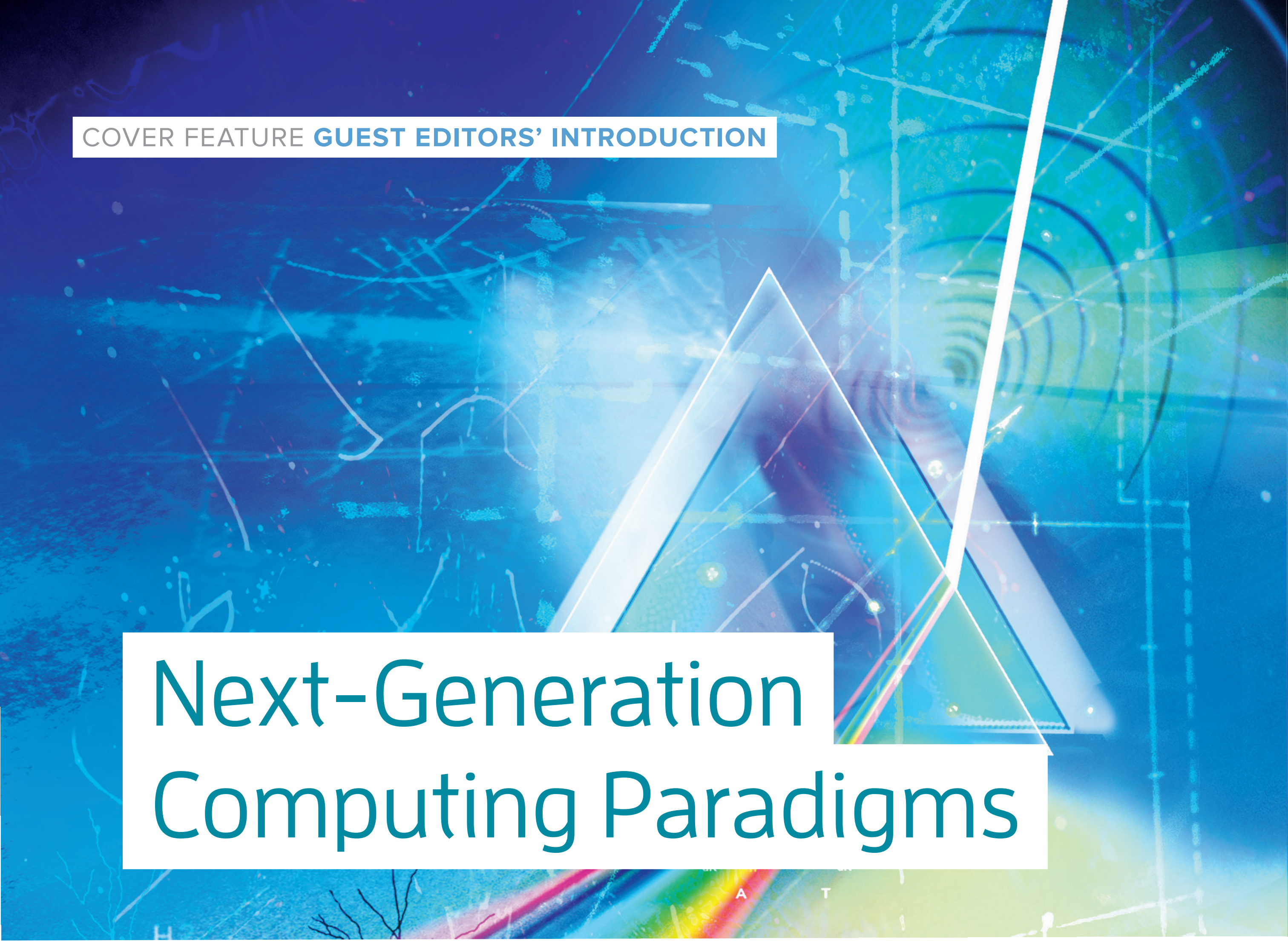

COVER FEATURE **GUEST EDITORS' INTRODUCTION**

Next-Generation Computing Paradigms

San Murugesan, BRITE Professional Services and Western Sydney University

Bob Colwell, R&E Colwell & Assocates

Faced with challenging new applications for computing, we must pursue radical new paradigms. Through quantum computing, biologically inspired computing, and nanocomputing, we can explore novel ways to transform life for the benefit of society.

As computers have evolved to redefine and transform almost every area of our lives in the past 50 years, they still function on the same fundamental computational concepts envisaged by Alan Turing and John von Neumann at the very beginning. As demands on computing, storage, and communication continue to escalate, digital computers based on silicon and conventional architecture approach their fundamental physical limits and face issues related to economics and reliability. Thus, certain kinds of problems in domains such as weather forecasting, bioinformatics, robotics, and autonomous systems are faced with limitations tied to the conventional computing paradigm.

Do these fundamental principles and assumptions that have shaped current conventional computing require revolutionary rethinking? Do we need to explore and harness new computing paradigms to address unresolved and as yet unforeseen challenges? The answer of course is "yes," and the journey to redefine computing and to search for next-generation computing paradigms has begun.[1–4]

0018-9162/16/$33.00 © 2016 IEEE

THE JOURNEY TO REDEFINE COMPUTING AND TO SEARCH FOR NEXT-GENERATION COMPUTING PARADIGMS HAS BEGUN.

See **www.computer.org/computer-multimedia** for multimedia content related to this article.

Research and industry are exploring radical new computing paradigms[3] such as quantum computing, biologically inspired computing, nanocomputing, and optical computing—all of which have the potential to bring about a variety of challenging new applications. Understanding, mastering, and applying these kinds of emerging, innovative approaches will empower us to chart the future course of computing. This special issue explores the principles of and potential for some of these paradigms and examines their current status and future prospects. We hope to inspire further study and implementation along these directions.

IN THIS ISSUE

The five feature articles in this issue explore quantum computing, molecular computing, nature-inspired algorithms, and synergistic human–machine interaction through cortically coupled computing. These approaches help us in our quest to address current and future computing challenges through innovation. In addition, two experts offer their insights on next-generation computing and how quantum computing will impact information security (see the "Perspective: Next-Generation Computing Paradigms and the Information Revolution" and "Perspective: How Quantum Technology Will Impact Security" sidebars). Furthermore, to help readers quickly gain a better understanding of some of these new paradigms, we put together a video album to accompany this issue (www.computer.org/web/computer-multimedia).

Quantum Computing Advances

Computational problems that are out of reach of current classical computers can in some cases be solved through devices that use the quantum mechanical properties of superposition and entanglement. This approach enables us to design devices with capabilities that exceed those of any classical computer. Recently, quantum devices and quantum techniques have attracted significant interest from researchers and industry. Quantum technologies for creating random numbers and securely encrypting communication are in fact already commercially available.

In "The Quantum Future of Computation," Krysta M. Svore and Matthias Troyer describe the principles of quantum bits, gates, and algorithms. The authors also outline the use of a quantum computer as a special-purpose coprocessor; highlight the use of quantum algorithms in a range of applications, such as cryptography, privacy, and search; and propose a software stack for quantum computing.

In "The Path to Scalable Distributed Quantum Computing," Rodney Van Meter and Simon J. Devitt present architectural models for large-scale quantum computation. They describe the classical resources needed to operate a large-scale quantum computer and explore experimental progress in a variety of different systems that support construction of a scalable quantum computer.

Molecular Computing

The quest for radical new algorithms and physical implementation to solve computational challenges better, cheaper, and faster than conventional computers has led to some research in molecular computing. This methodology has the potential to transform conventional computation by addressing such things as information density, parallelism, and energy efficiency.

In "Embodied Molecular Computation: Potential and Challenges," Victoria Coleman describes a type of computer in which living cells can be "programmed" by biological modification to perform computational tasks. In embodied molecular computing, computation is carried out via biological systems including the use of cellular materials such as DNA molecules. This article not only describes embodied molecular computing principles and potential, but also outlines challenges associated with building and using a universal molecular computer.

Inspiration for Computing from Nature

Nature inspires all kinds of ingenious problem-solving and optimization strategies. In fact, nature-inspired algorithms are particularly well suited

PERSPECTIVE: NEXT-GENERATION COMPUTING PARADIGMS AND THE INFORMATION REVOLUTION

Erik DeBenedictis, Sandia National Laboratories

New computing paradigms could drive the information revolution to completion. Society had defined "computing" based on the contributions of Alan Turing, John von Neumann, and Gordon Moore. Turing showed how to describe the solution to any computable problem in what is essentially a C program. Von Neumann architected a computer for running the program, and Moore described how semiconductor scaling would make the computers grow exponentially more capable over time.

Belief in Moore's law suppressed work on alternative paradigms. If semiconductor improvements would speed up the solution of any computable problem exponentially, what more could we want? I recall people seeking funding for a new computer architecture years ago, claiming it would be ten times as efficient as a microprocessor. The counter argument was "let's do nothing for four years and then buy a regular computer, which will be ten times faster due to Moore's law."

Nevertheless, the traditional computing paradigm has several major limitations that even Moore's law does not address:

- While a computer may require infinite memory for some problems, real computers have only finite memory.
- A computer will not do anything at all until a human programs it.
- A computer may run forever and still not solve some problems, like factoring a large number.
- Gordon Moore only projected exponential growth through 1975.

So, it is now appropriate to shift our attention to addressing these limitations by other means, such as biological computing, human–computer teaming, and quantum computing.

BIOLOGICAL COMPUTING

Some biologically inspired computing approaches have a remedy to the problem of a computer running out of memory. Some algorithms really do need a lot of memory, but a von Neumann computer is unable to increase its own memory because it does not have the ability to fabricate memory by itself. However, a biological cell can be modified to perform computing without necessarily shutting off the cell's reproductive capability. This makes a cell equivalent to both a computer and a memory fabrication facility. A cluster of cells that is too small for a particular computation can grow bigger without human help.

HUMAN–COMPUTER TEAMING

Computing today is the result of teamwork between the programmer and the hardware, but the nature of the teaming can change. In recent deep learning breakthroughs, humans architected a program's structure and the computer did a very large amount of simple programming within that structure.[1] Also, advances in human–computer interfaces enable a new type of team at runtime. This could lead to future human–computer partnerships with the computational throughput of a computer and the problem-solving ability (programming), motivation, and intuition of humans.

QUANTUM COMPUTATION

Some problems demand really long run times when run on traditional computers. According to computational complexity theory, a program to solve a problem of size N, such as having N-bits of input data, is "tractable" only if the number of steps in a solution is polynomial in N or less. If the number of steps is larger, such as exponential in N, even the exponential scaling of Moore's law could be insufficient.

Quantum computers address this limitation. As an example, consider factoring the number N. The best nonquantum algorithm for factorization is the number field sieve, where the number of steps is on the order of $\exp(1.52\ (\log N)^{1/3}\ (\log \log N)^{2/3})$ operations. The expression is complicated, but the initial exponential function indicates it is of greater than polynomial order. Factoring is thus called "intractable." However, the running time of the best quantum algorithm is only of the order of $(\log N)^2\ (\log \log N)\ (\log \log \log N)$ quantum operations, which is within polynomial range. For values of N typical in cryptanalysis, the first expression represents elapsed time greater than the age of the universe, whereas the second one is reasonable.

LOOKING AHEAD

There is apparent interest in continuing the information revolution and resulting economic expansion. The initial technological driver was the implicit extension of Moore's projection of exponential growth from ten years to forever. Although the original projection has reached it limits, new models of computers and computation, including those in this special issue, could be realistic and practical alternatives for driving the information revolution further and in ways unimaginable so far.

Reference

1. E.P. DeBenedictis, "Rebooting Computers as Learning Machines," *Computer*, vol. 49, no. 6, 2016, pp. 84–87.

ERIK P. DEBENEDICTIS is a technical staff member in the Non-Conventional Computing Technologies Department at Sandia National Laboratories. Contact him at epdeben@sandia.gov.

for a certain class of applications—optimization, machine learning, and multi-objective and highly complex design problems.

In "From Swarm Intelligence to Metaheuristics: Nature-Inspired Optimization Algorithms," Xin-She Yang, Suash Deb, Simon Fong, Xingshi He, and Yu-Xin Zhao describe recent developments in nature-derived algorithms and give an overview of those derived from species-based behaviors. To solve a diverse range of real-world application-based problems, they urge continuing research in a few specific areas to advance this area further.

Synergetic Human–Machine Interaction and Teamwork

How humans and machines interact and collaborate is poised for radical improvement. In "Cortically Coupled Computing: A New Paradigm for Synergistic Human–Machine Interaction," Sameer Saproo, Josef Faller, Victor Shih, Paul Sajda, Nicholas R. Waytowich, Addison Bohannon, Vernon J. Lawhern, Brent J. Lance, and David Jangraw postulate that as machine intelligence approaches the general effectiveness of human intelligence, the need for explicit programming of machines by humans will be disrupted. Through examples of real systems, the authors explain the concept of cortically coupled computing—that is, both human and machine are actively involved in performing computational tasks in which communication is enabled through brain–computer interfaces (BCIs). Such systems use brain-derived information

PERSPECTIVE: HOW QUANTUM TECHNOLOGY WILL IMPACT SECURITY

Jane Melia, QuintessenceLabs

The conversation around quantum technologies tends to focus for a large part on quantum computers and their capabilities, as well as on the threat they pose to our current cybersecurity infrastructure. What is less well known is that quantum technologies also present a security solution—they hold tremendous promise for protecting the most sensitive data.

THE THREAT: QUANTUM COMPUTERS' SECURITY CHALLENGE

Quantum computers are touted as the next computing revolution. By relying on the principles of superposition and entanglement, some purely quantum mechanical phenomena, they could solve some previously intractable problems. At present they are known to be able to solve certain specific categories of problems (such as factorization).As research continues, additional quantum-appropriate algorithms might well be discovered. This can have many positive ramifications, for example in medical research.

However, quantum computers also challenge our security infrastructure's status quo. Current strategies for sharing encryption keys rely in part on the difficulty in factoring a large multiplication back into its prime constituents, a problem that is beyond the reach of classic computers in a reasonable timeframe. Once quantum computers mature, they will be able to crack this mathematical challenge quickly, rendering the process of sharing keys through public-key infrastructure insecure.

Symmetric encryption is itself expected to remain safe, as long as the key length is increased (doubled) and fully random. This is because a quantum-based search using Grover's algorithm is only expected to have a quadratic speedup, and an exponential speedup for search algorithms has been shown to be impossible. Unfortunately, in a post-quantum world in which public key sharing is insecure, this quantum-resistance of symmetric encryption becomes irrelevant unless we find a way to securely exchange them.

The US National Institute of Standards and Technology (NIST) estimates that mature quantum computers will be able to crack our public-key infrastructure within 15 years.[1] This may seem far out, but we are in fact in a race for time: upgrading infrastructure takes years, and a lot of sensitive data needs to be kept secure for long periods of time, making it vulnerable to being captured and stored for later decryption as quantum computers become available. Any organization that handles personal or financial information with a long shelf life needs to get ready as soon as possible.

NOW, FOR THE PLUS SIDE

Quantum technology also delivers capabilities that can be used to enhance data security—both from today's attacks, and those from future quantum computers. This is typically known as quantum cybersecurity.

Aside from the quantum computing–related threat, poor quality or insufficient quantity of random numbers also present a security risk. Generating high-quality random numbers at high rates has proven a surprisingly hard problem to solve. Fortunately, quantum technology provides an elegant and powerful solution.

Many processes in quantum physics are random, and this inherent randomness has been harnessed into commercial quantum random-number generators capable of producing fully random numbers at high rates and cost-effectively, putting this issue to rest. These devices are starting to be integrated into cloud security infrastructure, in finance and beyond—a trend that is expected to increase over the coming years. As a bonus, the use of longer, higher-quality keys was identified by the National Security Agency (NSA) as a strategy for protecting data from the threat of quantum computers,[2] so using a high-quality quantum random bit generator enables security-aware companies to get a head start in that direction. True random bits are also necessary prerequisites to using one-time pad (OTP) encryption. This is a type of encryption for which the encrypted text provides no information about the clean text, so that it is safe, independent of the processing power of the attackers, including from quantum attacks.

At a more advanced level, quantum key distribution (QKD) uses the laws of quantum mechanics to enable private and secrete key sharing between two parties, even if they have no control over their communication link. It therefore solves the thorny key-exchange problem mentioned before. Its security is based on a fundamental characteristic of quantum mechanics: that is, the process of measuring a quantum system disturbs the system. An attacker trying to intercept the key exchange will inevitably leave detectable traces, allowing that information to be discarded. QKD has proved to be informationally secure, meaning it remains safe independent of the processing power of the attackers, and is not vulnerable to quantum computers.[3] This developing technology has challenges to overcome, but corporations are beginning to roll out commercial implementations, and there is development under way to move beyond point-to-point capability and emancipate this from its current fiber-optic constraints to free space and ultimately mobile devices. It is certainly worth watching.

SO, WHAT WILL THE FUTURE LOOK LIKE?

In addition to these technology-driven solutions, a search is also underway for algorithms believed to be secure from both classical and quantum-computing attacks. These quantum-resistant algorithms will have challenges: they can't serve as a drop-in replacement for current solutions (thus they will require changes in current protocols), and they may be vulnerable to new attacks or advances in mathematical knowledge as they emerge. It will also take many years to reach standardization around new algorithms. However, they will provide flexibility, and an important element to an overall quantum safe security approach.

In the race to protect our data from the power of quantum computers, it is likely that hybrid solutions will emerge. Keys will be stronger, with what we call "full entropy" or true randomness. Crucial links will be protected using a global, flexible QKD network, invulnerable to quantum computers. Finally, for shorter, less-exposed links, improved algorithms could provide enhanced protection, regularly updated against growing threats.

Whereas the quantum computer is certainly a major threat to cybersecurity, approaches such as quantum random-number generators, QKD, and quantum-resistant algorithms are ramping up to take on this challenge, allowing us to reap the benefits of that technology while remaining secure.

FINDING OUT MORE

There is currently a lot of interest, activity, and development in quantum-safe security—from enterprises and government institutions seeking to protect confidential information, standardization bodies looking to structure new safer ways of communicating, and companies and research institutions developing solutions to these challenges. If you are interested in finding out more, I recommend connecting with the Quantum Safe Security Working Group (QSS-WG), which was formed within the Cloud Security Alliance at the end of 2014. QSS-WG is a forum for interested corporations, organizations, and individuals; its mission is to stimulate the understanding, adoption, use, and widespread application of quantum-safe cryptography to commercial institutions, policy makers, and all relevant government bodies.

JANE MELIA is the vice president of strategic business development at QuintessenceLabs and co-chair of the CSA Quantum Safe Security Working Group. Contact her at jm@quintessencelabs.com.

References

1. D. Moody, "Post-Quantum Cryptography: NIST's Plan for the Future," report, Nat'l Inst. Standards and Technology (NIST); http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf.
2. K. Kennedy, "NSA Recommendations Include High Entropy and Longer Keys to Protect Against Quantum Computer Developments," *CTOVision.com*, 12 Oct. 2015; https://ctovision.com/2015/10/nsa-recommendations-include-high-entropy-longer-keys-protect-quantum-computer-developments.
3. C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proc. IEEE Int'l Conf. Computers, Systems, and Signal Processing*, 1984, pp. 175–179; www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf.

ABOUT THE AUTHORS

SAN MURUGESAN is director of BRITE Professional Services and an adjunct professor at the Western Sydney University. He is the editor in chief of *IT Professional*; an editorial board member of *Computer* and *IEEE Transactions of Cloud Computing*; a co-editor of the *Encyclopedia of Cloud Computing* (Wiley-IEEE, 2016) and *Harnessing Green IT: Principles and Practices* (Wiley-IEEE 2102); and the editor of *Computer*'s Cloud Cover column. Murugesan is a Fellow of the Australian Computer Society and the Institution of Electronics and Telecommunication Engineers (IETE). Contact him at san@computer.org or via http://bitly.com/sanprofile.

BOB COLWELL is an independent consultant at R&E Colwell & Associates, and he served as director of DARPA's Microsystems Technology Office from 2012–2014. Previously, Colwell was Intel's chief IA32 (Pentium) microprocessor architect from 1992–2000. He is the Perspectives editor for *Computer*, an author of the "At Random" column from 2002–2005, and an author of *The Pentium Chronicles*. He is a Fellow of IEEE. Contact him at bob.colwell@gmail.com.

to "teach" a machine that has not been programmed a priori, thus giving rise to future possibilities in which smart computers (that have advanced artificial intelligence) and humans team up to cooperatively execute tasks and enhance human–machine synergy. Cortically coupled computing in which human–machine interaction is synergistic can be more computationally powerful than the sum of the parts.

Computing paradigms will continue to emerge and evolve to offer new capabilities that extend computing's reach and utility. To successfully embrace the potential offered by new computing paradigms, researchers, developers, and industry have to address several questions: How can we effectively address the challenges these paradigms pose? Will such paradigms be viable and evolve as next-gen computers? Are they transformational?

Through the articles in this special issue, we give you a glimpse of what is on the horizon for emerging computing technologies, and we encourage researchers and developers from multidisciplinary fields to learn from each other and work together to further advance computing.

REFERENCES

1. "Rebooting Computing,"special issue, *Computer*, vol. 48, no. 12, 2015; www.computer.org/csdl/mags/co/2015/12/index.html.
2. "Rebooting Computing Initiative," website, IEEE; http://rebootingcomputing.ieee.org.
3. S. Murugesan, "Radical Next-Gen Computing," *Computing Now*, vol. 8, no. 6, June 2015; www.computer.org/web/computingnow/archive/radical-next-gen-computing-june-2015.
4. W. Mazurczyk and E. Rzeszutko, "Security–A Perpetual War: Lessons from Nature," *IT Professional*, vol.17, no. 1, 2015, pp. 16-22; www.computer.org/cms/Computer.org/ComputingNow/issues/2015/06/T-mit2015010016.pdf.

computing in SCIENCE & ENGINEERING
NERSC: 40 Years and Counting
IEEE
AIP