International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 2
Article Received: *25 April 2026* ***Revised:*** *12 May 2026* ***Accepted:*** *30 June 2026*

An overview of Shor's Algorithm and Distributed Algorithms in Quantum Computing

Balaji Gowda. N

MS Ramaiah University of Applied Sciences Bengaluru, India balajigowda.n@gmail.co m

Avinash M

MS Ramaiah University of Applied Sciences Bengaluru, India avizenith.dev@gmail.co m

Gagan M

MS Ramaiah University of Applied Sciences Bengaluru, India gagan2004v@gmail.co m

Shanmuga Sundaram M

Department of Computer Applications MS Ramaiah University of Applied Sciences Bengaluru, India
shanmugasundaramm.cs.et@msruas.ac.in

Abstract—In this paper, we consider two of the most important paradigms in quantum computing, namely, Shor's algorithm used to perform integer factorisation and distributed quantum computing algorithms. The algorithm proposed by Peter Shor in 1994 is one of the most important achievements in quantum computing, as it allows for polynomial factorisation of large integers and thus compromises today's encryption algorithms. Distributed quantum computing solves the scalability problem by linking several quantum computation devices with each other using classical and quantum means of communication. The following review focuses on the state-of-the-art developments in quantum computing and applications of such algorithms to cryptography and scalability problems.

Keywords—Shor's algorithm, distributed quantum computing, quantum Fourier transformation, quantum gate teleportation, post-quantum cryptography.

I. INTRODUCTION

Quantum computing takes advantage of quantum mechanical properties like superposition, entanglement, and interference to accomplish computationally infeasible calculations with respect to

classical computation[1][2][3]. The two most significant topics in quantum computation include: (i) algorithms with quantum advantages in terms of exponential improvements over classical methods; and

(ii) quantum computing distributed systems to cope with hardware scaling problems.

The most illustrative application of the first issue is given by Shor's algorithm[4] that reduces the sub-exponential computational complexity of O(e^(log N)^(1/3)(log log N)^(2/3)) of integer factorization via classical computer technology to O((log N)^3) concerning the polynomial complexity via quantum computer technology. This enhancement has major consequences with regard to the security of RSA cryptographic systems.

The other issue is named distributed quantum computing (DQC) and deals with solving the implementation challenge of manufacturing monolithic quantum processors comprising millions of qubits. In these systems, a few quantum processor modules are interconnected via photonics interconnection [5].

II. SHOR'S ALGORITHM: MATHEMATICAL FOUNDATION

A. Problem Statement and Classical Reduction

Shor's algorithm factors a composite integer N by reducing the factorisation problem to period-finding[4]. Given N and a randomly chosen a where 1

< a < N and gcd(a, N) = 1, the algorithm finds the period r of the modular exponential function:

$$f(x) = a^x \bmod N \quad (1)$$

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 14 Issue: 2
***Article Received:** 25 April 2026 **Revised:** 12 May 2026 **Accepted:** 30 June 2026*

where r is the smallest positive integer such that:

$a^r \equiv 1 \pmod N$ (2)

Once the period r is determined, with high probability, gcd(a^(r/2) ± 1, N) yields a non-trivial factor of N, provided r is even and a^(r/2) ≢ -1 (mod N).

B. Quantum Period Finding

The quantum period-finding procedure consists of two primary quantum subroutines:

Quantum Phase Estimation (QPE): This circuit prepares a superposition state and performs modular exponentiation to encode the period in the phase of quantum states. The quantum circuit sends

$|0\rangle^{\otimes 2n}|\psi j\rangle$ to $|\phi j\rangle|\psi j\rangle$ such that the probability distribution:

$pk \equiv |\langle k|\phi j\rangle|^2$ (3)

is peaked around k = 2^(2n)j/r, with $p_{(2^{(2n)}j/r)} \geq 4/\pi^2 \approx 0.4053$.

Quantum Fourier Transform (QFT): The inverse QFT is used to convert the final quantum state from modular exponentiation to classical data that can reveal the period. The QFT for an n-qubit system is as follows:

$QFT|j\rangle = (1/\sqrt{2^n}) * \Sigma [e^{(2\pi ijk/2^n)} |k\rangle]$ (4)

The QFT can be implemented with O(n^2) quantum gates using controlled phase rotations and Hadamard gates.

C. Quantum Algorithm Workflow

- Initialise two quantum registers; one is initialised with 2n qubits in superposition and the other with n qubits in state $|1\rangle$.
- Use the unitary transformation $U|x\rangle|y\rangle = |x\rangle|a^x y \bmod N\rangle$ to induce an entangled state between both registers.
- Perform the inverse QFT on the first register.
- Measure the first register and record its value, denoted by m, satisfying the equation m/2^(2n) ≈ s/r where s < r.
- Extract the integer r using the continued fraction algorithm on the fraction m/2^(2n).
- Calculate the greatest common divisor (gcd(a^(r/2) ± 1, N)) to get the factors.

D. Complexity Analysis

An important breakthrough was achieved recently in 2023 by Regev that shows how to factorise n-bit integers with an implementation of the quantum algorithm using a circuit of O(n^(3/2)) gates repeated n+4 times.

Approach	Time Complexity	Space Complexity
Classical (General Number Field Sieve)	O(e^(log N)^(1/3)(log log N)^(2/3))	Polynomial
Shor's Algorithm (Quantum)	O((log N)^3)	O(log N) qubits
Regev's Variant (2023)	O(n^(3/2)) gates	O(log N) qubits

TABLE I. Complexity comparison of integer factorisation algorithms

III. CRYPTOGRAPHIC CONSEQUENCES

A. RSA Vulnerability

The security provided by RSA encryption is based on the difficulty of determining the factors of the product of two large primes. The current RSA scheme employs 2048-bit or 4096-bit key pairs. The application of Shor's algorithm in an appropriately powerful fault-tolerant quantum computer would break the RSA algorithm[5][6].

RSA Key Size	Classical Security	Quantum Vulnerability
1024-bit	Moderate (breakable)	High
2048-bit	Strong (current standard)	High
4096-bit	Very Strong	High

TABLE II. RSA security levels against classical and quantum attacks

B. Post-Quantum Cryptography

The danger of Shor's algorithm led to an investigation into post-quantum cryptography algorithms that rely on problems that are believed to be difficult even for quantum computers, such as:

- Lattice-based cryptography (including NTRU, LWE)
- Code-based cryptography (McEliece)

- Polynomial multivariate cryptography
- Hash-based signatures (SPHINCS+)
- Isogeny-based cryptography

The National Institute of Standards and Technology (NIST) has been developing standards for post-quantum algorithms since 2016 in order to face the quantum computing age.

C. Beyond Factoring

The period-finding and QFT techniques in Shor's algorithm extend to other cryptographically relevant problems:

- Discrete logarithms: Breaking Diffie-Hellman key exchange
- Elliptic curve discrete logarithms: Attacking elliptic curve cryptography (ECC)
- Principal ideal problem: Relevant to certain lattice-based schemes

IV. DISTRIBUTED QUANTUM COMPUTING

A. Motivation and Architecture

The scalability challenge in quantum computing arises from increasing qubit counts, maintaining coherence, implementing error correction, and achieving all-to-all connectivity. Monolithic quantum processors face engineering limitations as qubit numbers grow into the thousands or millions required for practical applications[8].

The distributed quantum computing architecture addresses these challenges by:

- Partitioning computations across multiple quantum processing modules
- Interconnecting modules via photonic networks and classical communication channels
- Maintaining reduced complexity within individual modules
- Scaling through adding modules rather than increasing module size

B. Key Technologies

Quantum Gate Teleportation (QGT): Entanglement between the matter qubits remotely connected within the network leads to all-to-all connectivity by means of quantum gate teleportation. The quantum operations can be performed non-locally in the case of remote matter qubits without any physical link connecting the qubits[7].

Two qubits $|\psi\rangle A$ and $|\psi\rangle B$, which share an entangled pair in different modules, may interact under the two-qubit gate operation expressed by the following relation:

$$U_{AB}|\psi\rangle A|\psi\rangle B = \text{Local operations} + \text{Bell measurement} + \text{Classical communication} \quad (5)$$

Optical Interconnects: Optical fibre is capable of offering flexible and reconfigurable interconnect layers within the photonic network system.

C. Recent Experimental Demonstrations

The first example of real-world distributed quantum computing took place in February 2025, when researchers from Oxford University managed to link two individual trapped-ion quantum computers with the help of photonic networks. Important milestones that have been achieved during the research include:

- Grover's algorithm applied in distributed modules
- Qubit quantum gate teleportation in distributed quantum computers
- Preservation of quantum coherence in distributed calculations
- Fault tolerance in distributed quantum computation

Such results confirm the efficiency of a distributed approach to quantum computing.

D. Distributed Quantum Algorithms

Distributed Counting Algorithm: In one such example, a newly proposed distributed quantum algorithm can solve counting problems via the use of the Grover operator alongside classical post-processing. Such applications involve estimation of inner products among quantum states, computation of Hamming distance, and data similarity comparisons. The algorithm offers a significant reduction in circuit depth and quantum gates relative to a monolithic approach and is suitable for NISQ platforms[9][10].

Distributed Quantum Architecture Search: Variational quantum algorithms are enabled by automated

optimization of circuit structures. A distributed quantum architecture search platform optimizes parameterized quantum circuits running on interconnected quantum processing units with restricted qubit connectivity.

V. COMPARATIVE ANALYSIS

A. Algorithm Complexity

Algorithm	Problem	Classical Complexity	Quantum Complexity
Shor's	Integer factorization	O(e^((log N)^(1/3)))	O((log N)^3)
Grover's	Unstructured search	O(N)	O(√N)
QFT	Fourier transform	O(N log N)	O((log N)^2)
Element distinctness	Find duplicates	O(N)	O(N^(1/3))

TABLE III. Quantum speedups for selected algorithms

B. Hardware Requirements

Task	Qubits Required	Gate Depth	Architecture
Factor 2048-bit RSA	~4000-6000	10^9 - 10^12	Fault-tolerant
Grover on 2^20 items	~20-40	2^10	NISQ-compatible
Distributed VQE	50-100	10^3 - 10^4	Networked modules

TABLE IV. Hardware requirements for quantum algorithms

VI. CURRENT LIMITATIONS AND FUTURE DIRECTIONS

A. Hardware Issues

- Qubit fidelity: Today's physical qubits have error rates of 10^-3 to 10^-4, while fault-tolerant operations require 10^-15.
- Times of coherence: Only possible in the microseconds to milliseconds range, restricting circuit depth.
- Qubit connectivity: Engineering limitations restrict qubit interaction capabilities.
- Scalability: Creating a system with millions of qubits is a difficult problem.

B. Algorithmic Research Areas

- Resource optimisation for implementations of Shor's algorithm.
- Hybrid quantum and classical algorithms for NISQ technologies.
- Optimising distributed quantum algorithms for network topologies.
- Exploring quantum advantage in optimisation and machine learning.

C. Distributed System Advances

Recent research focuses on efficient entanglement distribution protocols, quantum network routing algorithms, error mitigation in distributed computations, and integration with classical high-performance computing infrastructure. IBM's quantum computing roadmap emphasizes networked quantum computers as essential for scaling beyond single-processor limitations, with research initiatives targeting modular quantum systems.

VII. CONCLUSION

The Shor's algorithm is one such example that shows how disruptive quantum computing can be, especially in cryptanalysis. Turning integer factorisation into polynomial time complexity using quantum period finding and quantum Fourier transform breaks the security assumptions of conventional public key cryptography systems. Although a fully functional implementation would require fault-tolerant quantum computers with thousands of logical qubits, this algorithm has been the driving force behind the creation of post-quantum cryptographic schemes.

Another practical approach to creating scalable quantum

computing is to build quantum computing systems in a distributed fashion. This involves connecting several quantum processing units via photonic interconnects. Recent experiments at Oxford University in 2025 have proven the feasibility of this approach. It not only allows quantum gate teleportation but also ensures all-to-all logical connectivity between all the modules of quantum computing.

REFERENCES

[1] Peter W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124–134, doi: 10.1109/SFCS.1994.365700.

[2] Peter W. Shor, "Polynomial-time algorithms for prime factorisation and discrete logarithms on a quantum computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, Oct. 1997, doi:10.1137/S0097539795293172.

[3] Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information. Cambridge, U.K.: Cambridge University Press, 2010.

[4] Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," Reviews of Modern Physics, vol. 68, no. 3, pp. 733–753, 1996.

[5] Anocha Yimsiriwattana and Samuel J. Lomonaco Jr., "Distributed quantum computing: A distributed Shor algorithm," arXiv preprint quant-ph/0403146, 2004.

[6] Lieven M. K. Vandersypen et al., "Experimental realisation of Shor's quantum factoring algorithm using nuclear magnetic resonance," Nature, vol. 414, no. 6866, pp. 883–887, 2001.

[7] Stephen P. Jordan and Yi-Kai Liu, "Quantum cryptanalysis: Shor, Grover, and Beyond," IEEE Security & Privacy, vol. 16, no. 5, pp. 68–71, 2018.

[8] David Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," Proceedings of the Royal Society A, vol. 400, no. 1818,pp. 97–117, 1985.

[9] Daniel Gottesman, "An introduction to quantum error correction and fault-tolerant quantum computation," in Proceedings of Symposia in Applied Mathematics, vol. 68, pp. 13–58, 2010. (Useful for distributed quantum systems.)

[10] Enrique Martín-López et al., "Experimental realization of Shor's quantum factoring algorithm using qubit recycling," Nature Photonics, vol. 6, no. 11, pp. 773–776, 2012.