Luo et al. *EPJ Quantum Technology* (2026) 13:1
https://doi.org/10.1140/epjqt/s40507-025-00449-9

EPJ.org

EPJ Quantum Technology

RESEARCH Open Access

General integer factorization algorithm based on Ising machine

Zhang Luo[1], Yifan Yuan[1], Zhicheng Wang[1], Mingche Lai[1] and Pingjing Lu[1*]

*Correspondence:
pingjinglu@nudt.edu.cn
[1]College of Computer Science and Technology, National University of Defense Technology, Changsha, 410073, China

Abstract

Integer factorization, a fundamental problem in computational mathematics, holds critical significance for modern cryptography, particularly in RSA encryption. Traditional approaches such as the number field sieve face exponential complexity limitations, while Shor's quantum algorithm remains impractical due to hardware constraints. This study proposes a universal algorithm for integer factorization based on Ising machines by transforming the problem into a Quadratic Unconstrained Binary Optimization (QUBO) formulation. The algorithm introduces an optimal reduction formula to optimize the parameter ranges of local field coefficients (h) and coupling coefficients (J) in the Ising model. Additionally, a non-uniform column grouping method is employed to resolve the conflict between coefficient ranges and carry auxiliary quantum bits(qubits), minimizing the number of auxiliary qubits with minimal compromise on coefficient ranges. Using this approach, we successfully factorized the 22-bit integer 2,093,809 with only 118 qubits. Extrapolating to existing photonic Ising machines with 100,000 qubits, our method demonstrates the potential to factorize 631-bit integers, highlighting its promise for efficient large-scale integer factorization. All results presented in this paper are obtained from simulations on Fixstars Amplify and D-Wave simulators.

Keywords: Integer factorization; Ising machine; QUBO; Hamiltonian

1 Introduction

Integer factorization is a fundamental problem in computational mathematics with significant implications for modern cryptography, particularly RSA encryption. The security of RSA encryption is based on the computational difficulty of factoring large numbers, making integer factorization a computationally challenging task. As the size of an integer increases, classical factorization methods, such as trial division and the general number field sieve (GNFS) method [1], become infeasible due to their exponential time complexity. Shor's algorithm is considered one of the most promising quantum approaches for integer factorization [2], with a computational complexity of $O(\log^3 N)$, which may provide a potential computational advantage over all currently known classical algorithms. Furthermore, multiple studies have demonstrated the feasibility of Shor's algorithm for small-scale integer factorization [3–6]. However, despite its theoretical efficiency, its practical

Springer

application—such as factoring a commonly used 2048-bit RSA key—requires large-scale, fault-tolerant quantum computers, which remain beyond the reach of current technology. This limitation has motivated researchers to explore alternative approaches.

The Ising model has gained increasing recognition as an effective framework for solving combinatorial optimization problems. Many NP-hard and NP-complete problems can be reformulated as Quadratic Unconstrained Binary Optimization (QUBO) problems and subsequently mapped onto an Ising Hamiltonian. By solving the Ising model and determining the ground state (i.e., the lowest energy configuration) of the Hamiltonian, the optimal solution to the original problem can be obtained. Zheng et al. mapped the Perfect Matching Problem and the Subset Sum Problem (SSP) onto the Ising model and demonstrated small-scale implementations of the solution on a superconducting quantum computer, showing good success probability [7, 8]. N. Mohseni et al. employed the Ising machine to solve various combinatorial optimization problems, including the Traveling Salesman Problem (TSP) and the Boolean Satisfiability Problem (SAT), and compared the performance of different types of Ising machines [9–11]. Additionally, the MAX-CUT problem has also been formulated as an Ising model and successfully solved using various types of Ising machines [5, 12–14]. In this context, the Ising model has been introduced to the integer factorization problem, offering a novel possibility for cryptographic research. Since integer factorization involves finding the optimal combination of two prime factors in a vast and complex solution space, it can be considered a special case of combinatorial optimization. This characteristic provides the theoretical foundation for transforming the problem into an energy optimization problem within the Ising model. By constructing a specific objective function, the integer factorization problem can be mapped onto the Ising model, where the system tends to find low-energy configurations that correspond to the optimal or near-optimal solution of the problem.

Recent advancements in the development of Ising machines have led to substantial improvements in scalability and computational efficiency. Quantum Ising Machines (QIMs), such as D-Wave's quantum annealers, efficiently solve optimization problems through the quantum tunneling effect of qubits, showing promising results in combinatorial optimization. Raouf Dridi et al. applied algebraic geometry methods to prime factorization [15], using quantum annealing to solve these equations on quantum devices. They demonstrated the factorization of 200,099 on the D-Wave 2X system. Jiang et al. used 94 logical qubits on the D-Wave 2000Q system to construct a universal model for the factorization of the integer 376,289 [16]. Building upon Jiang's work, Wang et al. proposed a new method based on optimizing Ising model parameters [17, 18], factoring the integer 1,028,171. Additionally, numerous studies have shown that optimizing Ising model parameters can significantly enhance the application of quantum computing in prime factorization [19–22]. Quantum computing for integer factorization holds great promise, but it is still constrained by hardware limitations. The latest D-Wave Advantage system, equipped with over 5000 qubits, can tackle optimization challenges but is only capable of factoring integers of moderate size [23]. The Photonic Ising Machine (PIM) represents the spins of the Ising model photonically, with the spins traveling through the physical hardware of the Ising solver, rather than being fixed to specific locations. PIMs exhibit significant potential for large-scale combinatorial optimization [24–27]. They utilize optical interference, degenerate optical parametric oscillators (DOPO), and photon coupling to solve optimization problems by simulating spin interactions [28, 29]. Compared to traditional methods, PIMs offer su-

perior speed, parallelism, and energy efficiency. In typical photonic Ising machines, each Ising spin s_i is encoded in the binary phase of a degenerate optical parametric oscillator (DOPO) pulse (0 or π), and pairwise couplings J_{ij} are implemented by optical interference, mutual injection, or measurement-feedback loops that modulate the injection field. Under gain competition and nonlinear saturation, the network relaxes toward low-energy configurations of the effective Ising Hamiltonian:

$$H = -\sum_{i<j} J_{ij} s_i s_j - \sum_i h_i s_i$$

The resulting steady-state phase configuration corresponds to a low-energy solution of the Ising problem. This mechanism forms the foundation of the coherent Ising machine (CIM), which has been extensively studied in both theoretical and experimental contexts [25]. The collective coherence among DOPOs plays a critical role in determining computational performance. Phase locking ensures global coupling across the oscillator network, enabling the system to explore a high-dimensional energy landscape simultaneously rather than through sequential updates. The first experimental validation was reported by Marandi et al. [30], who demonstrated that optical interference and mutual injection among time-multiplexed DOPO pulses can realize binary spin representation and collective energy minimization. From a theoretical perspective, stochastic and Fokker–Planck models describe the CIM dynamics as a Boltzmann-like distribution, with an effective optical temperature defined by quantum noise [31]. This model explains how gain saturation and quantum fluctuations jointly guide the system toward the ground state. In contrast to electronic or quantum annealers, PIMs utilize deterministic nonlinear relaxation rather than thermal or quantum tunneling to reach low-energy configurations. Consequently, they operate at room temperature and achieve nanosecond-level update rates with extremely low power consumption. For example, fiber-based CIM implementations have demonstrated per-spin energy dissipation at the femtojoule scale [32]. Recent large-scale experiments further extended this concept to more than one hundred thousand optical spins, confirming the scalability of the CIM approach. These developments establish photonic Ising machines as an intermediate computational paradigm between analog optical computing and quantum-inspired optimization, combining physical parallelism, scalability, and energy efficiency. On fiber-optic platforms, PIMs have achieved 20,736 spins and solved combinatorial optimization problems, leveraging high parallelism [33]. In integrated photonic platforms, PIMs demonstrate compactness, supporting 16,384 spins while solving Max-Cut and other optimization problems [34]. T. Honjo et al. employed a coherent Ising machine (CIM) based on 100,512 decoherent optical parametric oscillator pulses as Ising spins and successfully solved the Max-Cut problem for a graph with 100,000 nodes [35]. Overall, Ising machines have seen remarkable progress, transitioning from theoretical models to practical computational tools with growing capabilities. Quantum and photonic implementations have expanded the potential of Ising machines, offering promising solutions for solving complex combinatorial optimization problems.

This study builds upon the prior work of Jiang [16] and Wang [17, 18] but abandons their instance-specific derivations aimed at reducing quantum space complexity. The proposed general integer factorization algorithm can be implemented on optical Ising machines, as illustrated in Fig. 1, with $\left\lfloor \frac{1}{4}(\log_2 N + 2)^2 \right\rfloor - 4$ qubits, the classical preprocessing

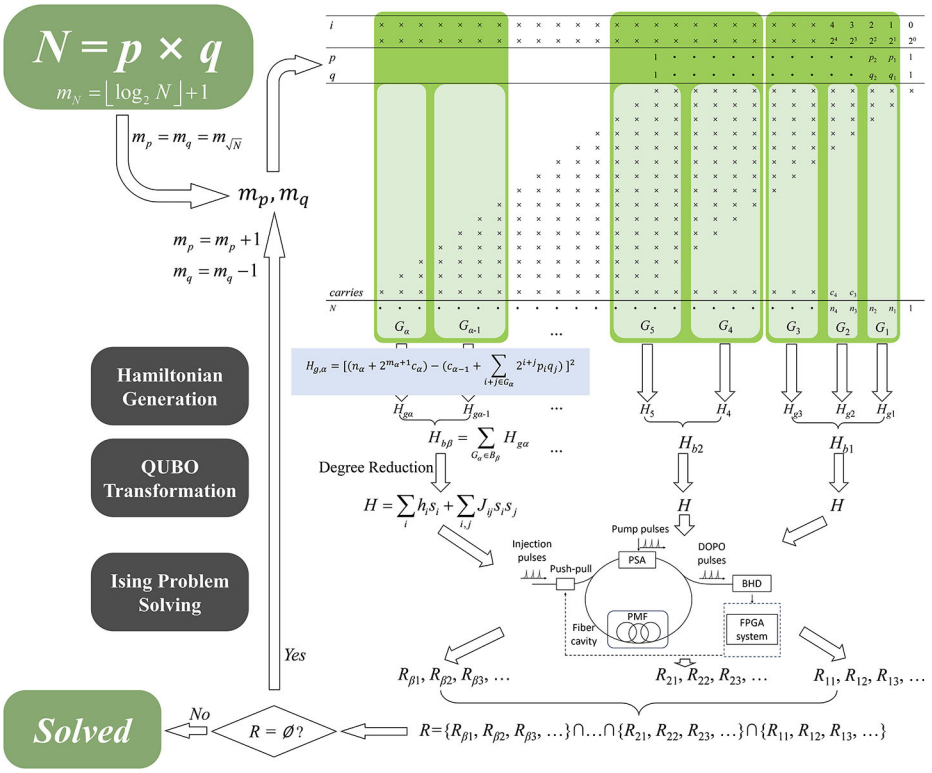


Figure 1 General integer factorization algorithm based on the Ising model. The overall process includes the transformation of the integer factorization problem into a QUBO problem, the column group division algorithm, and the optimization of the Ising model's local field coefficients *h* and coupling coefficients *J*. Finally, use the Ising machine to solve it

step required to map the problem into QUBO form has a time complexity of $O(\log^3 N)$, where N is the integer to be factorized. By introducing a minimal degree-reduction formula and a non-uniform grouping strategy, the algorithm significantly narrows the required parameter ranges of the Ising model's pairwise interaction terms (J_{ij}) and external magnetic field terms (h_i), thereby simplifying problem-solving while maintaining minimal quantum space complexity. Simulations on the D-Wave Hybrid and Fixstars Amplify platforms demonstrated the successful factorization of a 22-bit integer (2,093,809) using 118 qubits. To further reduce quantum resource demands, we adopted a section-based solving approach, decomposing a 20-bit integer (1,028,171) with only 44 qubits; however, the algorithm's completeness and robustness under this approach require further validation for broader reliability. Even though, our approach demonstrates the potential of Ising model-based algorithms for efficient integer factorization and presents promising results for scaling to larger integers.

2 Results

2.1 Multiplication table for factorization

The integer factorization problem involves decomposing a known integer N into its prime factors p and q (where $p \geq q$ without loss of generality), which is the inverse problem of computing $p \times q$. Since primes other than 2 are all odd numbers, p and q can be represented in binary as $p = (1p_{m_p-2}p_{m_p-3}\ldots p_1 1)_2$ and $q = (1q_{m_q-2}q_{m_q-3}\ldots q_1 1)_2$, respectively.

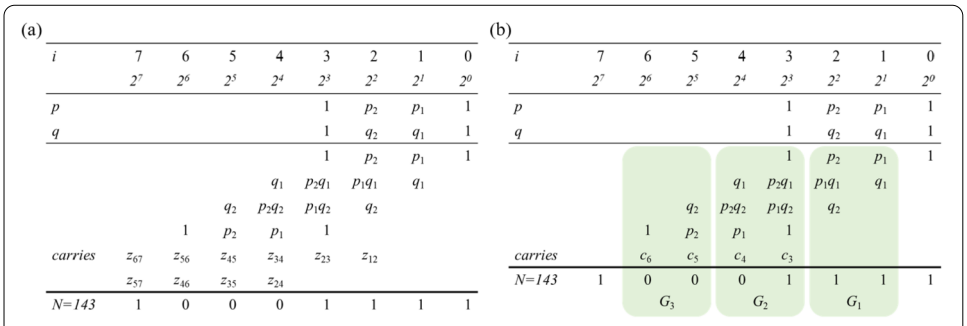


Figure 2 Multiplication table for 143 = 13 × 11 in binary. In the multiplication table, z_{ij}, the carry terms from Column i to Column j, is replaced by fewer carry term c_i due to the grouping advantage. All the variables in the table are either 0 or 1

Here, p_i and q_i denote the i-th binary digit of p and q, while $m_p = \lfloor \log_2 p \rfloor + 1$ and $m_q = \lfloor \log_2 q \rfloor + 1$ represent the binary bit-lengths of p and q, respectively. A multiplication table is introduced to illustrate the binary processing approach for integer factorization.

The traditional factorization of 143 = 13 × 11 is shown in Fig. 2a. The Hamiltonian is defined as the column-wise sum of squared deviations as follows:

$$\begin{aligned} H = {} & (p_1 + q_1 - 1 - 2z_{12})^2 + (p_2 + p_1q_1 + q_2 + z_{12} - 1 - 2z_{23} - 4z_{24})^2 \\ & + (1 + p_2q_1 + p_1q_2 + 1 + z_{23} - 1 - 2z_{34} - 4z_{35})^2 \\ & + (q_1 + p_2q_2 + p_1 + z_{24} + z_{34} - 2z_{45} - 4z_{46})^2 \\ & + (p_2 + q_2 + z_{45} + z_{35} - 2z_{56} - 4z_{57})^2 \\ & + (1 + z_{56} + z_{46} - 2z_{67})^2 + (z_{56} + z_{46} - 1)^2 \end{aligned} \tag{1}$$

where auxiliary bit z_{ij} is the carry term from Column i to Column j. Obviously, the Hamiltonian H reaches its minimum value 0 when it is a solution of the factorization problem. To reduce auxiliary variable overhead, Jiang et al. introduced a grouped-column multiplication table [17], as shown in Fig. 2b, where each column has only a single carrier bit. And the Hamiltonian, which is redefined as the sum of squared deviations for each column group, is simplified as follows:

$$\begin{aligned} H = {} & (2p_2 + 2p_1q_1 + 2q_2 + p_1 + q_1 - 8c_4 - 4c_3 - 3)^2 \\ & + (2q_1 + 2p_2q_2 + 2p_1 + 2c_4 + c_3 - 8c_6 - 4c_5 + p_2q_1 + p_1q_2 + 1)^2 \\ & + (p_2 + q_2 + 2c_6 + c_5 - 2)^2 \end{aligned} \tag{2}$$

It is worth noting that Wang et al. determined the exact values of certain bits through manual analysis and calculation, further proposing a method to factor 143 using only 4 bits. However, this strategy is only effective for smaller factorization values and lacks general applicability. In this work, we still adopt their original multiplication table approach.

Since the Ising model can only handle 2-local terms, higher-local terms need to be reduced to 2-local terms. In the binary system, squared terms can be simplified as $p^2 = p$, $q^2 = q$, $c^2 = c$. For 3-local terms, the equations presented as follows were utilized by Jiang et al. for degree reduction [36].

Table 1 Parameter comparison of different methods of factoring the integer 143

	$\begin{cases} x_1x_2x_3 \le x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4) \\ -x_1x_2x_3 \le -x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4) \end{cases}$	$\begin{cases} x_1x_2x_3 \le x_1x_2 - x_1y_{12} - x_2y_{12} + x_3y_{12} + y_{12} \\ -x_1x_2x_3 \le -x_1y_{12} - x_2y_{12} - x_3y_{12} + 2y_{12} \end{cases}$
$\boldsymbol{h}$	[130.5 107.5 130.5 107.5 –41 –82 3 6 –137 –81 –107 –81] range: [–137, 130.5]	[–22.25 –22.75 –22.25 –22.75 20.5 41 –1.5 –3 16 10 10 19] range: [–22.75, 41]
$\boldsymbol{J}$	$\begin{bmatrix} 2 & 79 & 47.5 & -2 & -4 & -8 & -16 & -148 & -84 & 0 & 0 \\ & 47.5 & 71 & -8 & -16 & 1 & 2 & 6 & 6 & -124 & -84 \\ & & 2 & -2 & -4 & -8 & -16 & -148 & 0 & 0 & -84 \\ & & & -8 & -16 & 1 & 2 & 6 & -84 & -124 & 6 \\ & & & & 34 & -4 & -8 & -8 & 1 & 2 & 1 \\ & & & & & -8 & -16 & -16 & 2 & 4 & 2 \\ & & & & & & 34 & 0 & -4 & -8 & -4 \\ & & & & & & & 0 & -8 & -16 & -8 \\ & & & & & & & & 0 & 1 & 0 \\ & & & & & & & & & 0 & 0 \\ & & & & & & & & & & 0 \end{bmatrix}$ range: [–148, 79]	$\begin{bmatrix} 1 & 6.5 & 6.75 & -1 & -2 & -4 & -8 & -16 & -10 & 1 & 2 \\ & 6.75 & 11.5 & -4 & -8 & 0.5 & 1 & 2 & 1 & -10 & -19 \\ & & 1 & -1 & -2 & -4 & -8 & -16 & 1 & -10 & 2 \\ & & & -4 & -8 & 0.5 & 1 & 2 & -10 & 1 & -19 \\ & & & & 17 & -2 & -4 & -4 & 0.5 & 0.5 & 1 \\ & & & & & -4 & -8 & -8 & 1 & 1 & 2 \\ & & & & & & 17 & 0 & -2 & -2 & -4 \\ & & & & & & & 0 & -4 & -4 & -8 \\ & & & & & & & & 0 & 0 & 0 \\ & & & & & & & & & 0.5 & 0 \\ & & & & & & & & & & 0 \end{bmatrix}$ range: [–19, 17]

$$\begin{cases} x_1x_2x_3 \le x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4) \\ -x_1x_2x_3 \le -x_4x_3 + 2(x_1x_2 - 2x_1x_4 - 2x_2x_4 + 3x_4) \end{cases} \tag{3}$$

To clarify the auxiliary variable definition, we modify the original expression by introducing y_{12} as an auxiliary variable explicitly defined as $y_{12} = x_1x_2$. This substitution ensures that the equality constraint in the inequality formulation is properly satisfied. The integer factorization problem has been transformed into a QUBO problem. Further, replace the binary variables $x_i \in \{0, 1\}$ with qubits s_i that take values in $\{+1, -1\}$ using $x_i = (1 + s_i)/2$, and transform them into matrix form, then we have the coupling matrix $\boldsymbol{J}$ and the local fields $\boldsymbol{h}$ that an Ising model is formulated.

In fact, the reduction of the model parameters is beneficial to reducing the hardware requirements and the precision of an Ising machine. However, coefficients "2" and "3" in Eq. (3) violate such guideline. Wang et al. optimized Eq. (3) and proposed a new order reduction method from the 3-local term to 2-local term [37], as shown below:

$$\begin{cases} x_1x_2x_3 \le x_1x_2 - x_1y_{12} - x_2y_{12} + x_3y_{12} + y_{12} \\ -x_1x_2x_3 \le -x_1y_{12} - x_2y_{12} - x_3y_{12} + 2y_{12} \end{cases} \tag{4}$$

The equality holds for both inequalities when the auxiliary variable $y_{12} = x_1x_2$. The optimization of the 3-local terms has reached its optimal form, yet no formulation exists where coefficients are all 1 or −1. By iteratively applying the degree-reduction formula for 3-local terms and introducing only two replicable auxiliary variables, we can directly reduce positive 4-local terms to 2-local terms as follows

$$x_1x_2x_3x_4 \le x_1x_2 + x_3x_4 - x_1y_{12} - x_2y_{12} - x_3y_{34} - x_4y_{34} + y_{12}y_{34} + y_{12} + y_{34} \tag{5}$$

Based on Eq. (4) and Eq. (5), the parameters of the model are significantly reduced, as shown in Table 1.

3 Non-uniform column groups division

As previously discussed, the grouping strategy proposed by Jiang et al. effectively reduces the quantum space complexity of integer factorization by minimizing carry variables and

qubit count. However, determining an optimal group width remains a fundamental challenge. A group width that is too small cannot always limit the number of carry terms to one per column, especially in columns with numerous summation terms—degenerating, in the extreme case, into the basic multiplication table shown in Table 1. Conversely, excessively large group widths introduce high-bit weights within each group, generating overly large coupling coefficients (J) and disrupting the balance of the Ising system.

Although nonuniform column-grouping strategies have been previously explored, such as those employed in Wang et al., these approaches rely on manually determined and problem-specific grouping rules. Their group widths are typically chosen empirically for individual instances, lacking a generalizable or reproducible principle for selecting the optimal configuration. Consequently, such heuristic methods cannot guarantee balanced carry control or coefficient stability when applied to different composite numbers or bit-lengths.

To address these limitations, this work proposes a general and fully automated nonuniform column-grouping algorithm. The algorithm adaptively assigns smaller group widths to sparse regions with fewer summation terms and larger widths to dense regions with more terms. This ensures exactly one carry term per column while keeping the coefficient range within a stable bound. By balancing the trade-off between carry reduction and coefficient magnitude, the proposed method provides a systematic, hardware-independent, and reproducible grouping mechanism that extends and generalizes previous heuristic approaches.

Examining the multiplication table, the summation terms in each column first incrementally increase from 1 to a maximum value of m_q, then progressively decrease back to 1 starting from the m_p-th column. For subsequent discussions, we define a column group G_α as an increasing group if the summation terms of its constituent columns exhibit a strictly increasing trend. Conversely, a column group G_α is termed a decreasing group if the summation terms of its columns strictly decrease. The group containing the longest column (i.e., the column with the length of m_q) is designated as the peak group.

The width w_α of a column group G_α is determined by the carry width provided by its preceding column group $G_{\alpha-1}$. The carry of a column group G_α providing to its next column group is given by:

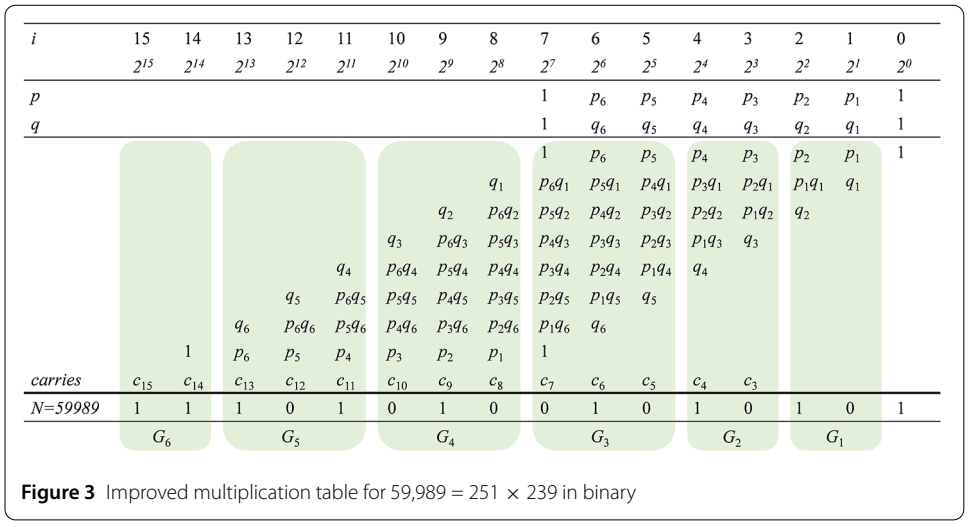
$$c_{out,\alpha} = \begin{cases} h_{t,\alpha} - 1 & \text{if } G_\alpha \text{ is an increasing group} \\ h_{t,\alpha} & \text{elsewise} \end{cases} \tag{6}$$

where $h_{t,\alpha}$ represents the length of the longest column in G_α.

$$h_{t,\alpha} = \begin{cases} \sum_{i=0}^{\alpha} w_i & \text{if } G_\alpha \text{ is an increasing group} \\ m_p + m_q - \sum_{i=0}^{\alpha} w_i & \text{elsewise} \end{cases} \tag{7}$$

The proof of this theory is provided in the supplementary materials by mathematical induction. At last, we have the recurrence formula of group width

$$w_\alpha = \begin{cases} 1, \ \alpha = 0 \\ 2, \ \alpha = 1 \\ \left\lfloor \log_2 \sum_{i=0}^{\alpha-1} w_i \right\rfloor + 1, & \text{if } G_{\alpha-1} \text{ is an increasing group} \\ \left\lfloor \log_2 (m_p + m_q - \sum_{i=0}^{\alpha-1} w_i) \right\rfloor + 1 & \text{elsewise} \end{cases} \tag{8}$$



i	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
	2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
p									1	p_6	p_5	p_4	p_3	p_2	p_1	1
q									1	q_6	q_5	q_4	q_3	q_2	q_1	1
									1	p_6	p_5	p_4	p_3	p_2	p_1	1
								q_1	p_6q_1	p_5q_1	p_4q_1	p_3q_1	p_2q_1	p_1q_1	q_1	
							q_2	p_6q_2	p_5q_2	p_4q_2	p_3q_2	p_2q_2	p_1q_2	q_2		
						q_3	p_6q_3	p_5q_3	p_4q_3	p_3q_3	p_2q_3	p_1q_3	q_3			
					q_4	p_6q_4	p_5q_4	p_4q_4	p_3q_4	p_2q_4	p_1q_4	q_4				
				q_5	p_6q_5	p_5q_5	p_4q_5	p_3q_5	p_2q_5	p_1q_5	q_5					
			q_6	p_6q_6	p_5q_6	p_4q_6	p_3q_6	p_2q_6	p_1q_6	q_6						
		1	p_6	p_5	p_4	p_3	p_2	p_1	1							
carries	c_{15}	c_{14}	c_{13}	c_{12}	c_{11}	c_{10}	c_9	c_8	c_7	c_6	c_5	c_4	c_3			
N=59989	1	1	1	0	1	0	1	0	0	1	0	1	0	1	0	1
	G_6		G_5			G_4			G_3			G_2		G_1		

Figure 3 Improved multiplication table for 59,989 = 251 × 239 in binary

Table 2 The parameter values of different column group division for 59,989 = 251 × 239

	Column group division methods	Qubits	*J* ranges	*h* ranges
Wang's [17, 18]	[3, 5, 6, 7, 8, 9, 12]	68	[–505, 520]	[–764, 375.5]
	[3, 5, 7, 9, 12]	62	[–501, 520]	[–860, 467.5]
	[3, 6, 9, 12]	59	[–682, 520]	[–892, 977]
	[4, 8, 12]	56	[–2413, 2056]	[–4380, 2789.5]
	[6, 12]	53	[–36,996, 32,776]	[–37,980, 29,257.5]
This Work	[2, 4, 7, 10, 13]	61	[–373, 206]	[–196, 260]

where the initial values, w_0 and w_1, are determined as 1 and 2 to optimize the grouping. By minimizing both the number of carry bits and the inter-bit coupling, this algorithm significantly reduces the overall computational complexity.

By employing this non-uniform grouping strategy, each column maintains a single-bit carry term, with each group contributing its carry solely to a single subsequent group while receiving its carry exclusively from a single preceding group. This approach minimizes the number of carry variables, reduces the width of each group to the minimum necessary, and eliminates unnecessary growth of coupling coefficients, thereby significantly reducing the overall computational complexity. Based on such algorithm, the decomposition multiplication table for N = 59,989 is shown in Fig. 3, which can be partitioned into 6 columns.

Table 2 presents a parameter comparison for factoring 59,989 under different column grouping strategies. In the "Column group division" column, the numbers within parentheses denote the boundaries of group divisions, where each number i signifies the grouping between column i and column i + 1. Notably, compared to Wang's approach, our column grouping strategy demonstrates superior performance in balancing the required qubit count and coupling coefficient ranges. When the quantum space complexity is comparable, our proposed grouping strategy achieves a narrower distribution of coupling coefficients. Although this advantage may not be evident in this specific example, it becomes more pronounced as the size of the integer to be factored increases.

Table 3 presents the results of our method for factoring 143, 59,989, 376,289, 1,005,973, 108,171, and 2,093,809, along with a comparison against other approaches.

Table 3 Comparison of different algorithms for integer factorization

Integers	$p \times q$	Wang's [17, 18]	Our method	Qubits
143	13 × 11	*h* [–82, 50.5] *J* [–61, 42]	*h* [–22.25, 41] *J* [–19, 17]	12
59,989	251 × 239	*h* [–860, 467.5] *J* [–501, 520]	*h* [–196, 260] *J* [–373, 206]	61
376,289	659 × 571	*h* [–2886, 5039] *J* [–2103, 2048]	*h* [–1365, 1628] *J* [–764, 1040]	96
1,005,973	1009 × 997	*h* [–3391, 4860] *J* [–2048, 2048]	*h* [–1380, 1340] *J* [–764, 1040]	97
1,028,171	1019 × 1009	*h* [–3005, 5032] *J* [–2078, 2048]	*h* [–1332, 1316] *J* [–764, 1040]	97
2,093,809	1447 × 1447		*h* [–884, 1040] *J* [–1473.5, 1116]	118

To verify the correctness of the factorization, the theoretical lowest value of the Hamiltonian for this model can be utilized to efficiently which is given by:

$$H_{\min} = -\sum_i h_i + \sum_{i,j} J_{ij} - \sum_i n_i \tag{9}$$

where h_i and J_{ij} are respectively elements in $\boldsymbol{h}$ and $\boldsymbol{J}$, and n_i are binary digits of N. Equation (9) denotes the theoretical ground-state energy of the proposed Ising Hamiltonian. When the quantum annealer or Ising machine reaches this energy, the associated spin configuration encodes the correct factors of the target integer. Thus, this value provides a reference criterion for verifying the correctness of the obtained factorization result.

It should be noted that the reduction in the coefficient ranges of h and J observed in the proposed formulation is not the result of any artificial rescaling or normalization. All coefficients are derived directly from the Hamiltonian constructed through the column-grouping and reduction process.

The observed narrowing of the coefficient range is therefore an intrinsic outcome of the modeling algorithm, which reorganizes the multiplication terms to achieve a more balanced distribution of interactions.

Although the degree of reduction may vary for different problem instances, the proposed framework generally produces smaller and more uniformly distributed coefficients, which facilitates numerical stability and solver compatibility without compromising formulation accuracy. The proposed modeling framework demonstrates improved scalability under given physical constraints. By optimizing the Hamiltonian formulation and eliminating redundant coupling terms, the model utilizes available qubits and coupling resources more efficiently. As a result, it can solve larger integer factorization instances within the same hardware limitations, showing better adaptability to constrained Ising architectures.

Figure 4. illustrates the energy distribution obtained from 2000 sampled solutions using the Fixstars Amplify platform for the factorization of 1,028,171 = 1019 × 1009. The histogram shows the frequency of each energy level encountered during the sampling process. Among these results, 513 samples reached the lowest energy state, corresponding to the correct factorization solution, indicating the effectiveness of the proposed Hamiltonian formulation and its convergence behavior during optimization.

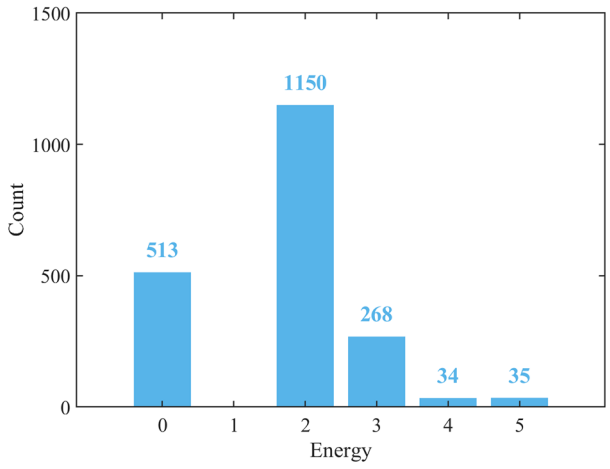


Figure 4 Histogram of energy values obtained from 2000 sampled solutions using the Fixstars Amplify platform for the factorization of 1,028,171 = 1019 × 1009. A total of 513 samples reached the lowest energy state, corresponding to the correct factorization result

Table 4 Complexity analysis of integer factorization

Process	Space complexity	Time complexity
Determine p, q bit length	$(m_p - 2) + (m_q - 2)$	
Build multiplication Table & carries	$m_N - 3$	$\Theta(\log N)$
Column group division		$\Theta(\log^2 N)$
Hamiltonian generation		$\Theta(\log^3 N)$
Degree reduction	$(m_p - 2)(m_q - 2)$	$\Theta(\log^3 N)$
Total	$Q = m_p m_q - (m_p + m_q - m_N) - 3$	$\Theta(\log^3 N)$

The reported complexity refers to the time required for the classical preprocessing step that maps the integer factorization problem into QUBO form, rather than the runtime of the quantum (or photonic) solver itself

4 Computational complexity

Table 4 presents the qubit requirements for various algorithms to factor different integers. For instance, our method requires 118 qubits to factor the largest integer 2,093,809. In reality, Ising machines are constrained by their physical characteristics and fabrication processes, limiting the scale of Ising problems they can solve—a key physical metric for Ising machines. Consequently, the quantum space complexity (i.e., the number of qubits required) of the factorization algorithm is a critical metric for evaluating its performance.

To formalize this, we define the bit length of integer N in binary representation as $m_N = \lfloor \log_2 N \rfloor + 1$, and the bit lengths of the factors p and q as m_p and m_q, respectively. Then the quantum space complexity Q is composed of three components:

1. Binary digits p_i and q_i to bits represent factors p and q: $(m_p - 2) + (m_q - 2)$ qubits.
2. Carrier auxiliary variables c_i: $m_N - 3$ qubits.
3. Auxiliary variables y_{ij} for order reduction: $(m_p - 2)(m_q - 2)$ qubits.

The total number of qubits required is

$$Q = m_p m_q - (m_p + m_q - m_N) - 3 \tag{10}$$

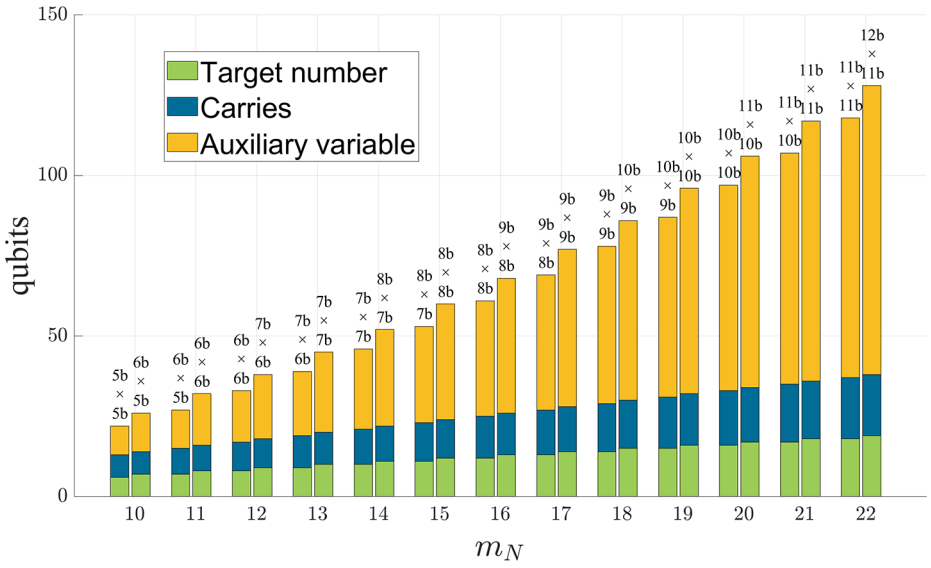


Figure 5 The Quantum space complexity of the algorithm. The number of qubits required to factorize an m_N-bit number N into m_p-bit and m_q-bit number pair

Notice that $m_p + m_q$ equals m_N or $m_N - 1$ according to the multiplication rule, and thus the quantum space complexity

$$Q \leq \frac{1}{4}m_N^2 - 3, \quad \text{for } m_N > 2 \tag{11}$$

It is quadratic, and the quadratic contribution comes from the auxiliary variables y_{ij} for order reduction, rather than the target factors p and q, as show in Fig. 5.

Following the scaling relation expressed in Eq. (11), and assuming performance comparable to existing photonic Ising architectures with 100,000 operational spins, we extrapolate that our proposed modeling framework is capable of handling integer factorization tasks up to 631 bits. This extrapolation provides a quantitative indication of the scalability and computational potential of the proposed Ising-based formulation.

Time Complexity for column group G_α, the Hamiltonian is

$$H_\alpha = (n_\alpha + 2^{m_\alpha+1}c_{out,\alpha} - c_{in,\alpha} - \sum_{i+j\in G_\alpha} 2^{i+j}p_i q_j)^2 \tag{12}$$

where n_α and $c_{in,\alpha}$ are both m_α-bit wide, and $c_{out,\alpha}$ is $m_{\alpha+1}$-bit wide. The count of $p_i q_j$ terms is $\sum_{i\in G_\alpha} h_i$.

Since only the terms involving n_α in the Hamiltonian need to be recalculated for different problems, the number of operations involving n_α is the focus of the subsequent discussion on time complexity. Ignoring the determined weights of each term, which is in the form of powers of 2, the multiply-add-operation in the Hamiltonian is:

$$op[H_\alpha] = op[(\sum_{m_\alpha} n_{\alpha,i} + \sum_{m_{\alpha+1}} c_{out,\alpha,i} - \sum_{m_\alpha} c_{in,\alpha,i} - \sum_{\sum_{i\in G_\alpha} h_i} p_i q_j)^2]$$

$$
\begin{aligned}
&= op[(\sum_{m_\alpha} n_{\alpha,i})^2] + op[2(\sum_{m_{\alpha+1}} c_{out,\alpha,i} - \sum_{m_\alpha} c_{in,\alpha,i} - \sum_{\sum_{i\in G_\alpha} h_i} p_i q_j) \sum_{m_\alpha} n_{\alpha,i}] \\
&= 2m_\alpha^2 + m_\alpha m_{\alpha+1} + m_\alpha \sum_{i\in G_\alpha} h_i
\end{aligned} \tag{13}
$$

It can be proved that

$$
\sum_\alpha m_\alpha \sum_{i\in G_\alpha} h_i = \Theta(h_m \sum_\alpha m_\alpha^2) = \Theta(m_N^3) \tag{14}
$$

where $m(N)$ is the binary bit width of the number to be factorized. The approximation $h_m \approx m(N)/2$ and the inequality

$$
\sum_\alpha m_\alpha^2 \leq (\sum_\alpha m_\alpha)^2 = m_N^2 \tag{15}
$$

are used in the proof process. Taking into account that $m_{\alpha+1} = m_\alpha$ or $m_\alpha \pm 1$, the time complexity of mapping the factorization problem to the Ising model is:

$$
\begin{aligned}
\sum_\alpha op[H_\alpha] &= \Theta(\sum_\alpha m_\alpha^2) + \Theta(\sum_\alpha m_\alpha m_{\alpha+1}) + \Theta(\sum_\alpha m_\alpha \sum_{i\in G_\alpha} h_i) \\
&= \Theta(m_N^2) + \Theta(m_N^2) + \Theta(m_N^3) \\
&= \Theta(m_N^3)
\end{aligned} \tag{16}
$$

The proof of this statement is provided in the supplementary materials.

5 Column blocks division

Recent studies have also explored dividing the multiplication table into several independent blocks to simplify large-number factorization. For instance, Zhang et al. proposed a hybrid quantum–classical approach in which the multiplication table is manually partitioned into multiple column blocks [20], each solved separately on the D-Wave system, and the correct factors are determined by intersecting the solution sets of all blocks. Their work demonstrated the feasibility of block-based decomposition for hardware-limited quantum annealers, though the partitioning strategy was heuristic and problem-specific.

Building upon this concept, the present study introduces a systematic and adaptive column-block division method integrated with the proposed column grouping algorithm. Based on the column groups division method, the multiplication table is partitioned into multiple blocks, each containing several groups. The Hamiltonian objective function for each block is defined as the sum of the objective functions of the groups it contains. By solving the Hamiltonian function of each block using an Ising machine, the resulting solution set is guaranteed to include the correct solution of the final decomposition. In other words, the correct solution of the final decomposition must be contained within the intersection of the solution sets obtained from solving each block separately.

Taking the multiplication table of 1,028,171 = 1019 × 1009 as an example, it is divided into seven groups using the aforementioned column grouping algorithm, as shown in Fig. 6. To ensure that the number of qubits required for solving each block is approximately equal, the first three groups are combined into one block, the fourth group is treated as

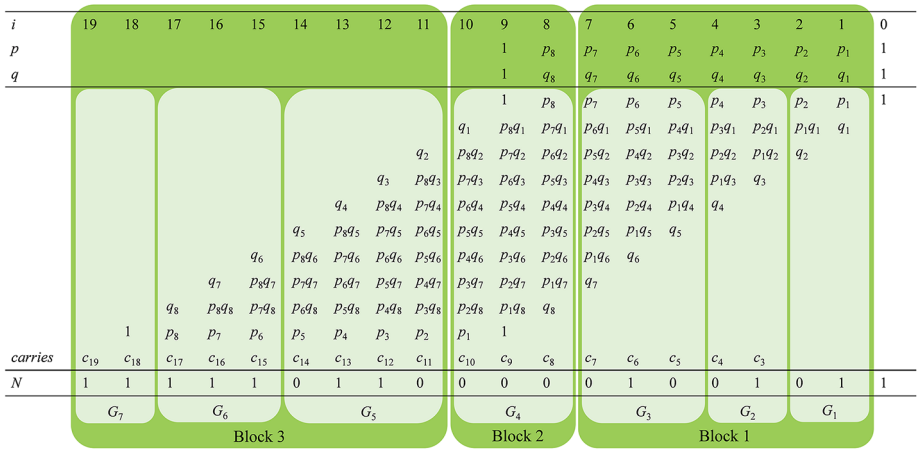


Figure 6 Multiplication table for 1,028,171 = 1019 × 1009 in binary based on column blocks division method

a separate block, and the last three groups form another block. With this division, the numbers of qubits required for solving each block are 43, 44, and 44, respectively.

The number of qubits required for block division is relatively small; however, due to the weakened constraints, the solution space expands significantly, resulting in an increased number of solutions with the lowest Hamiltonian states. We selected Block1 and Block3, which have relatively stronger constraints, for solving. Block1 yielded 127 solutions with a Hamiltonian value of 0, while Block3 produced 17 such solutions. By taking the intersection of these solutions, we ultimately obtained a unique decomposition result. Specifically, from Block1 we obtain solution sets for p_1-p_7 and q_1-q_7, while Block3 provides solution sets for p_2-p_8 and q_2-q_8. Crucially, p_2-p_7 and q_2-q_7 form an overlap region between these solution sets. By applying constraint filtering based on this overlap region, we ultimately identified only one set of valid solutions that maintain complete consistency in the overlap region (excluding symmetric equivalents), as shown below:

$$\begin{aligned} r_1 &= (p_1p_2...p_7q_1q_2...q_7) = (10111110001111) \quad r_1 \in R_1 \\ r_3 &= (p_2...p_7p_8q_2...q_7q_8) = (01111110011111) \quad r_3 \in R_3 \end{aligned} \tag{17}$$

we obtained the final solution by taking the intersection of these solution sets.

$$R = r_1 \cap r_3 = (p_1p_2...p_8q_1q_2...q_8) = (1011111100011111) \tag{18}$$

It is noteworthy that the correct decomposition result is necessarily included in this intersection, but the intersection process does not guarantee the uniqueness of the correct solution. To verify the correctness and completeness of the results obtained without using Block2, we considered all 8 possible cases for the 8th to 10th bits and analyzed their solutions. As shown in the Table 5, only when the 8th to 10th bits are (000), corresponding to the number we aim to factor, can the number be expressed as the product of two 10-bit binary numbers. The other 7 cases do not satisfy this condition. Therefore, it is reasonable to obtain a unique solution by taking the intersection.

The inherent constraint reduction and consequent solution space expansion caused by block division remains unavoidable. Our preliminary research shows that blocks contain-

Table 5 Numbers and factorization results corresponding to different $n_8 \sim n_{10}$

$n_8 \sim n_{10}$	Total number in binary	Factorization result
000	11111011000001001011	1,028,171 = 1019 × 1009
001	11111011000101001011	1,028,427 = 3 × 29 × 11,821
010	11111011001001001011	1,028,683
011	11111011001101001011	1,028,939
100	11111011010001001011	1,029,195 = 3 × 3 × 5 × 22,871
101	11111011010101001011	1,029,451 = 37 × 27,823
110	11111011011001001011	1,029,707 = 7 × 17 × 17 × 509
111	11111011011101001011	1,029,963 = 3 × 11 × 23 × 23 × 59

ing the least significant bits and most significant bits in the binary multiplication table maintain relatively complete constraints, thus yielding fewer low-energy solutions. We are currently investigating more sophisticated block partitioning strategies. Theoretical estimates indicate that while this approach cannot achieve orders-of-magnitude reduction in qubit requirements, it may still reduce the required qubits to 50% or less of the original amount. These findings collectively demonstrate the viability of Ising-model-based computational approaches for integer factorization, with experimental results showing promising scalability for handling larger integer values.

6 Methods

All simulation experiments were primarily conducted using Fixstars Amplify AE, while additional verification was performed on the D-Wave Sampler provided by D-Wave. It should be emphasized that the use of these platforms was intended solely to validate the correctness of the constructed Hamiltonian and QUBO formulation, rather than to evaluate the hardware performance of any specific solver.

The experimental results confirm that our proposed method maintains general applicability across different Ising-based solvers and achieves a broader and more stable range of local field coefficients $\boldsymbol{h}$ and coupling coefficients $\boldsymbol{J}$ compared to previously reported algorithms.

7 Discussion

Based on the Non-Uniform Column Groups Division strategy, this paper proposes an optimized integer factorization algorithm grounded in the Ising model. The algorithm achieves compression of the parameter ranges for the $\boldsymbol{J}$ and $\boldsymbol{h}$ terms in the Ising model while minimizing the number of carry auxiliary parameters, thereby enhancing the computational tractability of the resulting Ising problem. A comprehensive analysis of the scalability of integer factorization and the associated computational resource requirements is conducted, providing critical insights for evaluating the feasibility and performance of quantum factorization methods.

Leveraging the proposed algorithm, the research team successfully factored a 22-bit integer using 118 qubits on the D-Wave quantum computing platform and Fixstars Amplify AE. Although Ding et al. (Scientific Reports, 2024) reported the factorization of a numerically larger number (8,219,999 = 32,749 × 251), the two approaches focus on different aspects. Their work mainly optimizes hardware-level embedding on the D-Wave Pegasus topology, while our study improves the mathematical and algorithmic formulation of the factorization problem. Moreover, the instance in Ding et al. is highly unbalanced, with one factor only 8 bits long, which substantially simplifies the multiplier structure and carry

propagation. In contrast, our 22-bit composite involves two nearly balanced factors, leading to a denser Ising coupling network and representing a harder and more general class of factorization problems. Furthermore, a block-based methodology was explored to reduce the quantum spatial complexity of the algorithm. This approach enabled the factorization of a 20-bit integer utilizing 44 qubits instead of 97, demonstrating significant resource optimization. However, the completeness and time complexity of the algorithm necessitate further investigation to ensure robustness and practical applicability.

These advancements underscore the potential of quantum annealing-based approaches in addressing integer factorization challenges, particularly as quantum hardware continues to evolve. Future work will focus on refining the mapping process between factorization problems and the Ising model, investigating hybrid classical-quantum architectures, and advancing hardware scalability to tackle cryptographically relevant large integers.

Supplementary information

Supplementary information accompanies this paper at https://doi.org/10.1140/epjqt/s40507-025-00449-9.

Additional file 1. (PDF 133 kB)

Author contributions

Z.L. proposed the overall research concept, developed the main algorithm framework, and led the implementation. Y.Y. optimized the algorithm, designed the non-uniform column grouping strategy, conducted simulations, and analyzed results. Z.W. contributed to the mathematical modeling and computational complexity analysis. M.L. was responsible for platform testing, numerical verification, and visualization. P.L. supervised the research, provided theoretical guidance, and acquired funding. All authors contributed to writing and editing the manuscript. All authors read and approved the final manuscript.

Funding information

This work was supported by National Key Research and Development Program of China (2021YFB2206600).

Data availability

No datasets were generated or analysed during the current study.

Declarations

Competing interests

The authors declare no competing interests.

Received: 19 May 2025 Accepted: 17 November 2025 Published online: 21 November 2025

References

1. Lenstra AK, Lenstra HW Jr, Manasse MS, Pollard JM. The number field sieve. In: Proceedings of the twenty-second annual ACM symposium on theory of computing (STOC). 1990. p. 564–72.
2. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. 1999;41(2):303–32.
3. Cai JY. Shor's algorithm does not factor large integers in the presence of noise. Sci China Inf Sci. 2024;67(7):173501.
4. Vandersypen LMK, Steffen M, Breyta G, et al. Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature. 2001;414(6866):883–7.
5. Haribara Y, Utsunomiya S, Yamamoto YJP. A coherent Ising machine for MAX-CUT problems: performance evaluation against semidefinite programming and simulated annealing. In: M. o. Q. I. technologies. 2016. p. 251–62.
6. Dang A, Hill CD, Hollenberg LCL. Optimising matrix product state simulations of Shor's algorithm. Quantum. 2019;3:116.
7. Zheng Q, Zhu P, Wu C, et al. The quantum Ising model for perfect matching and solving it with variational quantum eigensolver. Sci China Inf Sci. 2024;67(9):192502.
8. Zheng Q, Yu M, Zhu P, et al. Solving the subset sum problem by the quantum Ising model with variational quantum optimization based on conditional values at risk. Sci China, Phys Mech Astron. 2024;67(8):280311.
9. Mohseni N, McMahon PL, Byrnes T. Ising machines as hardware solvers of combinatorial optimization problems. Nat Rev Phys. 2022;4(6):363–79.
10. Zhang Z. Mapping between spin-glass three-dimensional (3D) Ising model and Boolean satisfiability problem. Mathematics. 2023;11(1):237.
11. Hasegawa M, Ito H, Takesue H, et al. Optimization by neural networks in the coherent Ising machine and its application to wireless communication systems. IEICE Trans Commun. 2021;104(3):210–6.
12. Yamaoka M, Yoshimura C, Hayashi M, et al. A 20k-spin Ising chip to solve combinatorial optimization problems with CMOS annealing. IEEE J Solid-State Circuits. 2015;51(1):303–9.

13. Chou J, Bramhavar S, Ghosh S, et al. Analog coupled oscillator based weighted Ising machine. Sci Rep. 2019;9(1):14786.
14. Cen Q, Ding H, Hao T, et al. Large-scale coherent Ising machine based on optoelectronic parametric oscillator. Light: Sci Appl. 2022;11(1):333.
15. Dridi R, Alghassi H. Prime factorization using quantum annealing and computational algebraic geometry. Sci Rep. 2017;7(1):43048.
16. Jiang S, Britt KA, McCaskey AJ, et al. Quantum annealing for prime factorization. Sci Rep. 2018;8(1):17667.
17. Wang B, Hu F, Yao H, et al. Prime factorization algorithm based on parameter optimization of Ising model. Sci Rep. 2020;10(1):7106.
18. Wang B, Yang X, Zhang D. Research on quantum annealing integer factorization based on different columns. Front Phys. 2022;10:914578.
19. Zhang D, Wang H, Li S, et al. Progress in the prime factorization of large numbers. J Supercomput. 2024;80(8):11382–400.
20. Ding J, Spallitta G, Sebastiani R. Effective prime factorization via quantum annealing by modular locally-structured embedding. Sci Rep. 2024;14(1):3518.
21. Dhaulakhandi R, Behera BK, Seo FJ. Factorization of large tetra and penta prime numbers on IBM quantum processor. APL Quantum. 2024;1(2).
22. Shatnawi AS, Almazari MM, AlShara Z, et al. RSA cryptanalysis—Fermat factorization exact bound and the role of integer sequences in factorization problem. J Inf Secur Appl. 2023;78:103614.
23. Guo X, Miao G, Nishizawa S, et al. Prime factorization based on multiple quantum annealings on partial constraints with analytical variable reduction. In: 2023 IEEE 36th international system-on-chip conference (SOCC). IEEE; 2023. p. 1–6.
24. Yamamoto Y, Leleu T, Ganguli S, et al. Coherent Ising machines—quantum optics and neural network perspectives. Appl Phys Lett. 2020;117(16):160501.
25. Yamamoto Y, Aihara K, Leleu T, et al. Coherent Ising machines—optical neural networks operating at the quantum limit. npj Quantum Inf. 2017;3(1):49.
26. Li C, Zhang X, Li J, et al. The challenges of modern computing and new opportunities for optics. PhotoniX. 2021;2(1):20.
27. Cen Q, Ding H, Guan S, et al. Phase-diagram investigation of frustrated 1D and 2D Ising models in OEO-based Ising machine. Opt Lett. 2023;48(21):5459–62.
28. Gao Y, Chen G, Qi L, et al. Photonic Ising machines for combinatorial optimization problems. Appl Phys Rev. 2024;11(4):041401.
29. Sheldon F, Traversa FL, Di Ventra M. Taming a nonconvex landscape with dynamical long-range order: memcomputing Ising benchmarks. Phys Rev E. 2019;100(5):053311.
30. Marandi A, Wang Z, Takata K, et al. Network of time-multiplexed optical parametric oscillators as a coherent Ising machine. Nat Photonics. 2014;8(12):937–42.
31. Haribara Y, Utsunomiya S, Yamamoto Y. Computational principle and performance evaluation of coherent Ising machine based on degenerate optical parametric oscillator network. Entropy. 2016;18(4):151.
32. Inagaki T, Haribara Y, Igarashi K, et al. A coherent Ising machine for 2000-node optimization problems. Science. 2016;354(6312):603–6.
33. Ye X, Zhang W, Wang S, Yang X, He Z. Photonic spatial-Euler Ising machine for solving 20000-node Max-Cut problem. Opt Express. 2023;31(21):34779–91.
34. Li Z, Gan R, Chen Z, et al. Scalable on-chip optoelectronic Ising machine utilizing thin-film lithium niobate photonics. ACS Photonics. 2024;11(4):1703–14.
35. Honjo T, Sonobe T, Inaba K, et al. 100,000-spin coherent Ising machine. Sci Adv. 2021;7(40):eabh0952.
36. Boros E, Hammer PL. Pseudo-Boolean optimization. Discrete Appl Math. 2002;123(1–3):155–225.
37. Wang C, Wang Q, Hong C, Hu Q, Pei Z. Quantum annealing based public key cryptanalysis algorithm on D-Wave Advantage. Chin J Comput. 2024;47(5):1030–44.

Publisher's note