# Comparison of time complexity in factorizing large bi prime numbers using Grover's and Shor's algorithm

**Sahil Parvez[1], Bikash K. Behera[2], and Prasanta K. Paigrahi[3]**

*[1] Department of Physics, Aligarh Muslim University,*

*Aligarh 202002, Uttar Pradesh, India.*

*[2] Bikash's Quantum (OPC) Pvt. Ltd., Balindi,*

*Mohanpur, 741246, Nadia, West Bengal, India.*

*[3] Department of Physical Sciences, Indian Institute of Science Education and Research Kolkata,*

*Mohanpur, 741246, West Bengal, India.*

**Abstract.** Factorizing large biprime integer numbers[1][2] using quantum computers illuminates quantum-advantage[3][4] over classical computers. Finding the prime factors on classical computers would require sub-exponential[16] time period, however due to optimization its done in polynomial time[8] using quantum computers[6][7]. Our work is based on generalized Grover's algorithm, by Liu[9] and Shor's algorithm[10][11][12]. We have compared time-complexity of factorization on various quantum computers, the shortfalls in Shor's algorithm and experimentally factorized 12794893 using IBM's 5 and 15 qubit quantum processors utilizing phase-matching property[13], becoming the largest number being factorized on a quantum computer.

**Keywords :** Grover's exact search, Shor's algorithm, time comparison, largest number factorized on IBMQ.

Link of the pre-print: https://DOI:10.13140/RG.2.2.23597.51680.

**References**

[1] C. H. Bennett, and D. P. Di Vincenzo, Quantum information and computation. Nature 404, 247–255 (2000).
[2] B. E. Kane, A silicon-based nuclear spin quantum computer. Nature 393,133–137 (1998).
[3] S. Bravyi, D. Gosset, and R. K¨onig, Quantum advantage with shallow circuits. arXiv preprint quant-ph/9511026 (1995).
[4] D. Rist´e, et al. Demonstration of quantum advantage in machine learning. npj Quantum Inf. 3, 16 (2017).
[16] Y. Liu, An exact quantum search algorithm with arbitrary database. Int. J. Theor. Phys. 53, 2571–2578 (2014).
[8] Y. Wang, H. Zhang, and H. Wang, Quantum Polynomial Time Fixed Point Attack for RSA. China Commun. 15, 25–32 (2018).
[6] Chris J.C. Burges, Factoring as Optimization. Microsoft Research MSR-TR-200 (2002).
[7] Nanyang Xu,et al. Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance Sysytem. Phys. Rev. Lett. 108, 130501 (2012).
[9] Y. Liu, An exact quantum search algorithm with arbitrary database. Int. J. Theor. Phys. 53, 2571–2578 (2014).

[10] L. M. K. Vandersypen, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature 414,883–887 (2001).
[11] E. Mart´ın-L´opez, et al. Experimental realization of Shor's quantum factoring algorithm using qubit recycling. Nat. Photon. 6, 773–776 (2012).
[12] A. Bocharov, M. Roetteler, and K. M.Svore, Factoring with qutrits: Shor's algorithm on ternary and metaplectic quantum architectures. Phys. Rev. A 96, 012306 (2017).
[13] X. Li, K. Song, , N. Sun, and C. Zhao, Phase matching in grover's algorithm. Proc. 32nd Chin. Control Conf. , 7939–7942 (2013).