Written by Alice Marshall
05 October 2018

BlackBerry announces the latest addition to its selection of cryptography tools--quantum-resistant code signing software, allowing "software to be digitally signed using a scheme that will be hard to break with a quantum computer."

Developed in collaboration with Isara Corporation, a specialist in "agile quantum-safe security solutions," the solution promises to future-proof the security of long-lived assets (such as systems in critical infrastructure, industrial controls, aerospace and military electronics, telecommunications, transportation infrastructure, and connected cars) in case quantum computers able to easily break traditional code signing schemes become reality.

Quantum computers harness the properties of quantum mechanics to solve problems too complex for even current supercomputers. Such problems include the factor-based encryption securing everything from banking records and state secrets to connected devices and autonomous vehicles. BlackBerry says the move to quantum-resistant security will be a multi-year effort, and as such governments, enterprises and device vendors should start taking the first steps sooner, not later.

"Within the next 8 to 10 years, experts estimate there will be a large-scale quantum computer capable of breaking today's public key cryptography," Isara says. "The work we're doing with BlackBerry will give industries with durable connected devices the tools needed to secure their systems now and into the future."

Go BlackBerry Adds New Quantum-Resistant Solution to its Cybersecurity Arsenal