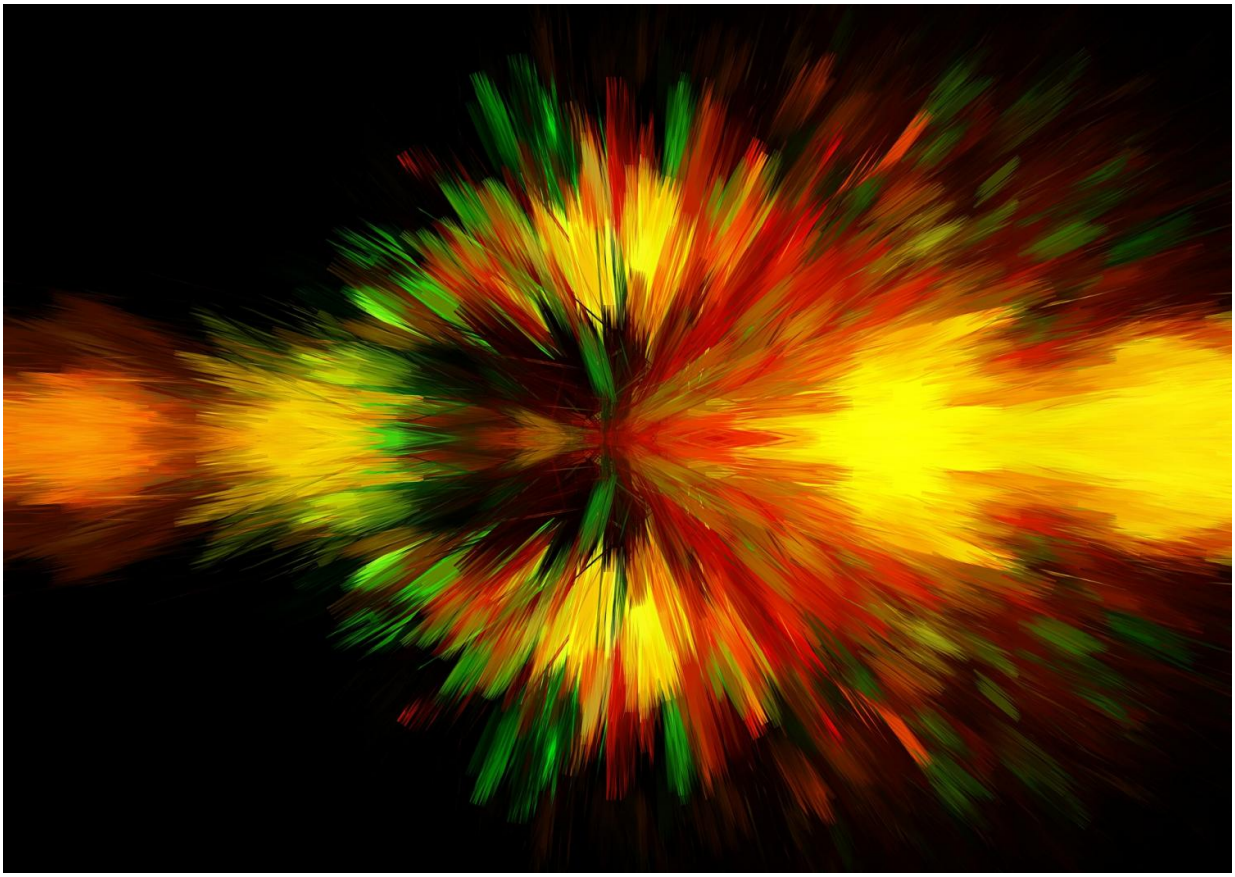
Mathematician breaks down how to defend against quantum computing attacks

February 28 2017



Credit: CC0 Public Domain

The encryption codes that safeguard internet data today won't be secure forever.

Future quantum computers may have the processing power and algorithms to crack them.

Nathan Hamlin, instructor and director of the WSU Math Learning Center, is helping to prepare for this eventuality.

He is the author of a new paper in the *Open Journal of Discrete Mathematics* that explains how a code he wrote for a doctoral thesis, the Generalized Knapsack Code, could thwart hackers armed with next generation quantum computers.

The paper clarifies misunderstandings about the complex field of public key cryptography and provides a common basis of understanding for the technical experts who will eventually be tasked with designing new internet security systems for the quantum computing age.

"Designing security systems to protect data involves experts from many different fields who all work with numbers differently," Hamlin said. "You are going to have pure and applied mathematicians, computer programmers and engineers all involved in the process at some point. For it to work in real life, all of these people need to have a common language to communicate so that they can make important decisions about how to safeguard online transactions and personal communications in the future."

Preparing for the future

Quantum computers operate on the subatomic level and theoretically provide processing power that is millions, if not billions of time faster than silicon-based computers. A hacker armed with a next generation quantum computer could in theory decrypt any internet communication that was sent today, Hamlin said.

In order to create an online security system better prepared for future demands, Hamlin and retired mathematics professor William Webb created the Generalized Knapsack Code in 2015 by retrofitting a previous version of the code with alternative number representations that go beyond the standard binary and base 10 sequences today's computer use to operate.

In his paper, Hamlin breaks down how the generalized knapsack code works in terms that computer scientists, engineers and other experts outside the field of pure mathematics can understand. He explains that by disguising data with number strings more complex than the 0s and 1s conventional computers use to operate, the generalized knapsack offers a viable security method for defending against quantum computing hacks.

"The Generalized Knapsack Code expands upon the binary representations today's computers use to operate by using a variety of representations other than 0s and 1," Hamlin said. "This lets it block a greater array of cyberattacks, including those using basis reduction, one of the decoding methods used to break the original knapsack code."

Hamlin said his hope is that his paper, Number in Mathematical Cryptography, clears up misunderstandings he has run into professionally so that the generalized knapsack code can be developed for future use.

"Quantum computing will change how we handle data and we, as a society, are going to have to make some important decisions about how to prepare for it," Hamlin said. "A code like this can be implemented on conventional hardware and yet it would also be secure from a hacker with a quantum computer. I think it is time for us to consider this code very seriously for adapting commerce and perhaps communication in light of the possibility of quantum computing."

More information: Nathan Hamlin, Number in Mathematical Cryptography, *Open Journal of Discrete Mathematics* (2017). DOI: 10.4236/ojdm.2017.71003

Provided by Washington State University