PART 4

Quantum Risk Assessment Report

A resource estimation framework for quantum attacks against cryptographic functions- Improvements

Authors: **Michele Mosca,** *evolutionQ Inc*
Vlad Gheorghiu, *SoftwareQ Inc.*

The Global Risk Institute provided funding for the research and the preparation of this paper. The authors are independent contributors to the Global Risk Institute. They are solely responsible for the content of the article

SUMMARY REPORT

Public-key cryptography, which underpins the security of most of the tools we rely on today including cloud computing, payment systems, the internet, and IoT, is susceptible to being broken by quantum computers in the not-so-distant future. Nonetheless, we are still many years away from a wide-scale transition to new systems designed to be quantum-safe.

The precise time at which our current systems will be vulnerable to systemic quantum attack depends on two key factors. Firstly, how large of a quantum computation is needed to break these systems, and secondly, how soon the required resources are available.

This reports focuses on the first part of this equation and presents our latest work on quantum resource estimates for breaking the public-key cryptography which is so heavily relied upon today.

The main recent advance that has made some impact is a new technique called "lattice surgery" that improves a state-of-the-art approach to fault-tolerant quantum error correction. Fault-tolerant quantum error correction is a complex process that takes faulty physical quantum bits being manipulated by imperfect processes and makes them collectively behave as an effectively noiseless quantum bit. This process is at the core of being able to harness the full power of quantum computation. The new lattice surgery technique is able to reduce the physical resource requirements of a quantum computer by nearly an order of magnitude.

For example, our revised quantum memory estimates for breaking RSA-2048 (based on a number of assumptions) in under 24 hours is now roughly 10 million physical quantum bits, compared to 50 million physical quantum bits in our last report. This is still a daunting number of physical qubits, but it will be important to keep tracking the downward trend of these resource estimates alongside progress in the development of relevant quantum computing platforms.

About the Author

Michele Mosca serves as a Special Advisor on Cyber Security to the Global Risk Institute. He is co-founder of the Institute for Quantum Computing at the University of Waterloo, a Professor in the Department of Combinatorics & Optimization of the Faculty of Mathematics, and a founding member of Waterloo's Perimeter Institute for Theoretical Physics. He co-founded and is director of CryptoWorks21, an NSERC funded training program in quantum-safe cryptography.

In 2015 he started the company evolutionQ Inc. with Norbert Luetkenhaus in order to help organizations evolve their quantum-vulnerable systems and practices to quantum-safe ones. EvolutionQ assesses the quantum threat, how it impacts specific organizations, how they can mitigate the risk, and helps them implement their mitigation strategies.