Charting the Course for Quantum Computing

Once upon a time, I was an undergraduate physics major studying a subject called quantum mechanics. At the time, I did not think anyone in the room, professor included, had an inkling that the use of quantum mechanics would ever be cited as the reason for a revolution in computing. However, as we have reached the end of Moore's Law[1] with respect to increasing chip densities, we have begun to look at many mechanisms for increasing the speed and power of computing.[2]

We have engineered new architectures for memory and central processing unit (CPU) proximity, introduced multiple speeds of cache memory, delved into multiprocessor architectures, and implemented machine learning (ML) and artificial intelligence (AI), all in our quest to do more faster than ever before. But even with all of those advances, quantum computing has the ability to completely outpace everything that we have developed thus far.

The Benefits of Quantum Computing

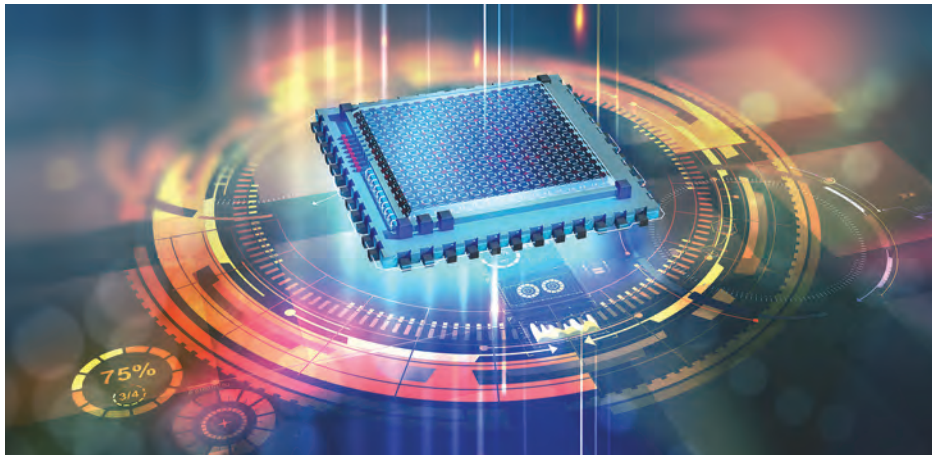
Quantum computing, because of the nature of the physical principles employed, can calculate and solve particularly complex problems exponentially faster than conventional hardware. ML and AI are mentioned as means to continue to make speed improvements even though we have reached the physical limits with respect to chips. Quantum computing can greatly enhance the speed of ML and AI. It can handle simulation models that current "classical" computers cannot.[3]

Other concepts of quantum mechanics can be used in communications to produce tamper-proof channels and networks[4]—tamper-proof in that if someone were to eavesdrop, the nature of the quantum concept of entanglement would reveal not only that someone was listening, but also the identity of that someone. This was a claim once made about fiber optic cables until someone proved that it could be done without noticeably affecting the transmission. In the case of quantum mechanics, entanglements do not allow for such a possibility.

In addition, many of today's security protocols rely on random number generation. However, what we have are algorithms that simulate random number generation. Hence the term, "pseudorandom." If one has the algorithm and the inputs, one is going to get the same value every time. Quantum computing provides the possibility of actual random number generation.

A Double-Edged Sword

There are a number of tech giants and next-tier vendors investing in quantum computing technology. Some already have working tiny quantum computers,



K. BRIAN KELLEY | CISA, CDPSE, CSPO, MCSE, SECURITY+

Is an author and columnist focusing primarily on Microsoft SQL Server and Windows security. He currently serves as a data architect and an independent infrastructure/security architect concentrating on Active Directory, SQL Server and Windows Server. He has served in a myriad of other positions, including senior database administrator, data warehouse architect, web developer, incident response team lead and project manager. Kelley has spoken at 24 Hours of PASS, IT/Dev Connections, SQLConnections, the TechnoSecurity and Forensics Investigation Conference, the IT GRC Forum, SyntaxCon, and at various SQL Saturdays, Code Camps and user groups.

and Microsoft has partnered with some of them to provide quantum computing research in Microsoft Azure.[5] As a result, there is every probability that threat actors will leverage quantum computing for themselves. What is the risk?

One arena of information technology that will fall with the advent of generally available quantum computers is current cryptography. The RSA algorithm, which is the algorithm used for public-private key cryptography and is what allows for certificates and, therefore, much of our secure communications, relies on the fact that given current computing power, by the time someone cracks a particular secure communications exchange, the information transmitted would no longer be of any value. The idea is to put compute time, even in massively parallel architectures, into a minimum time numbering in the thousands of years. However, estimates for quantum computing could crack those same communications in a matter of seconds. We are not there yet, but both IBM and Google have committed to producing quantum computers powerful enough to do so by 2030.[6]

Even as quantum computing and quantum communications solutions are implemented, those solutions should be examined carefully to see if there are nonquantum-based components.

Also, if the plan is to use quantum computing for ML and AI, security practitioners should expect threat actors to do the same, especially if access to quantum computing is available in the cloud. A classic example from science fiction is using AI to probe defenses and automate attacks. Other examples include using ML to avoid countermeasures defenders might deploy. The reality is that quantum computing will be used by both sides as it becomes more available.

Reading Between the Lines to Find Risk

In the push to be first, whether by researchers or those reporting the findings, details may be blurred or omitted. A great example is the report of the "first quantum network," which stretches from Beijing to Shanghai.[7] The article cited is an update on the initial network put in place in 2017. While it is an example of quantum key distribution (QKD), in the details is the fact that the network was achieved using something called "trusted relays" in much of the media. Any time I see the word "trusted," the first thing I think is how do I attack that trusted component?

As it turns out, at each of these trusted relays, the quantum communications are decrypted into a traditional bit structure and then reencrypted for the next transmission along the line. When we say quantum communications, we assume that they are tamper-proof because of entanglement. However, at each of these relays, there is a component of communications via conventional means, not quantum ones. As a matter of fact, there are 32 such relays in the network, meaning each of these points is susceptible to attack. Breaches of any of the relays will provide access to the communications passing through them.[8]

This is not to knock the significance of the advance but to point out that even as quantum computing and quantum communications solutions are implemented, those solutions should be examined carefully to see if there are nonquantum-based components. Nonquantum components are susceptible to known methods of attack. Therefore, even if a particular communications channel is touted as being a quantum communications channel, we still have to perform due diligence to determine what exactly that means for each particular case.

Preparing Organizations

Some may point out that we are actively using and developing solutions that are based on quantum mechanics today. That is true, but using the concepts of quantum mechanics is not the same as quantum computing. For instance, applying quantum mechanics has led to improvements in magnetic resonance imaging (MRI) technology, in laser outputs and in so many other areas. That is not the same thing as having deployed solutions in quantum computing or quantum communications. While MRI and laser technologies are well known, the future of quantum computing is not. However, given the progress already made, it is reasonable to assume that it is only a matter of time before products around quantum computing and communications will become viable and then transition into the mainstream. When they do, they will turn classical computing on its head. So how should an organization prepare for the coming tide?

Protiviti offered up six steps organizations can do right now:

1. **Name a champion**—Someone within the organization should be responsible for keeping up with progress in quantum computing and providing that information to the organization.

2. **Conduct a readiness assessment**—How prepared is the organization for embracing quantum computing? How knowledgeable are key players? Does the organization have a solid understanding of how quantum computing is likely to impact the industry? How does the organization stay competitive with the shift?
3. **Identify use cases and assess value**—To prevent organizations from engaging in conflict with imagined opponents, it is important to perform the legwork of determining where quantum computing makes sense within the organization. Some uses cases are not good fits and others may be, but the return on investment (ROI) is too small to embrace. Rather than be stuck in follower mode and playing catch up, it is important for an organization to have considered how to implement technologies as they become viable.
4. **Uncover potential risk scenarios for encryption and security**—Since quantum computing will invalidate the strength of current cryptography, and as threat actors begin to use the technologies, too, organizations must plan for and protect against those possibilities. Therefore, organizations must be proactive in understanding how advances will change the operating landscape and prepare accordingly.
5. **Chart the course**—It goes without saying that since the technology is not ubiquitous today, the organization should lay out a multiyear road map that takes into account the technology advances and when the organization would begin to onboard those technology changes.
6. **Begin the process and take an iterative approach**—As with any new technology, delays should be expected in some areas and unanticipated advances and developments in others. Therefore, we cannot adhere to a static road map nor can we assume that what we understand about quantum computing today is not going to be rendered obsolete by those changes tomorrow. Therefore, it behooves the organization to periodically reevaluate.[9]

Quantum computing is not available as a usable technology today. However, given the current state of research and forward progress in this arena, we need to prepare for it, most likely within the current decade. It changes the rules on key areas, such as cryptography and any kind of computational modeling, and should not be ignored. At this point, with the technology still in the preliminary stages, getting up-to-date is not that difficult, but as advances happen, the pace of progress will likely accelerate exponentially, similar to most new technology trends. Therefore, as the old saying goes, "A failure to plan [now] is a plan to fail."

We cannot adhere to a static road map nor can we assume that what we understand about quantum computing today is not going to be rendered obsolete by those changes tomorrow.

Endnotes

1 Rotman, D.; "We're Not Prepared for the End of Moore's Law," *MIT Technology Review*, 24 February 2020, *https://www.technologyreview.com/2020/02/24/905789/were-not-prepared-for-the-end-of-moores-law/*
2 Vellante, D.; Floyer, D.; "A New Era of Innovation: Moore's Law Is Not Dead and AI Is Ready to Explode," *siliconAngle*, 10 April 2021, *https://siliconangle.com/2021/04/10/new-era-innovation-moores-law-not-dead-ai-ready-explode/*
3 Microsoft, "What Is Quantum Computing? Quantum Computer Uses and Applications," *https://azure.microsoft.com/en-us/overview/what-is-quantum-computing/#real-world-uses*
4 Institute for Quantum Computing, "Quantum Communication," University of Waterloo, Ontario, Canada, *https://uwaterloo.ca/institute-for-quantum-computing/quantum-101/quantum-information-science-and-technology/quantum-communication*
5 Legrand, J.; "Quantum Computing: Threat to Cybersecurity?" *CISOMAG*, 24 September 2020, *https://cisomag.eccouncil.org/quantum-computing/*
6 Lipman, P.; "How Quantum Computing Will Transform Cybersecurity," *Forbes*, 4 January 2021, *https://www.forbes.com/sites/forbestechcouncil/2021/01/04/how-quantum-computing-will-transform-cybersecurity/*
7 University of Science and Technology of China, Hefei, Anhui, China, "The World's First Integrated Quantum Communications Network," *Phys.org.*, 6 January 2021, *https://phys.org/news/2021-01-world-quantum-network.html*
8 Giles, M.; "Explainer: What Is Quantum Communication?" *Technology Review*, 14 February 2019, *https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/*
9 Protiviti Insights, "Quantum Computing: Why the Board Should Care," Protiviti Board Perspectives; Risk Oversight, iss. 139, 21 June 2021, *https://www.protiviti.com/US-en/insights/newsletter-bpro139-quantum-computing*

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on emerging technology in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*