CYBERSECURITY
RESEARCH LAB

CRL 101 Series

The Quantum Computing Threat

By Annegret Henninger & Dr. Atefeh Mashatan

Quantum computing poses a serious threat to some of the current standardized cryptography, and thus a threat to cybersecurity.

Quantum computers function fundamentally differently from classical computers, allowing them to be more powerful in solving certain types of problems. Classical computers process sequences of bits (1s and 0s) that represent information and programmed instructions. While quantum computers also use 1s and 0s, instead of bits they use quantum bits known as *qubits*. The 1s and 0s are encoded onto atomic and subatomic particles which behave differently than bits in what's known as *superposition* where the state of a qubit is distinguishable, but not stationary. Superposition allows a quantum computer to process a large number of calculations simultaneously. While a classical computer must try the different paths to the right answer, one by one, a quantum computer can try all of the paths at once with high accuracy. This allows them to solve certain complex problems faster than classical computers. Although this can be an exciting opportunity for many researchers needing advanced computing to study, e.g., drug simulation, brain circuitry, or human DNA, it turns out to be a serious threat to our information security and privacy.

Information communication technology heavily relies on the security of encryption algorithms which are designed based on the difficulty of complex mathematical problems, such as *Integer Factorization Problem* and *Discrete Logarithm Problem*. A quantum computer, however, could easily solve these underlying math problems and, hence, threatens our security and privacy. A quantum computer would give a constant speed up against symmetric cryptography, but an exponential speed up against asymmetric cryptography. Encryption algorithms that quantum computing will be able to break include the asymmetric-key encryption algorithms of RSA and ECC.

We still have some engineering challenges to overcome to build a scalable quantum computer. There are different estimates as to when we could expect one and it varies from 10 to 30 years mostly. However, the threat they pose to information security is more imminent and is dubbed as "harvest then decrypt" attack scenario, where encrypted information is collected and can be decrypted later for as long as the data is still valuable. This threat is amplified by current large-scale data collection practices, known as traffic "mining" or "harvesting", where malicious third parties collect information for unintended uses. Personally identifiable information (PII) that have been 'securely' shared, could easily be accessed. Therefore, *current* asymmetric-key

cryptography infrastructure vulnerabilities leave communicated data, and entire legacy systems at risk. The CRL is working on a knowledge translation project for information security personnel, which covers the strategic implications of quantum computing for enterprises.

There is hope in that not all mathematical problems can be broken this easily by quantum computers. Those underlying mathematical hard problems that can resist the power of a quantum computer give rise to *quantum-resistant* cryptography. While quantum-resistant cryptographic primitives have already been proposed, none of them are commonly adopted yet. Before a new encryption scheme is deployed it needs to undergo extensive due diligence to ensure it is actually secure. As such, we rely on *standardized* cryptography. To protect our data against quantum computing, quantum-resistant algorithms are under review by standardization bodies such as NIST which has most recently revealed the 26 proposed quantum resistant algorithms that will advance to the 'semifinals' of this competition at NIST. However, during this process, we are vulnerable to attacks. In response to this threat, the CRL is developing classical/quantum hybrid solutions for present use, which protect against quantum attacks, while maintain current security guarantees.

July 16, 2019
CRL 101 series

The CRL 101 series is a knowledge transfer project designed to give readers an overview of trending security-related technologies that we are working on at the Cybersecurity Research Lab.