Quantum compute this—Mathematicians build code to take on toughest of cyber attacks

March 26 2015

Hamlin and Webb at Washington State University. Credit: Rebecca Phillips

Washington State University mathematicians have designed an encryption code capable of fending off the phenomenal hacking power of a quantum computer.

Using high-level number theory and cryptography, the researchers

reworked an infamous old cipher called the knapsack code to create an online security system better prepared for future demands.

The findings were recently published in the journal *The Fibonacci Quarterly*.

Quantum computers are near

Quantum computers operate on the subatomic level and theoretically provide processing power that is millions, if not billions of times faster than silicon-based computers. Several companies are in the race to develop quantum computers including Google.

Internet security is no match for a quantum computer, said Nathan Hamlin, instructor and director of the WSU Math Learning Center. That could spell future trouble for online transactions ranging from buying a book on Amazon to simply sending an email.

Hamlin said quantum computers would have no trouble breaking present security codes, which rely on public key encryption to protect the exchanges.

In a nutshell, public key code uses one public "key" for encryption and a second private "key" for decoding. The system is based on the factoring of impossibly large numbers and, so far, has done a good job keeping computers safe from hackers.

Quantum computers, however, can factor these large numbers very quickly, Hamlin said. But problems like the knapsack code slow them down.

Fortunately, many of the large data breaches in recent years are the result of employee carelessness or bribes and not of cracking the public

key encryption code, he said.

A new public key code

Looking to protect future online information, Hamlin and retired mathematics professor William Webb turned to the long-abandoned knapsack code. To bring it up to quantum level - and possibly use it as a new type of public key encryption - the researchers first engineered new numbering systems for the code.

"We used alternate ways of representing numbers," said Hamlin.

In effect, they created new digital systems with much greater complexity than society's day-to-day decimal and binary systems.

"By using very complicated number strings, we produced a new version of the knapsack code that can't be broken by the usual cyber attack methods," said Webb.

As a result, Hamlin and Webb believe the redesigned knapsack code could offer a viable alternative for public key encryption with quantum computing.

Knapsack code

The knapsack problem is a theoretical puzzle dating back to at least 1897 and is very difficult to solve in its most general form.

"Basically, it asks if you have one big number (the knapsack) and lots of small numbers (objects), what is the subset of small numbers (or objects) that will perfectly fill the knapsack? The concept was used to create a code called the knapsack code," explained Webb.

"The knapsack code was originally suggested as a tool for public key encryption in the 1970s, but it was broken by two different methods and people lost interest in it," he said.

Webb's idea to bring it out of storage was at first an intellectual exercise.

"Knapsack is a simple, elegant code but it was broken," said Webb. "We wondered if it could be fixed and redesigned to be secure. The challenge was intriguing."

Hamlin said they made corrections at the fundamental level of the code, which repaired many of its weak spots. This let it block a greater array of cyber attacks, including those using basis reduction, one of the decoding methods used to break the original knapsack code, he said.

"Basis reduction is a big hammer to use against this code and, after testing, we think it's secure against this type of attack and would offer an alternative code for quantum computing," Hamlin said.

Webb said although it still needs outside testing, the remodeled knapsack code holds promise for making future online computer transactions considerably more secure.

"Essentially any time you want to send secure messages over the Internet, you need a public key code. This is another candidate for a useful code," he said.

Provided by Washington State University