Three questions about quantum computing and secure communications

September 15 2022, by Taylor McNeil

Credit: cottonbro studio from Pexels

A radically different type of computing technology under development, known as quantum computing, could in theory decode secure communications and jeopardize military communications, critical

infrastructure, and financial transactions, the federal government warns.

The Biden administration recently published a National Security Memorandum about quantum computing that warns of the consequences of development of quantum computers "capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world."

The consequences, it says, could "jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most internet-based financial transactions."

Quantum computers employ a fundamentally different approach to computing than those existing now, using the laws of quantum mechanics—a branch of physics that describes the motion and interaction of subatomic particles—to store information and solve problems that are too complex for current computers. Quantum computers exist currently, but have limited abilities.

Peter Love, a professor in the Department of Physics and Astronomy and the Department of Computer Science, focuses his research on quantum computing. He is part of a center called the Quantum Systems Accelerator (QSA), which seeks to create the next generation of quantum computers and apply them to the study of some of the most challenging problems in physics, chemistry, materials science, and more.

Tufts Now talked with him about the National Security Memorandum, and the potential risks to secure communications that quantum computers might pose going forward.

Tufts Now: When do you think such quantum

computers might be developed and brought online? Would it start with governments having this capability first?

Peter Love: The sensible view would be that it will be more than a decade before such machines will be available—conservatively, several more decades. Fortunately, there are more interesting, smaller, and more benign applications of quantum computing that we can study along the way, as well as other quantum technology such as sensing and communications.

How do quantum computers work so much faster than current computers to be able to decrypt formerly secure communications?

That is a deep, open question in the field. We do not have a good general understanding of how quantum speedup over conventional computers is achieved, and we do not generally understand which problems are amenable to quantum speedup. This should not be surprising, as we do not have a good conceptual picture of quantum mechanics itself in terms of the classical concepts used to define most computational problems.

But what we do have is a small number of absolutely stunning examples of the power of quantum computing.

Public key cryptography is used in most secure communications on the internet. It works this way: Suppose I have two large numbers. I multiply them together and tell you the answer. Can you tell me what the two original numbers were? The hardness of that problem guarantees the security of the most widely used public key cryptography system.

Many examples of numbers that can't be factored exist despite large cash prizes being offered. In 1994 Peter Shor—then at Bell Labs, now at MIT—published a quantum algorithm that could factor these large numbers, given a sufficiently large quantum computer. The way this quantum algorithm works is totally unrelated to how the best classical algorithms work.

What can be done to ensure that secure communications are possible when a 'cryptanalytically relevant quantum computer,' as it is called in the memorandum, is up and running?

There are problems that can form the basis of cryptographic systems, where we have good reason to believe that quantum computing will not crack them. The federal National Institute of Standards and Technology has recently announced their latest candidates. These will be in use long before a large "cryptanalytically relevant quantum computer" becomes available.

However, one must remember that there are presumably large archives of recorded encrypted signals that might be quite interesting to read if one could decrypt them.

Finally, it is important to remember that there is no proof that factoring problems like that used in RSA cryptographic systems—commonly used to secure communications—is a hard computational problem, even for conventional computers. Who knows if advances in number theory might lead to an efficient classical factoring algorithm that could render RSA systems useless?

So RSA was never really secure in that very strict sense. Most people believe that RSA is secure because they believe factoring is hard,

because they think that number theorists are clever and would have found an algorithm if there was one. But that's not a mathematical proof—it's just a bet that number theorists are as smart as they think they are.

Provided by Tufts University