양자 정보 기술

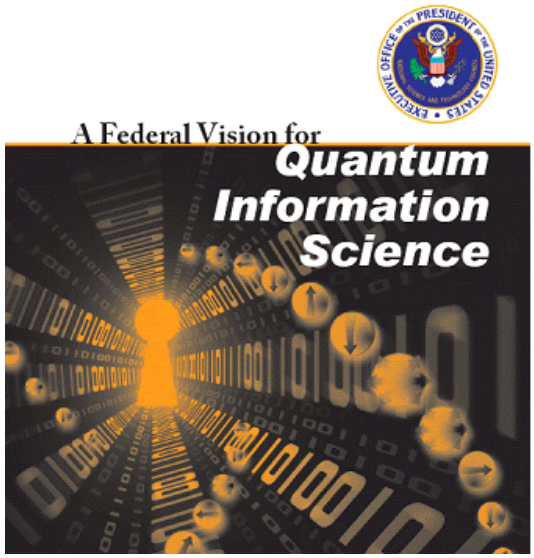
안 도 열

서울시립대학교
전자전기컴퓨터공학부

Ⅰ. 서 론

초연결 사회로의 진입과 함께 ICT 인프라에 대한 사회 의존도가 기하급수적으로 높아지면서, 퀀텀 테크놀로지로 대변되는 양자 정보 기술은 완벽한 보안, 천문학적인 정보 처리 속도의 향상 그리고 기존의 IT로는 불가능한 물질의 직접 전송 등을 가능하게 할, 미래 산업을 이끌 핵심 기술 중 하나로 각광받고 있다[1]. 비근한 예로 미국은 2008년 오바마 행정부에서 양자 정보 기술의 중요성을 인식하고, 연방정부 차원에서 국가적인 프로그램을 수립하여 연 10억 달러 이상을 R&D에 투자하고 있으며, 아시아의 경우, 일본, 중국, 싱가포르 등이 연 1천억 원 이상을 투자하고 있어, 양자 정보 기술은 미래 산업을 이끌 차세대 IT 기술의 화두로 전 세계적인 주목을 받고 있다[2]. 또한, 2012년도 노벨 물리학상은 양자 컴퓨터의 개발에 필요 불가결한 개별 양자계의 측정 및 조작을 가능하게 한 프랑스의 세르주 아로슈와 미국의 데이비드 와인렌드에게 돌아갔다. 노벨상이 양자 컴퓨팅 분야에 돌아간 것은 양자 컴퓨터와 양자 암호로 대변되는 양자 정보 통신 기술이 중요한 미래 기술임을 시사해 준다고 할 수 있다.

역사를 돌이켜 보면, 물리학의 혁명적인 진보는 새로운 공학 기술과 산업을 불러왔다. 17세기 뉴턴에 의해 정립된 중력과 역학 이론의 여파로 생겨난 기계공학과 산업혁명이 인류의 문명사에 큰 획을 그었다면, 19세기 말에 정립된 전자기학은 전기 문명으로 대변되는 오늘날의 IT 기술의 토대가 되었다. 전기가



[그림 1] 미국 오바마 행정부의 양자 정보 기술에 대한 연방정부 비전 보고서

없다면, 현재 우리들의 일상이 어떠할 지 생각해 보자. 조명은 물론이고, 컴퓨터와 스마트 폰도 존재하지 않을 것이다. 역사적인 관점에서 20세기에 정립된 양자 물리학이 차세대 기술과 산업의 요람이 될 것은 자명해 보인다.

미국의 저명한 매체 Market Research Media는 2015~2020년 사이의 양자 정보 통신 기술의 세계시장 규모를 260억 달러, 연 누적 성장률(CAGR)이 10.4%에 달하는 상당히 빠른 속도로 세계시장이 형성될 것으로 전망하고 있다. 따라서 퀀텀 기술의 시대에 여타 선진국에 비해 뒤떨어지지 않도록 R&D 능력의 조기 확보가 요구되고 있다.

이미 100 Mbps의 속도로 양자 암호 키를 100 km 전송할 수 있는 기술이 유럽, 일본, 중국 등에서 시현되었으며, 2011년 캐나다의 D-Wave 사는 미국의 대표적인 방위산업체인 록히드마틴사, 구글 및 미 항공우주국 등에 세계 최초의 상용 양자 컴퓨터를 판매하였다. 양자 컴퓨터의 천문학적인 연산 능력은 IT는 물론 국방, 제약 및 생명공학 등에 놀라운 파장을 불러일으킬 것으로 판단된다. 양자 물리학의 복사 불가능 원리를 이용한 양자 암호(QKD) 기술은 실용화 단계에 들어가고 있으며, 이 기술이 제공할 수 있는 완벽한 보안 가능성에 힘입어 오스트리아의 경우, 비엔나 정부가 적극적으로 연구를 지원하고 있으며, 중국은 2015년 서비스를 목표로 북경에서 상하이까지 양자 암호 네트워크를 구축하고 있다. 최근 미 항공우주국 NASA가 캐나다의 벤처회사인 D-Wave 사로부터 양자 컴퓨터를 1,500만 달러에 구매하여 세간의 화제가 되었다. D-Wave 사는 첫 번째 양자 컴퓨터를 미국의 록히드마틴사에 1,100만 달러에 판매한 바 있다. 2012년에는 하버드 대학의 연구팀이 슈퍼 컴퓨터로 수개월의 계산이 요구되는 20개의 아미노산으로 구성된 단백질 구조 해석 문제를, 양자 컴퓨터를 이용하여 실시간에 해결한 논문을 네이처지에 발표하여 양자 컴퓨터가 기존의 컴퓨터에 비해 천문학적인 연산 속도의 향상이 있었음을 보여주었다[3]. 이처럼 양자 컴퓨터는 기존의 컴퓨터로는 풀기 어려운 계산들을 매우 빠른 시간 내에 풀 수 있을 것으로 예측되고 있다. 많은 계산 과정을 필요로 하는 문제의 한 예로 소인수 분해 문제가 있다. 소인수 분해가 중요한 이유는 금융 보안 및 인터넷 등에 많이 쓰이고 있는 암호 체계가 바로 이 소인수 분해에 기초를 두고 있기 때문이다. 현재 잘 알려진 소인수 분해 알고리즘은 사용하는 비트 스트링의 개수에 대한 지수승의 연산과정을 필요로 한다. 예를 들면, 1994년 RSA129로 알려진 129비트의 암호를 소인수 분해하는 데에는 이 알고리즘을 이용하여 세계에 있는 1,600여 대의 워크스테이션을 병렬 연결하여 8개월이 걸렸다. 250비트라면, 800,000년이 걸릴 것이며, 1,000비트라면, 10^{25}년이 걸릴 것이다. 이것은 우주의 나이보다 더 긴 시간이다. 이러한 사실은 공개 키 방식의 암호화에 있어서 필수적이며, 현재 은행에서 이용하는 암호 코드는 약 250비트 스트링의 소인수 분해에 의존하고 있다. 반면에, 양자 컴퓨터에서 사용할 수 있는 소인수 분해 알고리즘의 경우는 오직 비트 스트링 비트 수의 다항식의 단계만을 필요로 하기 때문에 1,000비트 스트링조차도 충분히 빠른(Pentium PC 정도의 속도를 갖는) 퀀텀 컴퓨터가 존재한다면, 수 시간 내에 풀릴 수 있는 문제가 된다. 이것은 소인수 분해에 근거를 둔 공개 키 암호 시스템(public key crypto system)이 가까운 미래에 더 이상 유효하지 않을 수도 있음을 암시해 준다. 또, 다른 퀀텀 컴퓨팅의 장점으로 서치(search) 문제를 들 수 있다. 이미 구글사가 퀀텀 컴퓨터 연구에 막대한 자금을 투자하고 있다는 것은 주지의 사실이다.

Ⅱ. 본 론

통상적인 정보처리 과정이 비트 연산을 이용하는 반면, 양자 컴퓨터와 양자 정보 통신은 보다 근원적인 양자역학적인 비트인 큐빗(qubit)에 의한 연산을 필요로 한다. 양자 정보의 기본 단위가 되는 이들 큐빗은 광자의 경우, 편광 상태 전자의 경우는 스핀의 상태로 특징지어질 수 있다. 재미있는 점은 이러한 양자 상태는 행렬이라고 하는 아주 간단한 수학적 표현이 가능하다는 점이다. 대표적인 양자 상태인 광자의 편광 혹은 전자의 스핀은 2개의 상태만을 갖고 있어 2×1의 행렬로 표현이 가능하다. 다시 말해, 이들 양자 상태를 비트와 유사한 다음과 같은 행렬로 표현할 수 있다.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ 그리고 } |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \quad (1)$$

흔히 양자물리학에서는 캣 벡터(ket vector) 그리고 양자 정보 통신 기술에서는 큐빗(qubit)이라고 정의되는 행렬 $|0\rangle$과 $|1\rangle$이 정보의 기본 단위가 된다. 큐빗이 지금까지 사용되어오던 비트와 크게 다른 것은 $|0\rangle$과 $|1\rangle$의 중첩(Superposition)으로 표현되는 새로운 상태 즉,

$$|\Psi\rangle = c_0|0\rangle + c_1|1\rangle = \begin{pmatrix} c_0 \\ c_1 \end{pmatrix}, |c_0|^2 + |c_1|^2 = 1, \quad (2)$$

식 (2)로 정의되는 새로운 캣 벡터 상태 $|\Psi\rangle$가 가능하다는 점이다. 이때 $|\Psi\rangle$는 $|0\rangle$ 및 $|1\rangle$과는 구별되지만, $|0\rangle$의 특성도 그리고 $|1\rangle$의 특성도 갖고 있는 독특한 상태이다. 여기서 c_0 및 c_1은 복소수로 절대 값의 제곱이 주어진 양자 상태 $|\Psi\rangle$가 각각 $|0\rangle$ 및 $|1\rangle$ 상태에 있을 확률이 된다. 여기서 양자물리학이 고전물리학과 차별화 되는 두 번째 특징이 나타난다. 고전물리학은 입자 또는 계(system)의 특성을 무한한 정확도로 알 수 있다고 가정하고 있는 반면, 행렬로 표현되는 특성으로 인해 양자 물리학의 상태는 오로지 확률로만 나타내어질 수 있다. 원자 상태가 양자물리학에서는 중첩으로 표현이 가능하다는 증거는 1922년 독일의 실험물리학자인 오토 스턴(Otto Stern)과 발터 켈락(Walter Gelach)이 중성자 스핀에 자장을 인가하였을 때, 방출된 중성자가 입자 감지기(particle detector)를 통해 검출된 결과로 입증되었다. 바로 이 중첩이라는 수학적 표현이 양자 정보 통신의 핵심 원리 중의 하나라고 보아도 과장은 아니다. 이를 보기 위해서는 조금 더 수학적인 언어를 풀어 가야 한다. 통상적으로 하나의 비트로부터 00, 01, 10 그리고 11과 같은 두 개의 비트를 정의할 수 있음은 주지의 사실이다. 행렬의 경우는 텐서 곱셈(tensor product)이라는 형태로 다음과 같이 두 개의 큐빗을 정의할 수 있다.

$$|00\rangle = |0\rangle\otimes|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \; |01\rangle = |0\rangle\otimes|1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$
$$|10\rangle = |1\rangle\otimes|0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \; |11\rangle = |1\rangle\otimes|1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \quad (3)$$

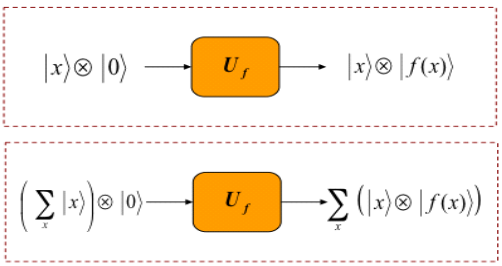
여기서 $\otimes$는 텐서 곱셈을 의미한다. 이상의 결과를 이용하여 다음과 같이 간단한 변환을 생각해 보자.

$$U_f(|x\rangle\otimes|0\rangle) = |x\rangle\otimes|f(x)\rangle. \quad (4)$$

여기서 U_f는 유니터리 변환(unitary transformation)이라고 불리는 양자 상태에 대한 양자물리학적인 변환으로 디지털 회로의 게이트와 유사한 역할을 수행한다. 양자 상태 $|x\rangle$는 $|0\rangle$ 또는 $|1\rangle$을 의미한다. 만약 양자 상태 $|x\rangle$가 중첩인 경우는 다음과 같이 쓸 수 있다.

$$\begin{aligned} &U_f((c_0|0\rangle + c_1|1\rangle)\otimes|0\rangle) \\ &= c_0 U_f(|0\rangle\otimes|0\rangle) + c_1 U_f(|1\rangle\otimes|0\rangle) \\ &= c_0|0\rangle\otimes|f(0)\rangle + c_1|1\rangle\otimes|f(1)\rangle. \end{aligned} \quad (5)$$

위의 결과를 도식적으로 나타내면 [그림 2]와 같다.

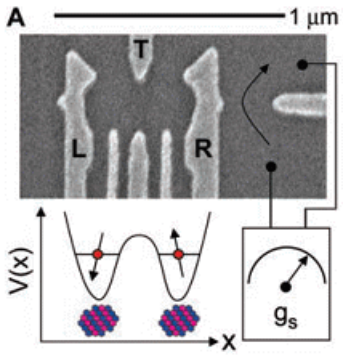


[그림 2] 텐서 곱셈으로 표현된 양자 상태의 유니터리 변환

위의 결과는 고전적인 정보처리 과정에서는 생길 수 없는 놀라운 결과를 제시한다. 임의의 양자 상태가 $|0\rangle$ 또는 $|1\rangle$처럼 2개의 기본 상태(base state)인 경우, 2개의 연산이 동시에 수행된다는 것이다. 만약 입력되는 양자 상태가 n 개의 기본 상태의 중첩으로 표현되는 경우는 n 개의 연산을 동시에 수행할 수 있다는 것으로 확장해서 해석을 할 수가 있다. 만약 입력 상태를 32개의 텐서 곱셈으로 표현할 수 있다면, 기본 상태는 $|000\cdots000\rangle$에서 $|111\cdots111\rangle$까지 모두 2^{32}개가 존재하므로, 이 경우에는 2^{32}개의 연산을 동시에 수행할 수가 있다. 2^{32}는 약 40억이므로 개당 1초가 걸리는 연산을 수행하려 한다면, 고전적인 컴퓨터로는 40억 초 다시 말해, 약 100년이 걸리는 연산을 양자 상태와 양자 상태의 유니터리 변환을 기본으로 하는 양자 컴퓨터는 불과 1초 만에 연산을 수행할 수 있을 것이다.

현재 양자 컴퓨터의 실용화를 위해 초기화가 가능하고, 양자역학적인 결맞음 상태가 오래 지속되며, 확장가능(scalable)한 큐빗의 구현을 위한 노력이 세계적인 프론티어 연구팀에 의해 수행 중이다. 지금까지 초전도 소자, 이온 트랩, 반도체 양자점, 고체 핵스핀 등 다양한 방법[2]에 의한 큐빗 구현 방법이 연구되고 있지만, 여기서는 필자가 주로 연구해온 반도체 소자를 이용하는 방법을 소개하려고 한다. 반도체 소자를 이용하는 방법은 그 확장 면에서 뿐만 아니라, 반도체 소자의 게이트에 가해지는 스위칭 전압에 의해 빠르게 큐빗을 제어할 수 있게 하기 때문에 매우 중요하다. 반도체 큐빗을 만들기 위한 방법의 하나로 반도체 양자점에 갇힌 전자를 이용하는 방법이 네덜란드 델프드대학의 쿠베노벤 교수, 하버드 대학의 마커스 교수 그리고 동경대학의 타루차 교수 등에 의해 개발되고 있다. 큐빗 구현을 위한 대표적인 양자점 양자 소자의 모양은 [그림 3]과 같다.

이런 구조에서 큐빗을 구현하는 방법은 두 가지가 있다. 하나는 전자가 왼쪽 양자 점에 있는가, 오른쪽



[그림 3] 게이트 제어 양자점 큐빗[4]

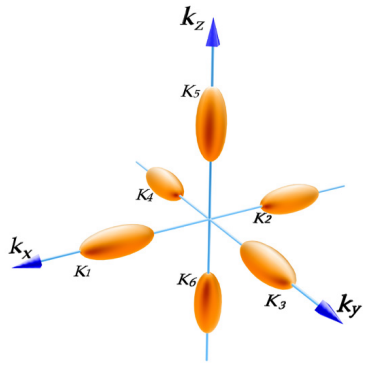
에 있는가에 따라, 즉 전하에 의한 큐빗을 정의하는 방법과 각 양자 점에 갇힌 전자의 스핀 방향을 이용하는 방법이 있다. 그러나 첫 번째 방법보다는 두 번째 방법으로 큐빗을 구현하려고 하는 노력이 주도적으로 이루어지고 있다. 이는 전자의 파동 함수는 전기적인 신호에 의해 제어는 용의하지만, 반면에 다른 외부 섭동에 대해 파동 함수가 취약하다는 약점을 가지고 있기 때문에 스핀보다 큐빗 상태의 유지가 용이하지 않기 때문이다.

필자는 스핀과 유사한 분극성을 갖는 실리콘 반도체 양자점의 intervalley 큐빗[5]을 제안하였으며, 이러한 intervalley 큐빗의 물리적 특성은 일본 NTT의 타카시나 박사팀에 의해 실험적으로 검증[6]이 된 바 있다.

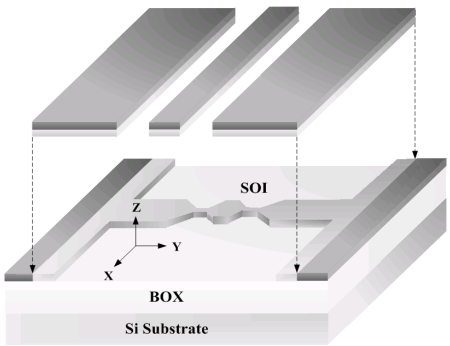
Si 양자점의 intervalley 큐빗은 스핀 큐빗과 전하 큐빗의 장점을 갖추고 있으며, 기 확보된 Si 반도체 공정을 활용할 수 있다는 장점이 있다.

[그림 5]는 필자가 미국 특허[7]를 등록 받은 intervalley 큐빗에 기초한 유니버설 양자 게이트인 CNOT (Controlled NOT) 게이트의 설계도이다. CNOT 게이트는 대표적인 두 개의 큐빗으로 구성된 유니버설 게이트로 퀀텀 프로세서의 기본 구성 요소가 된다.

또한, 호주의 시몬스 교수팀은 최근 Kane 모델에 기초한 impurity의 핵스핀 큐빗을 실험적으로 구현하는 데 성공하였다[8].

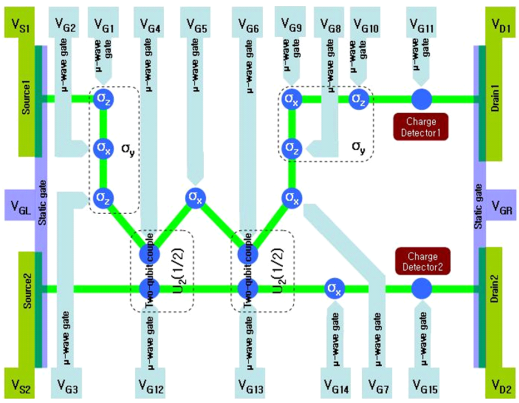


(a)



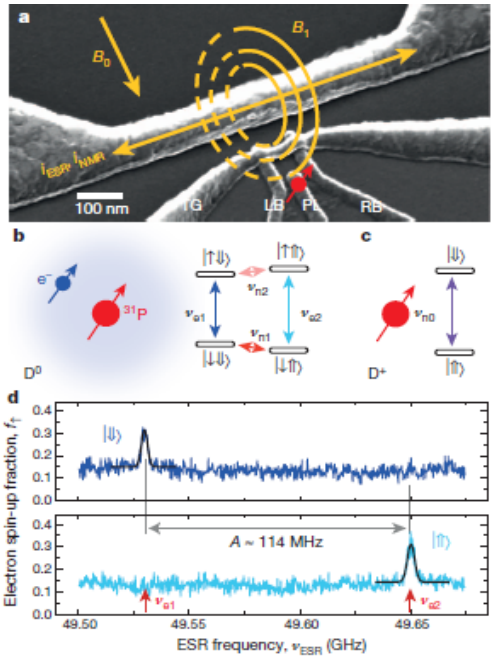
(b)

[그림 4] Si 양자점의 Intervalley state 큐빗[5]



[그림 5] Si 양자점의 Intervalley state 큐빗 CNOT 게이트

현재 반도체 큐빗에 대한 주요 연구 방향은 전술한 바와 같으며, 정보를 양자역학적으로 처리하는데



[그림 6] 고체 핵스핀 큐빗 및 제어[8]

있어서, 향후의 연구 방향 선정 시 양자 컴퓨터를 어떻게 하면 보다 쉽게 구현할 수 있는가에 대한 해답이 관건이 될 것이다.

양자 컴퓨터의 중요한 응용 분야의 하나로 신약 개발을 들 수 있다. 신약 개발에 있어 장애 요인 중 하나는 신약과 생체분자의 구조가 매우 복잡해, 분석이 매우 어렵고, 많은 시간이 걸린다는 점이다. 이 때문에 신약 개발은 장기적인 투자가 가능한 다국적기업의 전유물이 되어 있다. 삼성경제연구소의 2003년 자료에 의하면, 신약 개발에는 평균 8.8억 달러 이상이 소요되며, 이 중 후보 물질의 탐색 연구에 5년, 5.3억 달러가 투입되지만, 그나마 성공률이 0.02%에 불과하다고 발표한 바 있다. 서론에서 소개한 바와 같이 하버드 대학의 한 연구팀은 D-Wave 사의 양자 컴퓨터를 사용하여 20개의 아마노산으로 구성된 단백질의 폴딩 문제를 실시간 해석하는 데 성공하였고, 그 결과를 2012년 8월 네이처 자매지에 발표한 연구 성

과는 양자 컴퓨터를 이용한 양자 시뮬레이션이 향후 신약 개발에 핵심적인 기술의 하나가 될 것이라는 것을 시사해 준다. 그 외에도 물질의 직접 전송 같은 공상 과학 소설에나 나올 법한 장면도 양자 컴퓨팅을 이용하면 가능할 수 있는 미래 기술이다.

Ⅲ. 결 론

국내의 경우, 양자 컴퓨터 등 양자 정보 기술에 투입되는 절대적인 연구비 면에서 선진국에 비해 극히 영세성을 면치 못하고 있는 현실이나, 다행히 2012년 4월 (구)지식경제부는 양자 정보 통신 기술을 IT 미래 성장 동력 10대 기술과 3대 정책 목표에 포함시켜, 향후 우리나라가 퀀텀 테크놀로지에 매진할 수 있는 단초를 제공하였다. 19세기 말 산업혁명을 거친 국가가 세계를 지배하였듯이 미래는 퀀텀 테크놀로지를 확보한 국가와 기업에 의해 IT 기술뿐 아니라 신약 개발과 같은 생명과학 분야마저도 지배당하게 될 것이라고 필자는 생각한다.

참 고 문 헌

[1] http://qeurope.eu;QUIE2T

[2] 안도열, 양자정보통신의 기술동향 및 시장전망, 하얀출판, 2012년.

[3] A. Perdomo-Ortiz et al., "Finding low-energy conformations of lattice protein models by quantum annealing", *Scientific Report* 2, p. 571, 2012.

[4] R. Brunner et al., "Two-qubit gate of combined single-spin rotation and interdot spin exchange in a double quantum dot", *Phys. Rev. Lett.* p. 107, 146801, 2011.

[5] D. Ahn, "Intervalley interactions in Si quantum dots", *J. Appl. Phys.* p. 98, 033709, 2005.

[6] K. Takashina et al., "Valley polarization in Si(100) at zero magnetic field", *Phys. Rev. Lett.* 96, 236801, 2011.

[7] D. Ahn, "Universal quantum gate", US Patent 7,655, 850, 2010.

[8] M. Fuechsle et al, "A single-atom transistor", *Nature Nanotechnology* 7, p. 242, 2012.

≡ 필자소개 ≡

안 도 열

1983년 2월: 서울대학교 전자공학과 (공학사)

1985년 2월: 서울대학교 전자공학과 (공학석사)

1988년 10월: University of Illinois at Urbana-Champaign, 전기컴퓨터공학과 (공학박사)

2005년: IEEE 펠로우

2009년: 미국물리학회 (APS) 펠로우

2009년~현재: 서울시립대학교 전자전기컴퓨터공학부 석좌교수

[주 관심분야] 양자 정보 기술, 메타 물질 및 투명 망토, 광전자 소자