



**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, 34<sup>th</sup> 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 34<sup>th</sup> 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 연구의 현황

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

### 전반적인 요약

Quantum Computation에 대한 관심이 깊은 것은 세가지 근본적인 이유 때문이다. (가) 현재까지의 device 소규모화 속도에 의하면 오는 십년간에 integrated micro-circuit 안에서는 기본간격이 원자규모로 줄어 들 것이라는 점; (나) 전산 algorithm에 필요한 정보단위를 양자역학적으로 기록할 수 있다는 가능성; (다) 양자역학적인 정보단위는, 즉 qubit은, 안전할 뿐만 아니라 고전적인 algorithm으로는 불가능한 전산을 가능하게 한다는 점들이다. 이 세가지 이유는 기본적인 과학적 이유로 간주되고 있어서 quantum computation 발전에 속도변화는 있을 수 있으나 본질적인 과학자와 공학자들의 관심과 흥미를 좌절하는 것은 불가능하게 보인다. 정보를 양자역학으로 표시한다는 것을 떠나서도, 전산을 위한 device 규격의 소규모화는 원자크기 간격에서 일어나는 양자역학적인 현상이 고전적인 device내에서 나타나기 마련임으로, 고전적인 device 안에서도 정보의 양자역학적인 성격을 이해하지 않을 수가 없게 되고 있다.

현재까지 quantum computation에 관한 연구활동의 초점은 quantum computation을 실현화하는데에 필요한 전산기를 개발시키는 것보다는 기본적인 과학이 무엇이나하는데에 있기 때문에 이 분야의 연구발전에 참석하는데에 적절한 계기라고 본다. 연구활동이 대단히 활발하고 또 과학공학정책기관, 연구재단, 새로운 기술사업체 및 국방 strategist들만 아니라 보통 시민들도 이 quantum computation에 특별한 관심을 보이고 있다. 대학원 수준 교재가 많이 나오게 되고 있으면 수많은 대학교에서 실험적인 특강이 활발히 운영되고 있다. Quantum computation을 중심으로 일어나는 여러 가지 많은 구상들과는 별도로, 이 움직임은 미시세계에서 나타나는 많은 현상의 양자역학적인 근본적인 성격에 대해서 연구와 토론을 자극하고 있다. 더 명확하고 간결한 이해가 나타나고 있다. 예를 들자면, quantum computation 연구의 추구는 전산의 기본양인 qubit의 성격을 정확하게 정의를 하고 그 정보의 안전성에 미치는 열역학적인 환경변천으로 일어나는 영향을 어떻게 극복하는가를 이해하여야한다. 거기에 따른 정보의 변화를, 소위 말하는 decoherence를, algorithm에서 어떻게 격리하느냐가 대단히 중요한 문제이다. Peter Shor가 factorization에 필요한 quantum computation algorithm을 제의했을 뿐만 아니라 이 decoherence 때문에 일어나는 오차를 교정하는 방법을 보였다는 점은 특별히 중요한 quantum computation을 향한 큰 발걸음이 된다.

Shor의 성공적인 quantum computation algorithm이 제시하는 약속은 바로 양자역학적인 정보의 구성이 둘이나 그 이상의 물체나 광자의 양자역학적인 상태를 기술하는 eigenfunction인데 그 eigenfunction이 quantum entanglement를 포함한다는 사실에 있다. 기본 qubit가 순수한 wavefunction이나 혹은 둘이나 그 이상의 구성단위의 wavefunction들이 선형으로 섞인 상태로 표현될 수도 있다. 중요한 것은 이 entangled state를 기술하는 wavefunction이다. 미묘한 점은 entangled wavefunction은 여러가지 물리현상을 이용하여 구축할 수 있지만 일단 작성된 후 그 내역이 어떤가를 발견하려면 그 wavefunction을 파괴해야하는데 있다. 이 성격이 양자역학적으로 구축된 정보를 안전하게 주고 받고 할 수 있게하는 근본적인 힘이다. 그 뿐만 아니라, entangled wavefunction을 구축할 때 두 기본 wavefunction의 비례를 다르게 할 수 있다. 이런 자유는 정보 qubit의 가능한 값을 둘보다 더 크게 할 수 있다는 말이고, 결국은 qubit의 dynamic range가 고전적인 digital bit보다 넓게 만들수 있다는 것이다.

연구의 여러 가지 바쁜 활동들은 대개 두 모음으로 나눌 수 있다. 첫째는 새로운 quantum computation algorithm을 구상해내는 이론적인 활동이고, 둘째는 현실적인 실험연구활동으로 qubit을 어떻게 구성하고 어떤 장소에 보관했다가 어떤 순간에 주어진 algorithm에 의하여 전산에 필요한 변환을 일으키게 하느냐 등의 활동이다. Shor의 algorithm은 큰 수의 factorization이 목적인데 그 외로 Shor의 quantum computation algorithm이 고전적인 algorithm보다 혁신적으로 더 빠르다는 점이 벌써 확인되어 있다. 사실상, 숫자가 커지면, 고전 algorithm이 곧 불가능해진다. 현재로는 factorization이 quantum computation의 단 하나의 가능한 예로 알고 있다. 이 분야에서 연구 중인 과학자들은 모든 고전 algorithm들을 양자화할 수 있다고는 생각하지 않는다. 그러나 지속되는 연구는 새로운 quantum algorithm으로 풀 수 있는 문제들을 많이 발견 출력 할 것으로 예상하고 있다.

Quantum computation을 실현화하기 위한 연구활동이 여러가지 다른 방향으로 진전되고 있다. Qubit을 구축하는 방법이 entangled photon을 쓰거나, 한 입자의 다른 spin의 값들로 구성하거나, 또는 함정에 구속된 한 입자의 운동 eigenstate가 entangled state를 정의할 수도 있다. 다른 방법들을 서열하면 아래와 같다

- NMR을 이용하는 quantum computation
- 함정에 구속된 이온을 이용한 quantum computation
- 이온화하지 않은 원자를 기본으로 한 quantum computation
- matter wave의 resonant cavity를 기본으로 한 quantum computation
- 광자를 이용한 quantum computation
- 고체상태에 존재하는 spin이나 quantum dot를 중심으로 한 quantum computation
- 초전도체를 기본으로 한 quantum computation
- 액체 helium에 떠 있는 전자나 spectral hole burning을 기초로 한 특출한 qubit을 쓰는 quantum computation

현재, 세계각지에서 추진되는 연구활동을 관찰하면서 미국을 중심으로 한 사립 group이 소위 DiVincenzo 시험방법으로 연구결과를 검토 분석하고 있다. 그 방법은 아래와

같은 관점으로 구성되고 있다.

- 가) 잘 이해가 된 qubit으로 구성된 물리조직체로서 더 확장할 가능성이 있는가
- 나) 필요한 qubit들을 복잡하지 않은 상태를 시발점으로 모을 수 있는가
- 다) Decoherence 시간이 logic gate를 동작하는데 필요한 시간보다 훨씬 더 긴가
- 라) 일반화된 quantum logic gate가 가능한가
- 마) 한 qubit을 개별적으로 분석하는 것이 가능한가
- 바) Qubit을 정착된 상태와 동작중 상태 사이에 왕복 변천시킬 수 있는가
- 사) Qubit을 한 장소에서 다른 장소로 예척할 수 있게 움직일 수 있나

마지막 두 시험방법은 quantum computer를 network화하는데 필요한 조건을 검토하는 것이 목적이다.

DiVincenzo criteria는 여러가지 병행하는 문제점을 검토하는데 초점이 있다. 예를 들어서, two-level qubit로 구성된 정보일 경우 decoherence 속도가 어떻게 다른지를 꼭 알아야 한다. 실제 qubit 수가 늘어날때 quantum computation 기구의 크기가 선형으로 늘어나야만 전산시설로 쓸 수 있다. 관련된 모든 qubit들이 지정된 장소에서 같은 시작 시간에 출발할 수 있어야 한다. 한 quantum logic operation에 필요한 시간이 그 정보를 decoherence 때문에 잃어버릴 시간보다 짧아야 된다. 한 번에 한가지 일반적인 quantum logic operation을 일어나도록 하는 절차가 확정되어야 한다. Quantum computation의 결과를 채취하는 방법이 확정되어야 한다. 그 결과는 어떤 지정된 quantum register에 축적할 수 있어야 한다. Quantum computation의 결과를 한 register에서 다른 register로 옮기려면 두가지 networking에 필요한 조건이 확인되어야 한다.

Quantum computation을 성공적으로 실현하는데에는 백퍼센트 확실한 광자나 전자를 한번에 하나씩 만들어내는 기구와 방법이 필요할 것이다. 광자나 전자는 물질의 표면을 극복하여 방출이 되는데 그 숫자는 stochastic하다. 한번에 둘이 배출이 되거나 하나도 방출이 되지 않는 것이 아니라 매번 꼭 하나의 광자나 전자를 방출하는 물리 방법이 quantum computation의 정확한 gate나 logic operation에 필요한 것이다. 이런 quantum computation을 가능하게 만들 수 있는 물리는 지적인 의미가 있고 수확이 가능한 지적 투자 분야라고 생각한다. 이런 기초적인 연구는 지식의 분야를 넓힐 뿐만 아니라 quantum computation을 움직이는 영향을 보장할 것으로 보인다. 성공적인 quantum computation은 이런 기본적인 연구지식을 다시 지양시킨 결과일 것 같다. 실험물리학적 진전이 발전에 결정적인 영향을 보낼 것으로 결론이 된다.