INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND INNOVATIVE STUDIES
IJSRIS journal
ISSN: 2820-7157
Advancing Knowledge, Inspiring Innovation
www.ijsrisjournal.com
INDEXED JOURNAL
PEER REVIEWED Rigorous & Transparent
DOI: CROSSREF Member
OPEN ACCESS For Global Visibility
BI-MONTHLY Timely Publication
WIDE READERSHIP High Impact & Visibility
AUTHOR FRIENDLY Fast | Supportive | Reliable
RECEIVED 17 September
ACCEPTED 09 October
PUBLISHED 1 November 2026
September 2026
Volume 5
Number 6
Pages from 432 to 442

Quantum Computing: A Critical Analysis, Numerical Validation of Grover's Algorithm, and Prospects for Academic Adoption in the DRC

Blaise KAPALALA KAPENDA[1], Hervé KINKETE MFUMABI[2], Patrick KUNGUDI[3], Prof. Dr. Richard KITONDUA LUBANZADIO[4]

1 Department of Computer Science, Institut Supérieur Pédagogique de la Gombe, Kinshasa, Democratic Republic of the Congo, blaisekapalala94@gmail.com

2 Artificial Intelligence and Data Governance, William Booth University, Kinshasa, Democratic Republic of the Congo, hervekinkete@gmail.com

3 Artificial Intelligence (Deep Learning and Data Governance), National Pedagogical University, Kinshasa, Democratic Republic of the Congo, irpatrick2015@gmail.com

4 Faculty of Science and Technology, Department of Mathematics and Computer Science, National Pedagogical University, Kinshasa, Democratic Republic of the Congo, richardkitondua@gmail.com

LICENSE
This article is licensed under the Creative Commons Attribution 4.0 International License (CC BY 4.0).
https://creativecommons.org/licenses/by/4.0/
Crossref doi
PREFIX : 10.63883
IJSRIS JOURNAL
OPEN ACCESS
This is an open access article distributed under the terms of open access.

ABSTRACT

This study examines the foundations, performance claims, and conditions of use of quantum computing through a critical analysis of 19 scientific and standards references, combined with numerical validation of Grover's algorithm. An evaluation framework compares theoretical guarantees, experimental evidence, computational costs, and operational relevance. The experiment, executed and rerun in Python/NumPy, covers four unstructured search spaces (N = 16, 64, 256, and 1,024) and 20,000 simulated measurements.

Observed success rates are 95.88%, 99.58%, 100.00%, and 99.90%; the analytical probabilities fall within the 95% confidence intervals. At N = 1,024, classical sequential search required an average of 509.06 queries, compared to 25 idealized Grover

Iterations or an estimated 26.03 oracle-level calls per verified success under the stated assumptions. A second run using the same random seed reproduced all 20,000 observations and the associated statistics.

These findings validate the numerical implementation against Grover's theoretical behavior and demonstrate reproducibility, without measuring runtime on physical quantum hardware. The contribution consists of an evidence-based assessment framework tested in this experiment and an operational framework for assessing university readiness in the Democratic Republic of the Congo.

Keywords: quantum computing; Grover search; state-vector simulation; reproducible experiment; query complexity; critical review; post-quantum cryptography; DRC.

1. INTRODUCTION

1.1 Background and Rationale

Increases in classical computing power have enabled major advances in science and engineering. However, they do not eliminate the fundamental difficulties of certain tasks, particularly the study of physical systems with large state spaces. Feynman [1] highlighted the value of simulators that themselves rely on quantum laws; the conceptual and mathematical foundations were subsequently systematized in the seminal work of Nielsen and Chuang [2].

Quantum computing does not refer to a universally faster processor. It corresponds to a model for representing and manipulating information in which performance gains may exist for certain classes of problems. Preskill [3] showed that noisily implemented quantum computing (NISQ) constitutes a technological phase characterized by constraints related to coherence and error correction. The crux of the debate is therefore no longer merely what a quantum algorithm can achieve in theory, but at what cost and with what guarantees it can actually do so.

1.2 Problem Statement and Research Questions

The literature sometimes conflates mathematical results, experimental performance of specialized circuits, industrial roadmaps, and promises of applications. These categories are not interchangeable. Asymptotic acceleration can be offset by data preparation, the number of measurements, correction overhead, or the quality of a classical reference solver [3,6,7]. Therefore, how can we rigorously assess the current and future value of quantum computing, and what practical implications can we draw from this for educational and research institutions in the DRC?

Four questions guide this synthesis: (Q1) Which foundations and algorithms provide well-established theoretical guarantees? (Q2) What experimental results are available, and what are their limitations? (Q3) How can we distinguish between plausible, demonstrated, and operational advantages in applications? (Q4) What institutional actions are feasible in the DRC without assuming pre-existing capabilities?

1.3. Objectives and Contribution

The objective is to assess the scientific scope of the main quantum algorithms, to experimentally verify a mechanism for query gain, and to structure the conditions for academic adoption. The study addresses four specific objectives: analyzing levels of evidence, clarifying comparison criteria, numerically validating Grover's algorithm across multiple search sizes, and developing institutional evaluation indicators applicable to Congolese higher education.

Three key contributions form the basis of this research. The first is a cross-cutting framework combining level of evidence, oracle definition, resources utilized, classical reference, and transferability. The second is an original experiment involving 20,000 simulated measurements, accompanied by data, executable code, and an analytical and reproducible verification. The third is a four-dimensional framework for academic adoption, accompanied by indicators and an evaluation questionnaire. The originality lies in the integration of comparative analysis, numerical validation, and pedagogical application, rather than in the proposal of a new algorithm.

2. METHODOLOGY

2.1 Nature and Scope of the Study

The research combines a critical literature review with a controlled numerical experiment. The corpus comprises 19 references selected for their contributions to mathematical foundations, algorithms, hardware technologies, quantum machine learning, and cybersecurity standards [1–19]. The literature review is organized by scientific problems and levels of evidence, while the experimental study tests Grover's analytical predictions across four instance sizes.

The rationale for selection prioritizes seminal works, reviews with significant methodological scope, published experimental demonstrations, and official standards. Each major technical proposal is linked to its sources, assumptions, and conditions of validity. Editorial notes, DOIs, and institutional documents were used to verify bibliographic metadata and cited results. The analysis then compares the

claimed benefits with implementation limitations and relevant conventional comparators.

2.2 Areas of Analysis and Criteria

The analysis examines five categories: mathematical foundations, algorithms, hardware and logical computation, hybrid applications and artificial intelligence, and cybersecurity. Each claim is evaluated based on the distinction between (a) a proven theoretical result, (b) a numerical simulation, (c) a physical demonstration under circumscribed conditions, and (d) an operational benefit measured against a real-world problem.

Table 1: Explicit criteria used for the critical review of results. Summary grid proposed by the article.

Criteria	Verifiable Questions	Elements to Look For
Scope	What task and what sample size?	Formalized problem; data; assumptions; metric
Level of foresight	Theorem, simulation, experiment, or deployment?	Nature and scope of results; reproducibility
Standard reference	To which classical method is the comparison made?	Documented solver, optimization, and classical hardware
End-to-end cost	Does the advantage hold up after accounting for auxiliary operations?	Encoding, compilation, measurements, correction, energy, and time
Transferability	Are the results reproducible and scalable?	Noise, robustness, scalability, expertise, and costs

2.3 Validity Checks and Scope of the Analysis

The validity of the numerical study is verified by four tests: conservation of the state vector norm, agreement between theoretical and calculated probabilities, consistency of success rates with binomial intervals, and deterministic replication of outputs with a fixed seed. The simulation is performed on a classical computer starting from an ideal quantum state. The scope of the results therefore includes the probabilities, iterations, and query costs of the oracle model. The institutional framework is treated as an evaluation system operationalized through indicators; field responses constitute a data category distinct from the numerical simulations.

2.4 Experimental Protocol, Assumptions, and Reproducibility

Problem studied: searching for a single tagged solution in an unstructured set of $N = 2^n$ elements ($n = 4, 6, 8, 10$). Grover's oracle changes the sign of the amplitude of the tagged element $x = 0$; the diffuser applies the transformation $2|s\rangle\langle s| - I$ around the uniform superposition. The idealized circuits are represented by N-dimensional amplitude vectors stored in the classical computer's memory. The normalization condition and the theoretical probability are verified numerically [2,5].

For each size N, the angle is $\theta = \arcsin(1/\sqrt{N})$ and the number of iterations used is $r = \text{round}[\pi/(4\theta) - 1/2]$. The analytical probability of success is $p(N,r) = \sin^2[(2r + 1)\theta]$. The simulator calculates a state vector, then 5,000 independent measurements following Born's rule per configuration, for a total of 20,000 numerical observations. The rates are analyzed using 95% Wilson binomial intervals. Seed 20261117 allows the simulations to be reproduced exactly. The script, measurement details, and metadata are included with the article.

For classical unstructured search, the sought-after element is assumed to be uniformly distributed across N positions; the theoretical average number of queries is $(N + 1)/2$. For Grover's algorithm, the primary metric is the number r of phase oracle calls. Taking into account a final verification and retries when a measurement fails yields the estimated cost per success, observed as $(r + 1)/p$. The comparison provides insight into query complexity under explicit assumptions; execution times and the resources of physical hardware constitute other metrics [5].

3. FOUNDATIONS AND SCOPE OF QUANTUM ACCELERATION

3.1 Qubit, Superposition, Entanglement, and Measurement

A qubit in a pure state is written as $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. The amplitudes α and β are complex; their relative phase contributes to interference. During a measurement in the computational basis, the result is either 0 or 1, with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively. This notation should not lead one to believe that a single measurement would simultaneously yield all possible values; the algorithmic construction relies on coherent transformations rather than an unlimited readout of possibilities [2].

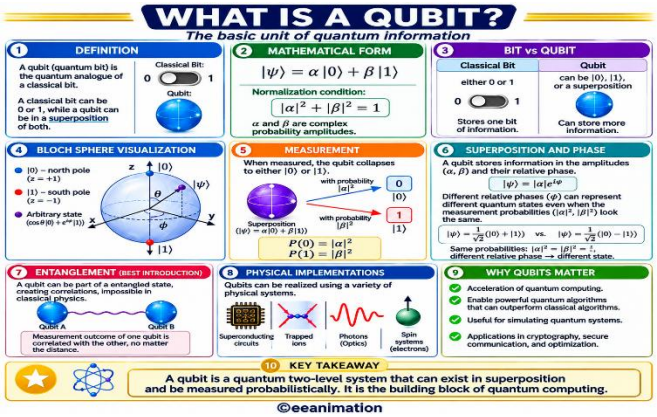


Figure 1: Bit to Qubit

For multiple qubits, the state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ illustrates entanglement: it cannot be factored into a product of two independent pure states. The correlation between measurement results is not, on its own, a sufficient criterion for entanglement, since certain correlations can be produced classically. Furthermore, realistic physical states can be mixed and subject to decoherence [2,3].

3.2 Gates and the Physical Cost of Circuits

The ideal gates X, H, Z, and CNOT correspond to unitary transformations; measurement operations and noisy channels require a different formalism. The depth of a circuit, the number of two-qubit gates, the connection topology, and readout errors can have a greater impact on its success than a simple count of qubits [2,3]. A comparison must specify the machine's characteristics and how the circuit is compiled.

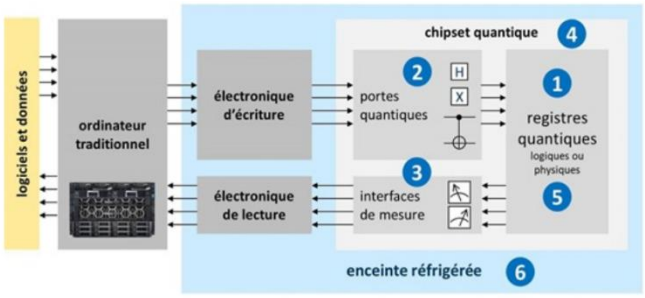


Figure 2: Quantum computer architecture

3.3 Shor: Strong Theoretical Guarantee, Considerable Physical Costs

Shor [4] demonstrates that a suitable universal quantum computer can solve integer factorization and the discrete logarithm in polynomial time, in contrast to the most efficient known classical algorithms for these tasks. The algorithmic proof is sound; however, it does not demonstrate the existence, to date, of a machine capable of breaking the corresponding industrial cryptographic systems on a large scale. Its practical implementation requires numerous reliable logical qubits, fault-tolerant operations, and a detailed assessment of resources [3,10].

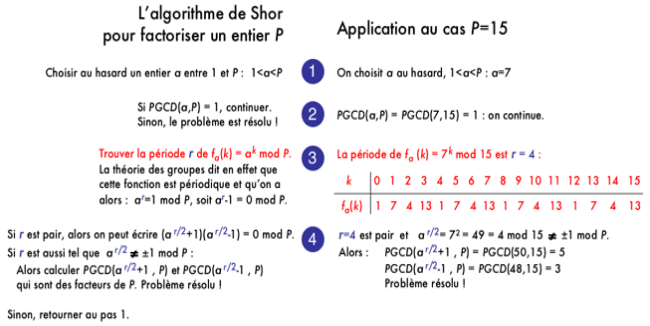


Figure 3: Shor's algorithm model

The implications pertain specifically to asymmetric cryptography based on these problems; they do not imply that all cryptographic mechanisms, particularly symmetric primitives, are affected in the same way [16–19].

3.4 Grover: Query Gain, Not Universal Database Acceleration

Grover [5] establishes, for an unstructured search and a suitable oracle, a complexity in terms of the number of calls of the order of $\sqrt{N}$, compared to the conventional order of N. The comparison must remain framed in terms of queries within an oracle model. The costs of preparing the superposition, constructing the oracle, managing noise, measuring, and accessing data determine whether a real-world time savings remains. A classical database with an index or relevant structure does not automatically correspond to the model under study [2,3,5].

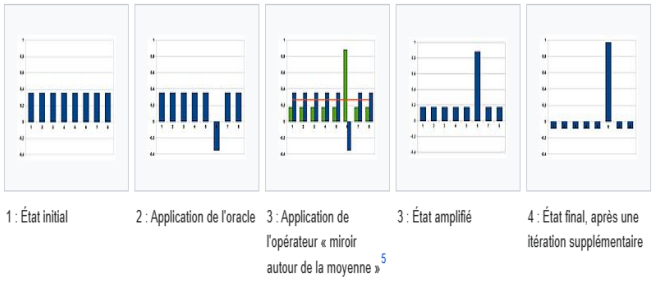


Figure 4: Quantum computing, Grover's algorithm: between myth and hope

3.5 Variational Algorithms: Promises with Conditions

Variational algorithms use parameterized circuits combined with classical optimization. For VQE, a fundamental expression is $E(\theta) = \langle\psi(\theta)|H|\psi(\theta)\rangle$, where H represents the Hamiltonian and θ represents the parameters to be adjusted.

QAOA applies a hybrid approach to combinatorial optimization problems. These techniques sometimes limit circuit depths, but their optimization can be compromised by noise, the number of measurements, local minima, or gradient plateaus ("barren plateaus") [6].

Their usefulness must be evaluated against appropriately parameterized classical computational chemistry and optimization solvers; a demonstration on a toy instance does not constitute proof of industrial effectiveness [6,7].

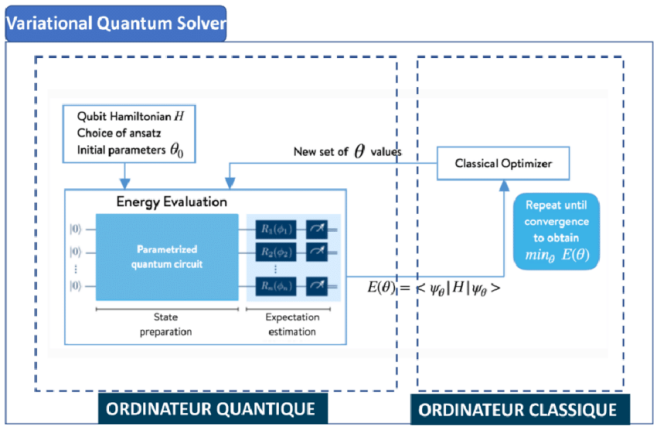


Figure 5: VQE algorithm from the class of hybrid algorithms using a variational method (Source: adapted from 1QBit)

4. COMPARATIVE ANALYSIS OF APPLICATIONS AND LEVELS OF PROOF

4.1 Critical Table of Algorithm Families

Table 2: Reasoned comparison; the assessments pertain to problem classes and do not constitute a definitive ranking.

Approach	What Is Established	Major Limitation	Conclusion of the Review
Shor	Theoretical speedup for factorization and discrete logarithm [4]	Logical qubits and large-scale error correction [3,10]	Mature theory; conditional operational impact
Grover	Quadratic gain in oracle queries [5]	Oracle, data access, and noise [2,3]	Theoretical proof; time savings to be demonstrated
VQE	Hybrid energy estimation framework [6]	Measurements, accuracy, training, classical comparison	Active search; advantage not generalized
QAOA	Variational circuits for certain optimization problems [6]	Instance dependence, depth, heuristics	Conditional potential and benchmark required
QML	Explored quantum learning models [13–15]	Encoding, training, baselines, generalization	No universal superiority demonstrated

4.2 Chemistry and Materials

Quantum chemistry is a conceptually motivated application, as the object of study is itself quantum in nature [1,2]. However, the evaluation of a result must compare useful chemical accuracy, the number of measurements, circuit cost, and the performance of appropriate classical approaches. A small-molecule simulation is a research step; without a comprehensive benchmark, it does not demonstrate superiority over established methods. Reviews of variational algorithms and quantum software specifically emphasize these constraints [6,7].

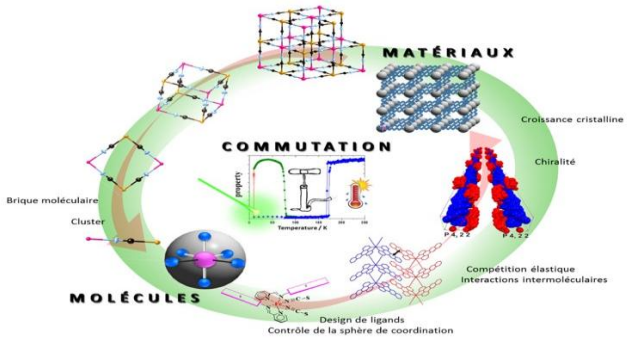


Figure 6: Diagram summarizing the molecular engineering activities developed at Gr6 ICMCB.

4.3 Resource Optimization

Scheduling, assignment, and transportation problems can be formalized in appropriate optimization models. However, reducing a problem to the format required by a quantum circuit, the choice of penalties, the use of auxiliary qubits, and the quality of the solution all influence the overall performance. QAOA should not be compared solely to exhaustive search: specialized heuristics, mathematical programming, and metaheuristic methods are necessary points of reference [6,7].

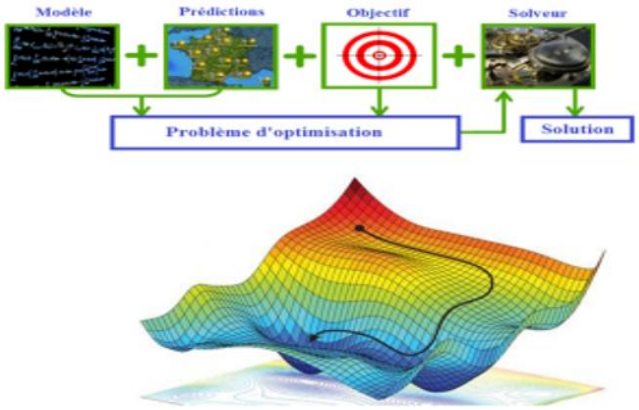


Figure 7: Stochastic optimization: an important tool for decision-making under uncertainty in industrial problems.

4.4 Quantum Machine Learning and AI for Quantum Computing

Two fields must be distinguished. The first, Quantum Machine Learning (QML), employs quantum circuits for certain representation or learning tasks. The second uses classical artificial intelligence to design, control, or correct quantum systems. Reviews by Wang and Liu [13], Peral-García et al. [14], and Devadas and Sowmya [15] describe the potential of QML as well as the challenges of data preparation and demonstrating a robust advantage. Alexeev et al. [11], for their part, examine the role of AI in the design and operation of quantum technologies.

Liao et al. [12] illustrate the use of classical learning to mitigate quantum errors; this result does not prove that quantum neural networks outperform their classical counterparts. QML evaluation protocols should specify the dataset, training split, test split, circuit depth, number of runs, hardware resources, stability, and an optimized classical baseline [11–15].

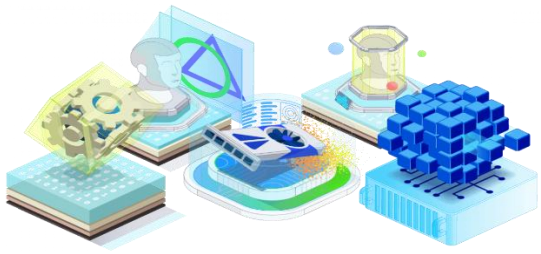


Figure 8: Quantum Machine Learning (QML)

4.5 Software, Reproducibility, and Engineering

Desdentado, Calero, Moraga, and García [7] map out quantum software solutions and their validation mechanisms. Their analysis highlights the importance of software and methodological criteria: a demonstration on specific hardware is not automatically replicable in another environment. This justifies publishing library versions, build scripts, data, and measurement parameters when experiments are conducted.

5. HARDWARE ARCHITECTURE, ERROR CORRECTION, AND RECENT RESULTS

5.1 Trade-offs Between Platforms

Superconducting circuits, trapped ions, photonics, neutral atoms, and spin qubits each involve different trade-offs in terms of fidelity, gate speed, connectivity, stability, experimental conditions, and integration potential. No single metric—such as the number of physical qubits—is sufficient on its own to rank these platforms [3,7,10].

Table 3: Qualitative comparison: device-specific performance, without a universal numerical ranking.

Platform	Frequently Studied Advantage	Limitations	Comparison Considerations
Superconductors	High-speed gates and circuit integration	Cryogenics, errors, wiring	Verify accuracy and topology
Trapped ions	Precise control and reconfigurable interactions	Throughput, scaling	Verify operation time and accuracy
Photonics	Optical information transport	Losses and probabilistic operations based on architectures	Document sources and detectors
Neutral atoms	Reconfigurable Networks	Control, Gates, and Correction	Compare with logical results
Solid-state spins	Potential for miniaturization	Uniformity, manufacturing, and consistency	Specify technology and material

5.2 Noise, Attenuation, and Error Correction

Decoherence and control errors prevent operations from being repeated indefinitely without a loss of reliability. Error attenuation uses measurement results and models to reduce certain estimation biases without, on its own, generating corrected logical information [12]. Error correction, on the other hand, encodes information across multiple physical qubits and relies on syndrome detection to protect the logical degrees of freedom. The complexity of these systems results in costs in terms of qubits, gates, time, and control electronics [3,8,10].

5.3 Experimental Progress in Logical Computation

The results from Google Quantum AI and collaborators [8] characterize the reduction in logical errors as the surface code distance increases within the studied device. Zhou, Cain, and Lukin [10] analyze "full-stack" architectures and design choices aimed at containing the additional cost of fault-tolerant computing. These contributions are complementary: one reports a physical measure of error correction, while the other examines the architectural conditions for scaling.

In January 2026, Butt and colleagues [9] presented an experimental demonstration of universal logical operations without intermediate measurements on a trapped-ion processor. Their device notably uses an error-detection code of eight physical qubits for three logical qubits and executes a small instance of Grover's search. The result establishes the experimental feasibility of the described set of logical operations and its algorithmic use in this device. It documents progress in logical computation, whose scale and resources are explicitly defined.

This work highlights three complementary levels of implementation: physical information protection, logical operations, and the execution of algorithmic circuits. Comparing these levels allows us to characterize the hardware's progress without attributing the performance of large-scale operational processing to a small-scale logical demonstration [8–10].

6. CYBERSECURITY AND THE POST-QUANTUM TRANSITION

6.1 Cryptanalytic Threat and Conceptual Distinction

The prospect of fault-tolerant quantum computers may eventually compromise certain asymmetric schemes based on factorization or the discrete logarithm [4]. Post-quantum cryptography, however, consists primarily of classical encryption, key exchange, and signature algorithms designed to withstand known quantum attacks. It differs from quantum cryptography, which uses quantum physical properties for communication protocols [16–19].

6.2 NIST Standards and the October 2026 Update

The FIPS 203, FIPS 204, and FIPS 205 standards, published in 2024, define ML-KEM for key encapsulation, ML-DSA for digital signatures, and SLH-DSA for hash-based signatures, respectively [16–18]. The final NIST IR 8547 report, published on October 27, 2026, outlines the transition from vulnerable algorithms to post-quantum mechanisms and provides a reference framework for the systems concerned [19]. Provisions specific to the United States should not be presented as legally binding in the DRC: their value lies in the technical approach and migration governance.

Table 4: Verified normative references; operational choices require a compatibility and risk analysis.

References	Subjects	Institutional Implications
FIPS 203 [16]	ML-KEM: Key Encapsulation	Inventory and test key establishment mechanisms
FIPS 204 [17]	ML-DSA: Digital Signatures	Examine certificates, chains of trust, and signatures
FIPS 205 [18]	SLH-DSA: hash-based signatures	Compare size and integration constraints
NIST IR 8547 (2026) [19]	Post-Quantum Transition Framework	Planning a Risk-Driven Migration

6.3 Implications for Organizations

Information intended to remain confidential for long periods warrants special attention to the "collect today, decrypt later" scenario. The first steps involve taking stock of the uses of asymmetric cryptography, protection periods, vendors, certificates, software libraries, and interoperability dependencies. A controlled migration—gradually tested and supported by cryptographic agility—is preferable to an unplanned replacement [19].

7. DISCUSSION: CONDITIONS FOR A SCIENTIFICALLY ACCEPTABLE BENEFIT

7.1 An Explicit Typology of Proof

This review distinguishes four levels that are not mechanically ranked. N1—theoretical guarantee in an abstract model; N2—reproducible simulation; N3—experimental demonstration on identified hardware; N4—robust operational benefit, verified against a high-quality conventional alternative, according to predefined metrics. An N3 result may be technically remarkable without meeting the N4 criteria. Conversely, an N1 theory may be foundational despite the absence of a machine capable of executing it at the desired scale [3–10].



Figure 9: Verification chain for a claim of a quantum advantage. Conceptual diagram developed for this study

7.2 Classical References and Full Cost

The requirement to compare results with classical methods is crucial. In factorization, the computational model, the size of the numbers, and the logical resources are essential; in search, access to data and the oracle model must be specified; in optimization, the best known heuristics and exact solvers must be used; in QML, the same data, training budget, and statistical criteria must be maintained [4–7,13–15].

The experimental comparison is based on a traceability sheet that includes the instance size, the data access model, the code, the software versions, the metrics, the sampling protocol, and the classical reference. In Grover's experiment, this information allows for a quantitative comparison of the probability of success and the number of queries, and then for separating the mathematical properties of the algorithm from the resources consumed by its classical simulator.

7.3 Review of the Literature

Table 5: Critical review of contributions and unjustified inferences to avoid.

Set of Sources	Documented Contribution	What the review cannot infer from this
Shor [4], Grover [5]	Mathematical accelerations for circumscribed problems	Superiority over any classical computation
Cerezo et al. [6], Desdentado et al. [7]	Challenges of variational methods and quantum software	Uniform maturity in industrial applications
Google [8], Butt et al. [9]	Physical results on correction/logical operations	A large-scale industrial universal machine
Alexeev et al. [11], Liao et al. [12]	Contributions of AI to error control and mitigation	A general advantage of QML models
Wang and Liu [13], Peral-García et al. [14]	Overview and limitations of quantum learning	Demonstrated acceleration on ordinary data
NIST Standards [16–19]	Mechanisms and approach for cryptographic transition	An automatic legal obligation outside the intended context

7.4 Numerical Experimental Validation of Grover's Algorithm

The numerical experiment was run using Python/NumPy and then reproduced in a second run with the same seed. Both runs produced the same 20,000 trials and the same summary statistics, excluding computation time, which varies by run. For N = 16, 64, 256, and 1,024, the norm of each state vector is equal to 1 at the displayed numerical precision, and the absolute difference between the analytical probability and the calculated probability remains less than 10^{-10}. The results in Table 6 include the four success rates, the confidence intervals, and the query costs.

Table 6: Results for the four configurations: 5,000 simulated measurements per size, seed 20261117. *Estimated cost (r + 1)/p observed with one-trial verification in the oracle model.

N	Grover r	Classic avg.	Success	95% CI	Grover/success*
16	3	8.49	95.88%	[95.29; 96.40] %	4.17
64	6	32.01	99.58%	[99.36; 99.73] %	7.03
256	12	129.52	100.00 %	[99.92; 100.00] %	13.00
1024	25	509.06	99.90%	[99.77; 99.96] %	26.03

The measured success rates are 95.88% for N = 16 (theoretical: 96.1319%), 99.58% for N = 64 (theoretical: 99.6586%), 100.00% for N = 256 (theoretical: 99.9947%), and 99.90% for N = 1,024 (theoretical: 99.9461%). In all four cases, the theoretical value falls within the 95% Wilson confidence interval. The absolute difference between the observed frequency and the theoretical prediction does not exceed 0.252 percentage points. The 5,000 successes in the case of N = 256 represent a sample frequency of 100%, without implying a theoretical probability exactly equal to 1.

The average number of queries to the classical comparator is 8.49, 32.01, 129.52, and 509.06, respectively. Depending on the chosen oracle model, Grover's estimated cost per verified success is 4.17, 7.03, 13.00, and 26.03 queries. The observed classical averages remain consistent with the expected values of (N + 1)/2: their absolute standardized deviations are all less than 1.9. These observations validate the protocol's behavior in its query model. The CPU resources of the classical simulator, the cost of physically implementing the oracle, and access to external data are the subject of a separate performance analysis.

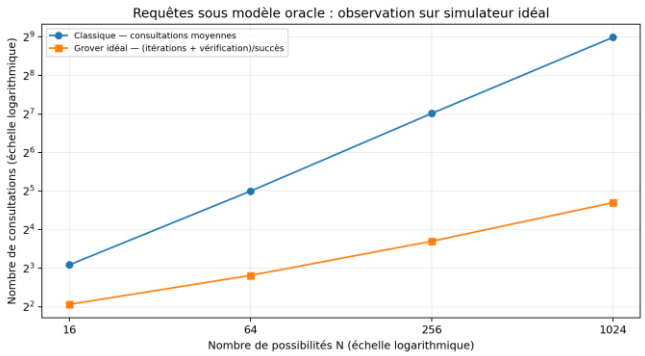


Figure 10: Evolution of the number of queries as a function of the size of the search space in the analyzed models (logarithmic axes). Data from the numerical experiment.

7.5 Verification of the Evaluation Grid Against Experimental Results

Applying the evaluation grid to the Grover case validates its ability to characterize the scope of an experimental result: (i) the problem and the oracle are formalized; (ii) the classical comparator is explicit; (iii) the probabilities are verified analytically; (iv) the experiment is reproducible; (v) costs and transfer conditions are distinguished. This internal verification establishes the consistency of the criteria for the case studied. A comparative analysis of Sections 4 through 6 extends their application to other families of algorithms without attributing the simulation results to them.

Table 7: Verification of the analysis framework for Grover's protocol and delineation of results.

Evaluated Dimension	Result Verified in the Protocol	Verification
Problem and metric	Marked solution, size N, and defined queries	Yes — 4 configurations
Replication of outputs	20,000 rows and identical statistical tables	Yes — second run
Agreement between theory and simulation	Normalization and probability deviation less than 10^{-10}	Yes — analytical verification
Measurements and uncertainty	Theoretical probabilities in Wilson's ICs	Yes — 4 configurations
Conventional comparator	Averages compatible with (N + 1)/2	Yes — explicit assumptions
Physical and institutional scope	Material costs and observations from separate institutions	Outside the numerical scope

7.6 Comparison of Results with the Literature

The agreement between the analytical calculation, the simulated state vectors, the stochastic measurements, and the program replication confirms that the implementation conforms to the mechanism described by Grover [5]. The study thus illustrates the quadratic advantage in queries at the oracle model level. The distinction between the operation of a classical simulator and that of a quantum processor remains essential for correctly interpreting performance. This finding aligns with Preskill's [3] characterization of NISQ systems and the methodological observations of Desdentado et al. [7].

The critical comparison also highlights a difference between the classes of algorithms: the asymptotic guarantees of Shor and Grover are based on precise mathematical models, whereas the performance of VQE, QAOA, and QML applications depends more on specific instances, computational budgets, and classical reference methods [4–7,13–15]. The hardware results from 2025–2026 reinforce the assessment of logical feasibility and fault tolerance [8–10]. The evaluation grid allows these proofs to be classified according to their subject matter and scope, without confusing them.

8. PROSPECTS FOR ADOPTION IN HIGHER EDUCATION IN THE DRC

8.1 Challenges of Integration into Higher Education

The pedagogical introduction to quantum computing can build on a sequence of accessible skills: linear algebra, probability, programming, simulation, and critical analysis of results [2,3,7]. Grover's digital experiment provides an example that has actually been executed on a classical computer with limited software dependencies. It demonstrates the technical feasibility of the lab exercise in this environment. Implementation at the university level then depends on the resources, expertise, and decisions specific to each institution.

8.2 Adoption Framework and Observable Variables

The adoption framework distinguishes four dimensions: D1, scientific and computational prerequisites; D2, instructional experimentation and reproducibility; D3, partnerships and scientific supervision; D4, usage assessment and cryptographic security. Each dimension is linked to observable indicators and concrete institutional actions (Table 8). Component D2 has technical proof of feasibility thanks to the execution of the Grover lab; the other dimensions structure the evaluation of institutions and the planning of their capabilities.

Table 8: Four-step institutional framework, actions, and evaluation indicators.

Proposed Step	Possible Action	Indicator to Collect	Risk to be assessed
1. Assessment	Identify courses, skills, and IT access	Prerequisites, equipment, and connection costs	Variability in resources
2. Training	Modules on linear algebra, probability, and circuits	Assessments of learning outcomes, number of lab sessions conducted	Curricular overload
3. Prototyping	Local Circuits and Conventional Comparisons	Code repositories, protocols, and reports	Confusion between simulation and material advantage
4. Consolidation	Partnerships, cybersecurity, review of practices	Agreements, projects, cryptographic inventory	Technical and budgetary dependence

8.3 Tool for Assessing University Capabilities

The pilot study provides educational support and a transferable technical protocol, including code, data, and consistency checks. To assess the conditions for adoption within an institution, the framework also includes institutional variables: access to equipment, faculty expertise, ability to replicate practical activities, collaborative networks, and cryptographic preparedness. These variables are directly linked to the four dimensions of the adoption matrix.

A 12-item questionnaire, included in Appendix A, operationalizes these dimensions on a scale from 1 to 5, with a "not specified" option. Authentic responses can be grouped by dimension, with calculations of frequencies, central tendencies, and dispersion, subject to consent and confidentiality rules. This framework provides a complementary institutional measurement tool to the technical validation already conducted.

9. CRITICAL DISCUSSION AND OUTLOOK

A comparison of the results demonstrates the robustness of the numerical verification: normalization of amplitudes, agreement with the theoretical formula, compatibility of frequencies with their confidence intervals, and exact reproducibility under a fixed seed. The protocol examines a labeled solution and four instance sizes on an ideal simulator; its scientific scope concerns the search mechanism and the number of queries. Measuring runtime on a quantum processor, the effects of noise, and the cost of external data constitute distinct experimental objectives. The academic framework is formalized and equipped with metrics; its generalization to other institutions depends on the data that will actually be observed in the field.

Three extensions arise from the results: integrating more realistic oracles and noise models into the simulations; replicating the tests on accessible quantum processors with measurements of latency and fidelity; and applying the institutional indicators to participating institutions. This work would make it possible to link numerical proof, hardware constraints, and conditions for educational adoption [7–10,19].

CONCLUSION

The study provides a critical comparison of the main families of algorithms and presents a reproducible numerical validation of Grover's search. Across 20,000 simulated measurements distributed across four search spaces, the observed success rates are consistent with the analytical probabilities; a second run of the program exactly reproduces the observations. The query costs follow the expected difference between classical unstructured search and Grover's algorithm in the oracle model studied. This convergence between theory, simulation, replication, and statistical testing confirms the validity of the numerical protocol for the configurations analyzed.

The scientific contribution brings together an evidence assessment grid, its validation through a traceable experiment, and a framework for evaluating academic capabilities tailored to reflections on higher education in the DRC. The normative and experimental references update the analysis of logical qubits and post-quantum cryptography. The validated results pertain to numerical experimentation; the institutional questionnaire serves as the tool for subsequently documenting the framework's organizational applicability.

REFERENCES

[1] Alexeev Y, Farag MH, Patti TL, Wolf ME, Ares N, Aspuru-Guzik A, et al. Artificial intelligence for quantum computing. Nat Commun. 2025;16:10829. doi:10.1038/s41467-025-65836-3.

[2] Butt F, Pogorelov I, Freund R, Steiner A, Meyer M, Monz T, Müller M. Demonstration of measurement-free universal logical quantum computation. Nat Commun. 2026;17:995. doi:10.1038/s41467-026-68533-x.

[3] Cerezo M, Arrasmith A, Babbush R, Benjamin S, Endo S, Fujii K, et al. Variational quantum algorithms. Nat Rev Phys. 2021;3:625–644. doi:10.1038/s42254-021-00348-9.

[4] Desdentado E, Calero C, Moraga MA, García F. Quantum computing software solutions, technologies, evaluation, and limitations: a systematic mapping study. Computing. 2025;107:110. doi:10.1007/s00607-025-01459-2.

[5] Devadas RM, Sowmya T. Quantum machine learning: a comprehensive review of integrating AI with quantum computing for computational advancements. MethodsX. 2025;14:103318. doi:10.1016/j.mex.2025.103318.

[6] Feynman RP. Simulating physics with computers. Int J Theor Phys. 1982;21:467–488. doi:10.1007/BF02650179.

[7] Google Quantum AI and Collaborators. Quantum error correction below the surface code threshold. Nature. 2025;638:920–926. doi:10.1038/s41586-024-08449-y.

[8] Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. ACM; 1996. pp. 212–219. doi:10.1145/237814.237866.

[9] Liao H, Wang DS, Sitdikov I, Salcedo C, Seif A, Minev ZK. Machine learning for practical quantum error mitigation. Nat Mach Intell. 2024;6:1478–1486. doi:10.1038/s42256-024-00927-2.

[10] Moody D, Perlner R, Regenscheid A, Robinson A, Cooper D. Transition to Post-Quantum Cryptography Standards. NIST Internal Report 8547. Gaithersburg (MD): NIST; 2026. doi:10.6028/NIST.IR.8547. https://csrc.nist.gov/pubs/ir/8547/final.

[11] National Institute of Standards and Technology. FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. Gaithersburg, MD: NIST; 2024. https://csrc.nist.gov/pubs/fips/203/final.

[12] National Institute of Standards and Technology. FIPS 204: Module—Lattice-Based Digital Signature Standard. Gaithersburg, MD: NIST; 2024. https://csrc.nist.gov/pubs/fips/204/final.

[13] National Institute of Standards and Technology. FIPS 205: Stateless Hash-Based Digital Signature Standard. Gaithersburg, MD: NIST; 2024. https://csrc.nist.gov/pubs/fips/205/final.

[14] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge: Cambridge University Press; 2010.

[15] Preskill J. Quantum computing in the NISQ era and beyond. Quantum. 2018;2:79. doi:10.22331/q-2018-08-06-79.

[16] Peral-García D, Cruz-Benito J, García-Peñalvo FJ. Systematic literature review: quantum machine learning and its applications. Comput Sci Rev. 2024;51:100619. doi:10.1016/j.cosrev.2024.100619.

[17] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science. IEEE; 1994. pp. 124–134. doi:10.1109/SFCS.1994.365700.

[18] Wang Y, Liu J. A comprehensive review of quantum machine learning: from NISQ to fault tolerance. Rep Prog Phys. 2024;87(11):116402. doi:10.1088/1361-6633/ad7f69.

[19] Zhou H, Cain M, Lukin MD. Opportunities in full-stack design of low-overhead fault-tolerant quantum computation. Nat Comput Sci. 2025;5:1110–1119. doi:10.1038/s43588-025-00895-6.