최신 ICT 이슈

I. 무어의 법칙 종언 이후, '양자 컴퓨팅'에 주목하는 반도체 업계

"DATE(Design, Automation & Test in Europe)"는 IC 설계 기술 등에 초점을 맞춘 유럽에서 개최되는 국제 학회임. 독일 드레스덴에서 개최된 DATE 18 행사는 최근 반도체 업계의 이슈에 큰 변화가 있음을 실감케 하는 자리였음. 지금까지 IC 설계 기술을 다루는 학회의 주제는 기본적으로 반도체의 미세화에 관한 것이었지만, '무어의 법칙' 종언이 눈앞에 다가오면서 미세화에 의존하지 않고 IC를 진화시키는 양자 컴퓨팅에 대한 관심이 급상승함에 따라 양자 컴퓨팅을 위한 IC 설계 기술의 R&D가 정식 의제로 등장하였음

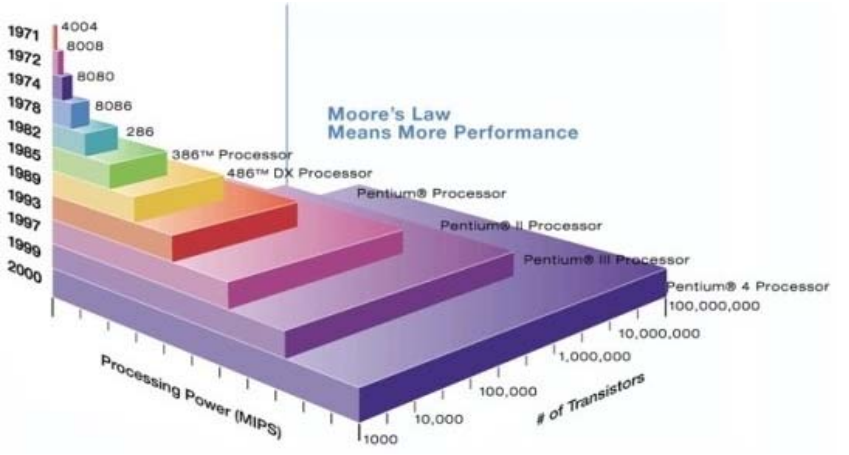
■ **지금까지 약 반세기 동안 IC(집적회로)의 진화는 기본적으로 미세화가 견인해 왔으며, 이 미세화에 의한 혜택을 누리기 위해 IC 설계 기술이 진전해 왔다고도 할 수 있음**

- IC 설계의 진전 방향은 크게 두 가지인데, 하나는 회로의 대규모화에 대한 대응이고 또 하나는 표면화되는 물리적 현상에 대한 대응임
- 전자는 높은 추상화 수준의 설계, 예를 들어 C 언어나 C++에서 IC를 설계하는 기술이며, 후자는 가령 미세화하지 않은 경우에는 보이지 않는 기생 용량(반도체 소자에서 부수적으로 생기는 정전 용량)과 기생 저항을 고려하기 위한 설계 기술임
- 진전을 계속해 온 설계 기술이 대상으로 하는 IC는 기본적으로 동일한 모습이었는데, 예를 들어 마이크로프로세서 및 마이크로컨트롤러(MCU는) 등 논리 IC는 논리 게이트로 구성되어 있음
- 논리 게이트는 하나 또는 그 이상의 입력을 받아 언제나 단 하나의 예측 가능한 출력을 산출하는 논리 회로로서 기존 컴퓨팅에서 '0'과 '1'의 값을 갖는 논리 비트를 연산하는 회로인데, 대표적으로 AND 게이트, NAND 게이트, OR 게이트 등이 있음

* 본 내용과 관련된 사항은 산업분석팀(☎ 042-612-8296)과 최신ICT동향 컬럼리스트 박종훈 집필위원(soma0722@naver.com ☎ 02-576-2600)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

■ **그러나 미세화가 종언을 고하면서, 기존 컴퓨팅에서 연산에 사용하는 논리 비트 수의 증가와 고속화도 거의 한계점에 다다르고 있음**

- 인텔 공동 창업자 고든 무어는 1965년에 자신의 이름을 따서 반도체 집적에 관한 방정식을 제창했으며, 이후 50년 가까이 반도체 업계를 설명해 온 법칙이 되었음
- 무어의 법칙은 생산되는 트랜지스터의 총량은 2년마다 2배로 증가한다는 것인데, 프로세서의 성능 향상과 생산비용의 개념을 연계한 것으로, 2배 많아진 트랜지스터를 생산하는데 소요되는 비용은 2년 전과 똑같이 유지됨을 의미함



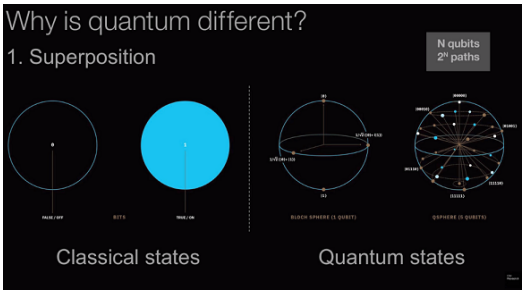
<자료> Intel

[그림 1] 무어의 법칙

- 무어의 법칙이 종말을 향해 가고 있다는 주장은 2011년 이론 물리학자 미치오 가쿠의 저서 "미래의 물리학"에서 제기되었음
- 가쿠 교수는 대안적인 반도체 집적 기술이 발견되지 않는다면 무어의 법칙은 2020년 이내에 자취를 감출 것이라는 예상을 내놓았는데, 실제 2013년에 AMD가 미세화에 실패하면서 큰 주목을 받기 시작하였음
- 이후 마이크로소프트 연구소가 "무어의 법칙에 관한 법칙"이 존재한다며, 무어의 법칙 종말을 예견하는 사람들의 숫자가 2년마다 2배로 증가한다고 있다고 말할 정도로 가쿠의 예언은 업계에서 사실로 받아들여지고 있음
- 무어의 법칙 종말은 아이러니하게도 반도체 집적이 놀라울 정도로 빠른 혁신을 지속적으로 이루어 냈기 때문으로, 일부 디바이스의 기능은 가장 기본적인 크기가 원자 단위로 너무 작고, 이는 많은 사람들이 무어의 법칙 종말에 동의하는 근거가 되고 있음

■ **무어의 법칙 종언은 자연스레 “차세대 컴퓨팅 기술은 무엇이 될 것인가”라는 화두와 연결되는데, 양자 컴퓨팅은 유력한 대안 중 하나로 수년 전부터 큰 주목을 끌고 있음**

- 가쿠 교수는 저서에서 무어의 법칙이 종말을 고한 후 차세대 컴퓨터 기술은 분자 트랜지스터와 양자 컴퓨터 등이 될 것이라는 전망을 내놓은 바 있음
- 양자 컴퓨팅은 양자 게이트라 불리는 회로가 양자 비트를 연산하는데, 양자 비트는 “중첩(관측될 때까지 0도 1도 아닌 중첩 상태에 있는 것)”과 “양자 얽힘(얽혀 있는 한 양자 비트의 상태가 다른 양자 비트의 상태에 영향을 주는 것)”의 성질이 있음



<자료> Towards Data Science

[그림 2] 양자 비트의 중첩(Superposition)

- 이러한 양자적 특성으로 인해 적은 양자 비트 수에서도 병렬도가 매우 높은 연산이 가능해지는 것으로 알려져 있으며, 이는 논리 비트 수의 증가나 고속화가 포화상태에 이른 가운데 양자 컴퓨팅이 주목받는 이유가 되고 있음
- 양자 컴퓨터는 여러 가지로 정의되고 있으며, 양자 게이트를 조합한 방식의 범용적인 양자 컴퓨터(양자 게이트식)와 조합 문제 해결 전용의 양자 컴퓨터(양자 어닐링식)의 두 종류로 구분하는 경우가 많음
- D-Wave를 비롯하여 상용화에 앞서 가고 있는 방식은 양자 어닐링식 양자 컴퓨터인데, 이는 풀고 싶은 문제를 이징 모델(Ising Model)에 떨어뜨리면 나머지는 컴퓨터가 최적의 솔루션(또는 가까운 솔루션)을 자동으로 도출하는 방식임
- 이징 모델은 통계역학에서 물질의 위상 전이(phase transition)와 임계 현상(critical phenomenon)을 기술하는 가장 간단한 모형을 말함
- 반면, 양자 게이트식 양자 컴퓨터는 현재 기존 컴퓨팅 설계 기술을 개발해온 연구자들이 더 많이 연구 대상으로 삼고 있는 방식임

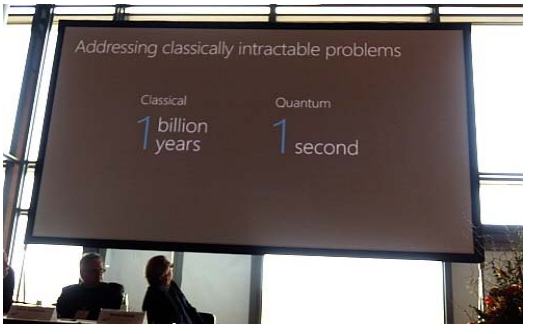
■ **지난 3월 독일 드레스덴에서 개최된 ‘DATE 18’ 컨퍼런스에서는 기존 컴퓨팅을 전제로 한 설계 기술 개발보다 양자 컴퓨팅을 위한 설계 기술 개발의 성과들이 소개되었음**

- 큐비트를 물리적으로 구현하는 기술은 여러 방식이 알려져 있지만, 실현할 수 있는 양자 비트 수가 아직 적어 이론이 아닌 현실에서 양자 컴퓨팅이 기존 컴퓨팅을 능가하려면 상당한 시간이 소요될 것으로 전망되고 있음

- 그렇지만 무어의 법칙의 종말이 바로 코앞에 다가오고 있는 가운데, 기존 컴퓨팅을 상정한 설계 기술의 연구 개발보다는 많은 수의 양자 비트가 실현된 미래를 전제로 한 양자 컴퓨팅을 위한 설계 기술 개발이 중요하다고 생각하는 연구자가 최근 급증하고 있음
- DATE(Design, Automation & Test in Europe, 유럽 설계자동화 및 테스트 학회)는 IC 설계 기술 관련 국제 컨퍼런스인데, 2018년에 열린 DATE 18 학회에서는 양자 컴퓨팅용 설계 기술을 개발해 온 연구자들의 활동성과가 발표되고 토론되었음
- 이는 현재의 한계에도 불구하고 양자 컴퓨팅에 대한 연구가 앞으로 더욱 활발히 전개될 것임을 시사하는 것이어서, 2018년 학회는 지금까지의 속도보다 그리고 예상 속도보다 훨씬 빠르게 양자 컴퓨팅의 발전이 전개될 수 있다는 기대감을 낳았음

■ **학회 첫날 경영자 세션에서는 향후 세계에 공헌할 기술의 하나로 양자 컴퓨팅이 소개되었는데 마이크로소프트 양자연구소가 양자 컴퓨팅의 잠재력을 강조하였음**

- 경영자 세션의 제목은 “How Electronics May Change Our Lives, and the World(전자가 인류의 삶과 세상을 어떻게 변화시킬 것인가”이었으며, 4가지 기술이 소개되었는데, 양자 컴퓨팅에 관한 토론은 마이크로소프트가 담당하였음
- MS 양자연구소의 양자 아키텍처와 연산 그룹(QuArC) 수석 연구원 마틴 로틀러는 양자 컴퓨팅의 잠재력을 호소했는데, 가령 2048 비트 RSA 암호를 해독하는데 기존 컴퓨팅은 10억 년이 걸리지만 양자 컴퓨팅으로는 1초에 가능함



<자료> xTech

[그림 3] 양자 컴퓨팅의 RSA 암호 해독 성능

- 그는 양자 컴퓨팅을 시험해 볼 수 있는 소프트웨어로 MS가 제공하는 “Microsoft Quantum Development Kit(양자 개발키트)”를 소개했는데, 양자 컴퓨팅용 알고리즘을 개발하는 GUI 환경과 개발된 알고리즘을 실행하는 양자 컴퓨팅 시뮬레이터 등으로 구성되며, 알고리즘의 기술은 MS가 개발한 양자 컴퓨팅용 언어인 ‘Q #’을 사용한다고 함

■ **MS는 또 다른 경영자 세션에서도 양자 컴퓨팅의 개요를 설명하며, 기존 가상통화의 근간 기술인 암호화가 깨질 수 있으며 양자 암호화로 방어할 수 있음을 설명하였음**

- 마틴 로틀러는 “양자 컴퓨팅을 위한 설계 자동화” 세션에도 등단하여 “Quantum algorithms: The Quest for scalable programming, synthesis, and test(양자 알고리즘: 확장 가능한 프로그래밍, 합성, 테스트를 위한 탐색)”를 주제로 강연하였음
- 그는 양자 컴퓨팅의 개요와 논리 게이트와 양자 게이트의 차이 등을 설명했으며, 큐비트를 실현하는 하드웨어 기술에는 여러 가지가 있고, 적절한 규모의 양자 컴퓨팅 실현을 통해 현재의 암호화 기술이 깨질 우려가 있음을 설명하였음
- 지금까지 다양한 양자 게이트가 제안되고 있지만, 로틀러에 따르면 “Clifford+T(클리포드+T)”라는 양자 게이트 세트가 만능 게이트 세트로 인식되고 있음
- “Clifford+T”에서 앞의 Clifford는 Hadamard(아다마르, 프랑스 수학자) 게이트와 위상 시프트 게이트, CNOT(Controlled NOT) 게이트의 집합을 의미하며, 뒤의 T는 T 게이트(π/8 게이트라고도 하며, 회전각이 π/4인 위상 시프트 게이트)를 나타낸다고 함
- ‘Clifford+T’ 게이트 세트를 만능이라고 하는 것은 임의의 양자 함수가 일정 이하의 에러율로 구현이 되도록 장애 허용 범위(fault tolerance)를 양자 계산에 결합할 수 있기 때문임
- 그러나 다른 3개의 양자 게이트(클리포드 게이트 세트)에 비해 T 게이트는 비용이 많이 들기 때문에 이를 줄이는 것이 필요하다고 함
- 이어 그는 양자 컴퓨터로 연산하는 연산 내용(양자 알고리즘)을 양자 게이트에 매핑하는 컴파일링(양자 컴파일러 처리)과 양자 컴퓨팅에서 발생하는 양자 오류(중첩 상태가 없어지는 것)의 수정 처리가 필요하다는 것 등을 설명하였음
- 이후 양자 연산 회로의 예를 소개하고, 양자 컴파일러에서 얻은 회로라 하더라도 기존 컴퓨팅과 마찬가지로 설계 검증이 필요하다는 것 등을 언급하였음
- MS의 뒤를 이어서는 스위스 ETHZ(에단 취리히)에서 개발한 오픈소스 양자 컴퓨팅을 위한 프레임워크 ‘ProjectQ’를 설명하였고, 스위스 EPFL(로잔 공대)은 독일 브레멘 대학이 개발한 양자 연산 회로 설계를 위한 오픈소스 툴킷인 ‘RevKit’을 설명하였음

<자료> xTech

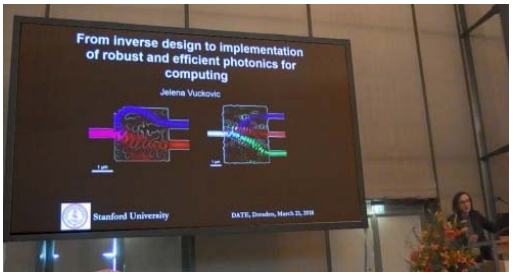
[그림 4] 양자컴퓨팅용 소프트웨어 프레임워크

■ **특별 세션의 주제는 “양자 컴퓨터의 검증”이었는데, 최근 학계와 산업계에서 양자 컴퓨팅의 진출이 시작되고 있으나, 설계와 검증 및 자동화에는 진전이 없었음이 지적되었음**

- 특별 세션의 제목은 “Theoretical and Practical Aspects of Verification of Quantum Computers (양자 컴퓨터 검증의 이론과 실제)”였는데, 세션 의장은 IBM과 이스라엘 Haifa(하이파)연구소가 맡았음
- 강연자들은 최근 양자 컴퓨팅의 긍정적 면은 학계와 산업계에서 양자 컴퓨팅의 진출이 시작되고 있다는 것으로, 양자 소자 등 하드웨어의 연구 개발 및 응용 분야의 개척에 의미 있는 진전이 있었다고 평가하였음
- 반면, 양자 컴퓨터의 설계와 검증, 그 자동화에 대해서는 별로 진전이 없었다고 평가하며, 설계・검증・자동화 기술 없이는 실제로 사용 가능한 양자 컴퓨터 시스템의 구축은 어렵다고 지적하였음
- 특히, 검증에 초점을 맞춰 논의가 전개되었는데, 가령 기존 컴퓨팅과 양자 컴퓨팅의 원리가 다르기 때문에 검증 방식에서도 차이가 있음을 지적하였음

■ **학회 중간에 열린 특별 기조 강연에서는 새로운 에너지 효율적인 컴퓨팅 회로 구현 기술을 양자 컴퓨팅에도 적용 가능하다는 의견이 소개되어 큰 관심을 끌었음**

- 기조 강연에 나선 스탠퍼드 대학의 옐레나 부코비치 교수는 에너지 효율이 높은 시스템온칩(SoC) 광컴퓨팅 회로의 구현 기술을 개발하였는데, 부코비치에 따르면 이 기술은 양자 컴퓨팅에도 적용이 가능함



<자료> Jelena Vuckovic

[그림 5] 에너지 효율적인 광 컴퓨팅 회로 기술

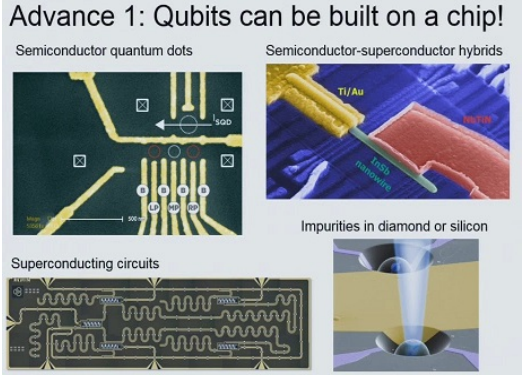
■ **DATE 18에서는 여느 학회와 마찬가지로 구두 발표로 이루어지는 일반 강연 이외에 포스터 발표도 많았는데, 많은 포스터 발표가 양자 컴퓨팅을 다루었음**

- 포스터 발표는 논문의 주요 내용을 포스터로 만들어 학회 장 곳곳에 붙이는 것인데, 관심을 모은 것 중 하나는 “Improved Synthesis of Clifford+T Quantum Functionality(클리포드+T 양자 기능성 합성의 개선)”이라는 포스터였음
- AI 관련 소프트웨어 연구소로는 세계 최대 규모를 자랑하는 독일 DFKI(German Research Center for Artificial Intelligence)를 비롯한 여러 대학이 공동 연구한 것으로, 발표자 명의는 DFKI의 필립 니만이었음

- 니만 교수의 연구 주제는 더 나은 클리포드+T 세트의 양자 회로 실현인데, 일반적으로 어떤 양자 연산을 실현하는 클리포드+T 세트의 양자 게이트 조합 방법은 다양하나, 앞서 언급한대로 T 게이트는 구현 비용이 다른 양자 게이트에 비해 높음
- T 게이트의 구현 비용 지표로는 T-count와 T-depth가 주로 사용되며, 전자는 양자 회로 전체에 포함되는 T 게이트의 개수, 후자는 T 게이트가 하나 이상인 회로 단락의 수를 의미함
- 니만 교수는 T 게이트의 구현 비용을 낮출 수 있도록 클리포드+T 세트 양자 게이트의 조합이 되도록 하는 컴파일 방법을 개발했으며, 그에 의하면, 종래에 비해 넓은 범위를 보고 대체하는 양자 게이트를 선택하면 비용을 줄일 수 있다고 함
- 포스터에는 기존 방법과 제안된 방법으로 컴파일 한 결과의 T-depth를 비교한 그래프가 게재되었으며 제안된 방법의 T-depth가 작아지는 것을 알 수 있었음

■ **DATE 18 학회는 IC 설계의 패러다임이 양자 컴퓨팅으로 전환할 수 있다는 것과 따라서 국내 기업들도 패러다임 전환에 대한 능동적 대처가 필요함을 시사하고 있음**

- 반도체 산업은 기술 혁신의 측면에서 두 가지 특징이 있는데, 하나는 산업 내에서 혁신이 지속되어 왔다는 것이고, 또 하나는 그 혁신의 패러다임이 동일했다는 점
- 그러나 이제 이러한 상황에 큰 변화가 일어나고 있으며, 무어의 법칙 종말은 이 변화가 돌이킬 수 없는 것임을 상징하고 있음
- DATE 18을 통해 이제 IC 설계의 기본 패러다임이 미세화가 아니라 양자 컴퓨팅이라는 관점에서 R&D가 진행될 것임을 시사하였음
- 이러한 변화는 현재 글로벌 반도체 산업의 주요 축을 구성하고 있는 우리나라 반도체 산업에도 향후 중대한 변화 동인이 발생할 수 있음을 의미하는 것임



<자료> ISSCC

[그림 6] 양자 컴퓨터를 위한 반도체 설계

- 국내 반도체 산업이 경쟁 우위를 지속적으로 확보하기 위해서는 양자 컴퓨팅, AI 등 새로운 기술에 대한 이해와 적극적인 연구개발 투자 및 협업 노력이 필요할 것임

[참고문헌]

[1] Forbes, “Adding A Little Quantum Computing To Your Business,” 2018. 4. 13.
[2] Digital Trends, “Computers can’t keep shrinking, but they’ll keep getting better. Here’s how,” 2018. 3. 17.
[3] DATE, “DATE 2018 in Dresden highlights: Future and Emerging Technologies and Designing Autonomous Systems,” 2018. 3. 6.
[4] xTech, “微細化から量子コンピューティングへ, IC設計技術のR&Dに地殻変動,” 2018. 4. 25.