Quantum Theory with Computer & Cyber Security Applications

Donn M. Silberman, Fellow of the OSSC & SPIE

The transition from classical to modern physics (including quantum) has dramatically changed our civilization. The people in the above photo ushered in this change beginning over 100 years ago and the effects are still making exponential change with current and future applications including quantum computing, encryption, sensing, materials development, logistics, communications and much more.

In December 2018, the US Federal Government passed the National Quantum Initiative[1] that recognized and funded some of the current efforts in developing the quantum industry in the United States. Other countries have done this[2,3,4] both before and after the US, making this a global race to capitalize on the significant progress that has been made in past decades. In the past two years, the amount of attention that has been focused on many advances has left companies, national laboratories, colleges, and universities with many open positions for people skilled with knowledge and experience in quantum technologies. Some very excellent work[5,6] has been done assessing the needs of the quantum industry. Most of this work has been for people with undergraduate[7] and graduate degrees in physics, chemistry, math, engineering, computer science, material science and related technologies. In line with some of my past educational endeavors, I have been consulting with EdQuantum to develop a hybrid curriculum in advanced optics, spectroscopy, and quantum technologies for technicians to fill the workforce gap between those with undergraduate and high school degrees.

Quantum Photonic (Silicon) Integrated Circuit (QPIC) test & measurement

How will quantum technologies Impact everyday life?

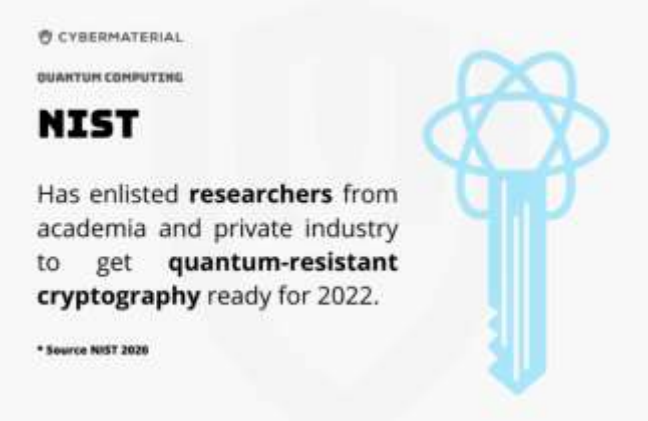
While there will be many aspects of modern life that will continue to be affected by the push to integrate quantum technologies, the remainder of this article will focus on quantum computing, encryption, and the internet, as they pose the greatest risks and opportunities to people's everyday economic life. Cryptocurrencies have been developed on Blockchain technologies and is a fast-growing sector of the modern financial landscape. Blockchain technologies are also being applied to many other industrial sectors; but quantum computer technologies poise a threat to all these currently secure applications. Quantum computers also may be used to hack all other encryption technologies currently in use. A global race is currently being run by private and public entities, some individually and some in consortium to develop both practical quantum computers[8] and quantum resistant technologies. Much of the work is being published in the public domain that can be tracked; and some must be held 'close to the vest' and their progress is unknown to the public. Herein lies the greatest risk, if an unknown entity develops a quantum computer with the capability to hack current encryption technology and does it without anyone knowing; losses could be substantial. There is also the concept that encrypted information could be collected from the current internet and stored until the quantum computer is available to crack the code and read the information later. In November 2020, a position paper titled, 'Post-Quantum Cryptography (PQC) and the Quantum Threat' was published by the Wells Fargo Technology[9] that details much of this situation. In the time since then, much more progress has been made and the story continues.

There are two paths that need to be tracked; the development of quantum computers and their ability to hack secure encrypted information and the development of quantum resistant encryption[10]. One parallel technology being developed is quantum secure communications over the internet. Millions and even billions of dollars are being spent on quantum technologies globally and China is clearly the leader in dollars spent. It is possible that they are also acquiring intellectual property in this domain faster than all other countries combined. So, the actual ability to successfully implement effective quantum technologies through trade secrets will likely be the deciding factor winning this global race.

The federal government wants to help.

In December 2021, the US Department of Homeland Security published an article titled, "DHS wants state & local governments to start planning for quantum computing; releases road maps and resources to help."[11] This short article describes this situation and mentions that the NIST has been working on new quantum-resistant encryption algorithms to provide guidance to US based entities and will be narrowing down the final entries and releasing the results in 2022. This article mentions that the DHS believes quantum computers may be attacking public and private information by 2030; my belief is that it will come

much sooner. This belief is based on my years of industry and academic experience with physics, optics, lasers, fiber optics, and Silicon (Photonic) Integrated Circuits (SICs). In the referenced article[8] above, the authors review over a dozen different quantum computing hardware technologies and companies that are all in this race to build and implement a practical quantum computer. The details and technical references are all provided for readers interested in exploring them further. My perspective is that Quantum Photonic Integrated Circuits (QPICs) will be the winning technology for multiple reasons that are reviewed in another recent blog article[12] that reviews 20 years at light speed – the future of photonic quantum computing.



In summary, my suggestion is that cybersecurity personnel become familiar with this topic and take as much appropriate action as possible for your organizations. Below is a link to all the references in this article and a few non-cited links to websites keeping up with the current news in this field.

Link to references

Donn M. Silberman is an SPIE Fellow, and Past President of the Optical Society of Southern California. He has provided technical engineering, management, and education to many precision optical and optical instrument companies and educational entities in Southern California for over 35 years. Recently retired from Starrett Metrology Solutions, he has been focusing on current and new quantum technological applications as they are impacting the lives of people globally.

Donn is currently consulting with EdQuantum, an NSF funded educational program to develop curriculum and lab experiments for community college students that have completed at least some laser electro-optics courses. He holds a BS in Engineering Physics from the Univ. of Arizona (Honors in Physics) and an MS in Technology Management from Pepperdine University.

He was an advisor to Irvine Valley College's Laser Electro-Optics Technology programs from the early 1990s to 2020, and he helped move the program to Pasadena City College. Donn founded the UC Irvine's Optical Engineering and Optical Instrument Design programs in 2009; and received the UC Irvine Extension's Dean's Outstanding Service Award in Nov 2012; and was the 2012-2013 Univ. of Arizona Honor's College Advocate for Education Award Winner.

Donn was a Senior Applications Engineer for PI (Physik Instrumente) L.P. for over 10 years, where he worked on many world-class optical instruments for science and industry, including the world's largest astronomical and solar telescopes and the highest precision measurement systems for today's Quantum Photonic (Silicon) Integrated Circuits (QPICs) that are being used in Quantum Computers.

For exercise, Donn trained for and participated in over 65 Sprint and Olympic distance triathlons starting in 2008 and is still training now. Organized races stopped during the COVID pandemic and may start up again in 2022. Donn lives with his wife Ana Maria in Rancho Mission Viejo.