Fast integer factorization on a smaller quantum computer

Bogdan Grechuk • 11 Feb 2026

In a paper recently accepted to *Forum of Mathematics, Pi* (Pilatte 2026), Pilatte proved the correctness of a recent quantum factoring algorithm that significantly reduces the quantum resources required compared to what was previously known.

One of the major technological open questions of our time is whether it is possible to build a full-scale, fault-tolerant quantum computer. Rather than giving a formal definition, let us provide some informal intuition. In a classical computer, memory consists of *bits*, each of which is definitely either 0 or 1. In contrast, the basic memory units of a quantum computer are *qubits*. A qubit can exist in a special "in-between" state called a *superposition*. Upon *measurement*, the qubit produces a classical outcome (0 or 1), with probabilities determined by its quantum state.

Qubits are manipulated by *quantum gates*, which are elementary operations acting on one or several qubits. These gates can modify the amplitudes of 0 and 1 in a superposition and can also create uniquely quantum correlations between qubits, known as *entanglement*. When qubits are entangled, their joint state cannot be described independently of one another.

A *quantum circuit* (or quantum program) is a sequence of quantum gates followed by measurements. Typically, one begins with a specified number of qubits in a simple initial state (often all 0), applies a sequence of gates—the computational phase—and then measures some of the qubits to obtain a classical output. Because measurement outcomes are probabilistic, the same circuit is usually executed many times in order to gather sufficient statistics for a reliable result.

It is known that, if large-scale quantum computers can be built, they will be able to efficiently solve certain problems for which no efficient classical algorithms are currently known. A celebrated example is the integer factorization problem. In 1994, Shor (Shor 1994) developed a polynomial-time quantum algorithm for factoring integers. More precisely, Shor showed that there exists a quantum

circuit with $O(n^2 \log n)$ quantum gates and $O(n \log n)$ qubits such that a classical randomized polynomial-time algorithm can factor n-bit integers with constant probability using a constant number of calls to this quantum circuit.

Shor's theorem has profound cryptographic implications. Much of modern public-key cryptography relies on the presumed difficulty of factoring large integers. In practice, cryptographic moduli consist of thousands of bits, so the $O(n^2 \log n)$ gate complexity in Shor's algorithm translates into millions (or more) quantum gates. Current quantum devices are far from being able to reliably execute circuits of this scale.

In 2025, Regev (Regev 2025) proposed a new variant of Shor's algorithm requiring only $O(n^{3/2} \log n)$ quantum gates, representing a substantial asymptotic improvement. However, this version used $O(n^{3/2})$ qubits and its correctness relied on an unproven number-theoretic conjecture. In 2026, Ragavan and Vaikuntanathan (Ragavan and Vaikuntanathan 2026) reduced the qubit complexity to $O(n \log n)$, matching that of Shor's original algorithm. Finally, Pilatte (Pilatte 2026) established a suitable version of Regev's conjecture and derived an unconditional variant of his algorithm.

Theorem 1 *There exists a quantum circuit with $O(n^{3/2} \log^3 n)$ quantum gates and $O(n \log^3 n)$ qubits with the following property. A classical randomized polynomial-time algorithm can solve the factoring problem*

Input: *A composite integer $N \leq 2^n$,*

Output: *A nontrivial divisor of N,*

using $O(\sqrt{n})$ calls to this quantum circuit, and succeeds with constant probability.

This result provides the first unconditional proof that integer factorization can be achieved with asymptotically fewer quantum gates than in Shor's original construction, while keeping the number of qubits nearly linear (up to polylogarithmic factors). It strengthens the theoretical evidence that large-scale quantum computers, if realized, would pose a concrete and scalable threat to classical cryptographic systems.

References

Pilatte, Cédric. 2026. "Unconditional Correctness of Recent Quantum Algorithms for Factoring and Computing Discrete Logarithms." *Forum Math. Pi* 14: Paper No. e5. https://doi.org/10.1017/fmp.2025.10023.

Ragavan, Seyoon, and Vinod Vaikuntanathan. 2026. “Space-Efficient and Noise-Robust Quantum Factoring.” *J. Cryptology* 39 (2): Paper No. 14. https://doi.org/10.1007/s00145-026-09572-x.

Regev, Oded. 2025. “An Efficient Quantum Factoring Algorithm.” *J. ACM* 72 (1): Art. 10, 13.

Shor, Peter W. 1994. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring.” *Proceedings of the 35th annual symposium on the Foundations of Computer Science*, 124–34.