

Optimization of Quantum Computing Models Inspired by D-Wave Quantum Annealing

Baonan Wang, Feng Hu, and Chao Wang*

Abstract: With the slow progress of universal quantum computers, studies on the feasibility of optimization by a dedicated and quantum-annealing-based annealer are important. The quantum principle is expected to utilize the quantum tunneling effects to find the optimal solutions for the exponential-level problems while classical annealing may be affected by the initializations. This study constructs a new Quantum-Inspired Annealing (QIA) framework to explore the potentials of quantum annealing for solving Ising model with comparisons to the classical one. Through various configurations of the 1D Ising model, the new framework can achieve ground state, corresponding to the optimum of classical problems, with higher probability up to 28% versus classical counterpart (22% in case). This condition not only reveals the potential of quantum annealing for solving the Ising-like Hamiltonian, but also contributes to an improved understanding and use of the quantum annealer for various applications in the future.

Key words: Quantum Annealing (QA); annealing schedule; quantum tunneling; optimization problem

1 Introduction

Combinatorial optimization is one of the important problems in computer science^[1], and is widely used in the traveling salesman, graph coloring, clustering, and other problems^[2–4]. However, some of these problems cannot be effectively solved by classical computing methods in polynomial time^[5].

Quantum Annealing (QA), as a new computing paradigm different from its classical counterpart, provides a quantum-inspired way to solve the aforementioned problems. This method first proposed

by Finnila et al.^[6] introduced a general method to solve optimization problems^[7], which are fundamentally different from Simulated Annealing (SA)^[8]. The latter is based on thermal dynamics, whereas the former is based on quantum mechanics, which has the potential to show parallel computing capacity based on the quantum tunneling effects. Derived from Adiabatic Quantum Computing (AQC), QA can exhibit superiority over thermal annealing in some special cases^[9].

A special-purpose machine, called D-Wave quantum annealer^[10], which has been constructed based on QA, has entered the commercialized point of quantum computing era. D-Wave has been widely used in sampling, optimization, machine learning, and other fields^[11–13].

In information science, Wang and Zhang^[14] first proposed the potential of D-Wave on cryptography design and analysis in 2012. In 2018, Peng et al.^[15] proposed a factor 20-bit large number using a quantum computing software environment superior to the theoretical value of IBM Q System One. Hu et al.^[16] implemented real D-Wave quantum computers for the cryptography design. D-Wave is expected to be applied to more fields in the future.

• Baonan Wang, Feng Hu, and Chao Wang are with Key laboratory of Specialty Fiber Optics and Optical Access Networks, Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai Institute for Advanced Communication and Data Science, Shanghai University, Shanghai 200444, China, and with the State Key Laboratory of Cryptology, Beijing 100878, China. Chao Wang is also with the Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen 518000, China. E-mail: wbn_shu0099@163.com; sdhf911103@163.com; wangchao@shu.edu.cn.

* To whom correspondence should be addressed.

Manuscript received: 2019-06-27; revised: 2019-06-27; accepted: 2019-07-17

In addition, the implementation of QA can be made in an exact numerical integration of the Schrödinger equation (for small systems), quantum Monte Carlo simulations^[17], and Green's function Monte Carlo^[18]. The Green's function Monte Carlo effectively simulates the real-time adiabatic evolution of the wave function from the quantum ground state toward the final ground states represented by the classical state. How to find good trial variational wave functions is the crucial theoretical question. Sarjala et al.^[19] experimented on turning the spins in two ways: global flips and one spin at a time. It turned out that the single-flip strategy is more effective than flipping all replicas of a given spin.

Most studies on QA so far have emphasized the role of annealing time and residual energy on the probability of obtaining the final ground state. Evidence has been accumulated to show QA apparently closer to the ground state than SA^[2,20]. As argued by De Simone et al.^[21], methods typically use Monte Carlo simulation including SA, evolutionary, and genetic algorithms have two main drawbacks: (1) Reliably determining the accuracy degree of the experimental results produced with these heuristic methods is not possible. (2) Two different states with almost the same energy may be completely different. Therefore, the state derived by one of these algorithms cannot yield any useful information on the structure of the ground state.

This paper is devoted to solving the second question, dealing with the implementation of Quantum-Inspired Annealing (QIA) with the 1D Ising spin glass as a benchmark example, and the metropolis algorithm as the technique of choice. We propose to simulate Ising spins using a matrix of $1 \times N$ columns, and as the field strength and temperature slowly decrease, different states of Ising spins are stored in the matrix, which effectively solves the second problem. After annealing, the ground state of Ising spins can be found. The annealing simulation helps us understand not only the quantum many-body problem^[22] and path-integral Monte Carlo problems, but also the working principle of the D-Wave system^[23].

The rest of the paper is organized as follows. Section 2 describes the Ising model with transverse field and the quantities of residual energy. In Section 3, we introduce basic ideas of quantum mechanics and describe the QIA framework. In Section 4, we present results of QIA and compare them with SA. In the final section, we summarize our work.

2 Ising Model

Ising model is an exactly solvable model of phase transition and is broadly used to solve problems in social science, neuroscience, and other fields^[22,24].

The standard Hamiltonian formulation for an Ising system consists of nearest-neighbor interactions and spins, each corresponding to two states $s = \{-1, 1\}$, where s represents the spin, and the spin interactions are dependent on the coupling parameter J . The Hamiltonian formulation can be given as

$$H = - \sum_i h_i \sigma_i^x - \sum_{\langle ij \rangle} J \sigma_i^z \sigma_j^z \quad (1)$$

where J is denoted as a coupling constant, which is the interaction between the spins i and j . σ_i^x , σ_i^y , and σ_i^z are Pauli matrices corresponding to a spin on lattice site i .

D-Wave^[25] is designed based on superconducting flux qubits, programmable fields $\{h_i\}$, and couplings $\{J\}$. The case $J > 0$ corresponds to ferromagnetic substances and $J < 0$ corresponds to antiferromagnetic. Quantum fluctuations are initially large (J is small) and then decrease in magnitude (as J increases) as the annealing schedule, which allows for calculating the residual energy as the difference between the true ground states and initial configurations.

Any optimization problem that can be written as Eq. (1), that can be handled by a D-Wave quantum annealing processor.

Residual Energies: The residual energy is defined by the energy difference between the true ground state and the solution obtained by an algorithm. The residual energy is appropriate to the error estimation.

The residual energy of the thermal annealing decreases with annealing time as follows^[26],

$$E_{\text{res}}^{\text{TA}} \sim \frac{A}{(\ln \tau)^\zeta}, \quad 1 \leq \zeta \leq 2 \quad (2)$$

where $E_{\text{res}}^{\text{TA}}$ and τ stand for the residual energy and annealing time, respectively, and A is a constant.

Reference [27] investigated the annealing-time dependence of the residual energy,

$$E_{\text{res}}^{\text{QA}} \sim \frac{A}{\tau^2} \quad (3)$$

This result is in contrast to the logarithmic behavior after a long thermal annealing time. Therefore the convergence of the QA is qualitatively faster than that by thermal annealing^[28].

3 New QIA framework

3.1 Quantum annealing

D-Wave, which is based on quantum annealing, is widely used in most fields, and derived from quantum adiabatic theorem. Studying the feasibility of QA is expected to help advance the commercialization of QA.

The basic idea of QA^[29] is to use quantum fluctuations to build optimization algorithms. The classical SA algorithm uses thermal fluctuation to search the optimal solution of the problem. QA algorithm uses the quantum tunneling effect to get rid of the local optimum and achieve the global optimum. Figure 1 shows the working principle between the QA and SA algorithms.

As shown in Fig.1, for SA, the system must rely on thermal fluctuations (temperature $T > 0$) to jump from P (spin configuration or travel route) to global minima P' . In QA, the system can use the quantum tunneling effect^[30,31] through the barrier directly from P to P' .

Here, the quantum fluctuation mechanism was originally used to find the ground state of a classical physical system, corresponding to the lowest energy state. A tunneling field^[32] searching for system potential minima is introduced into a classical physics system: We first set the strength of quantum fluctuations to a very large value to search for the global structure of the phase space. By decreasing the strength slowly from a high value to zero^[33], one hopes to drive the system to the state with the lowest-energy state. The penetrating field is a kinetic energy term to show the quantum tunneling, which does not affect each other with the potential field of the classical physical system. The final state of the system is the lowest energy state. QA optimizes the target system by simulating the aforementioned process.

The model of the QA algorithm, the Ising model with transverse field, is generally composed of two parts: one is called potential energy, where the quantum optimization problem is mapped into a quantum system

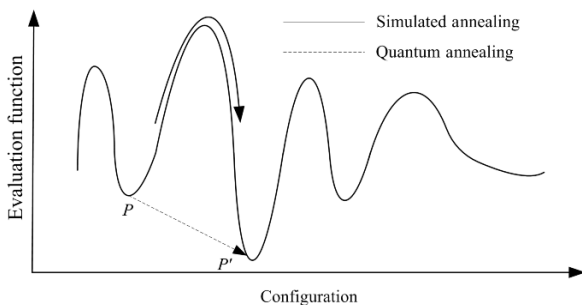


Fig. 1 Comparison of working principles of QA algorithm and simulated annealing algorithm^[30].

while the optimized objective function is mapped to a potential field applied to the quantum system. The second part is called quantum kinetic energy. A kinetic (tunneling) term is given to the interaction part of the classical glass Hamiltonian. Introducing a controllable kinetic energy term as a controlled field of quantum fluctuations is a common practice. Under the influence of these two fields, the quantum system evolution can be described by a Schrödinger equation as follows,

$$i\hbar \frac{d}{dt} |\psi(t)\rangle = H(t) |\psi(t)\rangle \quad (4)$$

However, the method of directly solving the Schrödinger equation is extremely expensive.

In the QA process, one considers a time-dependent Hamiltonian,

$$H(t) = H_{\text{pot}}(t) + H_{\text{kin}}(t) \quad (5)$$

The quantum Hamiltonian function is $H_q = H_{\text{pot}} + H_{\text{kin}}$, where H_{pot} is denoted as potential energy, and H_{kin} as kinetic energy. QA can activate the quantum tunneling effects^[34–36] to perform natural evolution toward the global optimum. It is the core advantage of QA compared with the classical methods that may easily get trapped in the local optimum in large-scale cases.

3.2 Quantum-inspired annealing

The Ising model with transverse field is widely used as a test model for the quantum annealing algorithm. Many combinatorial optimization problems can be mapped to this model, and then solved by the quantum annealing algorithm. The ground states of the Ising model encodes the answers of the optimization problem.

This study proposes a QIA framework for processing the problem of finding the ground state of the Ising model, aiming at exploring the potential of QA in processing the Ising model compared with SA. The general process of the QIA algorithm can be expressed in Algorithm 1.

T_0 is denoted as initial annealing temperature, h is the transverse field, h_0 is the initial field strength, and MaxSteps is the maximum number of iterations.

QIA Using Metropolis Criteria: One needs to flip a finite fraction of N spins to go from one minimum algorithm and accepts that with the probability $\min(1, e^{-\Delta E/k_B T})$ as the Metropolis criteria (k_B is the Boltzmann constant). The experimental steps of QIA are shown in Algorithm 2.

In QA, the transverse field in the Ising model can excite the actual quantum tunneling effects. Inspired

Algorithm 1 QIA algorithm

-
- 1: Quantum evaluation function is denoted as $H_q = H_{\text{pot}} + H_{\text{kin}}$.
 - 2: Initialization: T_0, h, h_0 , and MaxSteps, generating a random solution x .
 - 3: Producing a new solution x' with perturbation methods
 - 4: Compute $\Delta H_{\text{pot}} = H_{\text{pot}}(x') - H_{\text{pot}}(x)$ and $\Delta H_q = H_q(x') - H_q(x)$
 if $\Delta H_{\text{pot}} < 0$ or $\Delta H_q < 0$ then
 $x = x'$
 else
 if $\exp(\Delta H_q/T) < \text{random}(0, 1)$ then
 $x = x'$
 else
 turn to Step 3
 - 5: $h = h - (h_0/\text{MaxSteps})$
 - 6: Until termination condition
-

Algorithm 2 Experimental steps of QIA

-
- 1: **Input:** $1 \times N$ random matrix, number of spins N, T_0, h_0
 - 2: **Output:** Ground state configuration
 - 3: Initialize: $T = T_0, h = h_0$, and a set of N random Ising configurations
 - 4: Calculate E_{old} (the initial energy)
 - 5: For all Ising spins do
 - 6: Turn all spins in order
 - 7: Calculate E_{new} (the spin energy of the new Ising after flipping the spin)
 - 8: Calculation of energy change: $\Delta E = E_{\text{new}} - E_{\text{old}}$
 - 9: If $\Delta E < 0$ then
 - 10: $E_{\text{old}} = E_{\text{new}}$
 - 11: Else
 - 12: With probability $\exp(-\Delta E/k_B T)$, set $E_{\text{old}} = E_{\text{new}}$
 - 13: Repeat Steps 6–12
 - 14: End
-

by the QA and annealing schedules, the potential of quantum tunneling effects is simulated by introducing a kinetic term.

To further simulate the evolution process of QA, we introduce the Metropolis criterion to judge whether to accept current solutions with a certain probability in the annealing process. This approach can realize the “tunneling-like effect” as the basic principle of the QIA framework.

Our interest lies in the comparison of QIA and SA by studying the role of the initial value of the Ising spins, transverse field, and coupling constant in QIA and SA.

4 Results and Discussions

We have applied QIA and SA to the random-field Ising model with the system size $1 \times N$ in 1D. An optimal value of N spins was chosen to model this system

without periodic boundary conditions. The lattice was represented by a random matrix, with each element being randomly assigned with the value -1 or 1 . We use the method in Ref. [19] to flip the Ising spins.

The coupling strength is taken as $J = 1$. The entire procedure proceeds with different temperatures decreasing from 100°C to 0°C and different transverse fields h ranging from 1 to 0.

4.1 QIA with different configurations

In this section, we investigate the role of annealing schedules, coupling constant, and parameter selection of annealing process in QIA. The numerical results are shown in the following.

4.1.1 Role of annealing schedules in QIA

Annealing schedules are given as $h = h \times 0.99$, $h = 3/\sqrt{t}$, $h = 3/\ln(t + 1)$, and $h = 3/t$. As the time $t \rightarrow \infty$, the transverse field vanishes. The result is shown in Fig. 2.

Here, we discuss the ferromagnetic Ising model with constant J for all pairs of spins. Figure 2 shows the running time for the case of $h = h \times 0.99$, $h = 3/\sqrt{t}$, $h = 3/\ln(t + 1)$, and $h = 3/t$. The experimental run time obtained by reducing the field strength linearly is far less than that in the method^[33]. The experimental execution time obtained by the annealing schedule as $h = h \times 0.99$ is half the time of the other three non-linear annealing schedules. In the previous experiments^[28, 32], no comparison is made between linear and non-linear modes of field strength. We propose a simultaneous comparison of linear and non-linear modes of field strength in the QA experiments. No significant change

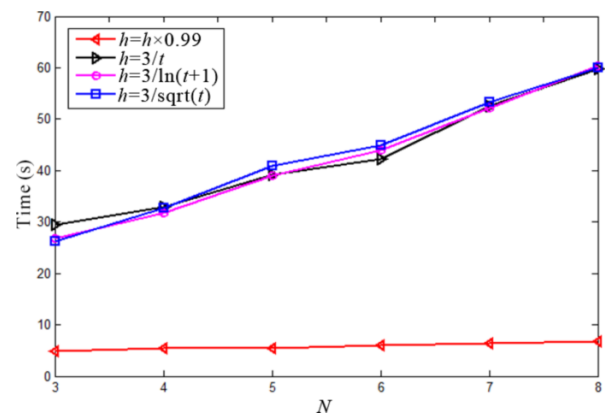


Fig. 2 Spin number dependence of running time of the ferromagnetic model with $h = h \times 0.99$, $h = 3/\sqrt{t}$, $h = 3/\ln(t+1)$, and $h = 3/t$. The lattice was represented by a $1 \times N$ random matrix in 1D with the same coupling constant $J = 1$ and same initial temperature $T_0 = 100^\circ\text{C}$.

occurs in the probability of Ising falling into the ground state for different field strength forms in the experiment.

4.1.2 Role of coupling constant in QIA

J is expressed as $J = 0.001$, $J = 0.25$, $J = 1$, $J = 2$, and $J = 4$.

The Ising model is represented by a $1 \times N$ random matrix in 1D with the same configurations ($h = h \times 0.99$ and $T_0 = 100^\circ\text{C}$).

Figure 3 shows that the experimental execution time of the small coupling constants is less than the execution time of large coupling constants with the same probability of the system following the ground state through annealing and reaching the final ground state. Thus, we can select a smaller coupling constant in the experiment to reduce the experimental running time.

4.1.3 Role of parameter selection on QIA

The Ising model with $N = 4$ is used to explore the role of parameter selection in the probability of spins reaching the ground state after QIA.

In Table 1, the initial temperature (T_0) is reduced to 1°C in the manner of $T_0 = T_0 \times 0.94$, and then the annealing step (Ecop) is followed. Dmax denotes a Markov chain, Num denotes the number of experiments, and the Probability denotes the number of reaching ground states.

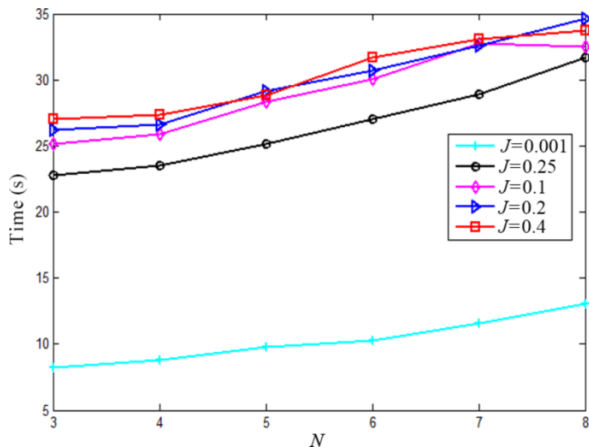


Fig. 3 Spin number dependence of time of the ferromagnetic model with $J=0.001$, $J=0.25$, $J=1$, $J=2$, and $J=4$.

Table 1 Role of parameter selection on QIA results.

T_0 ($^\circ\text{C}$)	Ecop	Dmax	Num	Probability
100	0.0010	30	20	0.15
100	0.0010	60	20	0.20
100	0.0010	80	20	0.25
100	0.0001	30	50	0.26
100	0.0010	30	50	0.14

As Table 1 shows, with the same number of experiments, the probability of Ising spins reaching the ground state after annealing increased when Dmax was larger. Dmax is the same as the number of experiments. With small Ecop, the Probability of Ising spin reaching the ground state after annealing increased.

Parameter selection has a strong influence on the final annealing precision of QIA. Good parameter selection is beneficial to maximize quantum tunneling effects, so that the algorithm can eliminate the local optimum to achieve the global optimal solution.

4.2 Comparison of QIA and SA with different initialized strategies

Here, we define two strategies representing the condition for selecting the initial value. Strategy 1 is denoted as the initial value of the experiment, which is given by the values obtained by previous experiments. The initial value of the first experiment is generated randomly. Strategy 2 denotes that all initial values are generated randomly.

(1) Comparison between Strategies 1 and 2 of QIA algorithm

Comparing Strategy 1 with Strategy 2 in QIA, the result is shown in Fig. 4.

In the annealing experiment, Strategy 1 is proposed. In Fig. 4, it can be seen that Strategy 1 is more likely to obtain the ground state than Strategy 2.

(2) Comparison between Strategies 1 and 2 of SA algorithm

Strategy 1 is compared with Strategy 2 in SA, as shown in Fig. 5.

Figure 5 shows that in the SA experiment, the Ising spins achieve the ground state with higher probability

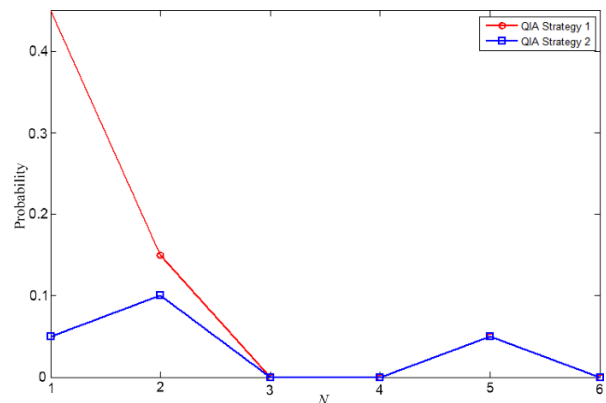


Fig. 4 Probability that Ising spins achieve the ground state. Ising spins are represented by a $1 \times N$ random matrix in 1D with the same configurations ($h = h \times 0.99$ and $T_0 = 100^\circ\text{C}$).

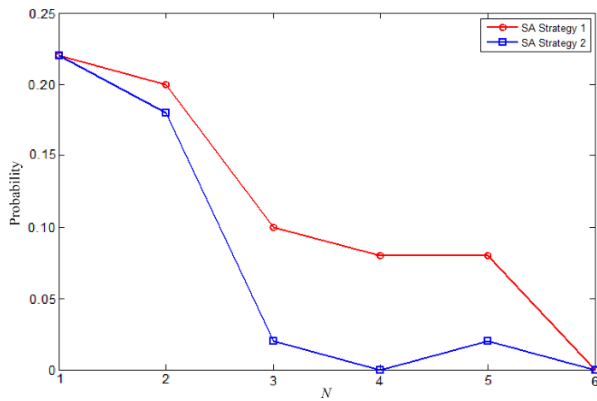


Fig. 5 Probability that Ising spins achieve the ground state. The Ising spins are represented by a $1 \times N$ random matrix in one dimension with the same configurations ($h = h \times 0.99$ and $T_0 = 100^\circ\text{C}$).

in Strategy 1 than Strategy 2. In the cases of QIA and SA, the Ising spins achieve the ground state with higher probability in Strategy 1 than Strategy 2. Therefore, we can improve the efficiency of the experiment and increase the probability to achieve the ground state with Strategy 1.

(3) Comparison between QIA and SA

To learn how effectively quantum tunneling processes possibly lead to the global minimum, this part presents a comparison between QIA and SA.

As shown in Fig. 6, QIA shows convergence to the ground state with a larger probability than SA in all cases if the same annealing schedule is used. Thus, QIA is a better option to achieve the global minima with respect to SA in most cases.

We simulate the quantum annealing mechanism by 1D Ising spins reaching ground state, and compare it with

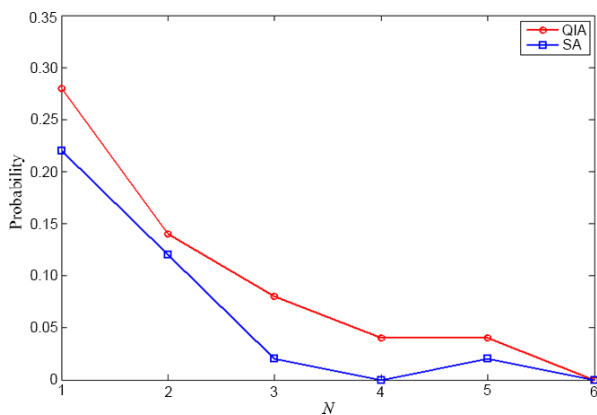


Fig. 6 Probability that Ising spins achieve the ground state in QIA and SA. The Ising spins are represented by a $1 \times N$ random matrix in 1D with the same coupling constant $J = 1$ and same initial temperature $T_0 = 100^\circ\text{C}$.

SA to show the potential of QIA to achieve the ground state with higher probability.

5 Conclusion

We propose a simultaneous comparison of linear and non-linear modes of field strength in QIA experiments. We find that the execution time obtained by the annealing schedule as $h = h \times 0.99$ is half the time of the other three non-linear annealing schedules. The execution time of small coupling constant is less than that of large coupling constants with the same probability of the system reaching the final ground state.

The results of the numerical study of QIA in the random field Ising model are compared with those of SA. If the system annealing schedule decreases as $h = h \times 0.99$, then QIA can obtain the ground states with higher probability than SA, which is consistent with that in Refs. [37, 38]. In some cases, the new framework can achieve the ground state with higher probability up to 28% versus the classical counterpart (22% in case).

In addition, in the annealing experiment, the probability to achieve the optimal states derived from Strategy 1 is higher than that from Strategy 2. QIA shows a better option to achieve the global minima with respect to SA in most cases.

Finally, we examine the role of different parameter selections on the final annealing precision of QIA. This approach suggests that a good value for the parameter can effectively improve the quantum tunneling effects. Annealing schedules with a combination of linear and non-linear characteristics may show better quantum effects.

Acknowledgment

This study was supported by the Special Zone Project of National Defense Innovation, the National Natural Science Foundation of China (Nos. 61572304 and 61272096), the Key Program of the National Natural Science Foundation of China (No. 61332019), and Open Research Fund of State Key Laboratory of Cryptology.

References

- [1] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*. New York, NY, USA: W. H. Freeman and Company, 1979.
- [2] R. Martoňák, G. E. Santoro, and E. Tosatti, Quantum annealing of the traveling salesman problem, *Physical Review E*, vol. 70, no. 5, p. 057701, 2004.
- [3] G. Ausiello, M. Protasi, A. Marchetti-Spaccamela, G. Gambosi, P. Crescenzi, and V. Kann, *Complexity and*

Approximation: Combinatorial Optimization Problems and Their Approximability Properties. Berlin Heidelberg, Germany: Springer-Verlag, 1999.

- [4] P. Brucker, On the complexity of clustering problems, *Optimization and Operations Research*. Berlin Heidelberg, Germany: Springer, 1978.
- [5] M. Troyer and U. J. Wiese, Computational complexity and fundamental limitations to fermionic quantum Monte Carlo simulations, *Physical Review Letters*, vol. 94, no. 17, p. 170201, 2005.
- [6] A. B. Finnila, M. A. Gomez, C. Sebenik, C. Stenson, and J. D. Doll, Quantum annealing: A new method for minimizing multidimensional functions, *Chemical Physics Letters*, vol. 219, nos. 5&6, pp. 343–348, 1994.
- [7] G. E. Santoro and E. Tosatti, Optimization using quantum mechanics: Quantum annealing through adiabatic evolution, *Journal of Physics A: Mathematical and General*, vol. 39, no. 36, p. R393, 2006.
- [8] S. V. Isakov, I. N. Zintchenko, T. F. Rønnow, and M. Troyer, Optimised simulated annealing for Ising spin glasses, *Computer Physics Communications*, vol. 192, pp. 265–271, 2015.
- [9] J. Brooke, D. Bitko, T. F. Rosenbaum, and G. Aeppli, Quantum annealing of a disordered magnet, *Science*, vol. 284, no. 5415, pp. 779–781, 1999.
- [10] T. Albash and D. A. Lidar, Adiabatic quantum computation, *Reviews of Modern Physics*, vol. 90, no. 1, p. 015002, 2018.
- [11] A. D. King, J. Carrasquilla, J. Raymond, I. Ozfidan, E. Andriyash, A. Berkley, M. Reis, T. Lanting, R. Harris, F. Altomare, et al., Observation of topological phenomena in a programmable lattice of 1800 qubits, *Nature*, vol. 560, no. 7719, p. 456, 2018.
- [12] F. Neukart, D. Von Dollen, G. Compostella, C. Seidel, S. Yarkoni, and B. Parney, Traffic flow optimization using a quantum annealer, *Frontiers in ICT*, vol. 4, p. 29, 2017.
- [13] R. Harris, Y. Sato, A. J. Berkley, M. Reis, F. Altomare, M. H. Amin, K. Boothby, P. Bunyk, C. Deng, C. Enderud, et al., Phase transitions in a programmable quantum spin glass simulator, *Science*, vol. 361, no. 6398, pp. 162–165, 2018.
- [14] C. Wang and H. G. Zhang, The impact of Canada's commercial quantum computer on cryptography, (Chinese), *China Information Security*, vol. 2, pp. 31–32, 2012.
- [15] W. C. Peng, B. N. Wang, F. Hu, Y. J. Wang, X. J. Fang, X. Y. Chen, and C. Wang, Factoring larger integers with fewer qubits via quantum annealing with optimized parameters, *Sci. China-Phys. Mech. Astron*, vol. 62, no. 6, p. 060311, 2019.
- [16] F. Hu, L. Lamata, M. Sanz, X. Chen, X. Y. Chen, C. Wang, and E. Solano, Quantum computing cryptography: Unveiling cryptographic boolean functions with quantum annealing, arXiv preprint arXiv: 1806.08706, 2018.
- [17] R. Martoňák, G. E. Santoro, and E. Tosatti, Quantum annealing by the path-integral Monte Carlo method: The two-dimensional random Ising model, *Physical Review B*, vol. 66, no. 9, p. 094203, 2002.
- [18] L. Stella and G. E. Santoro, Quantum annealing of an Ising spinglass by Green's function Monte Carlo, *Physical Review E*, vol. 75, no. 3, p. 036703, 2007.
- [19] M. Sarjala, V. Petäjä, and M. Alava, Optimization in random field Ising models by quantum annealing, *Journal of Statistical Mechanics: Theory and Experiment*, vol. 2006, no. 1, p. P01008, 2006.
- [20] S. Shinomoto and Y. Kabashima, Finite time scaling of energy in simulated annealing, *Journal of Physics A: Mathematical and General*, vol. 24, no. 3, p. L141, 1991.
- [21] C. De Simone, M. Diehl, M. Juenger, P. Mutzel, and G. Reinelt, Exact ground states of Ising spin glasses: New experimental results with a branch-and-cut algorithm, *Journal of Statistical Physics*, vol. 80, nos. 1&2, pp. 487–496, 1995.
- [22] G. Carleo and M. Troyer, Solving the quantum many-body problem with artificial neural networks, *Science*, vol. 355, no. 6325, pp. 602–606, 2017.
- [23] Z. Zhu, A. J. Ochoa, and H. G. Katzgraber, Efficient cluster algorithm for spin glasses in any space dimension, *Physical Review Letters*, vol. 115, no. 7, p. 077201, 2015.
- [24] S. M. Krause, P. Böttcher, and S. Bornholdt, Mean-field-like behavior of the generalized voter-model-class kinetic Ising model, *Physical Review E*, vol. 85, no. 3, p. 031126, 2012.
- [25] M. W. Johnson, P. Bunyk, F. Maibaum, E. Tolkacheva, A. J. Berkley, E. M. Chapple, R. Harris, J. Johansson, T. Lanting, I. Perminov, et al., A scalable control system for a superconducting adiabatic quantum optimization processor, *Superconductor Science and Technology*, vol. 23, no. 6, p. 065004, 2010.
- [26] D. A. Huse and D. S. Fisher, Residual energies after slow cooling of disordered systems, *Physical Review Letters*, vol. 57, no. 17, p. 2203, 1986.
- [27] S. Suzuki and M. Okada, Simulated quantum annealing by the real-time evolution, in *Quantum Annealing and Other Optimization Methods*. Berlin, Heidelberg, Germany: Springer, pp. 207–238, 2005.
- [28] G. E. Santoro, R. Martoňák, E. Tosatti, and R. Car, Theory of quantum annealing of an Ising spin glass, *Science*, vol. 295, no. 5564, pp. 2427–2430, 2002.
- [29] M. W. Johnson, M. H. S. Amin, S. Gildert, T. Lanting, F. Hamze, N. Dickson, R. Harris, A. J. Berkley, J. Johansson, P. Bunyk, et al., Quantum annealing with manufactured spins, *Nature*, vol. 473, no. 7346, pp. 194–198, 2011.
- [30] C. Wang, Y. J. Wang, and F. Hu, Shaping the future of commercial quantum computer and the challenge for information security, (Chinese), *Chinese Journal Network and Information Security*, vol. 2, no. 3, pp. 17–27, 2016.
- [31] G. Mazzola, V. N. Smelyanskiy, and M. Troyer, Quantum Monte Carlo tunneling from quantum chemistry to quantum annealing, *Physical Review B*, vol. 96, no. 13, p. 134305, 2017.
- [32] S. V. Isakov, G. Mazzola, V. N. Smelyanskiy, Z. Jiang, S. Boixo, H. Neven, and M. Troyer, Understanding quantum tunneling through quantum Monte Carlo simulations, *Physical Review Letters*, vol. 117, no. 18, p. 180402, 2016.
- [33] T. Kadowaki and H. Nishimori, Quantum annealing in the transverse Ising model, *Physical Review E*, vol. 58, no. 5, p. 5355, 1998.
- [34] I. Hen, J. Job, T. Albash, T. F. Rønnow, M. Troyer, and D. A. Lidar, Probing for quantum speedup in spin-glass problems

with planted solutions, *Physical Review A*, vol. 92, no. 4, p. 042325, 2015.

- [35] H. G. Katzgraber, F. Hamze, and R. S. Andrist, Glassy chimeras could be blind to quantum speedup: Designing better benchmarks for quantum annealing machines, *Physical Review X*, vol. 4, no. 2, p. 021008, 2014.
- [36] T. F. Rønnow, Z. Wang, J. Job, S. Boixo, S. V. Isakov, D. Wecker, J. M. Martinis, D. A. Lidar, and M. Troyer, Defining and detecting quantum speedup, *Science*, vol. 345, no.

6195, pp. 420–424, 2014.

- [37] S. Suzuki, H. Nishimori, and M. Suzuki, Quantum annealing of the random-field Ising model by transverse ferromagnetic interactions, *Physical Review E*, vol. 75, no. 5, p. 051112, 2007.
- [38] T. Albash and D. A. Lidar, Demonstration of a scaling advantage for a quantum annealer over simulated annealing, *Physical Review X*, vol. 8, no. 3, p. 031016, 2018.



Baonan Wang is a PhD candidate at the Electronic and Information Engineering Dept. of Shanghai University. Her main research interests include information security and quantum computing cryptography.



Feng Hu is a PhD candidate at the Electronic and Information Engineering Department of Shanghai University. His main research interests include information security and quantum computing cryptography.



Chao Wang received the PhD degree from Tongji University in 1999. He is a professor, a senior member of CCF, an IEEE senior member, the vice chair of IEEE China Council, the council member of China Institute of Electronic, the council member of China Association of AI, the deputy director of Information Security Experts Committee (China Institute of Electronic), the vice chair of IEEE Shanghai Computer Chapter, and the Committeeman of the Sixth Shanghai Expert Committee for Informatization. His research interests include AI, network information security and ECC, and quantum computing cryptography.