PART 3

Quantum Risk Assessment Report

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

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.

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.

While it is well known that, against generic quantum attacks, 128-bit AES (Advanced Encryption Standard) provides at least the equivalent of 64-bits of security against generic classical attacks ("64-bits of security" means breaking the scheme requires roughly 264 computational resources, such as clock-cycles or bits of memory), our previous report showed how in practice, breaking AES-128 on a quantum computer with today's methods and assumptions would have a cost of over 2100. Thus, in the short term there is no known imminent threat to AES-128. However, we anticipate methods will improve and assumptions may turn out to be wrong, so while there is no need to panic, migrating to AES-192 or AES-256 would provide a higher level of confidence against future quantum cryptanalysis.

The focus of this updated report is to assess the cost of parallelized quantum attacks on AES and SHA (Secure Hash Algorithm). Quantum searching is an intrinsically serial process, and thus the time-memory trade-off for exhaustive (or "brute-force") quantum search is not as efficient as the time-memory trade-off of classical exhaustive search. Doubling the number of quantum computers does not cut the search time in half — it only cuts the search time down by roughly $\sqrt{2} \approx 1.4$. To illustrate the different trade-offs with an example, roughly speaking, one can break AES-128 with 1 classical processor running for 2128 steps, or 220 classical processors running for 2108 steps, or 264 processors running for 264 steps, or 2128 processors running for 1 step. In other words, the product of time and memory is fixed at 2128.

In contrast, ignoring errors and other overheads, which we study in this report, one can break AES-128 with 1 quantum processor running for 264 steps, or 220 quantum processors running for 254 steps, or 264 quantum processors running for 232 steps, or 2128 processors running for 1 step. Note how the product of time and memory increases as we parallelize more. While quantum computing still offers a speed-up, there are diminishing returns as we continue to parallelize.

In practice, unlike today's classical digital computers which are very resilient to noise, quantum computers are much more susceptible to errors, and correcting them introduces significant overhead (in terms of time and number of

qubits) in the computation. We analyze and estimate the cost of fault-tolerantly implementing quantum brute-force attacks on AES and SHA, and the room for improvement by finding more efficient implementations of AES and SHA on a quantum computer.

For example, to break AES-128 in under a year, with our stated assumptions, would require roughly 280 quantum processors, a number far too large to be of practical relevance:

That's over 100 trillion quantum computers per living person; even if hypothetically the cost comes down to $1 per processor that would amount to over 10 billion times the current Gross World Product.

Thus, further improvements in quantum fault-tolerance and/or quantum implementations of AES, or some other major advance in software or hardware, would be required to break AES-128 in practice. Researchers continue to pursue such advances in hardware and software, which have to date reduced the cost by several orders of magnitude. The impact of ongoing and future advances on the overall cost of breaking AES and SHA will need to be evaluated as part of 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.