SCIENTIFIC REPORTS
nature research

OPEN

Prime factorization algorithm based on parameter optimization of Ising model

Baonan Wang[1,2], Feng Hu[1,2], Haonan Yao[1,2] & Chao Wang[1,2,3] ✉

This paper provides a new (second) way, which is completely different from Shor's algorithm, to show the optimistic potential of a D-Wave quantum computer for deciphering RSA and successfully factoring all integers within 10000. Our method significantly reduced the local field coefficient *h* and coupling term coefficient *J* by more than 33% and 26%, respectively, of those of Ising model, which can further improve the stability of qubit chains and improve the upper bound of integer factorization. In addition, our results obtained the best index (20-bit integer (1028171)) of quantum computing for deciphering RSA via the quantum computing software environment provided by D-Wave. Furthermore, Shor's algorithm requires approximately 40 qubits to factor the integer 1028171, which is far beyond the capacity of universal quantum computers. Thus, post quantum cryptography should further consider the potential of the D-Wave quantum computer for deciphering the RSA cryptosystem in future.

The majority of scholars think that Shor's algorithm is a unique and powerful quantum algorithm for the cryptanalysis of RSA. Therefore, the current state of the post quantum cryptography (constructing post quantum public key cryptosystems that would be secure against quantum computers) research has exclusively studied the potential threats to Shor's algorithm.

The security of the RSA cryptography system is based on the high complexity and security of the integer factorization problem. Shor's algorithm[1] can attack the RSA cryptosystem in polynomial time. There have been many simulations about quantum computers[2] and attempts to implement Shor's algorithm on quantum computing hardware[3–7]. Researchers have developed classic emulators based on reconfigurable technology, enabling efficient simulation of various quantum algorithms and circuits, and they have the potential to simulate number of quits than software based simulators[2]. Nuclear Magnetic Resonance (NMR) is the technology that we have for the implementation of small quantum computers. Vandersypen *et al.*[8] and Lu *et al.*[9] applied Shor's algorithm to factor the integer 15 via NMR and an optical quantum computer, respectively. Enrique *et al.* implemented a scalable version of Shor's algorithm via the iterative approach to factor 21[10]. Based on the characteristics of the Fermat number[11], Geller *et al.* used 8 qubits to successfully factor 51 and 85.

The real physical realizations of Shor's algorithm cannot breakthrough the scale of factorization beyond 100 for the moment, as shown by principle-of-proof simulations and experiments[12]. Actually, the number of qubits for performing Shor's algorithm to factor an n-bit integer still remains approximately 2n qubits[13]. Shor's algorithm requires not only a large number of qubits but also a general-purpose quantum computer with high precision. Achieving practical quantum applications will take longer, perhaps much longer, as said by John Martinis, the physicist who leads Google's efforts[14], and Science[15] commented that it will be years before code-cracking is achieved. Matthias Troyer said that "code-cracking and searching databases, are not good enough"[16]. The newest report by the National Academies of Sciences, "Quantum Computing: Progress and Prospects", stated that the current state of quantum computing and progress is highly unlikely to be able to attack RSA 2048 within the next decade. Therefore, in the case where Shor's algorithm cannot be practically applied, it is of great importance to find a more generalized and scalable way with the potential for practical attacks on integers while using fewer quantum resources.

[1]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. [2]State Key Laboratory of Cryptology, P. O. Box 5159, Beijing, 100878, China. [3]Center for Quantum Computing, Peng Cheng Laboratory, Shenzhen, 518000, China. ✉e-mail: wangchao@shu.edu.cn

The quantum adiabatic theorem was first introduced in 2001 by Burges[17]. The main idea is to construct the corresponding Hamiltonian based on the multiplication table[18–20]. Xu, N. *et al*. realized an experimental realization of factoring 143 via an NMR quantum processor[18]. By further employing the properties of some class of large integers, Dattani *et al*. factored the integer 56153 with only 4 qubits[19] and Li *et al*. factored 291311 with 3 qubits by combining the theoretical reductions and Hamiltonian transformation[20]. However, these methods are only available for integers with special properties and cannot be generalized to large integers, which can merely be seen as a principle-of-proof experiment. In adiabatic quantum computation, some researchers[21,22] realize the reduction of multiple terms to quadratic terms without introducing auxiliary qubits, but too many restrictions increase the complexity of the model. Thus, it is of great importance to find a more generalized way to conduct prime factorization.

D-Wave quantum computer is based on the quantum annealing principle. It has been widely used in sampling, optimization, machine learning, etc.[23–29]. Raouf Dridi *et al*.[27] applied the computational algebraic geometry to transform the factorization problem to the QUBO model to be solved by the cell algorithm and the column algorithm respectively. The experiments via the D-Wave 2X show that dividing the columns to construct the Hamiltonian that is to be solved via quantum annealing can factor the integer 200099. Jiang *et al*.[30] constructed a general model to factor the integer 376289 with 94 logical qubits via a D-Wave 2000Q System. However, it is still limited by the hardware restrictions of the quantum machine[31]. Peng *et al*.[32] further promoted Jiang *et al*.'s work by reducing the number of qubits according to the constraints of the target values and the number of carrying numbers involved in the multiplication table. XinMei Wang[33] commented that Peng *et al*.[32] supported the optimistic potential of a D-Wave quantum computer for deciphering the RSA cryptosystem in the future. In 2019, Lockheed Martin's Warren, R.H.[34] proposed a chain factorization algorithm to factor all integers within 1000 by setting the upper limit of the factorability. However, this model uses more logical qubits, which means there is qubit redundancy.

In this work, we put forward a new independent model for prime factorization with few qubits to be solved by QA, and it successfully factors 1028171 via 88 qubits with the *qbsolv* software environment (the quantum computing software environment provided by D-Wave). This is superior to the results obtained by any other quantum algorithm, including Shor's algorithm (factor up to 85) via different platforms (like the Hua-Wei quantum computing platform), quantum adiabatic computation via NMR (291311), and quantum annealing via the D-Wave platform (376289). Compared with ref. [30], in this paper, the local field coefficient h and coupling term coefficient J of Ising model are optimized to reduce the range of the model parameters, which reduces the coupling strength between qubits, further improves the stability of qubit chains and further improves the upper bound of the integer factorization. Our method has obtained the best index (20-bit integers (1028171)) of quantum computing for deciphering RSA, and it also exceeded the theoretical maximum (10-bit integers) of the IBM Q System One^{TM} with Shor's algorithm, the work of Shuxian Jiang *et al*. (376289), and the maximum scale (7781) of Lockheed Martin's Warren, R.H. It supports the optimistic potential of the quantum annealing algorithm and D-Wave quantum computer for deciphering the RSA cryptosystem in the future. The D-Wave provides a new (second) way, which is a completely different way than Shor's algorithm, and may be closer to cracking practical RSA codes than a general-purpose quantum computer using Shor's algorithm.

The rest of this paper is organized as follows. First, we describe the basic ideas of quantum annealing and the multiplication table for factorization. Second, we compare the methods and results with those of Shor's algorithm, NMR, and integer factorization by a D-Wave. Third, we illustrate the optimistic potential of the quantum annealing algorithm and D-Wave quantum computer for deciphering the RSA cryptosystem. Finally, we point out that post quantum cryptography should not only consider the potential attacks from universal quantum algorithms, such as Shor's algorithm but also consider real attacks from a D-Wave quantum computer in the near future.

Methods

Quantum annealing. Quantum annealing, as the core algorithm of a D-Wave quantum computer, has the potential to approach or even achieve the global optima in an exponential solution space, corresponding to the quantum evolution towards the ground state of the Hamiltonian problem[24]. The quantum processing units (QPUs), which are the core components for performing quantum annealing, are designed to solve quadratic unconstrained binary optimization (QUBO) problems[25,26], where each qubit represents a variable, and the couplers between qubits represent the costs associated with qubit pairs.

The objective form of the QUBO that the QPU is designed to minimize is as follows:

$$Obj(x, Q) = x^T \cdot Q \cdot x, \tag{1}$$

where *Obj* represents objective function of QUBO, x is a vector of binary variables of size N, and Q is an $N \times N$ real-valued matrix characterizing the relationship between the variables. Thus, any problem given in such a form can be solved by the D-Wave quantum annealer.

Multiplication table for factorization. Quantum annealing uses the quantum effects generated by quantum fluctuations to realize the global optimal solution of the objective function. The integer factorization problem can be transformed into a combination optimization problem that can be handled by the quantum annealing algorithm, and the minimum energy value can be output through the quantum annealing algorithm. At this time, the minimum value is the successful solution of integer factorization. To clarify the integer factorization method via quantum annealing, we introduce a multiplication table to illustrate the feasibility of mapping the integer factorization problem to Ising model (a model can be processed by a D-Wave quantum computer). We illustrate the factorization of the integer multiplication table by factoring $N = p \times q$, where p and q are prime numbers.

	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			
carries	z_{67}	z_{56}	z_{45}	z_{34}	z_{23}	z_{12}		
	z_{57}	z_{46}	z_{35}	z_{24}				
p × q = 143	1	0	0	0	1	1	1	1

Table 1. Multiplication table for $143 = 11 \times 13$ in binary.

Table 1 shows the factorization of $143 = 11 \times 13$. In Table 1, p_i and q_i represent the bits of the multipliers, and z_{ij} is the carried bits from ith bit to the jth bit. All the variables p_i, q_i, and z_{ij} in the equations are binary.

Note: All of the variables involved in Table 1 can only take the values of $\{0, 1\}$. Adding each column leads to the following equations:

$$p_1 + q_1 = 1 + 2z_{12} \tag{2}$$

$$p_2 + p_1q_1 + q_2 + z_{12} = 1 + 2z_{23} + 4z_{24} \tag{3}$$

$$1 + p_2q_1 + p_1q_2 + 1 + z_{23} = 1 + 2z_{34} + 4z_{35} \tag{4}$$

$$q_1 + p_2q_2 + p_1 + z_{34} + z_{24} = 0 + 2z_{45} + 4z_{46} \tag{5}$$

$$q_2 + p_2 + z_{45} + z_{35} = 0 + 2z_{56} + 4z_{57} \tag{6}$$

$$1 + z_{56} + z_{46} = 0 + 2z_{67} \tag{7}$$

$$z_{67} + z_{57} = 1. \tag{8}$$

Because each of the variables should be 0 or 1, we can get $z_{12} = 0$ and $p_1q_1 = 0$ according to the equation $p_1 + q_1 = 1 + 2z_{12}$. By applying similar judgments, we can get a simplified set of equations, as follows:

$$p_1 + q_1 - 1 = 0 \tag{9}$$

$$p_2 + q_2 - 1 = 0 \tag{10}$$

$$p_2q_1 + p_1q_2 - 1 = 0. \tag{11}$$

Obviously, $(p_1 + q_1 - 1)^2$, $(p_2 + q_2 - 1)^2$, and $(p_2q_1 + p_1q_2 - 1)^2$. The objective function is defined as the sum of squares of the three equations. It can be given as follows:

$$f = (p_1 + q_1 - 1)^2 + (p_2 + q_2 - 1)^2 + (p_2q_1 + p_1q_2 - 1)^2. \tag{12}$$

It can be seen from the above that the minimum value of Eq. (12) is 0, that is, (p_1, p_2, q_1, and q_2) are the values that minimize Eq. (12), and it is also the solution of Eqs. (9)–(11). This means that the values of (p_1, p_2, q_1, and q_2) represent the solution to the factorization problem.

The improved multiplication table for factorization. In the improved multiplication table for 143, c_1, c_2, c_3 and c_4 are the carried bits from the previous column. All the variables have a value of 0 or 1. Shuxian Jiang *et al.*[30] divided the multiplication table into 4 columns (from right to left are column 1, column 2, column 3, and column 4), as shown in Table 2.

The equation for each column is as follows:

$$(p_2 + p_1q_1 + q_2 - (c_2 \times 4 + c_1 \times 2)) \times 2 + (p_1 + q_1) = (11)_2 = 3 \tag{13}$$

$$(q_1 + p_2q_2 + p_1 + c_2 - (c_4 \times 4 + c_3 \times 2)) \times 2 + (1 + p_2q_1 + p_1q_2 + 1 + c_1) = (01)_2 = 1 \tag{14}$$

	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	
				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			
carries		c_4	c_3	c_2	c_1			
$p \times q = 143$	1	0	0	0	1	1	1	1
		column 4		column 3		column 2		column 1

Table 2. Improved multiplication table for $143 = 11 \times 13$ in binary.

$$(1 + c_4) \times 2 + (q_2 + p_2 + c_3) = (100)_2 = 4 \tag{15}$$

Equations (13)–(15) are further simplified to the following

$$2p_2 + 2p_1q_1 + 2q_2 - 8c_2 - 4c_1 + p_1 + q_1 - 3 = 0 \tag{16}$$

$$2q_1 + 2p_2q_2 + 2p_1 + 2c_2 - 8c_4 - 4c_3 + p_2q_1 + p_1q_2 + c_1 + 1 = 0 \tag{17}$$

$$q_2 + p_2 + c_3 + 2c_4 - 2 = 0 \tag{18}$$

We define the objective function as the sum of the squares of all the columns as follows:

$$\begin{aligned} f \;=\; & (2p_2 + 2p_1q_1 + 2q_2 - 8c_2 - 4c_1 + p_1 + q_1 - 3)^2 \\ & + (2q_1 + 2p_2q_2 + 2p_1 + 2c_2 - 8c_4 - 4c_3 + p_2q_1 + p_1q_2 + c_1 + 1)^2 \\ & + (q_2 + p_2 + c_3 + 2c_4 - 2)^2. \end{aligned} \tag{19}$$

Since Ising model can only deal with the interaction of two variables, it is necessary to process polynomials greater than the 2-local term. According to the properties $p^2 = p, q^2 = q$, and $c^2 = c$ (the values of p, q and c are 0 or 1), Eq. (19) is expanded and simplified, and the polynomials of more than 2-local term are replaced by the following equation[30] (for more information about factorization refer to ref. [30]):

$$\begin{cases} x_1x_2x_3 = \min\limits_{x_4}(x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4)) \\ -x_1x_2x_3 = -\min\limits_{x_4}(x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4)). \end{cases} \tag{20}$$

We replace p_1q_1, p_1q_2, p_2q_2, and p_2q_1 with t_1, t_2, t_3, and t_4, respectively. In Eq. (20), the variable x_i is used to represent the rule that the cubic term is reduced to the 2-local term. For example, the expansion term $p_1q_1q_2$ in Eq. (19) is replaced by $t_1q_2 + 2(p_1q_1 - 2p_1t_1 - 2q_1t_1 + 3t_1)$. Then, we perform variable replacement to transform the variables into the domain 0, 1 by using $x_i = (1 - s_i)/2$, $i = 1, 2, 3, \cdots$ if we let $x_1 = p_1, x_2 = p_2, x_3 = q_1$, $x_4 = q_2, x_5 = c_1, x_6 = c_2, x_7 = c_3, x_8 = c_4, x_9 = t_1, x_{10} = t_2, x_{11} = t_3$, and $x_{12} = t_4$. Finally, via the correspondence $p_1 = s_1, p_2 = s_2, q_1 = s_3, q_2 = s_4 \cdots, t_3 = s_{11}$, and $t_4 = s_{12}$, Eq. (19) finally simplifies to the following:

$$\begin{aligned} f' \;=\; & (p_1, p_2, q_1, q_2, c_1, c_2, c_3, c_4, t_1, t_2, t_3, t_4) \\ =\; & (261s_1)/2 + (215s_2)/2 + (261s_3)/2 + (215s_4)/5 - 41s_5 - 82s_6 + 3s_7 + 6s_8 \\ & - 137s_9 - 81s_{10} - 107s_{11} - 81s_{12} + 2s_1s_2 + 79s_1s_3 \\ & + (95s_1s_4)/2 + (95s_2s_3)/2 - 2s_1s_5 + 71s_2s_4 - 4s_1s_6 - 8s_2s_5 + 2s_3s_4 - 8s_1s_7 \\ & - 16s_2s_6 - 2s_3s_5 - 16s_1s_8 \\ & + s_2s_7 - 4s_3s_6 - 8s_4s_5 - 148s_1s_9 + 2s_2s_8 - 8s_3s_7 - 16s_4s_6 - 84s_1s_{10} + 6s_2s_9 \\ & - 16s_3s_8 + s_4s_7 + 34s_5s_6 \\ & + 6s_2s_{10} - 148s_3s_9 + 2s_4s_8 - 4s_5s_7 - 124s_2s_{11} + 6s_4s_9 - 8s_5s_8 - 8s_6s_7 - 84s_2s_{12} \\ & - 84s_4s_{10} - 8s_5s_9 - 16s_6s_8 \\ & - 84s_3s_{12} - 124s_4s_{11} + s_5s_{10} - 16s_6s_9 + 34s_7s_8 + 6s_4s_{12} + 2s_5s_{11} + 2s_6s_{10} + s_5s_{12} \\ & + 4s_6s_{11} \\ & - 4s_7s_{10} + 2s_6s_{12} - 8s_7s_{11} - 8s_8s_{10} - 4s_7s_{12} - 16s_8s_{11} - 8s_8s_{12} + s_9s_{11} + 794 \end{aligned} \tag{21}$$

The local field h represents the coefficient value of the single term of all s_i variables, and the coupling J is the coefficient value of the 2-local term for all $s_i s_j$ variables. The final model can be given as follows:

$$h = [130.5 \quad 107.5 \quad 130.5 \quad 107.5 \quad -41 \quad -82 \quad 3 \quad 6 \quad -137 \quad -81 \quad -107 \quad -81] \tag{22}$$

$$J = \begin{bmatrix} 2 & 79 & 47.5 & -2 & -4 & -8 & -16 & -148 & -84 & 0 & 0 \\ & 47.5 & 71 & -8 & -16 & 1 & 2 & 6 & 6 & -124 & -84 \\ & & 2 & -2 & -4 & -8 & -16 & -148 & 0 & 0 & -84 \\ & & & -8 & -16 & 1 & 2 & 6 & -84 & -124 & 6 \\ & & & & 34 & -4 & -8 & -8 & 1 & 2 & 1 \\ & & & & & -8 & -16 & -16 & 2 & 4 & 2 \\ & & & & & & 34 & 0 & -4 & -8 & -4 \\ & & & & & & & 0 & -8 & -16 & -8 \\ & & & & & & & & 0 & 1 & 0 \\ & & & & & & & & & 0 & 0 \\ & & & & & & & & & & 0 \end{bmatrix} \tag{23}$$

Then, the model given in Eqs. (22)-(23) can be directly solved by the D-Wave machine or the *qbsolv* software environment can be used to perform the quantum annealing algorithm. In this way, the model for the factorization can be generalized to any integer. Furthermore, it is a scalable model for any large integer in theory and it is a real potential application for D-Wave.

In the case when the factorization increases in Shuxian Jiang *et al.*[30], the growing number of qubits and the huge coupler strength in the theoretical quantum model will result in a nontrivial impact on the QA precision in the real D-Wave machine. Especially for limit-connectivity hardware, too high of costs regarding the number of qubits greatly limits the generalization and scalability of the factorization in large cases. In addition, the reduction from the 3-local term to the 2-local term increases the coupler strength and local field coefficient, especially for large integers.

This paper proposes a new model that addresses two perspectives: saving qubit resources and simplifying the quantum model to factor larger integers with fewer qubits. Using this way, we can reduce the number of involved qubits and the range of the coupler strength between qubits without any loss of generalization. It is expected to solve larger integers with fewer qubits so that the D-Wave can provide a more powerful capacity to factor large integers in the future.

Optimization of model parameters. In Ising model in ref. [30], they did not consider the restrictions on the final model derived from the target values, which may cause too many carries to be involved in the model. Here we introduce the constraints derived from the difference between the target values and the maximal output of each column. The carries involved can be directly removed in some cases.

As shown in the improved multiplication table of Table 2, because all variables have values of 0, 1, according to the first entry $p_1 + q_1 = 1$ of column 2, $p_1 q_1 = 0$ can be obtained. The second entry $p_2 + p_1 q_1 + q_2 = 1$ in column 2 is simplified to $p_2 + q_2 = 1$. Therefore, there is no carry from column 2 to column 3, that is, $c_1 = 0$ and $c_2 = 0$. Thus, only two carries (c_3 and c_4) are needed to represent the carry from column 3 into column 4. In addition, we can get $p_1 = 1 - q_1$ and $p_2 = 1 - q_2$ according to $p_1 + q_1 = 1$ and $p_2 + q_2 = 1$, respectively. Finally, the factorization of 143 only requires 5 qubits, a significant improvement compared to the original model with 12 qubits[30].

Based on the optimization of ref. [32], the final parameters of the model are as follows:

$$h = [-25 \quad -50 \quad 60 \quad 60 \quad -120] \tag{24}$$

$$J = \begin{bmatrix} 34 & -4 & -4 & 8 \\ & -8 & -8 & 16 \\ & & 41 & -96 \\ & & & -96 \end{bmatrix} \tag{25}$$

Actually, the method of ref. [32] is designed to reduce the number of qubits, and thus the improvements to the complexity of the model are limited. The main reason is that there is a "2" in Eq. (20), which leads to many high coupler strengths and local field coefficients in the final Hamiltonian resulting in fragile quantum states. Therefore, another optimization should be proposed to solve the above problem without the loss of generalization and scalability.

As mentioned above, we mainly focus on the optimization of the model parameters. Jiang *et al.*[30] a way to reduce the 3-local term to a 2-local term, which increased the local field coefficient and coupler strength parameters, especially for large integers. In the integer factorization problem based on quantum annealing, the reduction of the model parameters is beneficial to reducing the hardware requirements and the precision of quantum annealing. To reduce the 3-local term to a 2-local term in the integer factorization process, inspired by ref. [35], we optimize Eq. (20) of ref. [32] and form a new dimension reduction method from the 3-local term to 2-local term, as shown in Eq. (26)

x_1	x_2	x_3	x_4	$x_1x_2x_3$	Whether Eq. (27) achieves the minimum
0	0	0	0	0	0/√
0	0	0	1	0	1/×
0	0	1	0	0	0/√
0	0	1	1	0	2/×
0	1	0	0	0	0/√
0	1	0	1	0	0/√
0	1	1	0	0	0/√
0	1	1	1	0	1/×
1	0	0	0	0	0 /√
1	0	0	1	0	0/√
1	0	1	0	0	0/√
1	0	1	1	0	1/×
1	1	0	0	0	1/×
1	1	0	1	0	0/√
1	1	1	0	1	1/√
1	1	1	1	1	1/√

Table 3. The truth table for the dimension reduction.

$$\begin{cases} x_1x_2x_3 = \min\limits_{x_4}(x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4)) \\ -x_1x_2x_3 = -\min\limits_{x_4}(x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4)). \end{cases} \tag{26}$$

The negative term $-x_1x_2x_3 = -\min\limits_{x_4}(x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4))$ is the same as ref. [30]. We mainly prove our optimization of the positive term, that is, why the positive term $x_1x_2x_3 = \min\limits_{x_4}(x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4)$ holds.

$$x_1x_2x_3 = \min_{x_4}(x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4) \tag{27}$$

Table 3 is a combination of 16 values of x_1, x_2, x_3, and x_4. The values of x_1, x_2, x_3, and x_4 are 0 or 1. The output of is given in the last column, followed by √ or × to represent whether $x_1x_2x_3$ equals $\min_{x_4}(x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4)$ or not. As mentioned earlier, the integer factorization problem is the problem of finding the minimum value of a function. In other words, solving the minimum value of $x_1x_2x_3$ is the same as solving $\min_{x_4}(x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4))$. Take the first two rows of the Table 3 as an example for the following illustration.

In this case, where $x_1 = 0$, $x_2 = 0$, and $x_3 = 0$ are fixed, $x_1x_2x_3 = 0$; when $x_4 = 0$, $x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4 = 0$; when $x_4 = 1$, $x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4 = 1$. Therefore, $\min\limits_{x_4}(x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4) = 0$. At this time, $x_1x_2x_3$ is equivalent to $\min_{x_4}(x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4)$, and so $x_1x_2x_3 = \min_{x_4}(x_4x_3 + x_1x_2 - x_1x_4 - x_2x_4 + x_4)$.

The dimension reduction method in this paper is not only applicable to the integer 143, but it is also applicable to the case where the polynomial of the objective function of any integer is greater than the quadratic term, such as the factorization of the 20-bit integer 1028171. A detailed analysis of the factorization is shown in the supplemental material. The method is universal and extensible. We do the following analysis. Assume that the objective function of the integer factorization is as follows:

$$S(x)_{min} = g(x) + f(x_i, x_j, x_k), \tag{28}$$

where $g(x)$ and $f(x_i, x_j, x_k)$ are polynomials composed of two-local terms and 3-local terms, respectively. Then, it can be transformed based on Eq. (27) as follows:

$$S'(x)_{\min\limits_{x_n}} = g(x) + \min_{x_n}(x_nx_k + x_ix_j - x_ix_n - x_jx_n + x_n). \tag{29}$$

Therefore, the minimum value that solves the objective function $S(x)_{min}$ is equivalent to the minimum value of solving the 3-local term $f(x)$, namely, the value of $\min_{x_n}(x_nx_k + x_ix_j - x_ix_n - x_jx_n + x_n)$. Therefore, the objective function $S(x)_{min}$ has the same solution as $S'(x)_{\min\limits_{x_n}}$. Similarly, we analyze the 4-local term in the function.

$f(x_i, x_j, x_k, x_l)$ is a polynomial composed of 4-local terms. We consider x_k and x_l as a whole, and obtain Eq. (30) via $\min_{x_n}(x_n x_k + x_i x_j - x_i x_n - x_j x_n + x_n)$.

$$f(x_i, x_j, x_k, x_l) = \min_{x_n}(x_n x_k x_l + x_i x_j - x_i x_n - x_j x_n + x_n). \tag{30}$$

For the 3-local term $x_n x_k x_l$ in Eq. (30), the dimensionality reduction formula $\min_{x_n}(x_n x_k + x_i x_j - x_i x_n - x_j x_n + x_n)$ is used again to obtain the following:

$$f(x_n, x_k, x_l) = \min_{x_m}(x_m x_l + x_n x_k - x_n x_m - x_k x_m + x_m). \tag{31}$$

Finally, the final 4-local term is reduced to a 2-local term as follows:

$$f(x_i, x_j, x_k, x_l) = \min_{x_n}\left(\min_{x_m}(x_m x_l + x_n x_k - x_n x_m - x_k x_m + x_m) + x_i x_j - x_i x_n - x_j x_n + x_n\right). \tag{32}$$

In this way, the minimum value of the 3-local term and 4-local term can be transformed to a simpler polynomial with simple connections characterized by quadratic terms. The coupler strength and local field coefficient can be reduced further and the theoretical model can work better to describe the original problem with high precision in the simulations.

Simulations. All the simulations are performed via MATLAB 2014 and Python 3.6 with the *qbsolv* software environment (provided by D-Wave), which can successfully factor 1028171. For more information about the integer 1028171, please refer to the supplemental material. Table S1 of the supplemental material shows the factorization of integer 1028171. The *qbsolv* software environment is a decomposition solver that finds the minimum value given by a QUBO problem by splitting it into pieces that are solved either via a D-Wave system or a classical tabu solver. For more information about the tool, please refer to *http://github.com/dwavesystems/qbsolv*.

The simulations are based on the combination of the two optimizations, which can be divided into the following steps.

- Step 1. Give the improved multiplication table of Jiang *et al.*[30] that is divided into several columns. It's complexity is less than $O(log_2(N))$.
- Step 2. Give the original model based on the optimization in ref. [32]. The complexity of this step is less than $O((log_2(N))^3)$.
- Step 3. Give the final QUBO model based on the optimization of the model parameters. It's complexity is less than $O((log_2(N))^3)$.
- Step 4. Transform it to Ising model via $x_i = (1 - s_i)/2,\ i = 1, 2, 3, \cdots$, which is required for the quantum computing software environment. Note: x_i variables are mapped to s_i variables that could be processed by Ising model by the formula $x_i = (1 - s_i)/2,\ i = 1, 2, 3, \cdots$. The complexity of this step is $O(1)$.
- Step 5. Perform the simulations using the quantum computing software environment. By inputting the parameter values of h and J in the *qbsolv* quantum computing software, the quantum annealing algorithm factors the integers. It's complexity is less than $O((log_2(N))^2)$.

In the above simulations, Steps 1–4 are classical calculations, and the complexity is less than $O((log_2(N))^3)$. Step 5 performs a quantum annealing calculation. The complexity increases as the integer to be factored becomes larger, and the overall complexity is less than $O((log_2(N))^2)$. This algorithm realizes the hybrid computing structure of quantum and classical, and exerts the optimal computing power of the distributed processing problem of both quantum and classical.

Take the factorization on 143 as an example, the final input is given as follows:

$$h = [-12 \quad -50 \quad -25 \quad 12 \quad -24] \tag{33}$$

$$J = \begin{bmatrix} 34 & -4 & -4 & 8 \\ & -8 & -8 & 16 \\ & & 17 & -24 \\ & & & -24 \end{bmatrix} \tag{34}$$

Results

Due to the accuracy of the error correcting and quantum manipulation technique, the short-time decoherence, the susceptibility to various noises, etc., the progress of universal quantum devices is slow, which limits the development and practical applications of Shor's algorithm. The maximum factorization ability of Shor's algorithm is currently the integer 85. However, D-Wave quantum computers have rapidly developed, and the number of qubits has been doubling every other year. Based on the quantum annealing method, we factor the integer 1028171. Although our method requires more qubits than Shor's algorithm to factor the same integer, Shor's algorithm is highly dependent on high-precision hardware. Actually, Science, Nature, and the National Academies of Sciences (NAS) are consistent in that it will be years before code-cracking by a universal quantum computer is achieved.

Integers	$p \times q$	h ranges	J ranges
143	11×13	$[-137, 130.5]$	$[-148, 79]$
59989	251×239	$[-1842, 2947]$	$[-1832, 921]$
376289	659×571	$[-4268, 7505]$	$[-4848, 2500]$

Table 4. The parameter values of Jiang *et al.*'s[30] method for integer factorization.

Integers	$p \times q$	h ranges	J ranges
143	11×13	$[-85, 86.5]$	$[-109, 66]$
59989	251×239	$[-928, 1867]$	$[-1168, 701]$
376289	659×571	$[-2886, 5039]$	$[-2103, 2048]$
1005973	997×1009	$[-3391, 4860]$	$[-2048, 2048]$
1028171	1009×1019	$[-3005, 5032]$	$[-2078, 2048]$

Table 5. The parameter values of our method for integer factorization.

Models	Local field coefficient h	Coupler strength J	qubits
Ref. [34]	10^6	10^6	419
Ref. [32]	1256	872	27
Our method	758	554	27

Table 6. Comparison of different algorithms when factoring the integer $31 \times 251 = 7781$.

The existing works based on NMR utilize the special properties of certain primes to perform principle-of-proof experiments. The maximum integer of factorization based on an NMR platform is 291311. The integer factorization method based on the NMR platform is not applicable to all integers and is not universal and scalable.

Actually, our method is general and can factor up to 20-bit (1028171) integers, making it superior to the results obtained by any other physical implementations, including general-purpose quantum platforms (the Hua-Wei quantum computing platform), and far beyond the theoretical value (factor up to 10-bit integers) that can be obtained by the latest IBM Q System One^{TM} if it can run Shor's algorithm.

Table 4 shows the parameter values of Jiang *et al.'s* method[30] for integer factorization (please note that all the data of ref. [30] are given via our simulations, just for reference). Table 5 shows the factorization results of our method for the integers 143, 59989, 376289, 1005973 and 1028171. It can be seen from Table 5 that our method can successfully factor the integers 1005973 and 1028171. Jiang *et al.'s* method can factor up to the integer 376289, whereas ours method can achieve the factorization of the integer 1028171, making it superior to the results obtained by any other physical implementations. The reduction of the qubits can reduce the hardware requirements of the quantum annealing machine and further boost the accuracy of quantum annealing, which has great practical significance. In the case of the hardware restrictions of the quantum machine, our goal is to achieve the factorization of a larger-scale integer 1028171 with fewer qubits, which is the best integer factorization result solved by the quantum algorithm.

Tables 4 and 5 show that the optimization model can further reduce the weight of the qubits and the range of the coupler strength involved in the problem model, which can advance the large-scale integers in the D-Wave machine.

Table 6 shows a comparison of the different algorithms when factoring the integer $7778 = 31 \times 251$.

Note: The values of the local field coefficient h and coupler strength J are the absolute values of the parameter ranges. Table 6 takes the maximum integer 7718 that was factored by Warren, R.H.[34] as an example and compares the coefficients of Ising model and qubits. In the actual quantum annealing experiment, the excessive coupling strength between the qubits reduces the possibility of reaching the ground state, and finally reduces the success rate of the integer factorization. It can be seen from Table 6 that the proposed method achieves the lowest local field coefficient h and coupling coefficient J, reduces the ranges of the coefficients of Ising model, and uses far fewer qubits than Warren, R.H.[34]. The reduction of the parameter value ranges can reduce the demand for qubit coupling strength, make the physical qubit flip unified, effectively increase the possibility of quantum annealing reaching the global optimal, and improve the success rate of integer factorization. In the case of insufficient precision and the immature development of existing quantum devices, the proposed method can effectively reduce the hardware requirements and improve the success rate of deciphering RSA via quantum annealing. In addition, our method successfully factors all integers within 10000, whereas Warren, R.H.[34] traversed and factored all integers within 1000.

Discussion

The integer factorization method based on the NMR platform uses the special properties of integers, and the method is not universal. The quantum annealing method based on a D-Wave quantum computer for integer factorization is limited by the hardware connection limitations of the D-Wave quantum computer, which are not enough to apply the method to larger integers.

This paper shows the optimistic potential of the quantum annealing algorithm for deciphering the RSA cryptosystem. A D-Wave using quantum annealing provides a new (second) way, which is a completely different way from Shor's algorithm. The latest IBM Q System One^{TM} can theoretically factor up to 10-bit integers using Shor's algorithm, whereas our simulations showed the huge advantages of factoring 20-bit integers (1028171) using the quantum computing software environment provided by D-Wave. Our results are superior to the results obtained by any other quantum algorithm. Compared with ref. [32], the local field coefficient h and coupling term coefficient J of Ising model are optimized to reduce the range of the model parameters by more than 33% and 26%, respectively, which reduces the coupling strength between qubits, further improves the stability of qubit chains and further improves the upper bound of integer factorization. With the slow progress of general-purpose quantum computers and the limitation of D-Wave quantum computer's topological connections, the stability of Ising model can be improved by reducing the local field coefficient h and coupling coefficient J of Ising model, which can effectively improve the upper bounds of the decomposed integers.

From the perspective of practical code-cracking and generalization, we proposed a new general quantum spin model, which is a novel and further scalable way to conduct prime factorization with few qubits and QA. Lockheed Martin's Warren, R.H.[34] traversed and factored all integers within 1000. Our method successfully factors all integers within 10000 and has obtained the best index (20-bit integers (1028171)) of quantum computing for factoring integers. The result exceeded the work of Shuxian Jiang *et al.* (factor up to 376289)[30] and Warren, R.H.[34] (factor up to 7781).

At present, the fastest classical integer factorization algorithm is the number field sieve method. Its complexity is $O(exp(c(logN)^{\frac{1}{3}})(loglogN)^{\frac{2}{3}})$ and its complexity is exponential. In theory, Shor's algorithm requires 2n qubits to factor n-bit integers, where n is the number of binary digits of the integer[13]. The complexity of our method is less than $O_{(}log^2(N)_{)}$, where N is the number to be factored. In terms of theoretical complexity, the complexity of Shor's algorithm is better than the algorithm proposed in this paper. In terms of factoring the maximum integer index, due to the slow development of general quantum devices, Shor's algorithm currently factor up to integer 85, and the maximum number that can be factored by the integer factorization method based on quantum annealing of our method is integer 1028171. To achieve the factorization of the integer 1028171, Shor's algorithm requires more than 40 universal qubits, and the number of qubits and the precision of the quantum bits are far beyond the current hardware level. Therefore, through the analysis of the factored maximum integer index, the integer factorization method based on quantum annealing has more realistic attack power than Shor's algorithm, which is expected to result in more advantages when using the real D-Wave quantum computing platform.

The current state of post quantum cryptography research exclusively referred to the potential threatens of Shor's algorithm. From the above analysis, it can be seen that quantum annealing (the core principle of the D-Wave quantum computer) for prime factorization may be closer to cracking practical RSA codes than Shor's algorithm. Furthermore, the experts of the post quantum cryptography international standard organization (in the 6th ETSI/IQC Quantum Safe Workshop) expressed great interest in our method. They analyzed the reason for neglecting the attacks from the D-Wave machine in post quantum cryptography research since the D-Wave computers, which have been purchased by Lockheed Martin, Google, etc., have been initially used for image processing, machine learning, combinatorial optimization, software verification, etc. Thus, post quantum cryptography research should further consider the potential of the D-Wave quantum computer for deciphering the RSA cryptosystem in future.

The structure of large integers will have an impact on the complexity of the model. Future research work will further study the effects of the structure of large integers on the model and the scalability of the integer factorization when using a D-Wave quantum computer to achieve larger-scale integer factorization.

Data availability

All other data used in this study are available from the corresponding authors upon reasonable request.

Received: 20 October 2019; Accepted: 19 March 2020;
Published online: 28 April 2020

References

1. Shor P W. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings 35th annual symposium on foundations of computer science* **1**, 124–134 (Murray Hill, NJ, USA, 1994).
2. Mahmud, N., El-Araby, E. & Caliga, D. Scaling reconfigurable emulation of quantum algorithms at high precision and high throughput. *Quantum Engineering* **1**, e19 (2019).
3. Lucero, E. *et al.* Computing prime factors with a josephson phase qubit quantum processor. *Nat. Phys.* **8**, 719–723 (2012).
4. Politi, A., Matthews, J. C. & O'brien, J. L. Shoras quantum factoring algorithm on a photonic chip. *Science* **325**, 1221–1221 (2009).
5. Lanyon, B. *et al.* Experimental demonstration of a compiled version of shor's algorithm with quantum entanglement. *Phys. Rev. Lett.* **99**, 250505 (2007).
6. Monz, T. *et al.* Realization of a scalable shor algorithm. *Science* **351**, 1068–1070 (2016).
7. Dang, A., Hill, C. D. & Hollenberg, L. C. L. Optimising Matrix Product State Simulations of Shor's Algorithm, *arXiv:1712.07311v2* (2017).
8. Vandersypen, L. M. *et al.* Experimental realization of shoras quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414**, 883–887 (2001).

9. Lu, C. Y., Browne, D. E., Yang, T. & Pan, J. W. Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.* **99**, 250504 (2007).
10. Martíin-López, E. *et al*. Experimental realization of shor's quantum factoring algorithm using qubit recycling. *Nat. Photonics* **6**, 773–776 (2012).
11. Geller, M. R. & Zhou, Z. Factoring 51 and 85 with 8 qubits. *Sci. reports* **3** (2013).
12. Smolin, J. A., Smith, G. & Vargo, A. Oversimplifying quantum factoring. *Nature* **499**, 163–165 (2013).
13. Gidney, C. Factoring with n + 2 clean qubits and n-1 dirty qubits, *arXiv:1706.07884* (2017).
14. Adrian, C. DOE pushes for useful quantum computing. *Science* **359**, 141–142 (2018).
15. What's coming up in 2018. *Science* **359**, 10–12 (2018).
16. Gibney, E. Quantum Computer Quest. *Nature* **516**, 24 (2014).
17. Farhi, E. *et al*. A quantum adiabatic evolution algorithm applied to random instances of an np-complete problem. *Science* **292**, 472–475 (2001).
18. Xu, N. *et al*. Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system. *Phys. Rev. Lett.* **108**, 130501 (2012).
19. Dattani, N. S. & Bryans, N. Quantum factorization of 56153 with only 4 qubits. *arXiv:1411.6758* (2014).
20. Li, Z. *et al*. High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application to the experimental factorization of 291311. *arXiv:1706.08061* (2017).
21. Tanburn, R., Okada, E. & Dattani, N. S. Reducing multi-qubit interactions in adiabatic quantum computation without adding auxiliary qubits. part 1: The "deduc-reduc" method and its application to quantum factorization of numbers. *arXiv:1508.04816* (2015).
22. Okada, E., Tanburn, R. & Dattani, N. S. Reducing multi-qubit interactions in adiabatic quantum computation without adding auxiliary qubits. part 2: The "split-reduc" method and its application to quantum determination of ramsey numbers. *arXiv:1508.07190* (2015).
23. King, A. D. *et al*. Observation of topological phenomena in a programmable lattice of 1,800 qubits. *Nature* **560**, 456–460 (2018).
24. Das, A. & Chakrabarti, B. K. Colloquium: Quantum annealing and analog quantum computation. *Reviews of Modern Physics* **80**, 1061 (2008).
25. Neukart, F. *et al*. Traffic flow optimization using a quantum annealer. *Frontiers in ICT* **4**, 29 (2017).
26. Perdomo-Ortiz, A., Dickson, N., Drew-Brook, M., Rose, G. & Aspuru-Guzik, A. Finding low-energy conformations of lattice protein models by quantum annealing. *Sci. Reports* **2**, 571 (2012).
27. Dridi, R. & Alghassi, H. Prime factorization using quantum annealing and computational algebraic geometry. *Sci. Reports* **7** (2017).
28. Hu, F., Wang, B., Wang, N. & Wang, C. Quantum machine learning with D-wave quantum computer. *Quantum Engineering* **1**, e12 (2019).
29. Wang, B., Zhang, H. F., Wang, H. & From, C. Evolutionary Cryptography to Quantum Artificial Intelligent Cryptography (in Chinese). *Journal of Computer Research and Development* **56**, 2112–2134 (2019).
30. Jiang, S., Britt, K. A., McCaskey, A. J., Humble, T. S. & Kais, S. Quantum Annealing for Prime Factorization. *Sci. Reports* **8**, 17667 (2018).
31. Hu, F. *et al*. Quantum computing cryptography: Unveiling cryptographic Boolean functions with quantum annealing. *arXiv: 1806.08706* (2018).
32. Peng, W. *et al*. Factoring larger integers with fewer qubits via quantum annealing with optimized parameters. *SCIENCE CHINA Physics, Mechanics & Astronomy.* **62**, 60311 (2019).
33. Wang, X. Quest towards "factoring larger integers with commercial D-Wave quantum annealing machines". *SCIENCE CHINA Physics, Mechanics & Astronomy.* **62**, 960331 (2019).
34. Warren, R. H. Factoring on a quantum annealing computer. *Quantum Information and Computation* **19**, 0252–0261 (2019).
35. Boros, E. & Hammer, P. L. Pseudo-boolean optimization. Discret. *applied mathematics* **123**, 155–225 (2002).

Acknowledgements

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

Author contributions

B.W. designed the algorithm. B.W. and H.Y. conceived the experiments and analysed the results. B.W., F.H., H.Y. and C.W. wrote and reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information is available for this paper at https://doi.org/10.1038/s41598-020-62802-5.

Correspondence and requests for materials should be addressed to C.W.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.