PART 2

Quantum Risk Assessment Report

A resource estimation framework for quantum attacks against cryptographic functions- (RSA and ECC)

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.

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 a number n, such that it takes 2n 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 with 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 focused on symmetric key cryptanalysis, and this next installment is focusing on public key cryptanalysis, where the speed-ups offered by quantum computing are more devastating. Unlike the case with AES and SHA algorithms, increasing key length is not a viable approach to defending against the known quantum algorithms. For example, with AES, doubling key sizes from 128 bits to 256 bits increased our benchmark estimates of the work needed to cryptanalyze on a quantum computer from 2101.4 to 2169.9 which represents an astronomical increase in the required computing resources (by a factor of roughly $268.5 \approx 4.2 \times 1020$). In contrast, doubling RSA key sizes from 1024 bits to 2048 bits only increased the benchmark estimate from 3.6 hours to 28.6 hours and from 2.6 million physical qubits to 6.2 million physical qubits, which in comparison is a very modest increase in resources required.

The report also allows for comparisons between ECC and RSA, for example 2.5 hours and 1.8 million physical qubits for NIST ECC P-160 versus 3.6 hours and 2.6 million physical qubits for RSA-1024.

Our ongoing work will apply various optimizations and compare the result to the current benchmarks, and also analyze additional cryptographic functions.

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.