PART 5

GRI Quantum Risk Assessment Report:

RESOURCE ESTIMATION UPDATE

FEBRUARY 2020

Authors: Dr. Vlad Gheorghiu, *Co-Founder & CEO, softwareQ Inc.*
Dr. Michele Mosca, *Co-Founder, President & CEO, evolutionQ Inc.*

GLOBAL RISK INSTITUTE

evolution

EXECUTIVE SUMMARY

Currently deployed cryptographic systems, which include public-key cryptography, hash functions, and ciphers, underpin the security of virtually all communication protocols over the internet and related tools, including payment systems, internet of things, crypto-currencies, and other mechanisms.

Quantum computers threaten the security of the aforementioned systems, by completely shattering the security of public-key schemes such as RSA and weakening the security of the so-called symmetric schemes, such as the AES family of ciphers.

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.

In this report we focus on the first part. We update our previous security estimates in the light of new developments in the theory of quantum algorithms, quantum error correction, and quantum circuit optimization. We consider public-key systems such as RSA and ECDH (Elliptic-Curve Diffie-Hellman), as well as the AES family of symmetric ciphers. All of those schemes are heavily relied on today for a vast range of applications.

The most crucial recent advance in the research literature that made a significant impact for estimating the security of public-key systems is a technique "imported" to the quantum domain from classical circuit optimization called "windowed-arithmetic". This technique is able to significantly reduce the size of the quantum circuit required to attack public-key cryptosystems, in particular RSA. For example, in our revised estimates, we show that, under realistic assumptions (physical error rates of the order 1 in 1000), the physical resources required to break RSA-2048 in under 24 hours decreases by two orders of magnitude (from 172 million physical qubits to 1.17 million physical qubits, a two-order of magnitude reduction). The impact for public-key systems based on ECDH is less dramatic, but still substantial, due to the fact that windowed-arithmetic techniques cannot be applied so successfully to ECDH in comparison with RSA. Nevertheless, for example, for the curve NIST P-256, we show a reduction from 67.7 million physical qubits to only 7.43 million physical qubits, an order of magnitude reduction, in order to break the scheme in under 24 hours.

For symmetric ciphers such as AES, the main recent advances were made at the circuit level by slightly improving the number of components (gates) required by the quantum circuit. The net effect is a reduction in the security of AES by at most 5 bits. For example, the cost of attacking AES-256 under a very conservative physical error rate of 1 in 100 000 shows a security reduction from 171 bits (old estimates) to 166 bits (current estimates). This is by far a less dramatic decrease in security in comparison with public-key systems, but nevertheless is notable.

Estimating the strength of current cryptographic schemes against realistic quantum attacks is a moving target that depends on a variety of parameters, such as fault-tolerant quantum error correction, circuit optimization and compilation, novel cryptanalysis results, improved quantum algorithms, and other examples. Monitoring all those (future) advances is therefore of paramount importance and stresses the importance of preparing for migration to quantum-resistant cryptographic systems.