Quantum Complexity and Physical Bounds of the Eni6ma Cypher

by Frank Dylan Rosario and Dr. Lin Wang

Abstract

We quantify the hypothesis space and the fastest physically permitted quantum attack times against a membership-only proof-of-knowledge in which a prover holds **six distinct secrets** over a 72-symbol alphabet, each of length $L = 100$. For the tight "allow-repetitions" model (unordered multiset of six secrets, multiplied by the six-way private bijection), the global hypothesis count is

$$M \;=\; 6!\binom{U+5}{6} \;=\; U(U{+}1)\cdots(U{+}5), \qquad U = 72^{100}.$$

Because $U \gg 6$, one may write $M \approx U^6 = 72^{600}$ with negligible relative error at this scale. The quantum query lower bound for unstructured search is $\Theta(\sqrt{M})$ (Grover/BBBV). Converting oracle calls to wall-clock time under an **absolute physical ceiling**, a perfectly reversible, fully coherent "cosmic" computer that converts **all baryonic mass of the observable universe** into computation and runs at the **Margolus–Levitin** energy-limited rate, yields (i) a **best-case floor** assuming one elementary transition per Grover oracle call, and (ii) a **conservative upper bound** (still ideal hardware) that charges **one elementary transition per transcript round per oracle call**. For $L = 100$, these two time scales are approximately 7.27×10^{445} years and 1.04×10^{449} years, respectively.

Introduction

Quantum Computers Are Powerful, Not Omnipotent

In popular media and casual conversation, quantum computers are often portrayed as almost mythical devices—machines that, once built, will instantly break all cryptography, solve all hard problems, and render classical computing obsolete. This belief is understandable: the mathematics of quantum mechanics is exotic, and the phrase "quantum speedup" has a mysterious allure. However, the idea that quantum computers are *omnipotent* is not only inaccurate but

also dangerously misleading. To study computer science seriously, one must learn that quantum computing represents a new *model of computation* with both extraordinary capabilities **and** strict limitations.

The Source of the Myth

The myth begins with the dramatic examples of Shor's algorithm for factoring large integers and Grover's algorithm for unstructured search. These results were groundbreaking because they showed that some tasks thought to be nearly impossible for classical computers could be sped up significantly with quantum methods. From there, it was easy for the public to leap to the conclusion: if quantum computers can crack RSA encryption or search enormous databases faster, surely they can *solve anything*. But this leap is a logical mistake. The existence of a few celebrated quantum algorithms does not mean that *all* problems succumb to quantum magic.

What Quantum Computers Actually Do

A quantum computer encodes information in *qubits*, which unlike classical bits can exist in a superposition of states. Quantum gates manipulate these qubits through unitary transformations, and measurements collapse superpositions to classical outcomes. The mathematics enables powerful interference patterns, letting some computational paths cancel while others reinforce. This is the key to algorithms like Shor's.

However, the same rules that make quantum computing special also restrict it. Quantum computation is still bound by the Church–Turing thesis: it does not create a "new class" of computable problems. Any function computable by a quantum computer is also computable by a classical Turing machine. The difference lies only in *efficiency*—certain problems are solved faster, sometimes dramatically so, but many others see little to no improvement.

The Limits of Quantum Advantage

Take Grover's algorithm as an example. Classically, searching an unstructured list of N items requires $O(N)$ steps. Grover showed that a quantum computer can do it in $O(\sqrt{N})$ steps—a genuine speedup, but not a miracle. The algorithm does not turn exponential searches into polynomial ones. For cryptography, this means that doubling key lengths is enough to compensate against Grover's square-root attack.

More importantly, quantum computers **do not help** with the majority of problems we call "intractable." NP-complete problems, for instance, are not magically solved in polynomial time by quantum mechanics. Despite decades of research, there is no quantum algorithm known that cracks them efficiently. Quantum advantage is therefore narrow and problem-dependent, not universal.

Physical and Practical Boundaries

Even if quantum algorithms offered speedups in theory, building machines to realize them faces crushing practical limits. Quantum states are fragile, requiring extreme isolation and error correction. Maintaining coherence in hundreds or thousands of qubits demands engineering resources that grow explosively.

Physics itself imposes ceilings: the Margolus–Levitin bound limits how fast any physical system can evolve, and the Bekenstein bound restricts how much information can be stored in a given volume. A quantum computer cannot exceed these universal laws of nature. The dream of a machine that "tries all answers simultaneously" is a misconception. What actually happens is subtle interference, not parallel universes of brute force.

Why the Naïve View Is Dangerous

Believing in omnipotent quantum computers fosters two problems. First, it can breed **unnecessary fear**—the ignorant may assume that all encryption is doomed and that privacy is impossible. Second, it can lead to **unrealistic expectations**—assuming that any scientific or societal problem, from protein folding to climate change, will be instantly solved once "quantum supremacy" arrives. Both attitudes ignore the reality: quantum computing is a specialized tool, not a universal solver.

A More Accurate Picture

The truth is more interesting than the myth. Quantum computers offer profound insights into the relationship between physics and computation. They redefine the landscape of complexity theory, show us surprising ways to process information, and may open up applications we have not yet imagined. But they remain bounded: they cannot violate information theory, cannot overturn undecidability, and cannot shortcut every hard problem.

For practitioners entering the field, the lesson is this: **"Quantum computers are NOT omnipotent machines"**. They are powerful new instruments, with both strengths and limits, and they demand respect not as miracle boxes but as rigorously defined computational models rooted in the laws of physics.

Challenge

Can a quantum computer crack the Eni6ma cypher for secret of 100 characters?

In the all sense relevant to any form of Quantum Cryptanalysis, the answer is **NO**.

Why? The reason is twofold, one part information-theoretic, one part physical. On the information side, each transcript round exposes only a **six-way label** (think: a fair die outcome). Because the board is rebalanced in every round and the alphabet rings are independently rotated, those labels carry

(in expectation) **no persistent bias** toward any next secret character. Formally, the per-round leakage is bounded by the entropy of a six-way choice, $H = \log_2 6 \approx 2.585$ bits, and the expected mutual information about the next character is essentially zero when conditioned on the round's board. That throttling forces any adversary, classical or quantum, into **unstructured search** over a combinatorial hypothesis space.

Let $|\Sigma| = 72$ denote the alphabet size (30 lowercase + 30 uppercase + 12 digits). With **secret length** $L = 100$, the number of possible strings is $U = |\Sigma|^L = 72^{100} \approx 5.410652511578569 \times 10^{185}$ (about 186 digits). The prover possesses **six distinct secrets** and a **private six-way relabeling** (a bijection) of the leaves. Modeling the six secrets as an unordered multiset (repetitions permitted) and multiplying by the private bijection yields the tight hypothesis count

$$M \;=\; 6!\binom{U+5}{6} \;=\; U(U+1)(U+2)(U+3)(U+4)(U+5)$$

$$\approx\; U^6 \;=\; 72^{600} \;\approx\; 2.5089838091796364 \times 10^{1114}.$$

(At this scale, the difference between the exact rising product and U^6 is negligible in relative terms.)

Even before computation is considered, information theory dictates how much transcript is needed to isolate a unique hypothesis. Since each round leaks at most $\log_2 6$ bits, the number of rounds required for "uniqueness in expectation" is

$$R_{\min} \;\approx\; \left\lceil \frac{\log_2 M}{\log_2 6} \right\rceil \;=\; \left\lceil \frac{6L \log_2 72}{\log_2 6} \right\rceil \;\xrightarrow{L=100}\; \mathbf{1433} \text{ rounds.}$$

This is the sampling threshold; it says nothing yet about the **effort** of searching the space.

For **classical** attackers in an unstructured setting, one cannot do better than "guess-and-check." A clean lower bound on effort is

$$\text{classical work} \;\gtrsim\; R_{\min} \cdot M \;\approx\; (1433) \times (2.5089838091796364 \times 10^{1114})$$

$$\approx\; 3.60 \times 10^{1117} \text{ elementary checks.}$$

To interpret this against the strongest possible hardware, impose an absolute physical ceiling on execution rate by converting **all baryonic mass of the observable universe** (order 10^{53} kg) into a perfectly reversible, fully coherent processor and running it at the **Margolus–Levitin** limit (about 5.4256×10^{50} ops/s/kg). The resulting "cosmic computer" has an instantaneous operation rate

$$\nu_{\text{univ}} \;\approx\; (5.4256 \times 10^{50}) \times (10^{53}) \;=\; \mathbf{5.4256 \times 10^{103}} \text{ ops/s.}$$

Dividing the classical work by this ceiling produces an **absolute lower bound** on wall-clock time for classical exhaustive search:

$$t_{\text{class}} \gtrsim \frac{3.60 \times 10^{1117}}{5.4256 \times 10^{103}}$$

$$\approx 6.6 \times 10^{1013} \text{ s} \approx \mathbf{2.1 \times 10^{1006}} \text{ years.}$$

This number is so large that it dwarfs any cosmological timescale; it already renders classical brute force physically moot.

What about **quantum** computation? For unstructured search, the best asymptotic improvement is **quadratic** (Grover/BBBV): the required oracle calls scale as $\Theta(\sqrt{M})$ rather than M. With $M \approx 72^{600}$,

$$\sqrt{M} \approx 72^{300} \approx 1.584110994042681 \times 10^{557},$$

and the canonical Grover schedule makes

$$N_{\text{Grover}} \approx \frac{\pi}{4}\sqrt{M}$$

$$\approx \mathbf{1.244052793427124 \times 10^{557}}$$

oracle calls. Translating oracle calls to **time** under the same physical ceiling leads to two meaningful benchmarks:

1. **Physical floor (best-case):** treat one Grover oracle call as **one** Margolus–Levitin-limited elementary transition (a generous idealization). Then

$$T_{\text{min}} = \frac{N_{\text{Grover}}}{\nu_{\text{univ}}} \approx \frac{1.244052793427124 \times 10^{557}}{5.4256 \times 10^{103}}$$

$$\approx 2.2929312765907327 \times 10^{453} \text{ s} \approx \mathbf{7.265860764414064 \times 10^{445}} \text{ years.}$$

2. **Conservative upper bound (still ideal QC):** even an ideal, reversible oracle must process each transcript round, so charge **one elementary transition per round per oracle**. With $R_{\text{min}} = 1433$,

$$T_{(1 \text{ op/round})} = \frac{N_{\text{Grover}} \cdot R_{\text{min}}}{\nu_{\text{univ}}} \approx$$

$$\frac{(1.244052793427124 \times 10^{557}) \cdot 1433}{5.4256 \times 10^{103}} \approx 3.285770519354520 \times 10^{456} \text{ s}$$

$$\approx \mathbf{1.0411978475405354 \times 10^{449}} \text{ years.}$$

Both times already assume the **fastest hardware permitted by physics**; any realistic tally of oracle depth, ancilla management, routing, cryogenics, and fault-tolerant error correction **increases** them, often by many orders of magnitude, because a nontrivial Grover oracle is a deep reversible circuit, not a single energy-limited tick. The net picture is therefore unambiguous: with $L = 100$, (i) the hypothesis space $M \approx 2.5 \times 10^{1114}$ is so large that classical exhaustive search is physically out of the question, and (ii) the quantum advantage, while asymptotically quadratic, still leaves the required **number of coherent oracle calls** and the ensuing **wall-clock time** far beyond any plausible, or even cosmologically available, computational budget.

1. Model and Parameters

- **Alphabet and secrets.** Alphabet size $|\Sigma| = 72$. The prover holds **six** pairwise distinct secrets; each secret has length $L = 100$.
- **Universe size.** Number of possible 100-character strings:

$$U \;=\; 72^{100} \;\approx\; 5.410652511578569 \times 10^{185},$$

  i.e., **186 digits** in base-10.
- **Global hypothesis space (tight allow-repetitions + private map).**

$$M \;=\; 6!\binom{U+5}{6} \;=\; U(U{+}1)(U{+}2)(U{+}3)(U{+}4)(U{+}5) \;\approx\; U^6 \;=\; 72^{600}.$$

  Scientific form (using U^6):

$$M \;\approx\; 2.5089838091796364 \times 10^{1114},$$

  i.e., **1115 digits** in base-10.
- **Rounds to uniqueness (information bound).** Each round reveals at most $\log_2 6$ bits; the expected rounds threshold is

$$R_{\min} \;\approx\; \left\lceil \frac{\log_2 M}{\log_2 6} \right\rceil \;=\; \left\lceil \frac{6L \log_2 72}{\log_2 6} \right\rceil \xrightarrow{L=100} \boxed{R_{\min} = 1433}.$$

2. Quantum Query Lower Bound and Search Scale

- **Square root of the search space.** With $M \approx U^6$,

$$\sqrt{M} \;\approx\; U^3 \;=\; 72^{300} \;\approx\; 1.584110994042681 \times 10^{557},$$

  i.e., **558 digits** in base-10.
- **Grover iteration count.** The canonical schedule is

$$N_{\text{Grover}} \;\approx\; \frac{\pi}{4}\sqrt{M} \;\approx\; \boxed{1.244052793427124 \times 10^{557}} \text{ oracle calls.}$$

3. Physical Ceiling on Operation Rate

Let $\nu_{\max}$ denote the absolute operation-rate ceiling obtained by:
(i) converting **all baryonic mass of the observable universe** ($\sim 10^{53}\,\mathrm{kg}$) into a perfectly reversible processor, then
(ii) operating at the **Margolus–Levitin** limit ($\sim 5.4256 \times 10^{50}$ ops/s/kg).
Then

$$\nu_{\max} \;=\; (5.4256 \times 10^{50}) \times (10^{53}) \;\approx\; \boxed{5.4256 \times 10^{103}}\ \text{ops/s}$$

This is a **hard ceiling**: practical oracle depth, routing, cooling, and error-correction only **increase** real runtimes.

4. Ideal-Quantum Attack Times for $L = 100$

4.1 Best-Case Physical Floor (One Elementary Transition per Oracle Call)

Assume one Margolus–Levitin-limited elementary transition implements **one** Grover oracle call. The resulting **time floor** is

$$T_{\min} = \frac{N_{\mathrm{Grover}}}{\nu_{\max}} \;\approx\; \frac{1.244052793427124 \times 10^{557}}{5.4256 \times 10^{103}}$$

$$= \boxed{2.2929312765907327 \times 10^{453}\ \text{seconds}}$$

Converting to years (divide by 31 557 600 s/yr):

$$\boxed{T_{\min} \;\approx\; 7.265860764414064 \times 10^{445}\ \text{years}}$$

Plain-English scale: "about **seven point two seven** × **10^445** years," i.e., a **7** followed by **445 zeros** years.

4.2 Conservative Upper Bound (One Elementary Transition per Round per Oracle)

Even with an ideal quantum processor, a non-degenerate oracle must coherently process each of the R transcript rounds. Charging **one elementary transition per round per oracle** yields

$$T_{(1\ \mathrm{op/round})} = \frac{N_{\mathrm{Grover}} \cdot R_{\min}}{\nu_{\max}} \;\approx$$

$$\frac{(1.244052793427124 \times 10^{557}) \cdot 1433}{5.4256 \times 10^{103}} \;=\; \boxed{3.285770519354520 \times 10^{456}\ \text{seconds}}$$

In years:

$$\boxed{T_{(1\text{ op/round})} \approx 1.0411978475405354 \times 10^{449}\text{ years}}$$

Plain-English scale: "about **one point zero four** × **10^449** years," i.e., a **1** followed by **449 zeros** years.

Remark. If a (still ideal) oracle needs $c > 1$ elementary transitions **per round** (for lookups, arithmetic, comparisons, uncomputation, etc.), time scales **linearly**: $T \propto c$. For example, $c = 10$ inflates the upper bound to $\sim 1.04 \times 10^{450}$ years; $c = 100$ to $\sim 1.04 \times 10^{451}$ years.

5. 10^{45} Normalization (for M)

Some applications prefer reporting $M/10^{45}$. With $M \approx 2.5089838091796364 \times 10^{1114}$,

$$\frac{M}{10^{45}} \approx \boxed{2.5089838091796364 \times 10^{1069}}$$

6. Summary of Final Numbers (for $L = 100$)

- **Hypothesis count (tight allow-repetitions):**
  $M \approx 2.5089838091796364 \times 10^{1114}$ (≈ **1115 digits**).
- **Square-root search scale:**
  $\sqrt{M} \approx 1.584110994042681 \times 10^{557}$.
- **Grover iteration count:**
  $N_{\text{Grover}} \approx 1.244052793427124 \times 10^{557}$ oracle calls.
- **Physical operation-rate ceiling:**
  $\nu_{\max} \approx 5.4256 \times 10^{103}$ ops/s.
- **Ideal-quantum time, physical floor (1 op per oracle):**
  $T_{\min} \approx 2.2929312765907327 \times 10^{453}$ s ≈ $\boxed{7.265860764414064 \times 10^{445}\text{ years}}$.
- **Ideal-quantum time, conservative upper bound (1 op per round per oracle; $R_{\min} = 1433$):**
  $T_{(1\text{ op/round})} \approx 3.285770519354520 \times 10^{456}$ s ≈ $\boxed{1.0411978475405354 \times 10^{449}\text{ years}}$.

These bounds already assume the **most favorable hardware** consistent with known physics. Any realistic accounting of oracle depth, ancilla management, routing, cryogenics, and fault-tolerant quantum error correction increases the attack time, often by many orders of magnitude.

References

1. L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC'96)*, pp. 212–219, 1996. doi:10.1145/237814.237866

2. C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1510–1523, 1997. doi:10.1137/S0097539796300933

3. A. Y. Kitaev, A. Shen, and M. Vyalyi, *Classical and Quantum Computation*. American Mathematical Society, 2002.

4. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th Anniversary Edition. Cambridge University Press, 2010.

5. S. Aaronson, *Quantum Computing since Democritus*. Cambridge University Press, 2013.

6. S. Lloyd, "Ultimate physical limits to computation," *Nature*, vol. 406, no. 6799, pp. 1047–1054, 2000. doi:10.1038/35023282

7. N. Margolus and L. B. Levitin, "The maximum speed of dynamical evolution," *Physica D: Nonlinear Phenomena*, vol. 120, pp. 188–195, 1998. doi:10.1016/S0167-2789(98)00054-2

8. J. D. Bekenstein, "Universal upper bound on the entropy-to-energy ratio for bounded systems," *Physical Review D*, vol. 23, no. 2, pp. 287–298, 1981. doi:10.1103/PhysRevD.23.287

9. R. Landauer, "Irreversibility and heat generation in the computing process," *IBM Journal of Research and Development*, vol. 5, no. 3, pp. 183–191, 1961. doi:10.1147/rd.53.0183

10. C. H. Bennett, "Logical reversibility of computation," *IBM Journal of Research and Development*, vol. 17, no. 6, pp. 525–532, 1973. doi:10.1147/rd.176.0525

11. S. Lloyd, "Computational capacity of the universe," *Physical Review Letters*, vol. 88, no. 23, 237901, 2002. doi:10.1103/PhysRevLett.88.237901

12. R. Jozsa, "Quantum algorithms and the Fourier transform," *Proceedings of the Royal Society A*, vol. 454, no. 1969, pp. 323–337, 1998. doi:10.1098/rspa.1998.0164

13. P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 124–134, 1994. doi:10.1109/SFCS.1994.365700

14. D. 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. doi:10.1098/rspa.1985.0070

15. A. Ekert and R. Jozsa, "Quantum computation and Shor's factoring algorithm," *Reviews of Modern Physics*, vol. 68, no. 3, pp. 733–753, 1996. doi:10.1103/RevModPhys.68.733

16. S. Aaronson and A. Ambainis, "Quantum search of spatial regions," *Theory of Computing*, vol. 1, no. 1, pp. 47–79, 2005. doi:10.4086/toc.2005.v001a003

17. M. Mosca, "Quantum algorithms," in *Encyclopedia of Complexity and Systems Science*, R. A. Meyers, Ed. Springer, 2009, pp. 7088–7118.

18. D. R. Simon, "On the power of quantum computation," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1474–1483, 1997. doi:10.1137/S0097539796298637

19. S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983. doi:10.1145/1008908.1008920

20. J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, 79, 2018. doi:10.22331/q-2018-08-06-79

21. C. Zalka, "Grover's quantum searching algorithm is optimal," *Physical Review A*, vol. 60, no. 4, pp. 2746–2751, 1999. doi:10.1103/PhysRevA.60.2746

22. M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight bounds on quantum searching," *Fortschritte der Physik*, vol. 46, no. 4-5, pp. 493–505, 1998. doi:10.1002/(SICI)1521-3978(199806)46:4/5<493::AID-PROP493>3.0.CO;2-P

23. R. Raussendorf and H. J. Briegel, "A one-way quantum computer," *Physical Review Letters*, vol. 86, no. 22, pp. 5188–5191, 2001. doi:10.1103/PhysRevLett.86.5188

24. D. Gottesman, "Fault-tolerant quantum computation with constant overhead," *Quantum Information & Computation*, vol. 14, no. 15–16, pp. 1338–1372, 2014.

25. J. Preskill, "Quantum computing and the entanglement frontier," *arXiv preprint arXiv:1203.5813*, 2012.