TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 17/20 pp874–882
DOI: 10.26599/TST.2023.9010059
Volume 29, Number 3, June 2024

Deciphering a Million-Plus RSA Integer with Ultralow Local Field Coefficient *h* and Coupling Coefficient *J* of the Ising Model by D-Wave 2000Q

Chao Wang*, Qiaoyun Hu, Haonan Yao, Sumin Wang, and Zhi Pei

Abstract: This work is the first to determine that a real quantum computer (including generalized and specialized) can decipher million-scale RSA relying solely on quantum algorithms, showing the real attack potential of D-Wave machines. The influence of different column widths on RSA factorization results is studied on the basis of a multiplication table, and the optimal column method is determined by traversal experiments. The traversal experiment of integer factorization within 10 000 shows that the local field and coupling coefficients are 75%–93% lower than the research of Shanghai University in 2020 and more than 85% lower than that of Purdue University in 2018. Extremely low Ising model parameters are crucial to reducing the hardware requirements, prompting factoring 1 245 407 on the D-Wave 2000Q real machine. D-Wave advantage already has more than 5000 qubits and will be expanded to 7000 qubits during 2023–2024, with remarkable improvements in decoherence and topology. This machine is expected to promote the solution of large-scale combinatorial optimization problems. One of the contributions of this paper is the discussion of the long-term impact of D-Wave on the development of post-quantum cryptography standards.

Key words: quantum annealing; RSA; D-Wave 2000Q; post-quantum cryptography

1 Introduction

The security of RSA encryption system generally depends on the computational difficulty of the prime factorization problem[1]. However, since Shor[2] presented his outstanding work in 1994, which claimed that his algorithm can perform integer factorization in polynomial time if a scalable quantum computer can be built, the confidence of the industry in RSA encryption algorithms has considerably decreased. Building a scalable quantum computer generally means the end of RSA-type classical cryptosystems. Unfortunately, this "if" condition has not been met thus far.

A set of prime factorization schemes has been experimentally proposed due to the practical importance of prime factorization and the stimulation of Shor's algorithm. As shown in Table 1, the prime factorization scale based on Shor's algorithm remains in the hundreds of digits[3–5] due to the limited development of generalized quantum computers[6–8].

In 2014, the Netherlands Quantum Research Center planned to develop a 100-qubit general quantum computer in 10 years[9]. IBM Q System One, which has 27 qubits, emerged in 2019. IBM also released a hardware roadmap, which planed to develop a quantum computer with over 1000 qubits; however, a considerable gap still exists between this planned computer and the 2000-plus qubits required by Shor's algorithm to decipher 1024-bit RSA[10]. Moreover, the

• Chao Wang, Qiaoyun Hu, Haonan Yao, Sumin Wang, and Zhi Pei are with Joint International Research Laboratory of Specialty Fiber Optics and Advanced Communication, Shanghai University, Shanghai 200444, China. E-mail: wangchao@shu.edu.cn; hqy2020@foxmail.com; yaohn1996@foxmail.com; 25970264@qq.com; peizhiiii@163.com.
* To whom correspondence should be addressed.
Manuscript received: 2023-03-26; revised: 2023-05-12; accepted: 2023-06-13

© The author(s) 2024. The articles published in this open access journal are distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/).

Table 1 Integer factorization based on Shor's algorithm.

Scheme	Device	Year	Author	Factored integer	Qubit
Shor	Photonic	2012	Martín-López et al.[3]	21	6
Shor	CNOT gate	2013	Geller and Zhou[4]	51, 85	8
Shor	Ion trap	2016	Monz et al.[5]	15	6

1000-bit machine is still under work.

Scholars in the industry have long believed that Shor's algorithm is the only effective quantum algorithm for RSA attacks[11]. They also often ignore the potential of the D-Wave quantum annealing algorithm, which was originally used to solve optimization problems[12] in cryptanalysis. The development of the D-Wave quantum computer and the comparison of qubits between D-Wave and other remarkable generalized quantum computers are illustrated in Fig. 1. However, regardless of their remarkable performance, IBM quantum computer devices have not yet been used to realize Shor's algorithm for factorization.

The development of D-Wave has advantages over general-purpose quantum computers. In addition, the integer factorization based on quantum annealing has a relatively mature theoretical basis supported by numerous studies.

Adiabatic quantum computation (AQC), which has been proposed by Farhi et al.[13], is designed for a large class of optimization problems. Thus far, two main approaches have been used to transfer the factoring problem into the optimization problem (Table 2).

Since Wang and Zhang[20] analyzed the application potential of D-Wave in the field of cryptography in 2012, studies on Method B using quantum annealing have been conducted. Except for the studies presented in Table 2, various optimization schemes have continued to emerge.

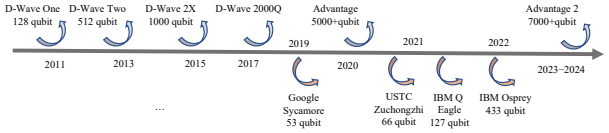

Fig. 1 Representative development of D-Wave and universal quantum computer.

Reference [21] used a multiplication table to factorize 56 153 using only 4 qubits. However, as stated in the article, "unless we know in advance that the factors will differ at two bits, this reduction will not allow us to crack big RSA codes." Hegade et al.[22] proposed a digitized AQC paradigm for factorization enhanced by shortcuts to adiabaticity techniques, which decreased the required circuit depth in quantum computers, and factored 235 with 4 qubits in an IBM quantum computer with up to 6 qubits. In March 2020, Wang et al.[23] proposed a distributed quantum annealing integer factorization scheme. Compared to Ref. [18], the range of the local field coefficient and the coupling term coefficient was further reduced, and a 20-bit integer 1 001 677 was factored[23, 24].

Numerous methods based on binary multiplication tables are available, but none of these methods fully consider the influence of column width on the resources required for quantum annealing. The current study analyze the influence of column width on integer factorization and find the optimal column width through traversal experiments. The local coefficient h and the coupling term coefficient J (hereinafter referred to as h and J) of the Ising model were improved by 75%–93% compared with those in the study of Wang et al.[23] by adopting the optimal block division method. Notably, a 21-bit large number, 1 245 407, is factored on the real D-Wave machine, indicating that the proposed scheme and D-Wave work well.

Table 2 Two methods transferring integer factorization to an optimization problem.

Method	Author	Year	Device	Factored integer
Mathematic formula	Peng et al.[14]	2008	NMR	21
Binary product table	Burges[15]	2002	—	—
	Schaller and Schutzhold[16]	2010	—	217
	Xu et al.[17]	2012	NMR	143
	Jiang et al.[18]	2018	D-Wave 2000Q	376 284
	Peng et al.[19]	2019	qbsolv	1 005 973

Some forecasting researches[25–27] have presented an optimistic view on cracking RSA-2048, but their predictions are mostly based on Shor's algorithm. Before the expected prototype mentioned in their paper emerges, their research is still far from cracking RSA-2048. Overall, D-Wave is currently the quantum machine with the most (theoretical and practical) advantages in deciphering RSA. The chip topology of D-Wave and the performance of qubit interaction are further improved. Meanwhile, the core principle of D-Wave, that is, quantum annealing, is unique and can be regarded as an unsupervised machine learning algorithm. The advantage of quantum annealing lies in its capability to solve mathematical problems with an unclear solution space (or regularity). Integer factorization is exactly one such problem. Origin quantum, guided by the academician Guangcan Guo, also recently wrote that D-Wave quantum computers have a better technical route for public key cryptanalysis than general quantum computers[28]. The complexity analysis of quantum annealing has been controversial. Without an explicit formulation to describe the search speed, quantum annealing has the advantage of jumping out of the local suboptimal by applying the quantum tunneling effect and reaching or approaching the optimal solution, which cannot be achieved by ordinary algorithms solving problems with a well-distributed solution space. Compared with traditional algorithms, quantum annealing has exponential acceleration potential[29].

Yan et al.[30] recently proposed a scheme to accelerate the classical mathematical method of attacking RSA with the quantum approximate optimization algorithm. Although there are still some unsolved issues in the article, this is a new idea to attack classical cryptography in addition to pure quantum methods such as Shor's algorithm and quantum annealing algorithm. All kinds of methods (quantum only and quantum mathematical) should still be developed.

Considering the three aforementioned kinds of algorithms, the current study is the first to factorize integers exceeding 1 million on a D-Wave real machine relying on quantum algorithms only. Moreover, this study illustrates the real threat from D-Wave in deciphering RSA and discusses the impact of D-Wave in the post-quantum era considering the capability of D-Wave to maintain pace with Moore's Law and its current capabilities.

2 Experiment

2.1 Quantum annealing

Quantum annealing is derived from adiabatic annealing theory[31, 32]. The theory indicates that if the quantum system is under adiabatic conditions and the time-varying Hamiltonian of the system slowly changes sufficiently, then the time-varying (instantaneous) Hamiltonian always remains in its ground state (with the lowest energy). Unlike traditional algorithms, a solution worse than the current state is temporarily ignored when searching the solution space considering the quantum tunneling effect. Instead, the energy barrier is directly crossed through quantum tunneling to reach the energy ground state, which is the global optimal solution. The search efficiency of quantum annealing has also been exponentially improved due to the wave–particle dualism of quantum[33]. Using quantum annealing to decipher the RSA can be summarized as solving the following two problems:

- Mapping the integer factorization problem to the Ising model.
- Mapping the Ising model to D-Wave hardware and performing quantum annealing to obtain the ground state.

This contribution mainly optimizes the first problem, reduces the hardware requirements of the quantum annealing machine, and improves the probability of successful factorization and the upper bound of integer factorization.

2.2 Multiplication table

A modified binary multiplication table is used to construct objective functions to map integer factorization into the optimization problem. Given integer N, to find its prime factors p and q, subject to $N = p \times q$ and assuming that $p \leqslant q$, p and q can be written in binary as follows:

$$p = \left(1 p_{l_1-1} p_{l_1-2} \cdots p_1 1\right)_2 \tag{1}$$

$$q = \left(1 q_{l_2-1} q_{l_2-2} \cdots q_1 1\right)_2 \tag{2}$$

$$N = \left(1 n_{l_3-1} n_{l_3-2} \cdots n_1 1\right)_2 \tag{3}$$

where $l_1 = \lfloor \log_2 p \rfloor$, $l_2 = \lfloor \log_2 q \rfloor$, $l_3 = \lfloor \log_2 N \rfloor$, and $p_i, q_j \in \{0,1\}$, $i \leqslant l_1$, $j \leqslant l_2$, $i, j \in \mathbb{Z}^+$.

The binary multiplication table is shown in Fig. 2. This method avoids calculating the equations of each column. Each block of the multiplication table

	k_{l_3-1}	k_{l_3-2}			...				2	1	0
p						1	p_{l_1-1}	...	p_2	p_1	1
q						1	q_{l_2-1}	...	q_2	q_1	1
						1	p_{l_1-1}	...	p_2	p_1	1
					q_1	$p_{l_1-1}q_1$	...	p_2q_1	p_1q_1	q_1	
				q_2	$p_{l_1-1}q_2$	...	p_2q_2	p_1q_2	q_2		
			...	...	...	...	...	...			
		q_{l_2-1}	$p_{l_1-1}q_{l_2-1}$	...	$p_2q_{l_2-1}$	$p_1q_{l_2-1}$	q_{l_2-1}				
	1	p_{l_1-1}	...	p_2	p_1	1					
Carry		c_i, c_{i-1}			...		c_2, c_1				
Column		col_i			...		col_2		col_1		col_0
N	1	n_{l_3-1}			...				n_2	n_1	1

Fig. 2 Modified binary multiplication table.

becomes equal to the corresponding block of the number to be factored by dividing the columns into blocks, which markedly reduces the computing resources.

2.3 Distributed factorization algorithm

Jiang et al.[18] proposed a prime factorization framework based on quantum annealing using the modified binary multiplication table. The maximum factored integer is 376 289. This framework differs from traditional algorithms in that it transforms the integer factorization problem into an optimization problem and maps it to D-Wave 2000Q for quantum annealing to conduct prime factorization. Under the above framework, the distributed integer factorization algorithm proposed by Wang et al.[23] uses distributed ideas to construct cost functions independently for each block of the multiplication table and perform independent annealing. Each block is independent. Thus, the coefficient superposition in the cost function is markedly reduced, and the number of qubits required for a single block is also decreased, which can effectively reduce the hardware requirements. This section takes 143 as an example to introduce the algorithm briefly.

As shown in Fig. 3, the column division method [2, 2, 3] is applied to the multiplication table of 143. The first column has no variables and generally does not participate in column calculations.

According to the relationship between the sum of product terms in each column and the target value of the corresponding block, the objective function of each column can be constructed as follows:

$$f_1 = (2p_2 + 2p_1q_1 + 2q_2 - 8c_1 + p_1 + q_1 - 3)^2 = 0 \quad (4)$$

$$f_2 = (2q_1 + 2p_2q_2 + 2p_1 + 2c_2 - 8c_4 - 4c_3 + p_2q_1 + p_1q_2 + c_1 + 1)^2 = 0 \quad (5)$$

	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
p					1	p_2	p_1	1
q					1	q_2	q_1	1
					1	p_2	p_1	1
				q_1	p_2q_1	p_1q_1	q_1	
			q_2	p_2q_2	p_1q_2	q_2		
		1	p_2	p_1	1			
Carry		c_4	c_3	c_2	c_1			
Target	1	0	0	0	1	1	1	1
Column	cols_3			cols_2		cols_1		cols_0

Fig. 3 Binary multiplication table of 143 = 11 × 13.

$$f_3 = (q_2 + p_2 + c_3 + 2c_4 - 2)^2 = 0 \quad (6)$$

The formula is simplified, and variable substitutions, such as $p_i^2 = p_i$, $q_i^2 = q_i$, are created. The objective function containing only constants, primary terms, and quadratic terms can be obtained in the form as follows:

$$f = \sum_{i=1}^{N} h_i s_i + \sum_{i,j \in f} J_{i,j} s_i s_j \quad (7)$$

where h_i is the primary term coefficient, corresponding to the local field coefficient in the Ising model; J_i is the quadratic term coefficient, corresponding to the coupling term coefficient in the Ising model; and s_i represents logical qubits. The local field and coupling term coefficients for the objective function of each column are extracted and embedded into D-Wave for solutions, respectively. Each column solution is not unique, and the final solution is obtained by finding the intersection of the set of solutions in each column.

2.4 Algorithm analysis

The quantum annealing integer factorization algorithm is executed on the basis of the binary multiplication table, and bit width determination of the factor is crucial for certain multiplication tables. Consequently, the objective function also depends on the aforementioned condition, which will ultimately affect the factorization result. The bit widths of the two factors (p, q) are generally similar by default; both are $\left\lceil \frac{\log_2 N}{2} \right\rceil$ bits. Two factors with relatively different bit widths will undeniably exist. However, the difficulty of deciphering is relatively low.

Table 3 shows a comparison of three 20-bit integers to be factored. The factors are all 10 bits. No difference is observed in the coupling term coefficient J and the number of variables used, which is inevitably related to

Table 3 Comparison of three 20-bit integer factorizations. 688 027 is a prime; thus, it cannot have two prime factors.

Integer	Column	Qubit	h	J
1 001 677 = 983 × 1019	4, 4, 4, 4, 3	88	7744	4594
682 267 = 823 × 829	4, 4, 4, 4, 3	88	8000	4594
688 027 = ? × ?	4, 4, 4, 4, 3	88	8768	4594

the same bit width of the factors. Accurately factoring the prime number 688 027 is impossible. However, the algorithm performs smoothly when the 10-bit factor is determined, and the obtained data still have a certain reference value.

For some large integers whose factorization results cannot be obtained theoretically, the algorithm can still run even if the factorization is unsuccessful (i.e., quantum annealing cannot reach the ground state) according to the above analysis. The involved parameters in the process play a supplementary role in the completeness and universality of algorithm research.

Each block constructs the objective function independently. Therefore, the target value of each block as an independent whole will affect the coefficient of the final cost function, which is reflected in the difference in local field coefficients in Table 3. This result shows that the choice of the column division method is also a crucial step. Therefore, further optimization experiments are expanded on the block division method.

A variety of column methods were proposed on the basis of the distributed quantum annealing factorization algorithm. All the integers were factored within 10 000 vertically, and various column methods were traversed horizontally to demonstrate the impact of column methods on factorization.

2.5 Experimental setup

First, the software package qbsolv provided by D-Wave company is used to solve the Ising model on a traditional computer. Tabu search is then implemented in this package to find the optimal solution. Additional details regarding qbsolv package can be found in Ref. [34]. Moreover, the D-Wave 2000Q is remotely connected by using the D-Wave Leap hybrid platform, and 1 245 407 = 1109 × 1123 is factored on a D-Wave machine using the proposed scheme. The performance and principles of multiple samplers provided by Leap, such as DWaveSampler, LeapHybridSampler, and ExactSolver, are fully investigated and compared before using D-Wave. The D-Wave Leap hybrid open-source platform is used to program the system, and the final problem is submitted as representing a series of values corresponding to the quantum ratio privilege and coupling strength. The system uses these values with the specified parameters to find the best configuration of the qubits and finally obtains the solution to the problem, which is the lowest point in the energy landscape. To this extent, the program is run on a real quantum computer.

3 Result and Discussion

The maximum decomposition result in this paper is a 21-bit integer 1 245 407 = 1109 × 1123, demonstrating a 75%–93% parameter improvement of the Ising model. This finding is better than the maximum decomposition result of the public literature of Warren[35], which is 7781. It is also better than the prime factorization experiment result (376 289) of Purdue University[18], and also exceeds the theoretical value (factor up to 10-bit integers), which can be obtained by the IBM Q System One if it can run Shor's algorithm. In addition, all integers are factored within 10 000, and all available column methods are applied to determine the optimal one.

3.1 Impacts of different column methods

Considering the column method, some rules are obtained from abundant experiment data. The factorization of 2419 = 41 × 59 is taken as an example.

As shown in Fig. 4, the number of variables used will be reduced with the increasing width of the column, but the local coefficient h and the coupling term coefficient J will be expanded accordingly. If the column is too wide (such as 5, 6, 7), then the corresponding h and J parameters will drastically increase.

As shown in Fig. 5, the selection of the maximum column width has an effect on reducing the number of variables, but this effect is not distinct. Meanwhile, the impact on the h and J parameters is substantial. Appropriate columns can improve the order of magnitude of the h and J parameters from 10^4 to 10^2. The position of the widest column also has a considerable influence on each parameter under uneven columns. Figure 5 shows that the h and J parameters performed well when the widest column moved toward the high bit, but the number of required variables slightly increased.

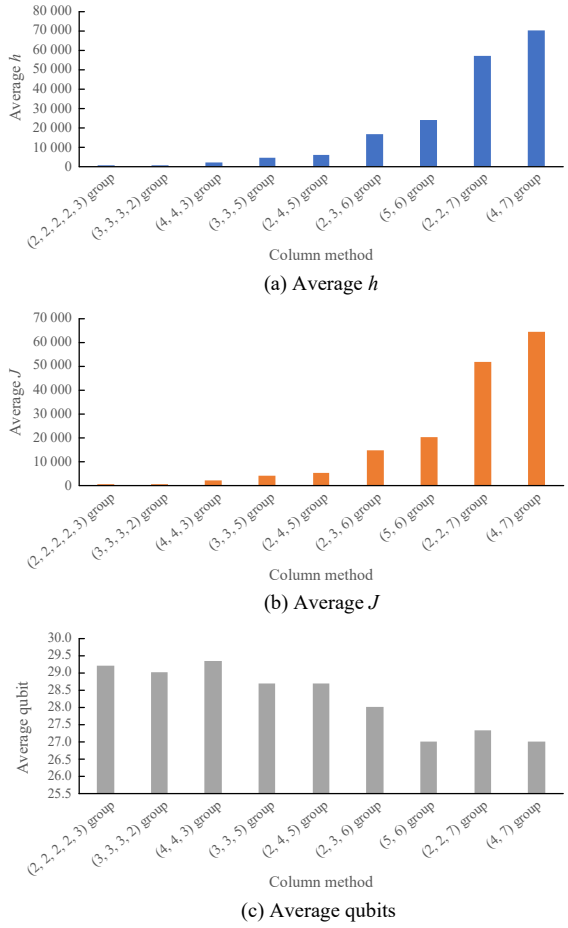

Fig. 4 Average parameter values of different column method groups for factorization of 2419.

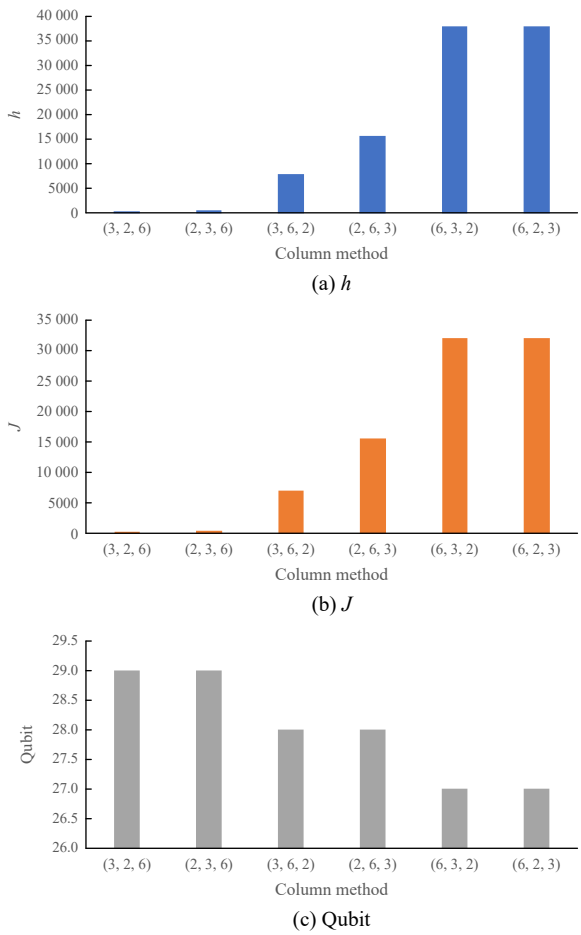

Fig. 5 Parameters under extreme column method for factorization on 2419.

In addition, some extreme column methods (such as 1) without experimental data exist. This condition exists because when the block has only one column, the block may not contain any variables. Thus, the cost function will not work. For some large integers, when the column width is too small, the original information transmission channel between the columns is cut off. Therefore, the correlation between the front and the rear is intricate, and the corresponding parameters may lose regularity, even contributing to the unavailability of a small number of column methods.

Overall, the column method has a considerable influence on integer factorization. Properly increasing the number of columns will help reduce the number of required variables and further minimize the hardware requirements for D-Wave. However, an excessively large column width will also drastically increase the local field coefficient h and the coupling term coefficient J. This condition results in inter-quantum interference problems, such as excessive coupling strength, which affect the successful execution of quantum annealing. Furthermore, uneven column methods should be intentionally avoided despite the acceptable maximum column width at the high position. The most suitable column width is 2 for most integers. The largest column width in the upper position rule is employed despite the unavoidable appearance of uneven column width.

3.2 Comparison of experimental results

The comparison of the three parameters between the two methods (Wang et al.'s[23] and ours) is depicted by Fig. 6. Qubits required subtle changes. However, a considerable reduction is still observed for integers above 100, and h and J are improved exactly by 75%–93%, which can directly reduce the coupling strength between qubits. The phenomena further improve the stability of qubit chains and, finally, enhance the upper bound of integer factorization.

Table 4 shows a comparison of the parameter

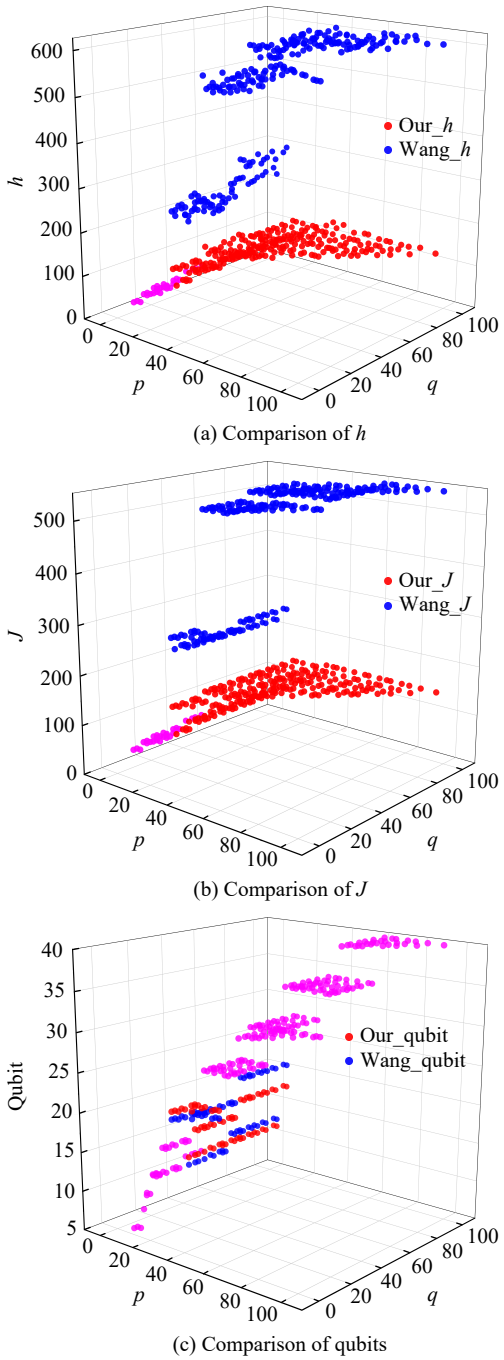

Fig. 6 Comparison of parameters between our method and Wang et al.'s[23]. The pink represents the overlap.

conditions required by different algorithms for factorizing 7781. Warren[35] factored 7781 as the maximum integer; therefore, 7781 is taken as an example. Table 4 shows that the experimental results in this paper significantly reduce the local field and coupling coefficients, and the number of qubits is markedly decreased compared to the study by Warren[35]. Compared with the results of Wang et al.[23], although the number of qubits only slightly varies, the optimal column method with each independent column annealing considerably decreases the local field and coupling term coefficients, improving the possibility of successful quantum annealing. This superiority cannot be ignored.

Table 4 Comparison of different algorithms for factorization of 7781.

Algorithm	h	J	Qubit
Warren[35]	106	106	419
Jiang et al.[18]	2462	1292	35
Wang et al.[23]	496	530	29
Proposed	131.25	142	29

The number of variables and the ranges of h and J parameters determine the feasibility of a dedicated D-Wave quantum computer performing quantum annealing to factor integers. The experiment has only single digits for the reduction of required variables. However, it can also guide the correct column method to a certain extent. Most importantly, the significant improvement of h and J parameters is prominent.

4 Conclusion and Prospect

Factorization of 21-bit integer 1 245 407 using an optimal column method is realized in this study. Ergodic factorization within 10 000 is presented to demonstrate universality, while some papers[21] claiming to factor large-scale integers with only a few qubits reveal that only a few special integers can be factored. The experimental data show that the most suitable column width is 2, and the columns should be evenly divided.

This study not only focuses on the increase in decomposition scale but also achieves considerable improvements in parameter optimization. The local field coefficient $h < 144.0$ and the coupling coefficient $J < 150.0$ in the Ising model of integer decomposition within 10 000, which is far superior to Warren's[35] order of 10 to the 6 power, are 75%–93% higher than those of Wang et al.[23] and 85% higher than that of Ref. [18]. This study also successfully factored 1 001 677 with 85 qubits (Wang et al.[23] factored the same integer with 87 qubits). This contribution provides a new clue for the improvement of the quantum annealing integer factorization algorithm and shows the capability and superiority of D-Wave to attack RSA.

Moreover, quantum annealing is analog quantum computing, which is limited by error correction.

Notably, the solution space distribution, starting search point, quantum annealing schedule[36], and even the temperature of D-Wave machines will affect the search efficiency of quantum annealing. With the continuous evolution of D-Wave machines, the scale of integers to be factored will expand rapidly in the near future as long as the above aspects are optimized.

Shor's and other quantum algorithms pose a subversive threat to public key cryptography, which is also the main reason for the development of post-quantum cryptography standards. However, quantum computation is generally believed to have no harmful effect on symmetric cryptography. Therefore, quantum computing attacks on symmetric cryptography must find new technical routes. D-Wave may be able to fill this role. The post-quantum cryptography standard currently mainly comprises asymmetric encryption schemes. If the above assumption is successful, then the post-quantum cryptography standard may absorb post-quantum symmetric cryptography. Further more, the American National Institute of Standards and Technology (NIST) should consider the threat from D-Wave when calling for post-quantum ciphers in the future.

The race to use quantum computers to attack cryptographic algorithms is ongoing, and D-Wave will surely be a strong competitor. In addition to using pure quantum algorithms, using quantum methods to accelerate traditional mathematical methods[30] may also be an option.

Acknowledgment

This work was supported by the Special Zone Project of National Defense Innovation.

References

[1] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[2] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proc. 35th Annual Symp. on Foundations of Computer Science*, Santa Fe, NM, USA, 1994, pp. 124–134.

[3] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X. Q. Zhou, and J. L. O'Brien, Experimental realization of Shor's quantum factoring algorithm using qubit recycling, *Nat. Photonics*, vol. 6, no. 11, pp. 773–776, 2012.

[4] M. R. Geller and Z. Zhou, Factoring 51 and 85 with 8 qubits, *Sci. Rep.*, vol. 3, p. 3023, 2013.

[5] T. Monz, D. Nigg, E. A. Martinez, M. F. Brandl, P. Schindler, R. Rines, S. X. Wang, I. L. Chuang, and R. Blatt, Realization of a scalable shor algorithm, *Science*, vol. 351, no. 6277, pp. 1068–1070, 2016.

[6] D. Castelvecchi, Quantum computers ready to leap out of the lab in 2017, *Nature*, vol. 541, no. 7635, pp. 9–10, 2017.

[7] A. Cho, DOE pushes for useful quantum computing, *Science*, vol. 359, no. 6372, pp. 141–142, 2018.

[8] M. Dyakonov, When will useful quantum computers be constructed? Not in the foreseeable future, this physicist argues. Here's why: The case against: Quantum computing, *IEEE Spectr.*, vol. 56, no. 3, pp. 24–29, 2019.

[9] E. Gibney, Physics: Quantum computer quest, *Nature* 516, https://doi.org/10.1038/516024a, 2014.

[10] C. Gidney, Factoring with n+2 clean qubits and n−1 dirty qubits, arXiv preprint arXiv: 1706.07884, 2017.

[11] C. Wang, H. Yao, B. Wang, F. Hu, H. Zhang, and X. Ji, Advances in cryptographic Attacks for quantum computing, (in Chinese), *Chinese J. Comput.*, vol. 43, no. 9, pp. 1691–1707, 2020.

[12] N. Chancellor, Fluctuation-guided search in quantum annealing, *Phys. Rev. A*, vol. 102, no. 6, p. 062606, 2020.

[13] E. Farhi, J. Goldstone, S. Gutmann, J. Lapan, A. Lundgren, and D. Preda, A quantum adiabatic evolution algorithm applied to random instances of an NP-complete problem, *Science*, vol. 292, no. 5516, pp. 472–475, 2001.

[14] X. Peng, Z. Liao, N. Xu, G. Qin, X. Zhou, D. Suter, and J. Du, Quantum adiabatic algorithm for factorization and its experimental implementation, *Phys. Rev. Lett.*, vol. 101, no. 22, p. 220405, 2008.

[15] C. J. C. Burges, Factoring as optimization, Microsoft Res MSR-TR-200, https://www.microsoft.com/en-us/research/publication/factoring-as-optimization/, 2002.

[16] G. Schaller and R. Schutzhold, The role of symmetries in adiabatic quantum algorithms, *Quantum Inf. Comput.*, vol. 10, nos. 1&2, pp. 109–140, 2010.

[17] N. Xu, J. Zhu, D. Lu, X. Zhou, X. Peng, and J. Du, Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system, *Phys. Rev. Lett.*, vol. 108, no. 13, p. 130501, 2012.

[18] S. Jiang, K. A. Britt, A. J. McCaskey, T. S. Humble, and S. Kais, Quantum annealing for prime factorization, *Sci. Rep.*, vol. 8, no. 1, p. 17667, 2018.

[19] W. Peng, B. Wang, F. Hu, Y. Wang, X. Fang, X. 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, pp. 1–8, 2019.

[20] C. Wang and H. G. Zhang, The impact of commercial quantum computer on cryptography, (in Chinese), *Inf. Secur. Commun. Priv.*, vol. 2, pp. 31–32, 2012.

[21] N. S. Dattani and N. Bryans, Quantum factorization of 56153 with only 4 qubits, arXiv preprint arXiv: 1411.6758, 2014.

[22] N. N. Hegade, K. Paul, F. Albarrán-Arriagada, X. Chen, and E. Solano, Digitized adiabatic quantum factorization, *Phys. Rev. A*, vol. 104, no. 5, p. L050403, 2021.

[23] B. Wang, H. Yao, F. Hu, and C. Wang, Quantum annealing distributed integer decomposition study of local field coefficient *h* and coupling coefficient *J* with stability Ising model, *Sci. Sin.-Phys. Mech. Astron.*, vol. 50, no. 3,

p. 030301, 2020.
[24] B. Wang, F. Hu, H. Yao, and C. Wang, Prime factorization algorithm based on parameter optimization of Ising model, *Sci. Rep.*, vol. 10, no. 1, p. 7106, 2020.
[25] C. Gidney and M. Ekerå, How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, *Quantum*, vol. 5, p. 433, 2021.
[26] M. Mosca and M. Piani, Quantum threat timeline, https://globalriskinstitute.org/publication/quantum-threat-timeline/, 2019.
[27] É. Gouzien and N. Sangouard, Factoring 2048-bit RSA integers in 177 days with 13436 qubits and a multimode memory, *Phys. Rev. Lett.*, vol. 127, no. 14, p. 140503, 2021.
[28] F. X. Cui, B. Wang, Y. Liu, and Y. Li, Research status and prospect of quantum attack on public key cryptography, (in Chinese), *Network Security and Data Governance*, vol. 41, no. 3, pp. 3–12, 2022.
[29] S. Muthukrishnan, T. Albash, and D. A. Lidar, Tunneling and speedup in quantum optimization for permutation-symmetric problems, *Phys. Rev. X*, vol. 6, no. 3, p. 031010, 2016.
[30] B. Yan, Z. Tan, S. Wei, H. Jiang, W. Wang, H. Wang, L. Luo, Q. Duan, Y. Liu, W. Shi, et al., Factoring integers with sublinear resources on a superconducting quantum processor, arXiv preprint arXiv: 2212.12372, 2022.
[31] D. A. Lidar, A. T. Rezakhani, and A. Hamma, Adiabatic approximation with exponential accuracy for many-body systems and quantum computation, *J. Math. Phys.*, vol. 50, no. 10, p. 102106, 2009.
[32] V. Choi, Minor-embedding in adiabatic quantum computation: I. The parameter setting problem, *Quantum Inf. Process.*, vol. 7, no. 5, pp. 193–209, 2008.
[33] W. L. Du, B. Li, and Y. Tian, Quantum annealing algorithms: State of the art, (in Chinese), *J. Comput. Res. Dev.*, vol. 45, no. 9, pp. 1501–1508, 2008.
[34] D-Wave systems, D-wave initiates open quantum software environment, https://www.dwavesys.com/press-releases/d-wave-initiates-open-quantum-software-environment, 2017.
[35] R. H. Warren, Factoring on a quantum annealing computer, *Quantum Inf. Comput.*, vol. 19, nos. 3&4, pp. 252–261, 2019.
[36] Y. Q. Chen, Y. Chen, C. K. Lee, S. Zhang, and C. Y. Hsieh, Optimizing quantum annealing schedules with Monte Carlo tree search enhanced with neural networks, *Nat. Mach. Intell.*, vol. 4, no. 3, pp. 269–278, 2022.

Chao Wang received the PhD degree from Tongji University, China in 1999. He is a professor at Shanghai University, China. His research interests include network information security and cryptography, artificial intelligence, and quantum computing.

Qiaoyun Hu is currently pursuing the master degree at Shanghai University, China. Her research interests include quantum computing and cryptography.

Haonan Yao is currently pursuing the master degree at Shanghai University, China. His research interests include quantum computing and cryptography.

Sumin Wang is currently pursuing the PhD degree at Shanghai University, China. Her research interests include network information security and cryptography, artificial intelligence, and quantum computing.

Zhi Pei is currently pursuing the PhD degree at Shanghai University, China. Her research interests include network information security and cryptography, artificial intelligence, and quantum computing