PART 1

Quantum Risk Assessment Report

A resource estimation framework for quantum attacks against cryptographic functions

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

GLOBAL RISK INSTITUTE

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.

CYBER SECURITY AND FRAUD

SUMMARY REPORT

"A resource estimation framework for quantum attacks against cryptographic functions improvements" provides an extension of our work on estimating the real-world effort it will take for a quantum computer to compromise symmetric cryptographic functions at the foundation of protecting our ICT infrastructure.

The cryptographic security of a protocol is typically measured in terms of a 'bit strength', which is an integer n, such that it takes 2^n basic operations, using the best known methods, to break the security of the protocol. Increasing computational power means that what is considered to be 'sufficient' strength increases over time, for example for many applications moving from 80 bits to 112 bits to 128 bits over the past years.

Sometimes cryptanalytic algorithms improve, and the bit strength of a protocol turns out to be substantially lower than previously believed, as happened with the RSA system in the 1980s. Quantum computing brought a paradigm shift that drastically reduces the operations needed to break the current public-key algorithms, and substantially reduces the resources needed to break symmetric key cryptography.

Our initial work has focused in symmetric key cryptanalysis. It is well known that, against generic quantum attacks, 256-bit AES or SHA provide at least the equivalent of 128-bits of security against generic classical attacks. However, given the overhead in the known approaches to fault-tolerant quantum computation, this is likely an overkill, and our work provides a more realistic assessment of the security of AES and SHA against known quantum attacks. For example, breaking AES-128 on a quantum computer with today's methods and assumptions would have a cost of over 2^100. These estimates, which may go down as algorithms, methods, and technology improve, are a useful guide for assessing the risk of a quantum attack on systems relying on these cryptographic algorithms.

About the Author

Michele Mosca serves as a Special Advisor on Cyber Security to the Global Risk Institute. He obtained his doctorate in Mathematics in 1999 at Oxford on the topic of Quantum Computer Algorithms. He joined the Waterloo faculty in 1999. 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.