Quest towards “factoring larger integers with commercial D-Wave quantum annealing machines”

XinMei Wang^{*}

School of Telecommunications Engineering, Xidian University, Xi'an 710071, China

Received November 23, 2018; accepted November 29, 2018; published online March 6, 2019

Citation: X. M. Wang, Quest towards “factoring larger integers with commercial D-Wave quantum annealing machines”, *Sci. China-Phys. Mech. Astron.* **62**, 960331 (2019), <https://doi.org/10.1007/s11433-018-9337-5>

Integer factorization (IFP), also called prime factorization, is an important problem in number theory, cryptography, and quantum computation. Factoring large integers to attack the RSA cryptosystem is intractable for powerful supercomputers, let alone classical computers. In 1994, Shor [1] presented an algorithm that potentially enabled a quantum computer to find prime factors in polynomial time. Because this algorithm requires $2n$ qubits to factor n -bit integers, its practical application is still limited by the scalability of universal quantum devices. Inspired by the adiabatic quantum computing, Li et al. [2] employed the theoretical reduction on IFP and utilized 3 qubits to factor a relatively large integer 291311. Recently, based on the quantum annealing algorithm via a D-Wave quantum computer, Jiang et al. [3] proposed a scalable Quadratic Unconstrained Binary Optimization (QUBO) model and realized the factorization on 376298 (the largest case by real quantum computing up to date), but still beset by the topological restrictions of the state-of-the-art commercial quantum computer.

Peng et al. [4] give a simplified version of QUBO model representing the IFP. This work explores the specific properties of the multiplication table for factoring prime numbers and introduces more constraints given by the target values and the number of carrying numbers involved in the multiplication table. By this way, it reduces the number of involved qubits while realizing relatively stronger quantum interactions to construct the modified problem Hamiltonians

without the loss of scalability. In principle, this model provides optimistic potentials and advantages for the D-Wave quantum computer with limited connectivity to find the exact solutions, especially in large cases.

Through the hybrid classical/quantum tool *qbsolv* provided by D-Wave Systems Inc., the principle-of-proof simulations show higher accuracies to get the unique solutions in most cases. Actually, the method reduces the accuracy demand of the real quantum annealer, allowing for solving large-scale cases with fewer qubits in a limit-connectivity annealer. It shows optimistic potentials of quantum annealing algorithm [5,6] and D-Wave quantum computer for deciphering the RSA cryptosystem in future. It is interesting if the authors can consider deciphering other famous cryptosystems by using quantum annealing algorithms [7].

- 1 P. W. Shor, *SIAM Rev.* **41**, 303 (1999).
- 2 Z. K. Li, N. S. Dattani, X. Chen, X. M. Liu, H. Y. Wang, R. Tanburn, H. W. Chen, X. H. Peng, and J. F. Du, arXiv: [1706.08061](https://arxiv.org/abs/1706.08061).
- 3 S. Jiang, K. A. Britt, A. J. McCaskey, T. S. Humble, and S. Kais, *Sci. Rep.* **8**, 17667 (2018).
- 4 W. C. Peng, B. N. Wang, F. Hu, Y. J. Wang, X. J. Fang, C. J. Wang, and C. Wang, *Sci. China-Phys. Mech. Astron.* **62**, 060311 (2019).
- 5 C. Wang, and H. G. Zhang, *Inf. Secure. Comm. Priv.* **2**, 31 (2012).
- 6 C. Wang, Y. J. Wang, and F. Hu, *Chin. J. Netw. Inf. Secure.* **2**, 17 (2016).
- 7 A. D. King, J. Carrasquilla, J. Raymond, I. Ozfidan, E. Andriyash, A. Berkley, M. Reis, T. Lanting, R. Harris, F. Altomare, K. Boothby, P. I. Bunyk, C. Enderud, A. Fréchet, E. Hoskinson, N. Ladizinsky, T. Oh, G. Poulin-Lamarre, C. Rich, Y. Sato, A. Y. Smirnov, L. J. Swenson, M. H. Volkmann, J. Whittaker, J. Yao, E. Ladizinsky, M. W. Johnson, J. Hilton, and M. H. Amin, *Nature* **560**, 456 (2018), arXiv: [1803.02047](https://arxiv.org/abs/1803.02047).

^{*}Corresponding author (email: xmwang_xd2018@sina.com)