Technical Assessment of the Feasibility and Implications of Quantum Computing

Committee

Mark A. Horowitz

Chair

Mark Horowitz (NAE), Chair, received his B.S. and M.S. in Electrical Engineering from MIT in 1978, and his Ph.D. from Stanford in 1984. Since 1984 he has been a professor at Stanford working in the area of digital integrated circuit design. While at Stanford he has led a number of processor designs including: MIPS-X, one of the first processors to include an on-chip instruction cache; Torch, a statically-scheduled, superscalar processor; Flash, a flexible DSM machine; and Smash, a reconfigurable polymorphic manycore processor. He has also worked in a number of other chip design areas including high-speed memory design, high-bandwidth interfaces, and fast floating point. His early work focused on designing high-performance digital systems by combining work in computer-aided design tools, circuit design, and system architecture. His current research interests are quite broad and span using EE and CS analysis methods to problems in molecular biology to creating new design methodologies for analog and digital VLSI circuits. He has worked on many processor designs, from early RISC chips, to creating some of the first distributed shared memory multiprocessors, and is currently working on on-chip multiprocessor designs. Recently he has worked on a number of problems in computational photography. In 1990, he took leave from Stanford to help start Rambus Inc., a company designing high-bandwidth memory interface technology, and has continued work in high-speed I/O at Stanford. His current research includes updating both analog and digital design methods, low energy multiprocessor designs, computational photography, and applying engineering to biology.

Alán Aspuru-Guzik

Member

Alan Aspuru-Guzik is currently a Canada 150 Research Chair in Quantum Chemistry and Professor of Chemistry and Computer Science at the University of Toronto. He is also a Faculty Member of the Vector Institute for Artificial Intelligence and CIFAR Senior Fellow. Alán was a Professor of Chemistry and Chemical Biology at Harvard University, where he started his independent career in 2006 and promoted to Associate Professor in 2010 and Full Professor from 2013 to 2018. Alán received his undergraduate degree in Chemistry from the National Autonomous University of Mexico (UNAM) in 1999. He received the Gabino Barreda Medal from UNAM, which prizes the top achiever in each field of study. After receiving his Ph.D. in Physical Chemistry from the University of California, Berkeley in 2004, under Professor William A. Lester, Jr., he was a postdoctoral scholar in the group of Martin Head-Gordon at UC Berkeley from 2005-2006. Professor Aspuru-Guzik carries out research at the interface of computer science, physics, and chemistry. In particular, he has pioneered the interface of quantum information and chemistry, with special focus on early applications of quantum computers such as dedicated quantum simulators for chemical systems. Aspuru-Guzik carries out research on materials acceleration platforms (MAPs) which integrate artificial intelligence, high-throughput quantum chemical screening and robotics to accelerate materials discovery. Applications include organic semiconductors, photovoltaics, organic batteries and organic light-emitting diodes. In 2009, Professor Aspuru-Guzik received the DARPA Young Faculty Award, the Camille and Henry Dreyfus Teacher-Scholar award and the Sloan Research Fellowship. In 2010, he received the Everett-Mendelsohn Graduate Mentoring Award and received the HP Outstanding Junior Faculty award by the Computers in Chemistry division of the American Chemical Society. In the same year, he was selected as a Top Innovator Under 35 by the Massachusetts Institute of Technology Review magazine. In 2012, he was elected as a fellow of the American Physical Society, and in 2013, he received the ACS Early Career Award in Theoretical Chemistry. He is associate editor of the journal Chemical Science.

David D. Awschalom

Member

David Awschalom (NAE, NAS) is Liew Family Professor in Spintronics and Quantum Information and Deputy Director at the Institute for Molecular Engineering at the University of Chicago. He was a Research Staff member and Manager of the Nonequilibrium Physics Department at the IBM Watson Research Center in Yorktown Heights, New York. In 1991 he joined the University of California-Santa Barbara as a Professor of Physics, and in 2001 was additionally appointed as a Professor of Electrical and Computer Engineering. Prior to joining IME, he served as the Peter J. Clarke Professor and Director of the California NanoSystems Institute, and Director of the Center for Spintronics and Quantum Computation. Professor Awschalom received the American Physical Society Oliver E. Buckley Prize and Julius Edgar Lilienfeld Prize, the European Physical Society Europhysics Prize, the Materials Research Society David Turnbull Award and Outstanding Investigator Prize, the AAAS Newcomb Cleveland Prize, the International Magnetism Prize and the Néel Medal from the International Union of Pure and Applied Physics, and an IBM Outstanding Innovation Award. He is a member of the American Academy of Arts and Sciences, the National Academy of Sciences, the National Academy of Engineering, and the European Academy of Sciences. Dr. Awschalom received his B.Sc. in physics from the University of Illinois at Urbana-Champaign, and his Ph.D. in experimental physics from Cornell University.

Robert Blakley

Member

Robert Blakley is Global Director of Information Security Innovation at Citigroup. He recently served as Plenary chair of the NSTIC Identity Ecosystem Steering Group and as Research and Development Co-Chair of FSSCC – the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security. He is currently a member of the Forum on Cyber Resilience – a National Academies Roundtable. Prior to joining Citigroup, Bob was Distinguished Analyst and Agenda Manager for Identity and Privacy at Gartner and Burton group. Before that, he was Chief Scientist for Security and Privacy at IBM. He is past general chair of the IEEE Security and Privacy Symposium and the ACSA New Security Paradigms workshop. He was awarded ACSAC's Distinguished Security Practitioner award in 2002, and is a frequent speaker at information security and computer industry events. Bob was general editor of the OMG CORBASecurity specification and the OASIS SAML specification, and is the author of "CORBASecurity: An Introduction to Safe Computing with Objects", published by Addison-Wesley. He was the first chair of the OATH Joint Coordinating Committee. He also participated in the National Academy of Science's panels “Authentication Technologies and Their Privacy Implications” and “Whither Biometrics”. Bob holds twenty patents in cryptography and information security, and he publishes regularly in the academic literature on information security and privacy. Bob received the A.B. in Classics from Princeton University, and the M.S. and Ph.D. in Computer and Communications Science from the University of Michigan.

Dan Boneh

Member

Dan Boneh (NAE) is a professor of computer science and heads the applied cryptography group at Stanford University, where he has been on the faculty since 1997. Boneh's research focuses on applications of cryptography to computer security. His work includes cryptosystems with novel properties, web security, security for mobile devices, digital copyright protection, and cryptanalysis. He is the author of over a hundred publications in the field and a recipient of the Packard Award, the Alfred P. Sloan Award, and the RSA award in mathematics. Last year Boneh received the Ishii award for industry education innovation. Professor Boneh received his Ph.D in computer science from Princeton University.

Susan N. Coppersmith

Member

Susan Coppersmith (NAS) is the Robert E. Fassnacht and a Vilas Professor of Physics at the University of Wisconsin, Madison. She is a theoretical condensed matter physicist who has worked on a broad range of problems in the area of complex systems, and has made substantial contributions to the understanding of subjects including glasses, granular materials, the nonlinear dynamics of magnetic flux lattices in type-II superconductors, and quantum computing. Dr. Coppersmith has served as Chair of the UW-Madison physics department, as a member of the NORDITA advisory board, as a member of the Mathematical and Physical Science Advisory Committee of the National Science Foundation, and as a Trustee at the Aspen Center for Physics. She has served as Chair of the Division of Condensed Matter Physics of the American Physical Society, Chair of the Section on Physics of the American Association for the Advancement of Science, Chair of the Board of Trustees of the Gordon Research Conferences, and Chair of the External Advisory Board of the Kavli Institute for Theoretical Physics at the University of California, Santa Barbara. Dr. Coppersmith is a fellow of the American Physical Society, the American Association for the Advancement of Science, and the American Academy of Arts and Sciences, and is a member of the National Academy of Sciences. Dr. Coppersmith received her Ph.D in physics from Cornell University.

Jungsang Kim

Member

Jungsang Kim is a Professor of Electrical and Computer Engineering, Physics, and Computer Science at Duke University. He leads the Multifunctional Integrated Systems Technology group there, focusing on construction of advanced information processing systems based on novel physical principles, design concepts and devices. His main area of current research is quantum information sciences, where his group uses trapped atomic ions and a range of photonics technologies in an effort to construct a scalable quantum information processors and quantum communication networks. His research concentrates on introduction of new technologies, such as micro fabricated ion traps, optical micro-electromechanical systems, advanced single photon detectors, compact cryogenics and vacuum technologies, towards a functional integration of quantum information processing systems. Dr. Kim received his Ph.D in physics from Stanford University, and served as a Technical Manager at Bell Laboratories in Murray Hill, NJ before joining Duke University in 2004.

John Martinis

Member

John M. Martinis is a professor of Physics at University of California, Santa Barbara and works with Google to build Quantum Computers. Dr. Martinis’s thesis was a pioneering demonstration of quantum-bit states in superconductors. After completing a post-doctoral position at the Commisiariat Energie Atomic in Saclay, France, he joined the Electromagnetic Technology division at NIST in Boulder. At NIST he developed a new fundamental electrical standard based on counting electrons, and invented microcalorimeters based on superconducting sensors for x-ray microanalysis and astrophysics measurements. In 2004 he moved to the University of California, Santa Barbara where he currently holds the Worster Chair in experimental physics. At UCSB, he has continued work on quantum computation, demonstrating a variety of new quantum devices and capabilities. Along with Andrew Cleland, he was awarded in 2010 the AAAS science breakthrough of the year for an experiment showing the first quantum behavior of a mechanical oscillator. In 2014 he was awarded the London Prize for low-temperature physics research. In 2014 he joined the Google quantum-AI team, and now heads an effort to build the first practical quantum computer. Dr. Martinis attended the University of California at Berkeley from 1976 to 1987, where he received two degrees in Physics: B.S. (1980) and Ph.D. (1987).

Margaret Martonosi

Member

Margaret Martonosi is the Hugh Trumbull Adams '35 Professor of Computer Science at Princeton University, where she has been on the faculty since 1994. She also holds an affiliated faculty appointment in Princeton Electrical Engineering. From 2005-2007, she served as Associate Dean for Academic Affairs for the Princeton University School of Engineering and Applied Science. In 2011, she served as Acting Director of Princeton's Center for Information Technology Policy (CITP). During the 2015-16 academic year, she served as a Jefferson Science Fellow within the U.S. Department of State. Martonosi's research interests are in computer architecture and mobile computing, with particular focus on power-efficient systems. Her work has included the development of the Wattch power modeling tool and the Princeton ZebraNet mobile sensor network project for the design and real-world deployment of zebra tracking collars in Kenya. Her current research focuses on hardware-software interface approaches to manage heterogeneous parallelism and power-performance tradeoffs in systems ranging from smartphones to chip multiprocessors to large-scale data centers. Martonosi is a Fellow of both IEEE and ACM. Martonosi is an author of the three papers that have the highest citation counts in the history of three different major conferences: ISCA, ASPLOS, and HPCA (according to Microsoft Academic Search data from 2015). In addition to many archival publications, Martonosi is an inventor on seven granted US patents, and has co-authored two technical reference books on power-aware computer architecture. She serves on the Board of Directors of the Computing Research Association (CRA), and is an emeritus member of CRA-W. Dr. Martonosi completed her Ph.D. at Stanford University, and also holds an M.S. from Stanford and a B.S. from Cornell University, all in Electrical Engineering.

Michele Mosca

Member

Michele Mosca is co-founder of the Institute for Quantum Computing at the University of Waterloo, a Professor in the Department of Combinatorics & Optimization of the Faculty of Mathematics, and a founding member of Waterloo's Perimeter Institute for Theoretical Physics. He is the co-founder and Director of CryptoWorks21, an NSERC-funded training program in quantum-safe cryptography. He co-founded the ETSI-IQC workshop series in Quantum-Safe Cryptography which brings together a broad range of stakeholders working toward globally standardized quantum-safe cryptography. He co-founded evolutionQ Inc. in order to support organizations as they evolve their quantum-vulnerable systems and practices to quantum-safe ones. He obtained his doctorate in Mathematics in 1999 from the University of Oxford on the topic of Quantum Computer Algorithms. His research interests include quantum computation and cryptographic tools that will be safe against quantum technologies. He is globally recognized for his drive to help academia, industry and government prepare our cyber systems to be safe in an era with quantum computers. Dr. Mosca's work is published widely in top journals, and he co-authored the respected textbook "An Introduction to Quantum Computing" (OUP). Dr. Mosca has won numerous academic awards and honours, including 2010 Canada's Top 40 Under 40, the Premier's Research Excellence Award (2000-2005), Fellow of the Canadian Institute for Advanced Research (CIFAR) since 2010, Canada Research Chair in Quantum Computation (2002-2012), University Research Chair at the University of Waterloo (2012-present), and Queen Elizabeth II Diamond Jubilee Medal (2013).

William Oliver

Member

William D. Oliver is a Laboratory Fellow at MIT Lincoln Laboratory, Professor of the Practice in the MIT Physics Department, and Associate Director of the MIT Research Laboratory of Electronics. He is a Principal Investigator in the Quantum Information and Integrated Nanosystems Group (MIT Lincoln Laboratory) and the Engineering Quantum Systems Group (MIT campus), where he provides programmatic and technical leadership for programs related to the development of quantum and classical high-performance computing technologies for quantum information science applications. His interests include the materials growth, fabrication, design, and measurement of superconducting qubits, as well as the development of cryogenic packaging and control electronics involving cryogenic CMOS and single-flux quantum digital logic. Dr. Oliver received his Ph.D from Stanford University in Electrical Engineering.

Krysta M. Svore

Member

Krysta Svore is a Principal Research Manager at Microsoft Research in Redmond, Washington, where she leads the Quantum Architectures and Computation group. Svore's research includes the development and implementation of quantum algorithms, including the design of a software architecture for translating a high-level quantum program into a low-level, device-specific quantum implementation, and the study of quantum error correction codes to enable fault tolerance and scalability. She has also developed machine-learning methods for web applications, including ranking, classification, and summarization algorithms. Dr. Svore received an ACM Best of 2013 Notable Article award. In 2010, she was a member of the winning team of the Yahoo! Learning to Rank Challenge. She is a Senior Member of the Association for Computing Machinery (ACM), serves as a representative for the Academic Alliance of the National Center for Women and Information Technology (NCWIT), and is an active member of the American Physical Society (APS). She currently serves as Chair of the Steering Committee for the Quantum Information Processing (QIP) Conference. She received her Ph.D. in Computer Science with highest distinction from Columbia University in 2006 and her B.A. from Princeton University in Mathematics and French in 2001.

Umesh V. Vazirani

Member

Umesh Virkumar Vazirani is the Roger A. Strauch Professor of Electrical Engineering and Computer Science at the University of California, Berkeley, and the director of the Berkeley Quantum Computation Center. His research interests lie primarily in quantum computing. He is also the author of a textbook on algorithms. Vazirani is one of the founders of the field of quantum computing. His 1993 paper with his student Ethan Bernstein on quantum complexity theory defined a model of quantum Turing machines which was amenable to complexity based analysis. This paper also gave an algorithm for the quantum Fourier transform, which was then used by Peter Shor within a year in his celebrated quantum algorithm for factoring integers. Dr. Vaziriani received his Ph.D. in computer science from the University of California, Berkeley.