Executive Summary

GRI quantum risk assessment report – resource estimation update

February 2021

Cryptography fundamentally impacts every aspect of human life. It underpins the security and availability of systems upon which we rely deeply. These include communication systems, digital identity, internet of things, financial systems, and so on. Today's cryptographic algorithms fall into three categories: public key (asymmetric) systems, private key (symmetric) systems, and cryptographic hash functions. Public key systems are used to establish secret keys between two remote participants that are only allowed to communicate over a public channel (i.e., a channel that can be listened to). Public key cryptography is also used to establish digital signature systems for authenticating the origin and integrity of information. Encryption algorithms, or ciphers (an instance of symmetric key systems) assume that a secret key is already shared between the participants (via, for example, the use of a public key scheme), and are used for fast encryption and decryption of data using the shared secret key. Finally, cryptographic hash functions are so called "one-way functions" from which one cannot efficiently recover the input by looking at the output - a main ingredient of digital identity schemes such as digital signatures.

Quantum computers offer another means to attack the above schemes. In this study we update our previous security estimates considering new developments in the theory of quantum algorithms, quantum error correction, and quantum circuit optimization. We consider public-key systems such as RSA, as well as the AES family of symmetric ciphers and the SHA hash functions. All those schemes are widely deployed today and are heavily used in most of today's cryptographic infrastructure.

Since our previous report was published in April 2020, experimental and theoretical progress has been incremental, with no significant breakthroughs. Hence, our current estimates do not differ dramatically when compared to our previous report - the most significant developments outlined below.

The currently deployed public key schemes, such as RSA and ECC, are completely broken by Shor's algorithm, whereas the security parameters of symmetric schemes and hash functions are reduced by, at most, a factor of two by the known attacks - by "brute force" searches using the Grover's searching algorithm. All those algorithms require large scale, fault-tolerant, quantum machines, which are not yet available. Most of the expert community agree that they will likely become a reality within 10 to 20 years, as highlighted in [Dr. Michele Mosca and Dr. Marco Piani, "*Quantum Threat Timeline Report*", GRI Jan. 2021, https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/].

Nevertheless, the risk must be mitigated today due to *harvest-now-and-decrypt-later* attacks which record encrypted documents in the present with intent to decrypt them in the future once a quantum computer is available. Furthermore, it takes many years to migrate systems to new cryptography designed to protect against quantum attacks.

Two key factors influence the precise time at which our current systems will be vulnerable to systemic quantum attack: firstly, how large a quantum computation must be to successfully break these systems and, secondly, how soon the required resources will be available.

Estimating the strength of current cryptographic schemes against realistic quantum attacks is a moving target that depends on a variety of factors; fault-tolerant quantum error correction, circuit optimization and compilation, novel cryptanalysis results, improved quantum algorithms, and so on. Monitoring ongoing advances in this broad range of research is therefore of paramount importance in assessing the urgency to migrate to quantum-resistant cryptographic systems.

For public-key cryptographic schemes, most progress was related to improving controlled modular adders in the quantum circuitry for attacking RSA with Shor's algorithm. Those contributed to a reduction in quantum resources by a factor of approximately five. So, for example, it will take a quantum computer 20 minutes to break RSA-2048, as opposed to the previous estimate of almost an hour and a half, assuming a more realistic physical error rate of one in 1000. The RSA optimization techniques that we used are not directly applicable to elliptic curve cryptographic systems, therefore we did not update our estimates for the latter.

For the AES family of ciphers and the SHA hash functions, novel dynamic programming techniques can reduce the complexity of their corresponding quantum circuits, resulting in an overall reduction of the AES security by two to three bits and hash functions by one to two bits. For example, the cost of attacking AES-256 under an optimistic physical error rate of one in 100,000 shows a security reduction from 166 bits (old estimates) to 164 bits (current estimates) since our last report. Similarly, under the same conservative physical error rates, the SHA-256 hash function showcases a one-bit reduction in security, from 166 bits to 165 bits.

Over the past three years, the security parameter estimates have gradually declined, but thus far at a rate that is not cause for alarm if using the stronger versions of AES and SHA. For example, if we use the average decline over the past three years, we can extrapolate that AES-256 will reach 152 bits of security by 2031, and SHA-256 by 2052, assuming a more optimistic physical error rate of one in 10,000 for both. On the other hand, if using “only” AES-128, at the current rate of decline, we would reach only 80 bits of security by 2031. We highlight that there is no certainty that the current rates of decline will continue, and that 2^{80} quantum surface code cycles still represent an immense amount of computation. Nonetheless, *assuming a steady degradation of security*, AES-256 provides more than sufficient security against the *known* attacks.

Still in the early days of quantum computing and the development of quantum algorithms, we are most worried about an algorithmic breakthrough that could drastically reduce the number of operations needed to break AES or SHA. In 2017, colleagues from China [Chen, Y.A., Gao, X.S., "*Quantum Algorithms for Boolean Equation Solving and Quantum Algebraic Attack on Cryptosystems*", arXiv:1712.06239] outlined a novel approach for attacking AES using quantum linear equation solvers. However, the cost of implementing the quantum algorithm remained unclear. One interesting development we highlight in this report, is evidence that the proposed quantum linear solver-based algorithms against symmetric ciphers are very unlikely to break AES using a faster-than-classical quantum algorithm for solving linear systems of equations. These conclusions are based on very recent work with our collaborators [Ding, J., Gheorghiu, V., Gilyén, A., Hallgren, S., Li, J., *"Limitations of the Macaulay matrix approach for using the HHL algorithm to solve multivariate polynomial systems"*, 24th Annual Conference on Quantum Information Processing (QIP) (2021)].

In summary, during the past year we have seen incremental improvements in quantum attacks on some of today's cryptography. We have also developed a better understanding of the effectiveness of one potential disruptive method and, fortunately, the findings strongly suggest that this approach will not be a threat to AES encryption. We must, of course, continue to monitor quantum cryptanalysis developments that could (1) drastically reduce the security of cryptographic algorithms believed to be resistant to quantum attacks, and (2) rapidly accelerate the compromise of algorithms known to be vulnerable to quantum attacks.