation Roadmap

The mid-level roadmap view is intended to describe in general terms how the entire field of QC is progressing towards the high-level goals and provides a simple graphical tool to characterize the promise and development status according to common sets of criteria and metrics, respectively. The requirements for quantum computer hardware capable of achieving the high-level goals are simply stated but are very demanding in practice. They are:

- i) a quantum register of multiple qubits must be prepared in an addressable form and isolated from environmental influences, which cause the delicate quantum states to decohere;
- ii) although weakly coupled to the outside world, the qubits must nevertheless be strongly coupled together to perform logic-gate operations; and
- iii) there must be a readout method to determine the state of each qubit at the end of the computation.

Many different routes from diverse fields of science to realizing these requirements are being pursued. Consequently, in order to adequately represent progress, the TEP decided to segment the field into several broad classes, based on their underlying experimental physics subfields. These subfields are:

- nuclear magnetic resonance (NMR) quantum computation,
- ion trap quantum computation,
- neutral atom quantum computation,
- cavity quantum electro-dynamic (QED) computation
- optical quantum computation,

- solid state (spin-based and quantum-dot-based) quantum computation,
- superconducting quantum computation, and
- “unique” qubits (e.g., electrons on liquid helium, spectral hole burning, etc.) quantum computation.
- the theory subfield, including quantum information theory, architectures, and decoherence challenges.

Each of the different experimental approaches has its own particular strengths as a candidate QC technology. For example, atomic, optical, and NMR approaches build on well-developed experimental capabilities to create and control the quantum properties necessary for QC, whereas the solid-state and superconducting approaches can draw on existing large investments in fabrication technologies and materials studies. However, the different approaches are at different stages of development. Insights from the more developed approaches can be usefully incorporated into other, less advanced approaches, which may hold out greater potential for leading to larger-scale quantum computers. The panel decided that to adequately represent this diversity required a set of criteria for the ‘promise’ of each approach, and a set of metrics for its ‘status’ (state of progress towards the high-level goals).

To represent the promise of each approach the panel decided to adopt the “DiVincenzo criteria.” Necessary conditions for any viable QC technology can be simply stated as:

- i) a scalable physical system of well-characterized qubits;
- ii) the ability to initialize the state of the qubits to a simple fiducial state;
- iii) long (relative) decoherence times, much longer than the gate-operation time;
- iv) a universal set of quantum gates; and
- v) a qubit-specific measurement capability.

Two additional criteria, which are necessary conditions for quantum computer networkability are:

- vi) the ability to interconvert stationary and flying qubits; and
- vii) the ability to faithfully transmit flying qubits between specified locations.

The physical properties, such as decoherence rates of the two-level quantum systems (qubits) used to represent quantum information must be well understood. The physical resource requirements must scale linearly in the number of qubits, not exponentially, if the approach is to be a candidate for a large-scale QC technology. It must be possible to initialize a register of qubits to some state from which QC can be performed. The time to perform a quantum logic operation must be much smaller than the time-scales over which the system's quantum information decoheres. There must be a procedure identified for implementing at least one set of universal quantum logic operations. In order to read out the result of a quantum computation there must be a mechanism for measuring the final state of individual qubits in a quantum register. The two networking criteria are necessary if it is desired to transfer quantum information from one location to another, (e.g. between different registers or between different processors in a distributed computing situation).

4. Experimental Subfields of Approaches to Quantum Computation

A. Nuclear Magnetic Resonance (NMR) Approaches

More than 50 years ago Bloch, Purcell, and coworkers demonstrated the coherent control and detection of nuclear spins via NMR. Shortly thereafter, pulse techniques were developed (e.g., by Ramsey, Torrey, Hahn, and Waugh) to extend coherent control to multispin systems, and to permit the measurement of decoherence and dissipation rates. Since then, NMR technologies have advanced to permit applications ranging from medical imaging, materials science, molecular structure determination, and reaction kinetics.[Abragam; Slichter; Ernst] The NMR approach to quantum information processing (QIP) capitalizes on the successes of this well-proven technology, in order to engineer a processor that fulfills the five requirements for a quantum computer as outlined in the DiVincenzo criteria. Electron and nuclear spins turn out to be nearly ideal qubits, which can be manipulated through well-developed radio-frequency (rf) irradiation. The natural interactions (chemical screening, dipolar, indirect, and hyperfine) provide the quantum communication links between these qubits and have been well characterized. The amplitude of noise and imperfections are small and understood enough

to realize proof-of-principle demonstrations of this technology for applications to quantum information science (QIS).

By now, many algorithms and other benchmarks have been implemented on liquid-state NMR QIPs, bringing theoretical ideas into the laboratory and enabling the quantitative evaluation of lacks in precision and imperfections of methods for achieving quantum control. In addition, manufacturers have begun work on improving commercially available spectrometers so as to facilitate these and future implementations of QIP. While liquid-state NMR is expected to remain the most convenient experimental testbed for theoretical QIP advances for some time to come, its limitations (low polarization, limited numbers of resolvable qubits) have been thoroughly documented.[Cory, Fahmy and Havel, 1997; Warren; Braunstein, et al, 1999; Havel, et al, 2000; LaFlamme, et al].

Its success has, however, also suggested several complementary new routes toward scalable devices, and contributed greatly to the drawing of this roadmap. Most of the new routes lead immediately into the realm of solid-state magnetic resonance, bringing NMR into closer contact with many of the other approaches to QIP now being pursued. In solid-state NMR, the manipulation of large numbers of spins has already been amply demonstrated [Warren, et al; Ramanathan, et al, 2000], e.g., by creating correlated states involving 100 or more spins, and with sufficiently precise control to follow their dynamics. This has enabled the first quantitative studies of decoherence as a function of the Hamming weight of the coherence. Solid-state NMR further permits the engineering of larger QIP devices [Cory, et al, 2000] than is possible in the liquid state, because: a) polarizations of order unity have been achieved; b) the interactions are stronger and hence two-qubit gates are faster; c) the decoherence times are much longer; and d) it is possible to implement resettable registers. In the longer term, investigations will be undertaken to achieve single-spin detection, by means of force detection, algorithmic amplification and/or optical hyperfine interactions. By integrating the control learned in the liquid state with the polarization and longer decoherence times of the solid state, along with the detection efficiency provided by optics, a firm foundation on which to design engineered, spin-based, and scalable QIP devices can be built. It is anticipated that

this experience will be combined with the engineering developments of the spintronic and solid-state proposals, as well as the knowledge on pure-state dynamics from optics and ion traps to provide a complete solution to building a quantum computer. Preliminary proposals for scalable implementations based on solid-state NMR have been suggested and are starting to be explored experimentally.[Abe, et al; Suter and Lim]

B. Ion trap quantum Approaches

Schemes for ion-trap quantum-information processing (QIP) are derived from the basic ideas put forth by Cirac and Zoller [Cirac and Zoller, 1995]. These schemes satisfy all of the DiVincenzo criteria and most of the criteria have been experimentally demonstrated. Scalability can be achieved by use of ion-trap arrays that are interconnected with: i) photons [Cirac, et al, 1997; Pellizzari; DeVoe; Duan, et al2004]; ii) a movable “head” ion that transfers information between ions in separate traps [Cirac and Zoller, 2000]; or iii) by moving ions between trap nodes in the array [Kielpinski, Monroe and Wineland; Wineland, et al]. Ion qubits can now be moved between nodes in a multiple-zone trap without decoherence in a time approximately equal to the gate time.[Row, et al] Efficient separation of ion qubits for transport to separate nodes will require smaller traps with good electrode surface integrity. This can likely be accomplished with the use of existing micro-electro-mechanical systems (MEMS) or nanofabrication technology. Multiplexing can also be accomplished with optical interconnects; efforts are currently underway at Garching [Guthoehrlein, et al] and Innsbruck [Eschner, et al] to develop efficient cavity quantum electrodynamic (QED) schemes for information transfer between ions and photons.

C. Neutral Atom Approaches

A system of trapped neutral atoms is a natural candidate for implementing scalable QC [Deutsch, Brennan and Jessen, 2000] given the simple quantum-level structure of atoms, isolation of neutrals from the environment, and present ability to trap and act on a very large ensemble of identical atoms. In much the same way as the groundbreaking work on QC in ion traps,[Monroe] such a system builds on years of expertise in coherent spectroscopy developed by the atomic/optical community for application in precision

measurements, most notably in atomic clocks. One might argue that a quantum computer is nothing more than a multi-atom atomic clock, with controlled interactions between the constituent atoms. More recent advances in laser cooling and trapping technology open the door to unprecedented levels of coherence and control,[Chu] as made evident [Anglin and Ketterle] through the production of Bose-Einstein condensates (BECs) and Fermi degenerate gases. The architecture of such a computer will depend strongly on the specific trapping techniques and the method for coupling atoms. Two basic interactions can be used to trap neutral atoms: fields interacting with the atom's induced electric dipole moment or with its permanent magnetic dipole moment.

The best-studied trapping technology is the optical lattice,[Jessen and Deutsch], in which electric dipole-force potential wells are produced by the standing waves of intersecting laser beams. This virtual crystal can be dynamically controlled through the parameters of the trapping lasers or other external fields. Optical dipole forces can also be used to trap atoms in other configurations, such as through engineered micro-optics [Birkel, et al; Buchkremer, et al; Eckert, et al] and particular configurations of time-varying fields[Milner, et al]. Magnetic trapping, especially in microtraps [Folman, et al; Reichel, et al], has also been demonstrated. Trapped atoms can be cooled to the motional ground state of the potential wells, and the internal atomic states can be prepared in a desired initial state using standard techniques of laser spectroscopy. The motional and internal states provide a number of choices of levels for defining qubits. The trap itself and additional fields make available a variety of “handles” for coherent control of the motional and internal states. That the atoms are neutral means that they are relatively poorly coupled to the environment, thus reducing decoherence. By the same token, however, the atoms interact only weakly with one another. Proposals for two-qubit gates rely on: i) moving pairs of atoms into close proximity to increase their coupling (coherent transport of atoms in an optical lattice has been demonstrated;[Maandel, et al] ii) turning on briefly much stronger electric-dipole or other interactions; or iii) both of these. These techniques pose an inherent risk of opening up additional decoherence channels during gate operation.

To implement a neutral-atom quantum computer, the logical encoding for qubits, the method for performing logical operations, and the read-out strategy must all be addressed as a whole, with the design contingent on the specific atom to be used and the trapping technology. For example, parallel operations are natural in the lattice geometry, but because the atoms in a filled optical lattice are spaced less than a trap-laser wavelength apart, there are difficult questions about how to address individual atoms. Various approaches might be used to overcome this difficulty. As another example, magnetic traps restrict the possible states available for logical encoding, but offer possible advantages for integrating with solid-state devices. Whichever approach proves superior, the highest priority for any experiment is to implement controlled high-fidelity quantum logic operations. This might be achieved in a geometry that does not provide the clearest route to a scalable quantum computer (e.g., ensemble operation without individual addressing), but nonetheless provide the proof-of-principle necessary to design such a scalable system.

D. Cavity Quantum Electro-dynamic (QED) Approaches

In the context of quantum information ‘cavity QED’ refers to the coherent interaction of a material qubit (such as a trapped atom or semiconductor dot system) with the quantized (usually single photon) field of a high-finesse optical or microwave resonator. To achieve coherent dynamics with just a single photon and atom, a small, extremely low-loss build-up cavity is used to enhance the electric field per photon such that the coherent Rabi frequency of the atom-field interaction is faster than the spontaneous emission rate of the atom or the decay rate of the field in the cavity—this is known as the strong coupling regime. While this is very challenging, this limit has been achieved in some 10 laboratories over the past 15 years or so in both the microwave and optical domains.[Berman; Mabuchi and Doherty; Raimand, Brun and Haroche; Walther, 2003; Walther, 2001] Applications of cavity QED systems to quantum information processing (QIP) derive mostly from the ability to coherently intra-convert quantum states between material qubits and photon qubits. Using this basic primitive, many two-qubit gate protocols have been developed for creating atom-photon, atom-atom, or photon-photon entanglements [Pellizzari, et al; van Enk, Cirac and Zoller; Pachos and Walther; Duan,

Kuzmich and Kimble, 2003; Yi, Su and You; You, Yi Su], and proof-of-principle experiments have been performed for some of these ideas [Turchette, et al; Rauschenbeutel, et al]. Scalable architectures have also been suggested using these gates. More uniquely, cavity QED systems are featured in many ideas relating to distributed quantum information processing and communication [Cirac, et al, 1997; van Enk, et al, 1997; van Enk, Cirac and Zoller, 1997; Briegel, et al, 1998a; Briegel, et al, 1998b; Cirac, et al, 1998; van Enk, Cirac and Zoller, 1998; Briegel, et al, 1999; Gheri, Torma and Zoller; van Enk, et al, 1999] and provide a leading candidate for robust, controllable single and multiple photon sources [Kuhn, et al, 1999; Law and Kimble; Lange and Kimble; Varcoe, et al; Bertet, et al; Kuhn, Hennrich and Rempe, 2002; McKeever, et al]. Additionally, the system provides an attractive method for single atom detection [Mabuchi, et al, 1996; Hood, et al; Munstermann, et al; Shimizu, et al; Sauer, et al]. There are several types of systems:

- i) *Rydberg atoms in microwave cavities*: the strong coupling limit has been achieved in microwave cavity QED experiments employing highly excited (Rydberg) states of neutral atoms. Some of the cleanest entanglement experiments performed to-date have been in these systems. The major obstacle to this implementation is scaling: microwave cavity QED experiments use atomic beams intersecting the cavity to deliver atoms and hence atomic delivery to the cavity is stochastic;
- ii) *Neutral atoms in optical cavities*: the strong coupling regime is also well-established in the neutral atom work with optical cavities. The principle obstacles to be overcome relate to incorporating a scalable trapping geometry using optical and/or magnetic trapping potentials, while still preserving the strong coupling regime. A key element to this challenge is controlling the atomic motion and atom localization so that the coupling is sufficiently well defined;
- iii) *Trapped ion cavity QED*: recently there has been experimental work incorporating linear ion traps with optical cavities.[Guthohrlein, et al; Mundt, et al] Achieving the strong coupling regime is the major outstanding challenge facing this approach. This requires shrinking the cavity size, without adversely affecting the fields confining the ion; and

iv) *Other systems*: there are several related systems that are actively pursued by different groups. These are listed here, but are not included in this section of the roadmap: Semiconductor quantum dots systems; Solid-state ion vacancy systems; Superconducting junctions + cavity systems; and Neutral atom ensemble (many atom) based cavity QED system.

E. Optical Approaches

Optical implementations of qubits have played an important role for quantum information science. In addition to their successful application for experimentally realizing quantum cryptography [Gisin, et al], photonic qubits have been among the first physical systems to enable the realization of multiparticle entanglement [Ou and Mandel; Shih and Alley; Kwiat, et al, 1995; Strekalov, et al; Kwiat, et al, 1999], quantum-state [White, et al; James, et al] and quantum-process tomography [Chuang and Nielsen, 1997; Polyatos, Cirac and Zoller; Mazzei, et al; Altepeter, et al; Mitchell, et al], teleportation [Boumeester, et al; Pan, et al, 1998; Pan, et al, 2001; Boschi, et al; Furusawa, et al; Kim, Kulik and Shi], decoherence-free subspaces [Kwiat, et al, 2000; Altepeter, et al, 2004], and even simple quantum algorithms [Kwiat, et al, 2000; Takeuchi, 2000a; Takeuchi, 2000b; Bhattacharya, et al; Howell, Yeazell and Ventura, 2000; Howell and Yeazell, 2000b]. Photons have an intrinsic lack of decoherence, as well as an extreme precision with which they may be controlled using standard off-the-shelf components. For these reasons, optical qubits have played, and will continue to play, an important role in investigating foundations of quantum information processing (QIP), and fundamentals of QC in systems with small numbers of qubits.

Photonic qubits for QC are particularly attractive because they could interface immediately to various quantum-communication applications (e.g., distributed QC). Due to the extremely small photon-photon coupling available in existing materials, it was at one point believed that optical qubits could never be used for scalable QC. However, recent advances with slow light [Haw, et al; Kash, et al; Budker, et al] and “stopped” light [Liu, et al; Phillips, et al] indicate that these limitations may be overcome [Lukin and Imamoglu]. In addition, interesting results have appeared, which indicate that light

that is initially prepared in a nonclassical “squeezed” state may enable additional gains for QIP (so called “continuous variable” encoding) [Lloyd and Braunstein; Gottesman, Kitaev and Preskill]. Finally, it is now understood that the process of photo detection itself can lead to effective photon-photon nonlinearities [Bartlett, et al]. For example, it has been shown that deterministic single photon sources (SPSs) and high-efficiency single-photon detectors (SPDs) may be used to realize scalable QC with only linear optical elements.[Knill, LaFlamme and Milburn] Below, we concentrate on this scheme as an example of optical QC. However, it should be emphasized that other approaches are also being followed, and may be critical for the overall progress toward scalable QC, even if these other approaches do not themselves realize it. For example, hybrid schemes involving qubits, qudits, and continuous variables, as can be realized in optical systems, have interesting and important properties—some of them display “hyper-entanglement” (simultaneous entanglement in multiple degrees of freedom), which may facilitate certain tasks in quantum information processing [Kwiat, 1997; Atature, et al], such as purification and quantum error correction. Similarly, optical systems can be used to explicitly study decoherence in a controlled manner and to implement proposals for avoiding the negative effects of decoherence (e.g., DFSs). It is a feature of optically encoded qubits that decoherence can be controllably introduced by artificially coupling the qubit to other degrees of freedom [Preskill]. This feature allows optically based systems to simulate other qubit realizations in a very clean, controllable way.

Linear optics quantum computing (LOQC) is a scheme for QIP using linear optics, SPSs, and SPDs.[Kwiat, 1997; Atature, et al] A number of authors have suggested simplifications and modifications of the original scheme [Pittman, Jacobs and Franson, 2001; Knill; Hofman and Takeuchi; Ralph, White and Milburn]. We take a broader view of optical QC that may also include nonlinear elements as a crucial component, provided those nonlinear elements are readily available or under development (e.g., entangled state via spontaneous parametric down conversion [SPDC], quantum memories, etc.). A number of simple experiments have been done to test the most elementary components of the scheme [Pittman, Jacobs and Franson, 2002a; Pittman, Jacobs and Franson, 2002b; O’Brien, et al; Pittman and Franson, 2002c; Kwiat, 2004]. All of these use SPDC

sources, which require that experiments be done in a post-selective manner using multicoincidence detection. Further progress in the KLM scheme will require on-demand SPSs and very efficient discriminating SPDs. One of the main challenges in an LOQC approach may be the generation of the required entangled ancilla states. This becomes especially difficult if the detector efficiency is low (less than 99%). Hence, development of entanglement sources could play a key role in achieving LOQC. In addition, other alternative schemes (not based on single-photon states) have been proposed. [Gottesman, Kitaev and Preskill; Ralph, et al]

F. Solid State Approaches

The work of recent years, starting in the mid 1990s, has uncovered a very large number of possible solid-state systems in which quantum computing might be achieved, reflecting the huge variety of quantum phenomena that are known in condensed matter physics. Given the current state of discussions and progress on these proposals, it is the judgment of the TEP that the most important existing progress in the laboratory, and the clearest prospects for continuing mid-term progress, is provided by localized “spin” or “charge” qubits, which will be described here in detail. We do not exclude the possibility that further progress on various other proposals, including electrons on liquid helium, quantum Hall edge states, carbon tubes and balls, semiconductor nanowires, or others might make them worthy of detailed assessment at a later date.

Many of the variations on the spin and charge approaches discussed here rely on the fact that in many solid state systems, the spin states of localized electrons or of nuclei, form well-defined, highly coherent two-level systems that are useable as qubits. The quantum-gate implementations typically rely on the most natural physical interaction between spins, the exchange interaction. It is envisioned that a highly miniaturizable, all-electronic or optoelectronic qubit is conceivable in this area. Localized spins are available via confinement to QDs or impurity atoms, by entrainment by surface acoustic wave (SAW) techniques, and by other methods. While the necessary device-fabrication techniques for QDs are available down to single-electron spins, this is not the case yet for impurity atoms. QDs are a versatile system for qubits; other schemes, including excitonic qubits

with optical addressing and coupling, have been devised as well as optically driven spin based QDs using a charged exciton as an optically induced transient high-speed gate. Quantum mechanical systems, using nano-cantilevers, can also play a role in coupling and reading out solid-state qubits.

In a system using optically driven quantum-dot excitons, charge refers to the fact that the state of the qubit is determined by the state of excitation of an electron-hole pair in a semiconductor QD. In this case, the qubit becomes the optical Bloch vector. The decoherence time in this system is then limited by the optical dipole, which determines the radiative recombination rate. Measurements have shown that there are generally no other dephasing mechanisms. The clock-speed is limited by the reciprocal pulse width that would excite higher lying states of the dot. This leads to a limiting figure of merit probably near or somewhat in excess of 10^3 . QDs are produced either epitaxially or by chemical synthesis. Two-qubit nonscalable devices can be demonstrated in single QDs using orthogonally polarized excitonic transitions. The interactions between the two qubits essential to creating entanglement are produced by higher-order Coulomb coupling leading to bi-exciton formation. Scalable systems have been envisioned where nearby QDs interact via dipole-dipole coupling, wavefunction overlap, or radiation coupling via an optical cavity. The relatively fast decoherence, determined by radiative lifetime, is often seen as a limiting liability in these systems. However, these systems represent the prototypical optical excitation needed to enable optical manipulation of single-electron spins for spin-based qubit.

Interestingly, the exciton QD is a charge-based system where the dot is neutral. In most cases of interest, the spin-based qubit in a QD is charged. The optical excitation path uses the same path as in the exciton system, but a second photon is needed to complete the rotation of the spin. The basic ideas that are being pursued in this area were laid out by Loss and DiVincenzo (QDs) [Loss and DiVincenzo], and were adapted to impurity spins by Kane [Kane], and extended to optically driven spin-based systems by Rossi and Zoller [Pazy, et al]. Two specific examples in solid state systems are impurity spins and spins in QDs.

i) Nuclear spin of P donors in Si

The nuclear spin ($I = 1/2$) of ^{31}P is a natural two-level system embedded in a spin-free substrate of ^{28}Si ($I = 0$). The nuclear spins of ^{31}P donors are separated by approximately 20 nm and there is a hyperfine interaction between donor electron spin and nuclear spin (qubit). Interaction between qubits is mediated through the donor-electron exchange interaction. The spins are maintained at mK temperatures in an external magnetic field of several Tesla, perpendicular to the plane of the substrate. Nanoscale surface A and J gates control the hyperfine and exchange interactions at qubit sites. Two distinct states have been observed in ensemble nuclear magnetic resonance (NMR) experiments, but not in single-spin systems. Radio frequency (rf) coils can be used to apply π -pulses (or surface control gates can be pulsed in the presence of a continuous wave rf field B_{ac}), demonstrated in ensemble-spin systems but not single-spin systems. Rabi oscillations are yet to be demonstrated for single spins. The system scales essentially linearly with respect to resources (gates, donors, etc).

ii) Electron spin in GaAs QDs

The spin of a single electron confined in a QD provides a natural qubit which can be manipulated either electronically or optically. The QD can be defined by 50-nm-wide electrostatic gates on top of a AlGaAs/GaAs two-dimensional electron gas, or by three dimensional (3-D) confinement in a patterned semiconductor heterostructure, with a center-to-center distance between dots of about 200 nm. It is currently possible to isolate a single electron in each of two such QDs. In equilibrium at 300 mK and 5 Tesla (T), the electrons will be in the ground state spin-up with $> 99\%$ probability. An essential idea of the proposal is an all-electrical control of spin via electrical gates, i.e., to make use of a “spin-to-charge conversion” based on the Pauli’s exclusion principle obeyed by electrons. The spin of the electron is used as storage of quantum information, while the charge and Coulomb interaction of the electron allows for fast gate operations and readout. In addition, if the magnetic field is oriented perpendicular to the substrate, the leads provide a reservoir of spin-polarized electrons, which can serve as a reference for qubit readout. Pulsed microwave fields on resonance with the spins give single-qubit rotations, and electrostatic control of the exchange interaction between spins in neighboring dots permits two-qubit gates. Both types of quantum gates still need to be demonstrated. The

resources (gates etc.) scale linearly with the number of qubits. An all-optical approach allows us to exploit the advances in ultra-fast laser technology, potentially integrated on-chip without the use of metallic gates and electrical coupling. QDs can be defined by 3-D confinement in a patterned semiconductor heterostructure, with a center-to-center distance between dots of about 200 nm. QDs can be doped with a single electron and operated at 4K at magnetic fields of order of 7 to 10 T. Quantum logic-gate operations involving spins of single electrons confined in QDs occur through the exchange interaction of spin to nearby QDs through the spin-spin interaction. The gate interaction is controlled by an ultra-fast solid-state laser, which transiently excite electron-hole pairs (excitons or trions) that mediate the spin-spin interaction.

G. Superconducting Approaches

The qubits are superconducting circuits made with Josephson junctions and operating at mK temperatures. The information is stored in either the charge on a nanoscale superconducting island, the flux or phase drop in a circulating current, or in the energy levels in a single junction [Maklin, Schoen and Shnirman]. The interactions are either capacitive for charge-based circuits or inductive for flux- or phase-based circuits. Because these are electrical circuits, other electrical coupling elements are possible, such as tunnel junctions, transformers, single-electron transistors (SETs), etc. The typical energy-level splitting between the qubit states varies between 1 and 10 GHz. Clock periods are estimated to be of the order of a nanosecond (this is the minimum time for a one-qubit rotation). The qubits are prepared in their initial state by cooling the system to their ground state. Then radio frequency (rf) electromagnetic pulses are used to manipulate the qubits to perform quantum operations. The manipulation of the superconducting qubits can be controlled by on-chip, ultra-fast superconducting circuitry. For example, simple single-flux quantum (SFQ) circuitry can operate at speeds up to 700 GHz with small power dissipation. There is a broad diversity of measurement options appropriate to different speeds and measurement bases. Most measurement schemes are based on superconducting quantum interference device (SQUID) magnetometers, SET electrometers, or switching of Josephson junctions.

H. “Unique” Qubits Approaches

In addition to the relatively well-established methods for performing quantum information processing (QIP) and quantum computing (QC) described in detail earlier in this document, there exist potentially fruitful approaches to QIP based on a variety of quantum technologies. Virtually any quantum system that is addressable, controllable, and coherent has the potential to perform QC. The situation is reminiscent of the early days of digital computing, when switches and circuits were constructed from a variety of technologies, including electromechanical relays, vacuum tubes, and even from purely mechanical and hydraulic components in environments where electrical systems were inappropriate. Even today, when virtually all computers are based on integrated circuits, memory technologies exhibit considerable diversity. There are a variety of types of integrated circuits for memory, as well as magnetic memories (hard disks) and optical memories (CDs). Perhaps as a result of the diversity of different memory technologies, the Moore's law rate of increase of density of memory circuits has followed a more rapid pace than that of processing circuits. Similarly, we anticipate that a variety of different QIP technologies may be used for different purposes as the field matures further. This section lists several such approaches to QIP. There exist tens of such “unique” approaches, and not all will be described here. Rather, this section will concentrate on approaches that have current, funded research programs: these approaches have been thoroughly researched and found worth further investigation. It is anticipated that in the future more unique approaches will arise; these will be evaluated as they arrive. In addition, the ongoing research will serve to show which of these various approaches are the most promising.

Summaries of existing efforts follow; which include general discussions of the state of the art for input-output, coherent computation, and decoherence. For two of these approaches, electronics on helium QC and spectral hole burning QC, short additional write-ups are included in the following sections.

- i) QIP using nanotubes and nanowires.

Carbon nanotubes and silicon nanowires represent a well-developed nanotechnology. Such systems are known to exhibit significant degrees of quantum coherence for electron

transport. Nanotubes can be used to create arrays of quantum dots (QDs) whose coupling can be turned on and off using silicon nanowires. Such systems share virtues and deficiencies with lithographed QD systems and potentially possess additional features, such as an enhanced degree of regularity of the dots due to the chemical synthesis of the nanotubes. Experimental efforts exist: further research is being performed on input-output, coherent control, and the properties of decoherence of electron spin in nanotube systems.

ii) Quantum logic using electrons on the surface of liquid helium

Electrons on the surface of liquid helium represent a clean system for registering and processing quantum information. The electrons effectively float above the surface of the helium, and their states can be manipulated by microwaves and by circuits embedded in the silicon substrate below the helium film. Experiments have been performed exhibiting single-electron detection, and are underway to exhibit coherent control of electrons on helium by the application of microwaves. Further investigations are taking place into the properties of decoherence and into the performance of quantum logic operations in such systems.

iii) Molecular spin arrays

Chemical techniques can be used to produce self-assembled arrays of molecules containing electron spins. Such systems represent natural candidates for quantum computers with a cellular-automata architecture. Experiments on such systems are in the initial phase. Issues of decoherence, input-output, and coherent control are understood to some degree in theory; more theoretical and experimental investigations are underway.

iv) Quantum hall effect QC

Quantum-Hall-effect systems are well studied experimentally and represent good potential systems in which to perform QIP. Quantum information can be stored on highly coherent, long-lived nuclear spins, then transferred to electron spins and excitons for information transmission and readout. Coherence times have been measured in such systems and are favorable for QC. Detailed studies of input-output characteristics, decoherence, and quantum logic operations are underway.

v) QC using non-abelian anyons

Topological methods for QC have attracted considerable interest because of their intrinsically fault-tolerant properties. In such methods, quantum information is stored on non-abelian anyons, and quantum logic operations are performed by ‘braiding’ the anyons around each other in a two-dimensional plane. Non-abelian anyons are relatively exotic systems, which could potentially be constructed using arrays of quantum logic gates (e.g., superconducting quantum logic circuits) or implemented using the higher order fractional quantum Hall effect. Preliminary theoretical investigations of both types of approaches indicate their feasibility. Experiments are forthcoming.

vi) QC using the fractional quantum Hall effect

QC can also be performed in a topological fashion using abelian anyons, such as the usual fractional quantum Hall quasiparticles. Abelian anyons share some, though not all, of the fault tolerance of the non-abelian anyons discussed above, and have the advantage that they have been investigated and manipulated experimentally. Theoretical and experimental investigations are currently underway to determine levels of decoherence for quantum Hall quasiparticles, and to perform simple quantum logic operations.

vii) Electro-mechanical systems for QIP

Nanofabricated mechanical resonators exhibit high Q’s and quantum coherence. Such mechanical devices represent natural structures on which to perform QIP. They can be coupled to electronic systems for measurement and control purposes. They can be interfaced, in principle, with superconducting quantum computers. Initial theoretical and experimental investigations on quantum control and decoherence for such systems have been performed; more extensive investigations are in progress.

viii) QC using spectral hole burning

Spectral hole burning is a well-established technique for addressing optically active atoms in solids. It allows for a potentially high density of quantum bits by using both spatial and frequency addressing techniques. A variety of models for quantum computing using spectral hole burning have been investigated, using optical cavities and/or dipolar coupling between spectral holes. Experimental investigations of the controllability and coherence properties of spectral holes have been performed and indicate a level of controllability comparable to normal quantum optical approaches to QC, with reduced coherence due to the solid-state nature of spectral-hole systems. Current experimental

investigations are aimed towards elucidating the coherence structure of spectral holes and towards coupling spectral holes to perform quantum logic operations.

5. Concluding Remarks

Between the Turing machine and the Church-Turing Thesis a strong foundation was made for study of what was computable and uncomputable. Complexity analysis allows for a more granular distinction between the tractability of any particular problem on a Turing machine. The components in classical computers are rapidly shrinking to a size where quantum behavior is inevitable. Through the principle of superposition in quantum systems we can create useful memory components that are on the scale of an atom or smaller. These quantum memory registers may facilitate exponential computational speed increases by taking advantage of quantum parallelism. Peter Shor has provided an algorithm, which makes factoring large numbers tractable, and in doing so has drawn great attention to the field of quantum computing. Due to Shor's algorithm, we may someday have to turn to other means of encrypting data than currently employed. L. K. Grover's database search algorithm shows another noteworthy task that a quantum computer can perform faster than any classical computer. (Brassard, Gilles. "Searching a Quantum Phone Book," *Science*, 31 January 1997.)

The efforts to build a functional quantum memory register are in the most preliminary stages. Operational quantum computers are by no means an inevitable consequence of this research. The problems of keeping a quantum memory register isolated from any disturbance long enough for a calculation to take place appears to be nontrivial, but quantum computing will remain an exciting topic for experimentalists and theorists alike for year to come. The existence of loosely organized efforts such as the 2004 quantum computation roadmap demonstrates the intrinsic interests in the scholarly communities of physics and other allied sciences and engineering and provides the basis for our optimism.

Acknowledgment

This assessment was initiated at the request of the Korean Federation of Science and Technology Societies (KOFST) through the Korean Scientists and Engineers in America (KSEA). The study was carried out as part of the KSEA studies in the area of Research and Development in Information Science and Technology during the six-month period ending in March 2006. The author gratefully acknowledges partial support of this investigation by the KOFST and Lehigh University.

References and Bibliography

Abe, E., K.M. Itoh, T.D. Ladd, J.R. Goldman, F. Yamaguchi, and Y. Yamamoto, "Solid-state silicon NMR quantum computer," *Journal of Superconductivity: incorporating Novel Magnetism* 16, 175–178 (2003).

Abragam A., *The Principles of Nuclear Magnetism* (Clarendon Press, Oxford, 1961).

Altepeter, J.B., D. Branning, E. Jeffrey, T.C. Wei, P.G. Kwiat R.T. Thew, J.L. O'Brien, M.A. Nielsen, and A.G. White, "Ancilla-assisted quantum process tomography," *Physical Review Letters* 90, 193601 (2003).

Altepeter, J.B., P.G. Hadley, S.M. Wendelken, A.J. Berglund, and P.G. Kwiat, "Experimental investigation of a two-qubit decoherence-free subspace," (to appear in *Physical Review Letters* 2004).

Anglin, J.Rand W Ketterle, "Bose-Einstein condensation of atomic gases," *Nature* 416, 211–218 (2002).

Aspect, A., Grangier, P., Roger, G(1982) "Experimental Tests of Bell's Inequalities Using Time-Varying Analyzers" *Physical Review Letters* 49: 1804-1807.

Atature, M., G. Di Giuseppe, M.D. Shaw, A.V. Sergienko, B.E.A. Saleh, and M.C. Teich, "Multi-parameter entanglement in femtosecond parametric down-conversion," *Physical Review A* 65, 023808 (2002).

Barenco, A., "Quantum Computation: An Introduction" in Lo, Popsu and Spiller, 1998.

Bartlett, S.D., B.C. Sanders, S.L. Braunstein, and K. Nemoto, "Efficient classical simulation of continuous variable quantum information processes," *Physical Review Letters* 88, 097904 (2002).

Bell, J.S(1964) "On the Einstein-Podolsky-Rosen Paradox" *Physics* 1: 195-200.

Berman, P., Ed , *Cavity Quantum Electrodynamics*, (Academic Press, Boston, MA, 1994).

Bertet, P., S. Osnaghi, P. Milman, A. Auffeves, P. Maioli, M. Brune, J.M. Raimond, and S. Haroche, "Generating and probing a two-photon Fock state with a single atom in a cavity," *Physical Review Letters* 88, 143601 (2002).

Bhattacharya, N., H.B. van Linden van den Heuvel, and R.J.C. Spreeuw, "Implementation of quantum search algorithm using classical Fourier optics," *Physical Review Letters* 88, 37901 (2002).

- Birkl, G., F.B. JBuchkremer, R. Dumke, and W. Ertmer, "Atom optics with microfabricated optical elements," *Optics Communications* 191, 67–81 (2001).
- Boschi, D., S. Branca, F. DeMartini, L. Hardy, and S. Popescu, "Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters* 80, 1121–1125 (1998).
- Bouwmeester, D., J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature* 390, 575–579 (1997).
- Braunstein, S.L., C.M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, "Separability of very noisy mixed states and implications for NMR quantum computing," *Physical Review Letters* 83, 1054–1057 (1999).
- Braunstein, S.L., and P. van Loock, "Quantum information with continuous variables," *Reviews of Modern Physics* 77, 513–577 (2005).
- Briegel, H.J., J.I. Cirac, W. Dür, S.J. van Enk, H.J. Kimble, H. Mabuchi, and P. Zoller, "Physical implementations for quantum communication in quantum networks," *Quantum Computing and Quantum Communications* 1509, 373–382 (1999).
- Briegel, H.J., T. Calarco, D. Jaksch, J.I. Cirac, and P. Zoller, "Quantum computing with neutral atoms," *Journal of Modern Optics* 47, 415–451 (2000).
- Briegel, H.J., W. Dür, J.I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Physical Review Letters* 81, 5932–5935 (1998a).
- Briegel, H.J., W. Dür, S.J. van Enk, J.I. Cirac, and P. Zoller, "Quantum communication and the creation of maximally entangled pairs of atoms over a noisy channel," *Philosophical Transactions of the Royal Society of London Series A-Mathematical, Physical, and Engineering Sciences* 356, 1841–1851 (1998b).
- Bub, J. (2006) "Quantum Information and Computation" John Earman and Jeremy Butterfield (eds.), *Handbook of Philosophy of Physics* (Elsevier/North Holland, forthcoming in 2006) Available at: arXiv e-print quant-ph/0512125.

Buchkremer, F.B.J., R. Dumke, M. Volk, T. Muther, G. Birkl, and W. Ertmer, "Quantum information processing with microfabricated optical elements," *Laser Physics* 12, 736–741 (2002).

Budker, D., D.F. Kimball, S.M. Rochester, and V.V. Yashchuk, "Nonlinear magneto-optics and reduced group velocity of light in atomic vapor with slow ground state relaxation," *Physical Review Letters* 83, 1767–1770 (1999).

Chu, S., "Cold atoms and quantum control," *Nature* 416, 206–210 (2002).

Chuang, I.L. and M.A. Nielsen, "Prescription for experimental determination of the dynamics of a quantum black box," *Journal of Modern Optics* 44, 2455–2467 (1997).

Cirac, J.I., and P. Zoller, "A scalable quantum computer with ions in an array of microtraps," *Nature* 404, 579–581 (2000).

Cirac, J.I., and P. Zoller, "Quantum computations with cold trapped ions," *Physical Review Letters* 74, 4091–4094 (1995).

Cirac, J.I., P. Zoller, H.J. Kimble, and H. Mabuchi, "Quantum state transfer and entanglement distribution among distant nodes in a quantum network," *Physical Review Letters* 78, 3221–3224 (1997).

Cirac, J.I., P. Zoller, H.J. Kimble, and H. Mabuchi, "Quantum state transfer and entanglement distribution among distant nodes in a quantum network," *Physical Review Letters* 78, 3221–3224 (1997).

Cirac, J.I., S.J. van Enk, P. Zoller, H.J. Kimble, and H. Mabuchi, "Quantum communication in a quantum network," *Physica Scripta T76*, 223–232 (1998).

Cory, D.G., A.F. Fahmy and T.F. Havel, "Ensemble quantum computing by NMR spectroscopy," *Proceedings of the National Academy of Science (USA)* 94, 1634–1639 (1997).

Cory, D.G., R. Laflamme, E. Knill, L. Viola, T.F. Havel, N. Boulant, G. Boutis, E. Fortunato, S. Lloyd, R. Martinez, C. Negrevergne, M. Pravia, Y. Sharf, G. Teklemarian, Y.S. Weinstein, and Z.H. Zurek, "NMR based quantum information processing: Achievements and prospects," *Fortschritte der Physik [Progress of Physics]* 48, 875–907 (2000).

Deutsch, D., "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer" *Proceedings of the Royal Society (London)* A400: 97-117 (1985).

- Deutsch, I.H., G.K. Brennen, and P. Sjessen, "Quantum computing with neutral atoms in an optical lattice," *Fortschritte der Physik [Progress of Physics]* 48, 925–943 (2000).
- DeVoe, R.G., "Elliptical ion traps and trap arrays for quantum computation," *Physical Review A* 58, 910–914 (1998).
- Dieks, D., "Communication by EPR Devices" *Physics Letters A* 92: 271-272 (1982).
- DiVincenzo, D.P., Review of "Quantum Computing: A Short Course from Theory to Experiment by J. Stolze and D. Suter (Wiley-VCH, 2004)", *American Journal of Physics* 73, 799-800 (2005).
- Duan, L.M., A. Kuzmich, and H.J. Kimble, "Cavity QED and quantum-information processing with "hot" trapped atoms," *Physical Review A* 67, 032305 (2003).
- Duan, L.-M., B.B. Blinov, D.L. Moehring, and C. Monroe, "Scalable trapped ion quantum computation with a probabilistic ion-photon mapping," (5-Jan-04) preprint quant-ph/0401020.
- Eckert, K., J. Mompart, X.X. Yi, J. Schliemann, D. Bruss, G. Birkl, and M. Lewenstein, "Quantum computing in optical microtraps based on the motional states of neutral atoms," *Physical Review A* 66, 042317 (2002).
- Ernst, R.R., G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Clarendon Press, Oxford, 1987).
- Eschner, J., ChRaab, FSchmidt-Kaler, and RBlatt, "Light interference from single atoms and their mirror images," *Nature*, 413, 495–498 (2001).
- Feynman, R., *Feynman Lectures on Computation*, edited by J.G. Hey and R.W. Allen (Reading, MA: Addison-Wesley Publishing Company, 1996).
- Folman, R., P. Krueger, D. Cassettari, B. Hessmo, T. Maier, and J. Schmiedmayer, "Controlling cold atoms using nanofabricated surfaces: Atom chips," *Physical Review Letters* 84, 4749–4752 (2000).
- Furusawa, A., J. Sorensen, S.L. Braunstein, C. Fuchs, H.J. Kimble, and E.S. Polzik, "Unconditional quantum teleportation," *Science* 282, 706–709 (1998).

Galindo, A., and M.A. Martı́n-Delgado, "Information and computation: Classical and quantum aspects," *Reviews of Modern Physics*, 74, 347-423 (2002).

Gheri, K.M., P. Torma, and P. Zoller, "Quantum state engineering with photonic qubits," *Acta Physica Slovaca* 49, 523-532 (1999).

Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics* 74, 145-195 (2002).

Gottesman, D., A. Kitaev, and J. Preskill, "Encoding a qubit in an oscillator" *Physical Review A* 64, 012310 (2001).

Grover, L.K., "A Fast Quantum Mechanical Algorithm for Database Search," *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (1996), pp212-219.

Guthohrlein, G.R., M. Keller, K. Hayasaka, W. Lange, and H. Walther, "A single ion as a nanoscopic probe of an optical field," *Nature* 414, 49-51 (2001).

Hayward, M, "Quantum algorithms," <http://alumni.imsa.edu/~matth/quant/299/paper/node18.html>.

Hau, L.V., S.E. Harris, Z. Dutton, and C.H. Behroozi, "Light speed reduction to 17 metres per second in an ultracold atomic gas," *Nature (London)* 397, 594-598 (1999).

Havel, T.F., S.S. Somaroo, C.-H. Tseng, and D.G. Cory, "Principles and demonstrations of quantum information processing by NMR spectroscopy," *Applicable Algebra in Engineering, Communication, and Computing* 10, 339-374 (2000).

Hofmann, H.F. and S. Takeuchi, "Quantum phase gate for photonic qubits using only beam splitters and post-selection," *Physical Review A* 66, 024308 (2002).

Holevo, A.S., "Statistical Problems in Quantum Physics" in G.Murayama and J.V.Prokhorov (eds) *Proceedings of the Second Japan-USSR Symposium on Probability Theory*, pp104-109 (Springer, Berlin; 1973).

Hood, C.J., M.S. Chapman, T.W. Lynn, and H.J. Kimble, "Real-time cavity QED with single atoms," *Physical Review Letters* 80, 4157-4160 (1998).

Howell, J.C. and J.A. Yeazell, "Linear optics simulations of the quantum baker's map," *Physical Review A* 61, 012304 (2000).

Howell, J.C., J.A. Yeazell, and D. Ventura, "Optically simulating a quantum associative memory," *Physical Review A* 62, 042303 (2000).

Itoh, K.M., "Silicon Quantum Computer," in *Conference Proceedings 772: Physics of Semiconductors*, eds J. Menéndez and C.G. Van de Walle (American Institute of Physics, 2005).

James, D.F.V., P.G. Kwiat, W.J. Munro, and A.G. White, "Measurement of qubits," *Physical Review A* 64, 052312 (2001).

Jessen, P.S. and I.H. Deutsch, "Optical lattices," in *Advances in Atomic, Molecular, and Optical Physics*, Vol. 37, B. Bederson and H. Walther, Eds., (Academic, San Diego, 1996), pp95–138.

Josza, R., "Quantum Information and its Properties" in [5] Lo, Popescu, and Spiller (1998).

Kane, B.E., "A silicon-based nuclear spin quantum computer," *Nature* 393, 133–137 (1998).

Kash, M.M., V.A. Sautenkov, A.S. Zibrov, L. Hollberg, G.R. Welch, M.D. Lukin, Y. Rostovtsev, E.S. Fry, and M.O. Scully, "Ultraslow group velocity and enhanced nonlinear optical effects in a coherently driven hot atomic gas," *Physical Review Letters* 82, 5229–5232 (1999).

Kielpinski, D., C. Monroe, and D.J. Wineland, "Architecture for a large-scale ion-trap quantum computer," *Nature* 417, 709–711 (2002).

Kiesel, N., C. Schmid, U. Weber, G. Toth, O. Guehne, R. Ursin, and H. Weinfurter, "Experimental Analysis of a Four-Qubit Photon Cluster State," *Physical Review Letters* 95, 210502 (2005).

Kim, Y.-H., S.P. Kulik, and Y. Shih, "Quantum teleportation of a polarization state with a complete Bell state measurement," *Physical Review Letters* 86, 1370–1373 (2001).

Knill, E., "Quantum gates using linear optics and post selection," *Physical Review A* 66, 052306 (2002).

Knill, E., R. Laflamme and G.J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature* 409, 46–52 (2001).

- Kuhn, A., M. Hennrich, and G. Rempe, “Deterministic single-photon source for distributed quantum networking,” *Physical Review Letters* 89, 067901 (2002).
- Kuhn, A., M. Hennrich, T. Bondo, and G. Rempe, “Controlled generation of single photons from a strongly coupled atom-cavity system,” *Applied Physics B* 69, 373–377 (1999).
- Kwiat, P.G., “Hyper-entangled states,” *Journal of Modern Optics* 44, 2173–2184 (1997).
- Kwiat, P.G., A.J. Berglund, J.B. Altepeter, and A.G. White, “Experimental verification of decoherence-free subspaces,” *Science* 290, 498–501 (2000).
- Kwiat, P.G., E. Waks, A.G. White, I. Appelbaum, and P.H. Eberhard, “Ultrabright source of polarization-entangled photons,” *Physical Review A* 60, R773–R776 (1999).
- Kwiat, P.G., J. Altepeter, J. Barreiro, D. Branning, E.R. Jeffrey, N. Peters, and A.P. van Devender, “Optical technologies for quantum information science,” *Proceedings of SPIE International Society of Optical Engineering* 5161, 87–100 (2004).
- Kwiat, P.G., J.R. Mitchell, P.D.D. Schwindt, and A.G. White, “Grover’s search algorithm: An optical approach,” *Journal of Modern Optics* 47, 257–266 (2000).
- Kwiat, P.G., K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko, and Y.H. Shih, “New high-intensity source of polarization-entangled photon pairs,” *Physical Review Letters* 75, 4337–4341 (1995).
- Laflamme, R., D.G. Cory, C. Negrevergne, and L. Viola, “NMR quantum information processing and entanglement,” *Quantum Information and Computation* 2, 166–176 (2002).
- Lange, W. and H.J. Kimble, “Dynamic generation of maximally entangled photon multiplets by adiabatic passage,” *Physical Review A* 61, 063817 (2000).
- Law, C.K. and H.J. Kimble, “Deterministic generation of a bit-stream of single-photon pulses,” *Journal of Modern Optics* 44, 2067–2074 (1997).
- Liu, C., Z. Dutton, C.H. Behroozi and L.V. Hau, “Observation of coherent optical information storage in an atomic medium using halted light pulses,” *Nature* 409, 490–493 (2001).

Lloyd, S. and S.L. Braunstein, "Quantum computation over continuous variables," *Physical Review Letters* 82, 1784–1787 (1999).

Lo, H.-K., Popescu, S., Spiller, T., *Introduction to Quantum Computation and Information* (World Scientific, Singapore; 1998).

Lo, H.-K., "Quantum Cryptology" in Lo, Popescu and Spiller (1998).

Loss, D. and D.P. DiVincenzo, "Quantum computation with quantum dots," *Physical Review A* 57, 120–126 (1998).

Lukin, M.D. and A. Imamoglu, "Nonlinear optics and quantum entanglement of ultraslow single photons," *Physical Review Letters* 84, 1419–1422 (2000).

Mabuchi, H. and A.C. Doherty, "Cavity quantum electrodynamics: Coherence in context," *Science* 298, 1372–1377 (2002).

Mabuchi, H., Q.A. Turchette, M.S. Chapman, and H.J. Kimble, "Real-time detection of individual atoms falling through a high-finesse optical cavity," *Optics Letters* 21, 1393–1395 (1996).

Maklin, Y., G.Schön, and A.Shnirman, "Quantum-state engineering with Josephson junction devices," *Reviews of Modern Physics* 73, 357–400 (2001).

Mandel, O., M. Greiner, A. Widera, T. Rom, T.W. Haensch, and I. Bloch, "Coherent transport of neutral atoms in spin-dependent optical lattice potentials," *Physical Review Letters* 91, 010407 (2003).

Mazzei, A., M. Ricci, F. De Martini, and G.M. D'Ariano, "Pauli tomography: Complete characterization of a single qubit device," *Fortschritte de Physik* 51, 342 (2003).

McKeever, J., A. Boca, A.D. Boozer, R. Miller, J.R. Buck, A. Kuzmich, and H.J. Kimble, "Deterministic generation of single photons from one atom trapped in a cavity," *Science* 303, 1992–1994 (2004).

Milner, V., J.L. Hanssen, W.C. Campbell, and M.G. Raizen, "Optical billiards for atoms," *Physical Review Letters* 86, 1514–1517 (2001).

Mitchell, M.W., C.W. Ellenor, S. Schneider, and A.M. Steinberg, "Diagnosis, prescription and prognosis of a Bell-state filter by quantum process tomography," *Physical Review Letters* 91, 120402 (2003).

Monroe, C., “Quantum information processing with atoms and photons,” *Nature* 416, 238–246 (2002).

Mundt, A.B., A. Kreuter, C. Becher, D. Leibfried, J. Eschner, F. Schmidt-Kaler, and R. Blatt, “Coupling a single atomic quantum bit to a high finesse optical cavity,” *Physical Review Letters* 89, 103001 (2002).

Munstermann, P., T. Fischer, P.W.H. Pinkse, and G. Rempe, “Single slow atoms from an atomic fountain observed in a high-finesse optical cavity,” *Optics Communications* 159, 63–67 (1999).

Nielsen, M.A., Chuang, I.L., *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

O’Brien, J.L., G.J. Pryde, A.G. White, T.C. Ralph, and D. Branning, “Demonstration of an all optical quantum controlled-NOT gate,” *Nature* 426, 264 (2003).

Ou, Z.Y., and L. Mandel, “Violation of Bell's inequality and classical probability in a two-photon correlation experiment,” *Physical Review Letters* 61, 50–53 (1988).

Pachos, J., and H. Walther, “Quantum computation with trapped ions in an optical cavity,” *Physical Review Letters* 89, 187903 (2002).

Pan, J.-W., D. Bouwmeester, H. Weinfurter, and A. Zeilinger, “Experimental entanglement swapping: Entangling photons that never interacted,” *Physical Review Letters* 80 3891–3894 (1998).

Pan, J.-W., M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, “Experimental demonstration of four-photon entanglement and high-fidelity teleportation,” *Physical Review Letters* 86, 4435–4438 (2001).

Pauli's letter to Born in *The Born-Einstein Letters* (Born, 1992) , p218.

Pazy, E., E. Biolatti, T. Calarco, I. D'Amico, P. Zanardi F. Rossi, and P. Zoller “Spin-based optical quantum gates via Pauli blocking in semiconductor quantum dots,” (19-Sep-2001), preprint cond-mat/0109337.

Pellizzari, T., “Quantum networking with optical fibers,” *Physical Review Letters* 79, 5242–5245 (1997).

Pellizzari, T., S.A. Gardiner, J.I. Cirac, and P. Zoller, “Decoherence, continuous observation, and quantum computing: A cavity QED model,” *Physical Review Letters* 75, 3788–3791 (1995).

- Phillips, D.F., A. Fleischhauer, A. Mair, R.L. Walsworth, and M.D. Lukin, “Storage of light in atomic vapor,” *Physical Review Letters* 86, 783–786 (2001).
- Pittman, T.B. and J.D. Franson, “Cyclical quantum memory for photonic qubits,” *Physical Review A* 66, 062302 (2002).
- Pittman, T.B., B.C. Jacobs and J.D. Franson, “Demonstration of feed forward control for linear optics quantum computation,” *Physical Review A* 66, 052305 (2002).
- Pittman, T.B., B.C. Jacobs and J.D. Franson, “Demonstration of non-deterministic quantum logic operations using linear optical elements,” *Physical Review Letters* 88, 257902 (2002).
- Pittman, T.B., B.C. Jacobs, and J.D. Franson, “Probabilistic quantum logic operations using polarizing beam splitters,” *Physical Review A* 64, 062311 (2001).
- Poyatos, J.F., J.I. Cirac and P. Zoller, “Complete characterization of a quantum process: the two-bit quantum gate,” *Physical Review Letters* 78, 390–393 (1997).
- Preskill, J., *Lecture Notes in Physics 229: Quantum Information and Computation*, California Institute of Technology (<http://www.theory.caltech.edu/people/preskill/ph229/>).
- Raimond, J.M., M. Brune, and S. Haroche, “Colloquium: Manipulating quantum entanglement with atoms and photons in a cavity,” *Reviews of Modern Physics* 73, 565–582 (2001).
- Ralph, T.C., A. Gilchrist, G.J. Milburn, W.J. Munro, and S. Glancy, “Quantum computation with optical coherent states,” *Physical Review A* 68, 042319 (2003).
- Ralph, T.C., A.G. White, and G.J. Milburn “Simple scheme for efficient linear optics quantum gates,” *Physical Review A* 65, 012314 (2002).
- Ramanathan, C., H. Cho, P. Cappellaro, G.S. Boutis, and D.G. Cory, “Encoding multiple quantum coherences in non-commuting bases,” *Chemical Physics Letters* 369, 311–317 (2003).
- Rauschenbeutel, A., G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.M. Raimond, and S. Haroche, “Coherent operation of a tunable quantum phase gate in cavity QED,” *Physical Review Letters* 83, 5166–5169 (1999).

Reichel, J., W. Haensel, P. Hommelhoff, and T.W. Haensch, "Applications of integrated magnetic microtraps," *Applied Physics B – Lasers and Optics* 72, 81–89 (2001).

Report of the Quantum Information Science and Technology, "A Quantum Information Science and Technology Roadmap – Part 1: Quantum Computation, Version 2," April 2, 2004 (Full text is available at <http://qist.lanl.gov>).

Rowe, M.A., A. Ben-Kish, B. DeMarco, D. Leibfried, V. Meyer, J. Beall, J. Britton, J. Hughes, W..M. Itano, B. Jelenkovi, C. Langer, T. Rosenband, and D.J. Wineland, "Transport of quantum states and separation of ions in a dual RF ion trap," *Quantum Information and Computation* 2, 257–271 (2002).

Sauer, J.A., K.M. Fortier, M.S. Chang, C.D. Hamley, and M.S. Chapman, "Cavity QED with optically transported atoms," (4-Sep-03) preprint quant-ph/0309052.

Schrödinger, E(1935) "Discussion of Probability Relations Between Separated Systems," *Proceedings of the Cambridge Philosophical Society* 31 (1935): 555-563; 32 (1936): 446-451.

Schumacher, B., "Quantum Coding" *Physical Review A* 51: 2738-2747 (1995).

Shannon, C.E., Weaver, W., *The Mathematical Theory of Communication* (University of Illinois Press, Urbana; 1949).

Shih, Y.H. and C.O. Alley, "New type of Einstein-Podolsky-Rosen-Bohm experiment using pairs of light quanta produced by optical parametric down conversion," *Physical Review Letters* 61, 2921–2924 (1988).

Shimizu, Y., N. Shiokawa, N. Yamamoto, M. Kozuma, T. Kuga, L. Deng, and E.W. Hagley, "Control of light pulse propagation with only a few cold atoms in a high-finesse microcavity," *Physical Review Letters* 89, 233001 (2002).

Shor, P., "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science* (1994), pp124-134.

Slichter C.P., *Principles of Magnetic Resonance* (Springer-Verlag, New York, 1980).

Stoltz, J., and Suter, D., *Quantum Computing*, Wiley-VCH, Weinheim, Germany (2004).

Strekalov, D.V., T.B. Pittman, A.V. Sergienko, Y.H. Shih, and P.G. Kwiat, "Post selection-free energy-time entanglement," *Physical Review A* 54, R1–R4 (1996).

Suter, D. and K. Lim, "Scalable architecture for spin-based quantum computers with a single type of gate," *Physical Review A* 65, 052309 (2002).

Takeuchi, S., "Analysis of errors in linear-optics quantum computation," *Physical Review A* 61, 052302 (2000).

Takeuchi, S., "Experimental demonstration of a three-qubit quantum computation algorithm using a single photon and linear optics," *Physical Review A* 62, 032301 (2000).

Turchette, Q.A., C.J. Hood, W. Lange, H. Mabuchi, and H.J. Kimble, "Measurement of Conditional Phase-Shifts for Quantum Logic," *Physical Review Letters* 75, 4710–4713 (1995).

van Enk, S.J., H.J. Kimble, J.I. Cirac, and P. Zoller, "Quantum communication with dark photons," *Physical Review A* 59, 2659–2664 (1999).

van Enk, S.J., J.I. Cirac, P. Zoller, H.J. Kimble and H. Mabuchi, "Quantum state transfer in a quantum network: a quantum-optical implementation," *Journal of Modern Optics* 44, 1727–1736 (1997).

van Enk, S.J., J.I. Cirac, and P. Zoller, "Ideal quantum communication over noisy channels: A quantum optical implementation," *Physical Review Letters* 78, 4293–4296 (1997).

van Enk, S.J., J.I. Cirac, and P. Zoller, "Photonic channels for quantum communication," *Science* 279, 205–208 (1998).

van Enk, S.J., J.I. Cirac, and P. Zoller, "Purifying two-bit quantum gates and joint measurements in cavity QED," *Physical Review Letters* 79, 5178–5181 (1997).

Vandersypen, L.M.K., and I.L. Chuang, "NMR techniques for quantum control and computation," *Reviews of Modern Physics* 76, 1037–1069 (2004).

Varcoe, B.T.H., S. Brattke, M. Weidinger, and H. Walther, "Preparing pure photon number states of the radiation field," *Nature* 403, 743–746 (2000).

Walther, H., "Generation and detection of Fock-states of the radiation field," *Zeitschrift Fur Naturforschung Section A (Journal of Physical Sciences-A)* 56, 117–123 (2001).

Walther, H., "Generation of photon number states on demand," *Fortschritte Der Physik (Progress of Physics)* 51, 521–530 (2003).

Warren, W.S., "The Usefulness of NMR Quantum Computing," *Science* 277, 1688–1690 (1997).

Warren, W.S., D.P. Weitekamp, and A. Pines, "Theory of selective excitation of multiple quantum transitions," *Journal of Chemical Physics* 73, 2084–2099 (1980).

White, A.G., D.F.V. James, P.H. Eberhard, and P.G. Kwiat, "Non-maximally entangled states: Production, characterization, and utilization," *Physical Review Letters* 83, 3103–3107 (1999).

Williams, C.P. and Clearwater, S.H., *Explorations in Quantum Computing*, Springer-Verlag, New York; 1998.

Wineland, D.J., C. Monroe, W.M. Itano, D. Leibfried, B.E. King, and D.M. Meekhof, "Information issues in coherent quantum-state manipulation of trapped atomic ions," *Journal of Research of the National Institute of Standards and Technology* 103(3), 259–328 (1998).

Wootters, W.K., Zurek, W.H., "A Single Quantum Cannot be Cloned," *Nature* 299: 802-803 (1982).

Yavuz, D.D., P.B. Kulatunga, E. Urban, T.A. Johnson, N. Proite, T. Henage, T.G. Walker, and M. Saffman, "Fast Ground State Manipulation of Neutral Atoms in Microscopic Optical Traps," *Physical Review Letters* 96, 063001 (2006).

Yi, X.X., X.H. Su, and L. You, "Conditional quantum phase gate between two 3-state atoms," *Physical Review Letters* 90, 097902 (2003).

You, L., X.X. Yi, and X.H. Su, "Quantum logic between atoms inside a high-Q optical cavity," *Physical Review A* 67, 032308 (2003).

Author's Narrative Vita

Dr. Yong W. Kim was educated in Seoul National University (B.S. in Physics, 1960; and M.S. in Physics, 1962). After the military service in Korea, he completed his doctoral studies at the University of Michigan (Ph.D. in Physics, 1968). First joined the Lehigh University faculty as assistant professor of physics in 1968, he has been a professor of physics since 1977. Also, he had been chairman of the Physics Department from 1984 to 1987. He became a naturalized U.S. citizen in 1976. He has maintained active research programs in two areas: statistical physics of fluctuations and atomic physics of nonideal plasmas, with support from various federal, state, foundation and industrial sponsors. His original research on the following topics are widely recognized: the memory effects in Brownian motion; elucidation of laser-produced plasmas as applied to composition and thermophysical property determination of molten metallic alloys; and novel concepts in shock wave generation.

He has produced eighteen Ph.D. students in the general areas of research mentioned above. He was elected a fellow of the American Physical Society in 1982 for his original research contributions. He served the Korean-American Scientists and Engineers Association as a councilor (physics, 1988-91) and auditor (1994-97), and the Association of Korean Physicists in America as president (1990-91). He was chairman of the International Advisory Committee on Shock Wave Symposium and organized its 17th biennial meeting held at Lehigh University in 1989, and published its proceedings volume (*Current Topics in Shock Waves*, Y.W. Kim, editor, American Institute of Physics, 1990). He was for ten years an editor and a member of the editorial board of *Shock Waves, An International* (Springer-Verlag) Journal, and has been an overseas editor of the *Journal of the Korean Physical Society* since 1994. He spent the calendar year 2003-04 at Seoul National University as Distinguished Foreign Visiting Professor of Physics at the invitation of the University and the Ministry of Education of the Republic of Korea.