Simon's Algorithm as a Cryptanalytic Benchmark

Csaba Czabán[1,3] **András Gilyén**[2] **and Zoltán Zimborás**[3,4]

[1] *Eötvös Loránd University, Faculty of Informatics, Budapest, Hungary*
[2] *HUN-REN Alfréd Rényi Institute of Mathematics, Budapest, Hungary*
[3] *HUN-REN Wigner Research Centre for Physics, Budapest, Hungary*
[4] *University of Helsinki, Faculty of Science, Department of Physics, Helsinki, Finland*

As we further advance into the Fault-Tolerant Quantum Computing (FQTC) regime from the current Noisy Intermediate-Scale Quantum era, concerns over the security of existing cryptographic systems grow. Notably, Shor's algorithm, which can efficiently factor large integers and thus compromise RSA encryption, remains impractical on current quantum hardware [1]. Nonetheless, organizations still require reliable estimates of when the quantum threat becomes tangible to plan appropriately. To mitigate threats such as "Harvest Now, Decrypt Later" attacks, organizations should begin transitioning to post-quantum solutions in a timely yet measured manner—early enough to stay ahead of the threat, but not too soon, as a rushed transition might introduce new vulnerabilities in the process [2]. This makes it crucial to develop clear, practical benchmarks that track quantum computing progress toward breaking existing cryptographic standards, enabling informed and secure migration strategies.

To address this, we propose a benchmark based on Simon's algorithm, the precursor of Shor's algorithm, that has the potential to already demonstrate quantum advantage in the early fault-tolerant regime and shares structural similarities with period-finding tasks critical to cryptanalysis. The proposed benchmark quantifies the largest input size for which quantum execution followed by classical post-processing is more efficient than the best possible classical method for solving the black-box Simon's problem in the average case. The benchmark is also feasible to implement, as we can omit the classical post-processing and evaluate the benchmark score according to the empirical success probability of a single execution of Simon's circuit.

This metric provides a meaningful and interpretable measure of the crypto-breaking capabilities of quantum computers, enabling both quantum computing experts and classical cryptanalysts to assess their potential impact on cryptographic systems. Importantly, the benchmark score serves as an upper bound on the number of bits for which Shor's algorithm could feasibly break RSA, given current quantum hardware and post-processing capabilities. We demonstrate the utility of this benchmark with experimental results obtained on devices from IBM, Quantinuum, Rigetti, IQM, and IonQ.

[1] X. Liu, H. Yang, and L. Yang, Security and Communication Networks 2023.1, 2963110 (2023). DOI:10.1155/2023/2963110.
[2] Global Risk Institute, Quantum Threat Timeline Report 2024, Glob. Risk Inst. (2024), https://info.quintessencelabs.com/hubfs/PDFs/Global-Risk-Institute-Quantum-Threat-Timeline-Report-2024.pdf [Jun. 2025].