Tsinghua Science and Technology
Doi: 10.26599/TST.2026.9010101

Research Article

Quantum annealing-assisted framework for Search-LWE: a proof-of-concept study on a real quantum computer

Chunlei Hong, Zhi Pei, Yidan Chen, Shuaizhi Xiong, Yiliang Han, Shuaishuai Zhu, Yibo Li and Chao Wang(✉)

Abstract The Learning With Errors (LWE) problem is fundamental in post-quantum cryptography, and its hardness ensures the security of many lattice-based cryptosystems. This paper proposes a quantum-classical framework for solving Search-LWE instances on real quantum annealing hardware using quantum tunneling to explore a restricted correction space around the Babai solution. First, the Search-LWE is formulated as a lattice decoding problem, and the restricted binary correction space around the Babai solution is encoded into an Ising Hamiltonian. Then, forward and reverse quantum annealing are implemented on the D-Wave Advantage2 to explore the correction space. In particular, reverse quantum annealing uses the Babai solution as the initial state for quantum annealing. The outputs of both quantum annealing schemes are refined by a classical local search to improve solution quality. Experimental results show that both quantum annealing approaches obtain lattice candidates with smaller residual error norms than the Babai solution for a considerable number of tested instances. Simulated annealing further confirms the effectiveness of the Ising formulation. Moreover, our framework demonstrates successful secret recovery for Search-LWE instances with dimensions up to 15 on D-Wave Advantage2. These results provide a proof of concept on quantum hardware, but do not demonstrate a practical threat to cryptographically relevant LWE-based cryptosystems.

Keywords Learning With Errors, Post-quantum, Quantum tunneling, Ising Hamiltonian, D-Wave

• Chunlei Hong, Shuaizhi Xiong, and Chao Wang are with the Key Laboratory of Specialty Fiber Optics and Optical Access Networks, Shanghai University, Shanghai 200444, China. E-mail: hcl@shu.edu.cn; xszshu@126.com; wangchao@shu.edu.cn.
• Yidan Chen and Chao Wang are with the National and Local Joint Laboratory of Cyberspace Security Technology, Zhengzhou 450000, China. E-mail: 18638180100@139.com; wangchao@shu.edu.cn.
• Zhi Pei is with the College of Software Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002, China. E-mail: peizhiiii@163.com.
• Yiliang Han and Shuaishuai Zhu are with the Department of the College of Cryptographic Engineering, Engineering University of PAP, Xi'an 710086, China. E-mail: Yilianghan@hotmail.com; zsseupap@163.com.
• Yibo Li is with the School of Mathematics and Statistics, Hubei University of Education, Wuhan 430205, China. E-mail: liyibo@hue.edu.cn.
* To whom correspondence should be addressed.
Manuscript received: 20xx-xx-xx; revised: 20xx-11-xx; accepted: 20xx-00-xx

1 Introduction

Public-key cryptographic algorithms, such as RSA[1] and ECC[2], which are based on the integer factorization and discrete logarithm problems, are widely used in information security. However, with the rapid development of quantum computing, the security of traditional public-key cryptography is under threat. Quantum algorithms (e.g., Shor's algorithm[3]) could, in theory, solve integer factorization and discrete logarithm problems in polynomial time, potentially undermining the security foundations of existing public-key cryptographic systems. Motivated by this theoretical threat, increasing research efforts have been devoted to validating quantum cryptanalysis against public-key cryptosystems on real quantum computers, including implementations of Shor's algorithm[4, 5], variational quantum algorithms[6], and quantum annealing algorithm[7–9].

In this context, post-quantum cryptography (PQC)[10], capable of resisting quantum computing attacks, has attracted significant attention. The National Institute of Standards and Technology (NIST) initiated the PQC standardization process in 2017 and announced the third-round candidates in 2020. In 2022, NIST announced four standardized PQC algorithms, three of which are based on lattice problems, including the Module-LWE-based public-key encryption algorithm CRYSTALS-Kyber[11], the CRYSTALS-Dilithium[12] signature algorithm, and the Falcon[13] signature algorithm based on the NTRU lattice structure. The Learning With Errors (LWE) problem[14], which serves as a crucial security foundation for numerous PQC schemes, is of significant importance for evaluating the security of the associated cryptographic systems.

The development of quantum computing has driven research into quantum methods for solving the LWE problem, which is primarily focused on two areas: theoretical research and practical implementation.

Theoretical research: In 2018, Esser et al.[15] proposed an algorithm based on the c-sum technique for solving LWE. The algorithm uses Grover's quantum search to accelerate its vector combination subroutine, providing a quantum speedup for this step. In 2022, Albrecht et al.[16] refined the dual-lattice attack against LWE by replacing a classical component

Just Accepted

with the Quantum Fourier Transform (QFT). In the same year, Liu et al.[17] further optimized the combinatorial algorithm by adapting it to the specific structure of LWE and relaxing its application conditions. In 2025, Cao et al.[18] combined side-channel leakage information with Gaussian elimination, significantly reducing the complexity of solving LWE with partial key leakage. Recent concrete benchmarking work by Wenger et al.[19] evaluated several attacks on Search-LWE and Decision-LWE and compared their practical performance with theoretical estimates. In related work, Qayyum[20] proposed an updated MIP model and a QUBO formulation of LWE for quantum annealing, although the QUBO formulation was not implemented or evaluated on quantum annealing hardware. In 2026, Chailloux and Hermouet[21] investigated the relationship between a quantum analogue of LWE and the Inhomogeneous Short Integer Solution (ISIS) problem, further extending the theoretical study of quantum approaches to LWE-related lattice problems. Together, these studies broaden the theoretical analysis, modeling, and practical evaluation of LWE attacks under different settings. Nevertheless, most proposed quantum approaches accelerate only selected stages of an attack, while some require special quantum resources or additional knowledge of the secret. Consequently, how effectively these methods can support Search-LWE secret recovery on current quantum hardware remains unclear.

Research on practical implementation: In 2022, Lv et al.[22] solved the LWE problem using variational quantum algorithms, successfully solving a 1-dimensional Search-LWE instance on an IBM quantum computer. In 2025, Zheng et al. [23] employed the Quantum Approximate Optimization Algorithm (QAOA) [24] to successfully solve a 2-dimensional Decision-LWE instance using 5 qubits on an IBM quantum computer. These studies demonstrate the feasibility of investigating different LWE variants on real quantum hardware. Nevertheless, the reported experiments are restricted to extremely low-dimensional instances implemented on gate-based quantum processors. Moreover, the latter study addresses Decision-LWE rather than the direct recovery of the hidden secret vector in Search-LWE.

Overall, most quantum studies of LWE remain theoretical, while experiments on quantum processors based on the gate model have been limited to very small instances, especially for Search-LWE secret recovery. Moreover, directly solving general lattice decoding problems on current quantum hardware remains challenging due to limited qubit resources and embedding overhead. Therefore, exploring structured correction strategies around classical lattice approximations provides a practical direction for evaluating the capability of current quantum annealing hardware.

Motivated by this gap, we study a hybrid quantum and classical framework for small Search-LWE instances on the D-Wave Advantage2 quantum annealer. In this work, Search-LWE lattice decoding is formulated as a restricted binary correction problem around the Babai solution, and the corresponding objective function is encoded into an Ising Hamiltonian. Since the Babai solution is always contained in the encoded correction space, the exact optimum of this formulation is guaranteed to be no worse than the Babai solution with respect to the squared residual error norm. We implement forward and reverse quantum annealing on real quantum hardware to explore the encoded correction space. The resulting annealing solutions are further refined by a limited classical local search, and the performance is compared with classical optimization methods. Finally, we evaluate the complete hybrid framework on small Search-LWE instances and demonstrate secret recovery for instances with dimensions up to $n = 15$. These experiments provide a proof of concept for the proposed framework on current quantum annealing hardware but do not demonstrate a practical threat to cryptographically relevant LWE parameters.

2 Preliminaries

First, the notation used in this paper will be introduced. $\mathbb{R}$ and $\mathbb{Z}$ denote the set of real numbers and the set of integers, respectively. For $a \in \mathbb{R}$, $\lfloor a \rceil$ denotes the integer obtained by rounding a to the nearest integer. We use lowercase bold letters $\mathbf{a}$ to denote row vectors and uppercase bold letters $\mathbf{A}$ to denote matrices. $\|\mathbf{a}\|$ denotes the Euclidean norm for vectors $\mathbf{a} \in \mathbb{R}^m$ in m-dimensional Euclidean space. Next, the lattice theory fundamentals, classical lattice algorithms, and quantum annealing algorithm related to this work will be introduced separately.

2.1 Lattice Theory

Lattice: Suppose $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{R}^{m \times n}$ is a matrix consisting of n linearly independent column vectors in the m-dimensional Euclidean space $\mathbb{R}^m$. Then the lattice $\mathcal{L}(\mathbf{B})$ is defined as:

$$\mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^n\} = \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \right\}.$$

That is, the lattice $\mathcal{L}(\mathbf{B})$ is the set of all integer linear combinations of the column vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Here, m and n are called the dimension and rank of the lattice $\mathcal{L}(\mathbf{B})$, respectively, and matrix $\mathbf{B}$ is called a basis of the lattice $\mathcal{L}(\mathbf{B})$.

Just Accepted

q-ary lattice: Given a matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$, the m-dimensional q-ary lattice is defined as

$$\mathcal{L}_q(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m \mid \exists\, \mathbf{y} \in \mathbb{Z}^n,\ \mathbf{x} \equiv \mathbf{A}\mathbf{y} \pmod q\}.$$

Closest vector problem (CVP): Given a lattice $\mathcal{L}(\mathbf{B})$ and a target vector $\mathbf{t} \in \mathbb{R}^m \setminus \mathcal{L}$, the problem is to find a non-zero lattice vector $\mathbf{v} \in \mathcal{L}$ closest to the target vector $\mathbf{t}$, such that for any non-zero lattice vector $\mathbf{u} \in \mathcal{L}$, it necessarily satisfies: $\|\mathbf{v}-\mathbf{t}\| \leqslant \|\mathbf{u}-\mathbf{t}\|$.

Bounded distance decoding (BDD): Given a lattice $\mathcal{L}(\mathbf{B})$ and a target vector $\mathbf{t} \in \mathbb{R}^m \setminus \mathcal{L}$, satisfying $\mathrm{dist}(\mathbf{t},\mathcal{L}) < \gamma\lambda_1(\mathcal{L})$, where $\gamma < 1/2$. The problem is to find a non-zero lattice vector $\mathbf{v} \in \mathcal{L}$ to the target vector $\mathbf{t}$, such that $\|\mathbf{v}-\mathbf{t}\|$ is minimized.

LLL algorithm [26]: Given an arbitrary basis of a lattice, this algorithm can transform this basis into an approximately orthogonal basis with good orthogonality, making the vectors in this approximate orthogonal basis as short as possible. Specific steps can be referred to in Algorithm 1.

Algorithm 1 LLL algorithm

Require: A lattice basis $\mathbf{B} = [\mathbf{b}_1, \cdots, \mathbf{b}_n] \in \mathbb{R}^{m\times n}$, parameter $\delta \in (1/4, 1)$.
Ensure: A reduced lattice basis.
1: Performing Gram-Schmidt orthogonalization on the lattice basis $\mathbf{B}$ can obtain $\hat{\mathbf{B}} = [\hat{\mathbf{b}}_1, \cdots, \hat{\mathbf{b}}_n] \in \mathbb{R}^{m\times n}$.
2: **for** $i = 2$ to n **do**
3: **for** $j = i-1$ to 1 **do**
4: $\mathbf{b}_i \leftarrow \mathbf{b}_i - \lfloor \mu_{i,j} \rceil \mathbf{b}_j$, where $\mu_{i,j} = \frac{\langle \mathbf{b}_i, \hat{\mathbf{b}}_j\rangle}{\langle \hat{\mathbf{b}}_j, \hat{\mathbf{b}}_j\rangle}$;
5: **end for**
6: **end for**
7: **if** $\exists\ \delta\|\hat{\mathbf{b}}_i\|^2 > \|\mu_{i+1,i}\hat{\mathbf{b}}_i + \hat{\mathbf{b}}_{i+1}\|^2$ **then**
8: $\mathbf{b}_i \leftrightarrow \mathbf{b}_{i+1}$;
9: Return to the first line;
10: **end if**
11: Output the reduced lattice basis $\mathbf{B}' = [\mathbf{b}_1, \cdots, \mathbf{b}_n]$.

Babai's algorithm [27]: Suppose an n-dimensional lattice $\mathcal{L}$ is given, along with a lattice basis $\mathbf{D} = [\mathbf{d}_1, \ldots, \mathbf{d}_n]$ and a target vector $\mathbf{t} \in \mathbb{R}^n \setminus \mathcal{L}$. The algorithm finds a lattice vector close to the target vector $\mathbf{t}$. The specific procedure is given in Algorithm 2.

2.2 Learning With Errors Problem

LWE distribution: Given positive integers n and q, a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$, and an error distribution χ over $\mathbb{Z}$, the LWE distribution $A_{\mathbf{s},\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is defined by sampling $\mathbf{a} \leftarrow \mathbb{Z}_q^n$ uniformly at random and $e \leftarrow \chi$, and outputting

$$(\mathbf{a}, b) = (\mathbf{a}, \langle \mathbf{a}, \mathbf{s}\rangle + e \bmod q).$$

Algorithm 2 Babai's algorithm

Require: A lattice basis $\mathbf{D} = [\mathbf{d}_1, \cdots, \mathbf{d}_n] \in \mathbb{R}^{n\times n}$ and a target vector $\mathbf{t} \in \mathbb{R}^n$.
Ensure: An approximate lattice vector $\mathbf{t} - \mathbf{v} \in \mathcal{L}$ close to $\mathbf{t}$, and the corresponding error vector $\mathbf{v}$.
1: Perform Gram–Schmidt orthogonalization on $\mathbf{D}$ to obtain $\hat{\mathbf{D}} = [\hat{\mathbf{d}}_1, \cdots, \hat{\mathbf{d}}_n]$.
2: $\mathbf{v} \leftarrow \mathbf{t}$;
3: **for** $i = n$ to 1 **do**
4: $u_i \leftarrow \frac{\langle \mathbf{v}, \hat{\mathbf{d}}_i\rangle}{\langle \hat{\mathbf{d}}_i, \hat{\mathbf{d}}_i\rangle}$, $k_i \leftarrow \lfloor u_i \rceil$;
5: $\mathbf{v} \leftarrow \mathbf{v} - k_i\mathbf{d}_i$;
6: **end for**
7: **Output** $\mathbf{t} - \mathbf{v}$, $\mathbf{v}$.

The LWE problem has two variants: Search-LWE and Decision-LWE. Existing research has shown that, under appropriate parameter settings, these two problems are computationally equivalent.

Search-LWE: Given $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ and $\mathbf{c} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \pmod q$, where $\mathbf{s} \in \mathbb{Z}_q^n$ is an unknown secret vector and $\mathbf{e} \in \mathbb{Z}^m$ is an error vector sampled from a discrete Gaussian distribution, the goal is to recover $\mathbf{s}$.

Decision-LWE: Given $(\mathbf{A}, \mathbf{c}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, the task is to distinguish whether $(\mathbf{A}, \mathbf{c})$ is sampled from the LWE distribution or uniformly at random.

2.3 Quantum Annealing Algorithm

Quantum annealing[28] is an optimization algorithm inspired by quantum-mechanical evolution. Its essential mechanism relies on quantum tunneling to overcome local minima in complex energy landscapes, thereby facilitating the search for the global optimum, as illustrated in Fig. 1. This subsection describes the quantum annealing mechanism in terms of two main paradigms: forward annealing and reverse annealing.

2.3.1 Forward Quantum Annealing

Forward quantum annealing (FQA) is governed by the time-dependent evolution of the system Hamiltonian. Its fundamental mechanism follows an adiabatic process, in which the system evolves from the easily prepared ground state of an initial Hamiltonian to the ground state of a problem Hamiltonian that encodes the optimization objective. In this way, the solution of the optimization problem can be obtained by identifying the final ground state of the system. The

Just Accepted

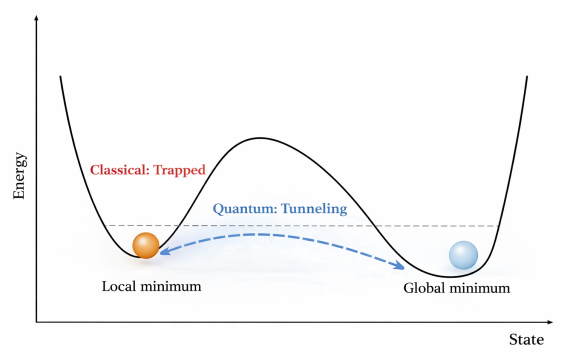


Fig. 1 Comparison between classical and quantum Physics.

time-dependent Hamiltonian is expressed as

$$H(t) = A(s)H_{\text{init}} + B(s)H_{\text{problem}},$$

where $s = t/T \in [0, 1]$ denotes the normalized annealing time, and T is the total annealing time.

The initial Hamiltonian, H_{init}, is typically chosen as a transverse-field Hamiltonian

$$H_{\text{init}} = -\sum_i \hat{\sigma}_i^x.$$

Under this Hamiltonian, all qubits are initialized in an equal superposition state of $|+\rangle$, which provides a random starting point for the subsequent annealing process and enables broad exploration of the solution space.

The problem Hamiltonian, H_{problem}, is constructed by encoding the objective function of the optimization problem into the spin variables of an Ising model, thereby establishing a correspondence between the mathematical cost function and the physical energy landscape. The Ising Hamiltonian can be written as

$$H_{\text{Ising}}(s) = \sum_i h_i s_i + \sum_{i<j} J_{ij} s_i s_j,$$

where $s_i \in \{-1, +1\}$ denotes the spin variable of the $i-$th site, h_i represents the local bias term, and J_{ij} denotes the coupling coefficient between spins i and j. The vector $\mathbf{s} = \{s_i\}$ represents the set of all spin variables. Under this mapping, the global optimum of the objective function corresponds to the ground state, i.e., the minimum-energy state, of the problem Hamiltonian. In practical quantum annealing hardware, the limited numerical precision and dynamic range of the Ising coefficients can affect the quality of sampled solutions [29].

The annealing schedules $A(s)$ and $B(s)$ determine the relative weights of the initial and problem Hamiltonians during the evolution. As s increases from 0 to 1, $A(s)$ monotonically decreases to zero, while $B(s)$ monotonically increases from zero to its maximum value. According to the adiabatic theorem, if the annealing time T is sufficiently long, the system remains in the instantaneous ground state of the time-dependent Hamiltonian with high probability throughout the evolution. Consequently, at the end of the annealing process ($s = 1$), the system reaches the ground state of H_{problem}, which corresponds to the optimal solution of the original optimization problem.

2.3.2 *Reverse Quantum Annealing*

Unlike FQA, which starts from a uniform superposition state and performs a global exploration of the solution space, reverse quantum annealing (RQA)[30] begins from a known classical candidate solution. By exploiting prior information, it reintroduces quantum fluctuations through a non-monotonic annealing schedule, thereby enabling a targeted local search in the vicinity of the initial state and potentially improving the solution quality. This strategy has been implemented in practical quantum annealing hardware. For example, D-Wave quantum computer natively supports reverse annealing schedules together with user-specified initial states, allowing the system to be initialized from a known classical configuration and then driven into a local quantum search regime by temporarily increasing the transverse-field strength.

In RQA, the system no longer follows the conventional monotonic annealing path. Instead, its evolution is controlled by a non-monotonic schedule parameter $s(t)$. The process of the physical mechanism is as follows. First, quantum fluctuations are reintroduced by reversing the annealing schedule, so that the system can escape from the initial local minimum through quantum tunneling and thermally assisted transitions. Next, the system may remain for a certain time near a predetermined reversal point s^*, providing an evolution window for local exploration. Finally, the schedule is driven forward again toward $s = 1$, so that the system evolves toward a low-energy state of the target Hamiltonian. In this way, RQA provides a refinement mechanism centered around a given candidate solution rather than a fully global search starting from a random initial state, as illustrated in Fig. 2.

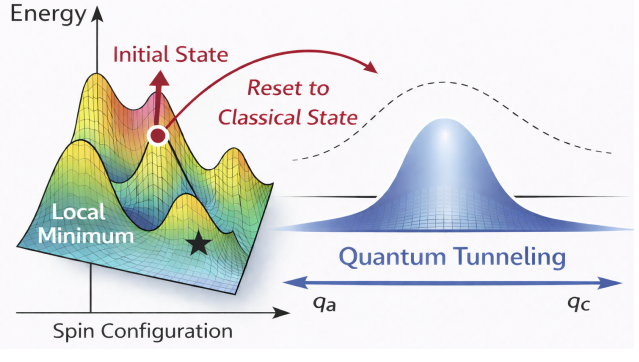


Fig. 2 The process of RQA.

Just Accepted

Initialization phase. At the beginning of the evolution ($t = 0$), the schedule parameter is set to $s(t) = 1$. At this point, an approximate solution obtained from a classical algorithm is mapped onto the quantum processor as the initial state, such that the system is initialized in a computational-basis state corresponding to the classical candidate solution.

Reverse annealing phase. During this stage, the schedule parameter is decreased from $s(t) = 1$ to a preset reversal point s^*. As the schedule moves backward, the coefficient $A(s)$ associated with the Hamiltonian increases, while the relative weight of the problem Hamiltonian decreases accordingly. As a result, the transverse-field component is reintroduced into the system, driving it away from the deterministic classical state toward a locally delocalized quantum state centered around the initial solution. This process restores quantum fluctuations and enables the wavefunction to explore a local region of the Hilbert space, thereby creating the physical conditions for tunneling across nearby energy barriers.

Pause and re-annealing phase. After the schedule reaches the reversal point s^*, the system may be held for a finite pause time to enhance local exploration under relatively strong quantum fluctuations. During this interval, coherent tunneling and thermally assisted relaxation may help the system probe neighboring configurations with lower energy than the initial candidate. Subsequently, the schedule is increased from s^* back to $s(t) = 1$, and the system undergoes a second forward evolution toward the problem Hamiltonian. At the end of this process, the wavefunction collapses to a classical candidate solution, which may exhibit lower energy and better objective value than the initial state.

3 Quantum-Classical Hybrid Framework for Solving the Search-LWE Problem

This section presents a quantum-classical hybrid framework for solving the Search-LWE problem, as illustrated in Fig. 3. First, the LWE problem is formulated as a lattice decoding problem, and a restricted correction neighborhood around the Babai solution is mapped to an Ising Hamiltonian. Next, the resulting Hamiltonian is optimized using FQA and RQA on the D-Wave quantum computer. Finally, the sampled low-energy solutions are refined by a limited bit-flip local search and used for secret vector recovery.

3.1 Construction of the Ising Hamiltonian for the Search-LWE Problem

Given m LWE samples $(\mathbf{A}, \mathbf{c} \equiv \mathbf{A}\mathbf{s} + \mathbf{e} \pmod q)$, where $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$, $\mathbf{c} \in \mathbb{Z}_q^m$, $\mathbf{s} \in \mathbb{Z}_q^n$, and the error vector $\mathbf{e}$ follows a discrete Gaussian distribution, one can construct the q-ary lattice

$$\mathcal{L}_q(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m \mid \exists \mathbf{y} \in \mathbb{Z}^n,\ \mathbf{x} \equiv \mathbf{A}\mathbf{y} \pmod q\}.$$

By treating $\mathbf{c}$ as the target vector, the Search-LWE problem can be formulated as a lattice decoding problem on $\mathcal{L}_q(\mathbf{A})$. The objective is to find a lattice vector close to the target vector. Since the LWE error is sampled from a centered discrete Gaussian distribution, a smaller residual norm corresponds to a higher likelihood under the assumed error model. Therefore, minimizing the distance to the target remains a natural decoding criterion.

For the lattice vector corresponding to the true secret, its distance to the target is determined by the error norm $\|\mathbf{e}\|$. If

$$\|\mathbf{e}\| < \frac{1}{2}\lambda_1(\mathcal{L}_q(\mathbf{A})),$$

this lattice vector is guaranteed to be the unique closest lattice vector, and the instance lies in the BDD regime. Therefore, BDD is treated as a special case of the general lattice decoding problem under this additional distance condition.

Let $\widetilde{\mathbf{A}} \in \mathbb{Z}^{m\times n}$ denote an integer lift of $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$. The q-ary lattice $\mathcal{L}_q(\mathbf{A})$ is represented by the integer generating matrix

$$\mathbf{G} = \begin{bmatrix} q\mathbf{I}_m \\ \widetilde{\mathbf{A}}^T \end{bmatrix} \in \mathbb{Z}^{(m+n)\times m}.$$

For any $\mathbf{z} \in \mathbb{Z}^m$ and $\mathbf{y} \in \mathbb{Z}^n$,

$$\mathbf{G}^T \begin{bmatrix} \mathbf{z} \\ \mathbf{y} \end{bmatrix} = q\mathbf{z} + \widetilde{\mathbf{A}}\mathbf{y}.$$

Therefore,

$$\mathcal{L}_q(\mathbf{A}) = \left\{ \widetilde{\mathbf{A}}\mathbf{y} + q\mathbf{z} \mid \mathbf{y} \in \mathbb{Z}^n, \mathbf{z} \in \mathbb{Z}^m \right\},$$

and $\mathbf{G}$ is an overcomplete generating matrix of $\mathcal{L}_q(\mathbf{A})$. Since $\mathbf{G}$ contains $q\mathbf{I}_m$, it has rank m.

To extract a full-rank lattice basis, we compute the row Hermite normal form of $\mathbf{G}$. The row Hermite normal form is obtained through unimodular integer row transformations. Thus, for a unimodular matrix $\mathbf{U} \in \mathrm{GL}_{m+n}(\mathbb{Z})$, the transformed matrix can be written as

$$\mathbf{U}\mathbf{G} = \begin{bmatrix} \mathbf{B}_0 \\ \mathbf{0} \end{bmatrix},$$

where $\mathbf{B}_0 \in \mathbb{Z}^{m\times m}$ consists of the nonzero rows of the row Hermite normal form. Since unimodular row transformations preserve the generated integer lattice, $\mathbf{B}_0$ is a basis of $\mathcal{L}_q(\mathbf{A})$.

The basis $\mathbf{B}_0$ is then reduced using the LLL algorithm. Since LLL performs unimodular basis transformations, the reduced basis generates the same lattice. Let $\mathbf{d}_1^T, \ldots, \mathbf{d}_m^T$ denote the rows of the LLL-reduced basis matrix, and define

$$\mathbf{D} = [\mathbf{d}_1, \ldots, \mathbf{d}_m] \in \mathbb{Z}^{m\times m}.$$

Thus, $\mathbf{D}$ is an LLL-reduced basis of $\mathcal{L}_q(\mathbf{A})$.

Just Accepted

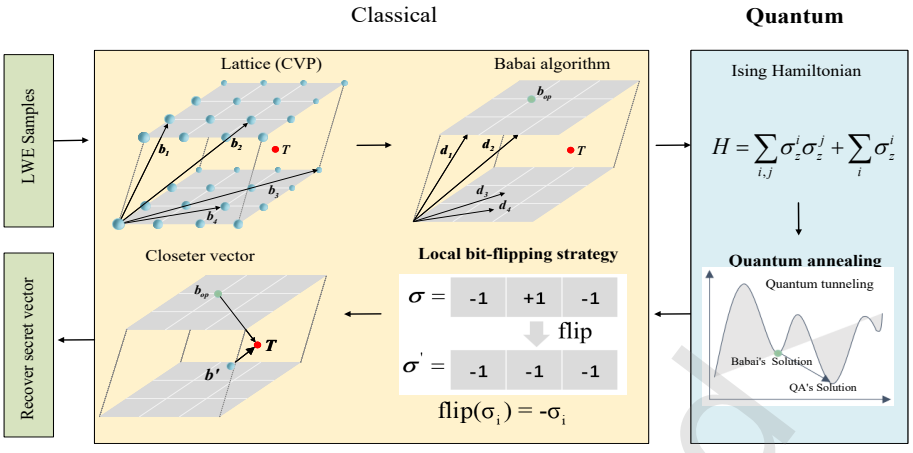


Fig. 3 Quantum-classical hybrid framework for solving the Search-LWE problem.

Given the target vector $\mathbf{c}$, Babai's nearest-plane algorithm returns an approximate lattice vector

$$\mathbf{b}_{\text{Babai}} = \sum_{i=1}^{m} k_i \mathbf{d}_i \in \mathcal{L}_q(\mathbf{A}).$$

Starting from the residual vector $\mathbf{v} = \mathbf{c}$, the coefficient at the i-th step is computed as

$$u_i = \frac{\langle \mathbf{v}, \hat{\mathbf{d}}_i \rangle}{\langle \hat{\mathbf{d}}_i, \hat{\mathbf{d}}_i \rangle}, \qquad k_i = \lfloor u_i \rceil,$$

followed by the residual update

$$\mathbf{v} \leftarrow \mathbf{v} - k_i \mathbf{d}_i.$$

Thus, Babai's algorithm selects a single nearest-integer coefficient at each step. For each coefficient, we additionally consider the alternative adjacent integer value, which defines a binary correction relative to the Babai solution. Exploring these choices jointly for all coefficients leads to a correction space of size 2^m. We therefore introduce binary correction variables y_i and define the candidate lattice vector through

$$F(y_1, \cdots, y_m) = \|\mathbf{c} - \mathbf{b}_{new}\|^2 = \left\| \mathbf{c} - \mathbf{b}_{\text{Babai}} - \sum_{i=1}^{m} y_i \mathbf{d}_i \right\|^2. \tag{1}$$

Therefore, the smaller the value of $F(y_1, \cdots, y_m)$, the closer the lattice vector $\mathbf{b}_{new}$ is to the target vector $\mathbf{c}$. By mapping the variable y_i to Pauli matrices, the Hamiltonian function of $F(y_1, \cdots, y_m)$ can be constructed as follows:

$$\begin{aligned} H_b &= \left\| \mathbf{c} - \mathbf{b}_{Babai} - \sum_{i=1}^{m} \hat{y}_i \mathbf{d}_i \right\|^2 \\ &= \sum_{j=1}^{m} \left| c_j - b^j_{Babai} - \sum_{i=1}^{m} \hat{y}_i d_{i,j} \right|^2, \end{aligned} \tag{2}$$

where $\hat{y}_i \in \{0, 1, -1\}$ is a quantum operator mapped to Pauli matrices according to a single-qubit encoding rule. The mapping rule is determined by the relative magnitude between the orthogonal coefficients u_i and k_i in the Babai's algorithm, namely:

$$\hat{y}_i = \begin{cases} (I - \sigma_z^i)/2, & \text{if } k_i \leqslant u_i \\ (\sigma_z^i - I)/2, & \text{if } k_i > u_i \end{cases}. \tag{3}$$

As shown above, when the coefficient is rounded down to the nearest integer, i.e., $k_i \leqslant \mu_i$, the value of k_i either remains unchanged or increases by 1. Under this encoding scheme, the binary variable $y_i \in \{0, 1\}$ is associated with the eigenvalues of the quantum operator $(I - \sigma_z^i)/2$, and vice versa. Hence, the rounding behavior of k_i in Babai's algorithm determines the encoding of the binary variable y_i. Accordingly, lower-energy states correspond to better lattice vectors within the encoded correction space. The resulting Ising model searches a restricted neighborhood around the Babai solution, rather than the full lattice decoding search space.

Importantly, the zero correction $\mathbf{y} = (0, \ldots, 0)$ is always contained in the encoded correction space and corresponds exactly to the original Babai solution. Therefore, if $F^\star = \min_{\mathbf{y}} F(\mathbf{y})$, then

$$F^\star \leqslant \|\mathbf{c} - \mathbf{b}_{\text{Babai}}\|^2.$$

Hence, the exact optimum of the proposed correction formulation is guaranteed to be no worse than the Babai solution with respect to the squared residual error norm. This guarantee applies only to the exact optimum within the encoded correction space and does not imply that a practical quantum annealing run will always obtain this optimum.

3.2 Solving the Ising Hamiltonian via Quantum Annealing

This subsection introduces the solution of the constructed Ising Hamiltonian using the quantum annealing mechanism of

Just Accepted

the D-Wave quantum computer. Based on Eq. (2) and Eq. (3) in Section 3.1, the corresponding Ising Hamiltonian can be expressed as

$$H(t) = \sum_i h_i(t)\sigma_i^z + \sum_{i<j} J_{ij}(t)\sigma_i^z\sigma_j^z + \sum_i \Gamma_i(t)\sigma_i^x, \quad (4)$$

where $h_i(t)$ and $J_{ij}(t)$ denote the local bias and coupling coefficients derived from the problem Hamiltonian, and $\Gamma_i(t)$ represents the strength of the transverse field that introduces quantum fluctuations.

This study considers two quantum annealing schemes for solving the Ising Hamiltonian: FQA and RQA.

■ **FQA for solving the Ising Hamiltonian**

First, the local bias coefficients and coupling coefficients extracted from Eq. (4) are mapped onto the D-Wave quantum processor. The system is initialized in the ground state of the transverse-field Hamiltonian and gradually evolves, under the control of the annealing schedule, toward a regime dominated by the problem Hamiltonian. According to the adiabatic evolution principle, the system tends to evolve toward low-energy states of the problem Hamiltonian, where the ground state corresponds to the optimal solution within the restricted correction space encoded by the Ising Hamiltonian.

In practical quantum computer, factors such as finite annealing time, thermal noise, and control errors make it difficult to consistently obtain the ground state in a single annealing run. Therefore, multiple annealing runs are performed by selecting appropriate annealing times and sample numbers. The resulting spin configurations are evaluated using the Ising Hamiltonian, and the samples are ranked according to their energy values. The lowest-energy spin configurations are selected as approximate solutions of the problem Hamiltonian.

Since FQA starts from an initial state determined solely by the transverse field, which is independent of the problem structure, the evolution process explores the encoded Ising energy landscape without using a prescribed classical initial state. Consequently, FQA searches for low-energy configurations within the restricted correction space but does not directly exploit structural information from the Babai solution.

■ **RQA for solving the Ising Hamiltonian**

In contrast to FQA, RQA allows the system to be initialized from a given classical spin configuration, enabling local quantum search in the neighborhood of the initial solution. In this work, the approximate lattice vector obtained from Babai's algorithm is used to construct the initial state for RQA.

According to the objective function defined in Section 3.1 (Eq. (1)), the Babai solution $\mathbf{b}_{\text{Babai}}$ is recovered when $y_i = 0$ for all i. Therefore, the vector $\mathbf{y} = (0, 0, \ldots, 0)$ is chosen as the initial classical state for RQA. Under the encoding rule in Eq. (3), this initialization corresponds to the uniform $+1$ spin configuration, i.e., $\sigma_z^i = +1$ for all i.

During RQA, the system is initialized in the classical spin configuration $(+1, +1, \ldots, +1)$ corresponding to the Babai solution. The system is then annealed backward to an intermediate point where quantum fluctuations are reintroduced, and subsequently annealed forward toward the problem Hamiltonian. This process enables local exploration and refinement of the energy landscape in the neighborhood of the Babai solution.

The annealing schedule plays a critical role in the performance of RQA. Specifically, the reversal depth and pause duration together determine the strength of quantum fluctuations and the effective search range. If the reversal is too shallow, the system may remain trapped in local minima; if it is too deep, the advantage of the structural information contained in the classical initial state may be diminished. Therefore, the annealing schedule should be adjusted for different problem sizes to achieve more stable low-energy solutions.

Through repeated sampling, candidate spin configurations are generated according to the problem Hamiltonian, with the low-energy configurations retained as candidate solutions.

3.3 Classical Post-Processing and Secret Vector Recovery

This subsection presents the final stage of the quantum-classical hybrid framework. The low-energy solutions obtained from quantum annealing are refined by classical local search and then used to recover the secret vector of the Search-LWE problem.

■ **Classical post-processing**

The spin configurations obtained from quantum annealing, including both FQA and RQA, are inevitably affected by practical hardware factors such as noise, embedding errors, and limited sampling numbers. For larger-scale problems, it is difficult to consistently obtain the exact ground state of the problem Hamiltonian. Nevertheless, quantum annealing typically samples low-energy regions near the optimum, thereby providing candidate solutions located in the vicinity of low-energy basins.

Based on this observation, we introduce a classical local search strategy to further refine the solutions returned by quantum annealing. The goal is to further decrease the objective value of the Hamiltonian and thereby achieve a

Just Accepted

hybrid optimization scheme that combines quantum search with classical local refinement.

Let the spin configuration returned by quantum annealing be $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_m)$, where $\sigma_i \in \{-1, +1\}$, and let its corresponding Ising energy be

$$E(\sigma) = \sum_i h_i \sigma_i + \sum_{i<j} J_{ij} \sigma_i \sigma_j.$$

To further approach the ground state within the low-energy neighborhood, a limited-range spin-flip local search strategy is adopted to iteratively optimize the solution.

Specifically, taking a low-energy sample returned by quantum annealing as the initial solution σ, each iteration flips the $k-$th spin to generate a candidate configuration σ', where $\sigma'_k = -\sigma_k$ and $\sigma'_i = \sigma_i$ for $i \neq k$. The corresponding energy difference $\Delta E = E(\boldsymbol{\sigma}') - E(\boldsymbol{\sigma})$. is then evaluated. If $\Delta E < 0$, the flip is accepted and the current solution is updated; otherwise, the original configuration is retained. Since this search is restricted to the local neighborhood of the quantum annealing output and exploits the quadratic structure of the Ising Hamiltonian, the energy difference can be computed incrementally with very low classical overhead.

To enlarge the explored local neighborhood, multiple rounds of scanning or an extension to two-spin flips can be used. The iterative process terminates when no further energy reduction is observed or when a preset maximum number of iterations is reached. In this way, locally suboptimal spin assignments can be corrected, yielding a refined spin configuration $\hat{\boldsymbol{\sigma}}$.

Following the mapping defined in Eq. (3) of Section 3.1, the final optimized spin configuration $\hat{\boldsymbol{\sigma}}$ is converted into the correction vector $\mathbf{y} = (y_1, y_2, \ldots, y_m)$. Each y_i is the binary correction variable introduced in Section 3.1, whose allowed value is determined by the rounding direction of the corresponding Babai coefficient. It changes the corresponding Babai coefficient by at most one. The candidate lattice vector is then reconstructed as

$$\mathbf{b}_{\text{new}} = \mathbf{b}_{\text{Babai}} + \sum_{i=1}^{m} y_i \mathbf{d}_i.$$

If

$$\|\mathbf{c} - \mathbf{b}_{\text{Babai}}\|^2 > \|\mathbf{c} - \mathbf{b}_{\text{new}}\|^2,$$

then $\mathbf{b}_{\text{new}}$ is retained as the lattice vector $\mathbf{b}$ for secret recovery; otherwise, $\mathbf{b}_{\text{Babai}}$ is retained.

■ **Secret vector recovery**

Given the selected lattice vector $\mathbf{b}$, a candidate secret vector can be obtained through the modular relation

$$\mathbf{b} \equiv \mathbf{A}\mathbf{s} \pmod{q}.$$

Since $\mathbf{A}$, q, and $\mathbf{b}$ are known, an estimated secret vector $\hat{\mathbf{s}}$ is obtained by solving

$$\mathbf{A}\hat{\mathbf{s}} \equiv \mathbf{b} \pmod{q}.$$

The resulting $\hat{\mathbf{s}}$ is used as the recovered candidate secret. In the experiments, exact secret recovery is declared only when $\hat{\mathbf{s}}$ matches the true secret vector $\mathbf{s}$.

4 Analysis of Experimental Results

This section evaluates the proposed quantum-classical hybrid framework for small Search-LWE instances. We first describe the experimental setup and compare FQA and RQA with classical baselines. We then analyze the scaling characteristics of the Ising formulations and the physical resources required for their implementation on quantum annealing hardware. Next, we evaluate classical local refinement of the quantum annealing solutions. Finally, exact secret recovery experiments are conducted to evaluate the complete hybrid framework under different small-scale Search-LWE parameter settings.

4.1 Experimental Setup

The quantum annealing experiments were performed on the D-Wave Advantage2 quantum annealing platform with a Zephyr topology. Four small-scale Search-LWE parameter settings were considered: $(n, m, q, \sigma) = (8, 18, 99, 3.2)$, $(13, 26, 129, 5.0)$, $(18, 36, 509, 8.0)$, and $(23, 46, 509, 8.0)$. Here, n, m, q and σ denote the secret dimension, number of LWE samples, modulus, and standard deviation of the discrete Gaussian error distribution, respectively. For each setting, 50 independent instances were generated, yielding 200 instances in total. The entries of $\mathbf{A}$ and $\mathbf{s}$ were sampled uniformly from $\mathbb{Z}_q$, while $\mathbf{e}$ was sampled from a centered discrete Gaussian distribution with standard deviation σ. The number of Ising variables is $N = m$, corresponding to the number of binary correction variables in the proposed formulation.

To describe the relative noise magnitude, we define $\alpha = \sigma/q$. The corresponding values for the four settings are approximately 0.0323, 0.0388, 0.0157, and 0.0157, respectively. Thus, the error standard deviation is less than 4% of the modulus in all cases. These parameters are used for small-scale proof-of-concept experiments and are not intended to represent standardized cryptographic parameter sets, such as those of Kyber or Dilithium.

For FQA, each Ising instance was sampled using a fixed annealing time of 20 μs, and the lowest-energy returned sample was selected as the output. For RQA, the annealing sequence was initialized from the Babai solution, corresponding to the all-$+1$ Ising configuration. The reverse annealing schedule

Just Accepted

was

$$(0\ \mu\text{s}, 1.0) \rightarrow (10\ \mu\text{s}, 0.5) \rightarrow (20\ \mu\text{s}, 1.0),$$

with a reversal point of $s^* = 0.5$ and no intermediate pause. The lowest-energy returned sample was selected as the RQA output. For simulated annealing (SA), the same Ising coefficients h_i and J_{ij} were used, so that SA optimizes the same encoded correction problem as FQA and RQA.

Solution quality is evaluated using the squared residual error norm, where a smaller value represents a lattice vector closer to the target. For the secret recovery experiments, three additional parameter settings, $(5, 10, 97, 2.5)$, $(10, 20, 127, 3.0)$, and $(15, 30, 251, 3.5)$, were considered, with 50 independent instances generated for each setting. Exact recovery is declared only when the recovered secret vector matches the true secret vector.

4.2 Comparison between Quantum Annealing and Classical Baselines

To provide a more comprehensive evaluation of the proposed quantum annealing framework, three classical baselines are considered: Babai's nearest-plane algorithm, SA, and a lattice embedding method with BKZ reduction. Babai's algorithm provides the initial lattice decoding solution. SA optimizes the same Ising formulation as FQA and RQA, while BKZ provides an additional classical lattice reduction baseline. All methods are evaluated on the same Search-LWE instances.

For the SA baseline, we used the `SimulatedAnnealingSampler` provided by the Python `dimod` package, which is part of D-Wave's Ocean software suite. For each Search-LWE instance, the corresponding Ising model was sampled with `num_reads`=2000, and the sample with the lowest Ising energy was selected as the SA result. All other sampler parameters were left at their default settings.

For the BKZ baseline, we used the `fpylll` library and constructed a Kannan embedding lattice with embedding parameter $M = 1$. For each instance, BKZ reduction was performed independently with block sizes $\beta = 5$, 10, and 15. Candidate error vectors were extracted from the reduced basis vectors whose last coordinate was $\pm M$. Among the candidate error vectors obtained from the three runs, the candidate with the smallest squared Euclidean norm was selected for comparison with Babai's solution. This selection was based solely on the candidate norms, without using the ground-truth error vectors or secret values. The remaining BKZ settings followed the defaults provided by `fpylll`.

For each Search-LWE instance, Babai's algorithm is first used to obtain an initial lattice solution. Based on the residual problem, an Ising Hamiltonian is constructed and optimized using FQA, RQA, and SA. The squared residual error norm is used to evaluate solution quality. Compared with the Babai solution, a result is classified as Superior, Equal, or Inferior if its squared residual error norm is smaller, equal, or larger, respectively. The statistical results over 50 independent Search-LWE instances for each parameter setting are summarized in Table 1.

Table 1 Comparison of FQA, RQA, SA, and BKZ with the Babai solution. Each entry denotes Superior/Equal/Inferior instances according to the squared residual error norm.

(n, m, q, σ)	FQA	RQA	SA	BKZ
$(8, 18, 99, 3.2)$	31/19/0	31/19/0	31/19/0	37/13/0
$(13, 26, 129, 5.0)$	36/4/10	38/2/10	43/7/0	50/0/0
$(18, 36, 509, 8.0)$	22/0/28	29/0/21	50/0/0	50/0/0
$(23, 46, 509, 8.0)$	14/0/36	20/0/30	49/0/1	50/0/0

As shown in Table 1, both FQA and RQA improve the Babai solution for a considerable number of the tested instances. These results demonstrate that the encoded correction problem can be implemented and explored on real quantum annealing hardware. The D-Wave Advantage2 system obtains lattice candidates with smaller residual error norms than the initial Babai solution for many tested instances.

The SA results further evaluate the effectiveness of the proposed Ising formulation. Since SA optimizes the same Ising Hamiltonian as FQA and RQA, its frequent improvement over the Babai solution provides empirical evidence that the encoded correction space contains lattice candidates with smaller residual error norms than the original Babai solution. Therefore, SA serves as a validation of the optimization landscape defined by the proposed formulation rather than a direct comparison of quantum advantage. This is particularly evident for the two larger tested parameter settings, where SA improves the Babai solution in 50 out of 50 and 49 out of 50 instances, respectively. At the same time, SA improves the Babai solution more consistently than FQA and RQA for several parameter settings. Therefore, the present results demonstrate the effectiveness of the Ising formulation, but do not indicate an advantage of quantum annealing over simulated annealing.

The lattice embedding method with BKZ reduction provides a stronger classical lattice baseline. BKZ improves the Babai solution in 37 out of 50 instances for the smallest parameter setting and in all 50 instances for the other three settings. Compared with FQA and RQA, BKZ provides more consistent improvements over the Babai solution for the tested instances. This result shows that classical lattice reduction

Just Accepted

remains highly effective for the small-scale instances considered in this work and motivates future improvements of the encoded correction space.

Overall, the comparison shows that the proposed Ising formulation provides an effective correction mechanism beyond the Babai solution and can be implemented on real quantum annealing hardware. However, the current experiments do not demonstrate an advantage of quantum annealing over SA and BKZ method.

As quantum annealing hardware continues to improve, including increased qubit resources, enhanced connectivity, and reduced embedding overhead, larger and more complex correction spaces may become feasible to explore. These advances may further improve the capability of the proposed framework for solving larger-scale Search-LWE instances. Accordingly, future work will focus on extending the encoded correction space, developing more effective quantum-classical optimization strategies, and evaluating the scalability of the framework on larger problem instances.

4.3 Analysis of Scaling Behavior and Classical Local Refinement

To investigate the impact of increasing Search-LWE problem sizes on the proposed quantum annealing framework, we analyze both the scaling characteristics of the encoded Ising problems and the corresponding optimization behavior. Furthermore, classical local refinement is investigated as a strategy to improve the quality of annealing solutions.

4.3.1 Scaling Characteristics of the Search-LWE Ising Formulation

The difficulty of solving Search-LWE instances using quantum annealing is closely related to the characteristics of the corresponding Ising formulations. For the considered Search-LWE formulation, the number of logical variables in the Ising model is determined by the number of LWE samples, i.e., $N = m$. Therefore, the corresponding Ising formulation contains 2^N possible spin configurations. As the parameter setting increases from $(8, 18, 99, 3.2)$ to $(23, 46, 509, 8.0)$, the number of logical variables grows from 18 to 46, resulting in an increase of the configuration space from $2^{18} = 2.62 \times 10^5$ to $2^{46} = 7.04 \times 10^{13}$. This exponential growth characterizes the increasing size of the encoded optimization problem as the Search-LWE parameters scale.

In addition to the configuration space, the connectivity of the generated Ising models also changes with the problem size. For the four parameter settings, the median numbers of nonzero quadratic couplings are 153, 324, 630, and 1035, respectively. These values are close to the maximum possible numbers of quadratic interactions, indicating that the generated Ising formulations become nearly fully connected for larger instances. The increasing number of interactions results in more complex optimization landscapes and may increase the difficulty of solving the encoded problems.

To further characterize the variation of the energy landscapes, we analyze the dynamic ranges of the linear and quadratic Hamiltonian coefficients. The coefficient ranges are defined as

$$R_h = \frac{\max_i |h_i|}{\min_{i:h_i \neq 0} |h_i|}, \qquad R_J = \frac{\max_{i<j} |J_{ij}|}{\min_{i<j:J_{ij} \neq 0} |J_{ij}|}.$$

The corresponding statistics are summarized in Table 2.

As shown in Table 2, increasing the Search-LWE parameters leads to simultaneous growth in the logical problem size, interaction density, and coefficient dynamic ranges. The median value of R_J increases from 216.50 to 2513.13, while the median value of R_h increases from 32.44 to 121.54. These results indicate that larger Search-LWE instances generate increasingly complex Ising energy landscapes, providing a quantitative explanation for the increased difficulty of obtaining high-quality low-energy solutions as the problem size grows.

4.3.2 Scaling Behavior of Quantum Annealing Performance

The resource requirements and optimization performance of the quantum annealing implementation are further investigated under different Search-LWE parameter settings. Specifically, we analyze the physical resources required for embedding the generated Ising problems and the corresponding empirical optimization performance, including the number of logical variables, physical qubits after minor embedding, embedding overhead, annealing repetitions, and the empirical improvement rate.

The logical problem size follows the Ising formulation described in the previous subsection. As the Search-LWE parameters increase, the resulting Ising models contain more logical variables and denser interactions, leading to increased physical resource requirements after minor embedding onto quantum annealing hardware.

For each parameter setting, the generated Ising models are embedded onto the Zephyr topology using minor embedding. Since the embedding process is not unique and may vary across independently generated instances, the physical qubit count, embedding overhead, and maximum chain length are reported as median values with interquartile ranges over 50 independent instances.

Just Accepted

Table 2 Scaling characteristics of the Ising formulations under different Search-LWE parameter settings. The number of nonzero J_{ij} terms is reported as the median, while R_h and R_J are reported as median [Q1, Q3] over 50 independent instances.

(n, m, q, σ)	N	2^N	Nonzero J_{ij}	R_h	R_J
$(8, 18, 99, 3.2)$	18	2.62×10^5	153	32.44 [16.40, 74.83]	216.50 [135.50, 264.75]
$(13, 26, 129, 5.0)$	26	6.71×10^7	324	78.40 [38.23, 139.23]	389.00 [310.00, 452.00]
$(18, 36, 509, 8.0)$	36	6.87×10^{10}	630	87.61 [38.98, 224.05]	1678.08 [750.22, 2840.00]
$(23, 46, 509, 8.0)$	46	7.04×10^{13}	1035	121.54 [74.76, 187.39]	2513.13 [1363.50, 5751.81]

The embedding overhead is defined as

$$\eta_{\text{emb}} = \frac{N_{\text{physical}}}{N_{\text{logical}}},$$

where N_{physical} denotes the number of physical qubits occupied after embedding and N_{logical} denotes the number of logical variables in the corresponding Ising formulation.

The scaling characteristics of the quantum annealing implementation are summarized in Table 3.

The number of annealing repetitions is controlled by the number of reads submitted to the quantum annealing processor. In all experiments, the annealing schedule parameters are kept identical across different problem sizes to ensure a fair comparison. The numbers of reads are set to 2000 and 100 for FQA and RQA, respectively.

Since the exact ground states of the encoded Ising formulations are not available for all tested Search-LWE instances, the conventional ground-state success probability cannot be directly evaluated. Instead, we define an empirical improvement probability based on the optimization objective of the Search-LWE problem:

$$P_{\text{succ}} = \frac{N_{\text{succ}}}{N_{\text{total}}},$$

where N_{succ} denotes the number of Search-LWE instances for which the annealing solution achieves a smaller squared residual error norm than the Babai solution, and $N_{\text{total}} = 50$ denotes the total number of tested instances.

As shown in Table 3, the required physical resources increase rapidly with the growth of the Search-LWE parameters. The median number of physical qubits increases from approximately 40 for the smallest parameter setting to more than 220 for the largest one, while the embedding overhead increases from approximately 2.2 to nearly 4.9. This indicates that larger Search-LWE instances require substantially more hardware resources due to the increasing size and connectivity of the corresponding Ising formulations.

Meanwhile, the empirical improvement probability decreases as the problem size increases. For FQA, the number of improved instances decreases from 31/50 for $(8, 18, 99, 3.2)$ to 14/50 for $(23, 46, 509, 8.0)$. A similar trend is observed for RQA. This behavior is consistent with the increasing complexity of the encoded Ising models, including the growth of the logical search space, interaction density, and coefficient dynamic range analyzed in the previous subsection.

Overall, the scaling analysis shows that larger Search-LWE instances require substantially increased embedding resources and exhibit lower empirical improvement rates on current quantum annealing hardware. Despite these limitations, the proposed framework continues to obtain improved solutions for a subset of larger instances, indicating that quantum annealing can still provide improved candidates for a subset of the tested instances.

4.3.3 Hybrid Quantum-Classical Local Optimization

The scaling analysis above shows that increasing Search-LWE parameters lead to more complex Ising formulations and increased difficulty in obtaining high-quality solutions using quantum annealing alone. Although FQA and RQA are able to improve upon the Babai solution for a subset of instances, some annealing results remain inferior to the classical baseline, particularly for larger problem sizes.

This motivates the introduction of a hybrid quantum-classical local refinement strategy to further improve the quality of the solutions obtained from quantum annealing. In practical quantum annealing systems, finite annealing time and hardware noise may prevent the system from consistently reaching lower energy configurations. Consequently, the returned spin configurations are often located in favorable low-energy regions, while further improvements may still be obtained through local adjustments of a small number of variables.

Motivated by this observation, we introduce a hybrid quantum-classical local optimization strategy. Specifically, the solution returned by quantum annealing, either FQA or RQA, is used as the initial state, and a classical local search procedure is subsequently applied by exploring a restricted neighborhood through one- and two-spin flips. A candidate flip is accepted if it decreases the Ising objective value, and the refinement procedure terminates when no further local improvement can be found.

The refinement process only explores a limited neighborhood around the initial annealing solution. When both one- and two-spin flips are considered, the computational complexity of the local search grows as $O(N^2)$ with the number

Just Accepted

Table 3 Scaling characteristics of the quantum annealing framework under different Search-LWE parameter settings. The physical qubit count, embedding overhead, and maximum chain length are reported as median [Q1,Q3] over 50 independent instances.

Parameters (n, m, q, σ)	N_{logical}	N_{physical}	η_{emb}	$L_{\max}$	Reads (FQA)	Reads (RQA)	$(P_{\text{succ}}^{FQA}, P_{\text{succ}}^{RQA})$
$(8, 18, 99, 3.2)$	18	40 [39,43]	2.22 [2.17,2.39]	3 [3,3]	2000	100	(31/50,31/50)
$(13, 26, 129, 5.0)$	26	74 [71,78]	2.85 [2.73,3.00]	4 [3,4]	2000	100	(36/50,38/50)
$(18, 36, 509, 8.0)$	36	136 [133,142]	3.78 [3.69,3.94]	5 [5,6]	2000	100	(22/50,29/50)
$(23, 46, 509, 8.0)$	46	225 [221,232]	4.89 [4.80,5.04]	7 [7,7]	2000	100	(14/50,20/50)

of logical variables. Under the flip range considered in this work, the additional computational overhead remains small compared with the quantum annealing sampling process.

To evaluate the effectiveness of the hybrid strategy, two larger-scale parameter settings, $(n, m, q, \sigma) = (18, 36, 509, 8.0)$ and $(n, m, q, \sigma) = (23, 46, 509, 8.0)$, are selected. These cases are chosen because the performance improvement of quantum annealing alone becomes more limited for larger instances. For each parameter setting, the solutions obtained by FQA and RQA are compared with their locally refined counterparts. The statistical results are summarized in Table 4 and Table 5.

Table 4 Comparison between FQA and FQA with local refinement

Parameters (n, m, q, σ)	Superior	Equal	Inferior
$(18, 36, 509, 8.0)$	11	39	0
$(23, 46, 509, 8.0)$	11	39	0

Table 5 Comparison between RQA and RQA with local refinement

Parameters (n, m, q, σ)	Superior	Equal	Inferior
$(18, 36, 509, 8.0)$	8	42	0
$(23, 46, 509, 8.0)$	10	40	0

From Table 4 and Table 5, it can be observed that classical local refinement further improves the solutions obtained by both FQA and RQA for a subset of instances, while maintaining comparable performance for the remaining cases. This indicates that the solutions sampled by quantum annealing often provide useful low-energy starting points, and that classical local search can effectively exploit nearby configurations to further reduce the residual error norm.

Overall, the hybrid quantum-classical strategy combines candidate generation by quantum annealing with local improvement by classical optimization. The experimental results show that the proposed refinement procedure improves the robustness of the framework and provides additional solution quality improvements for larger Search-LWE instances.

4.4 Secret Recovery on Real Quantum Annealing Hardware

To further evaluate the proposed quantum-classical hybrid framework on real quantum hardware, we conduct exact secret recovery experiments for small Search-LWE instances using the D-Wave Advantage2 quantum computer.

At present, experimental studies of LWE on real quantum hardware remain limited, and most existing work focuses on theoretical analysis or simulation-based evaluation. In particular, experimental investigations of Search-LWE secret recovery on real quantum hardware are still scarce. Motivated by this, we evaluate the exact secret recovery performance of the proposed framework under several small-scale Search-LWE parameter settings on real quantum annealing hardware.

For the secret-recovery experiments, three additional small-scale parameter settings are considered: $(n, m, q, \sigma) = (5, 10, 97, 2.5)$, $(10, 20, 127, 3.0)$, and $(15, 30, 251, 3.5)$. Because exact secret recovery is a stricter evaluation criterion than reducing the error norm relative to the Babai solution, small dimensions are selected to keep the resulting Ising models manageable on the available hardware. Within this range, the dimension n is increased from 5 to 15 to examine the change in recovery performance. In all three settings, the number of samples is set to $m = 2n$, maintaining the same ratio between the number of samples and the problem dimension.

The corresponding relative noise parameters $\alpha = \sigma/q$ are approximately 0.0258, 0.0236, and 0.0139, respectively. Thus, the error standard deviation is less than 3% of the modulus in all three settings. These parameters are used to generate small-scale synthetic instances for proof-of-concept experiments and do not correspond to a standardized parameter sequence or a concrete security level.

For each parameter setting, 50 independent Search-LWE instances are randomly generated. For each instance, secret recovery is performed separately using the Babai solution, the FQA-hybrid solution, and the RQA-hybrid solution. A method is regarded as successful if its recovered secret matches the true secret vector.

To evaluate the complementary recovery behavior of FQA-

Just Accepted

hybrid and RQA-hybrid, we additionally report a combined QA result. The combined result regards an instance as successfully recovered if either FQA-hybrid or RQA-hybrid recovers the correct secret vector. The Babai solution is not included in this combined quantum annealing result. The individual and combined recovery results are summarized in Table 6. Here, FQA-H and RQA-H denote the FQA-hybrid and RQA-hybrid methods, respectively, and QA-Union represents the union of their recovery results.

Table 6 Secret recovery results of different methods

(n, m, q, σ)	Babai	FQA-H	RQA-H	QA-Union
$(5, 10, 97, 2.5)$	25 (50%)	38 (76%)	38 (76%)	38 (76%)
$(10, 20, 127, 3.0)$	12 (24%)	23 (46%)	24 (48%)	24 (48%)
$(15, 30, 251, 3.5)$	7 (14%)	14 (28%)	15 (30%)	18 (36%)

As shown in Table 6, the exact secret recovery rate decreases as the problem dimension increases for all three individual methods. Babai achieves success rates of 50%, 24%, and 14% for $n = 5, 10$, and 15, respectively. The corresponding success rates are 76%, 46%, and 28% for FQA-H, and 76%, 48%, and 30% for RQA-H. Both FQA-H and RQA-H achieve higher recovery rates than Babai on the tested instances. The QA-Union strategy achieves success rates of 76%, 48%, and 36%, respectively. For the largest tested setting, FQA-H and RQA-H recover 14 and 15 instances, respectively, while their union recovers 18 instances, indicating partially complementary recovery behavior between the two approaches.

Finally, we compare the experimental results of this work with a representative existing study on real quantum hardware, as shown in Table 7.

Table 7 Comparison with existing experimental studies of LWE on real quantum computer

Type	Dimension	Algorithm	Platform	Source
Decision-LWE	2	QAOA	IBM	[23]
Search-LWE	15	QA	D-Wave	This work

As shown in Table 7, experimental studies of LWE on real quantum hardware remain limited. The representative prior study considers a low-dimensional Decision-LWE instance on a gate-based quantum processor, whereas this work experimentally evaluates Search-LWE secret recovery on a quantum annealing platform for small instances with dimensions up to $n = 15$. This comparison is intended to characterize the experimental scope of the present work rather than to claim a practical cryptanalytic advantage.

5 Conclusion

This paper proposes a hybrid quantum annealing-classical framework for solving the Search-LWE problem on real quantum annealing hardware. A restricted binary correction space around the Babai solution is encoded into an Ising Hamiltonian. Since the zero correction is always contained in this space, the exact optimum of the formulation is guaranteed to have a squared residual error norm no larger than that of the Babai solution. FQA and RQA are implemented to explore the encoded correction space, where RQA further exploits the classical information provided by the Babai solution through local quantum refinement. Experimental results show that the proposed framework can improve Babai solutions for a considerable number of small-scale instances. Simulated annealing results validate the effectiveness of the encoded correction formulation, while comparisons with BKZ-based lattice reduction reveal the limitations of the current correction space and motivate further expansion of the search space. A classical local search strategy is further introduced to refine quantum annealing outputs and reduce residual errors. Finally, secret vector recovery is demonstrated for Search-LWE instances with dimensions up to 15 on a D-Wave quantum computer. These results provide a proof of concept on current quantum annealing hardware, but do not demonstrate a practical threat to cryptographically relevant LWE-based systems.

As quantum hardware continues to advance, including improvements in qubit resources, connectivity, embedding efficiency, and the ability to handle complex Ising coefficient landscapes, future work will investigate larger encoded correction spaces and improved quantum-classical hybrid optimization strategies to further enhance the scalability of the proposed framework for larger Search-LWE instances.

Acknowledgment

This work was supported by the National and Local Joint Laboratory of Cyberspace Security Technology (Grant: No.NLCS-202512-002).

Declaration of competing interest

The authors have no competing interests to declare that are relevant to the content of this article.

Reference

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

[2] N. Koblitz, Elliptic curve cryptosystems, *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

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

Just Accepted

[4] A. Politi, J. C. F. Matthews, and J. L. O'Brien, Shor's quantum factoring algorithm on a photonic chip, *Science*, vol. 325, no. 5945, p. 1221, 2009.

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

[6] B. Yan, Z. Tan, S. Wei, H. Jiang, W. Wang, H. Wang, L. Luo, Q. Duan, Y. Liu, W. Shi, and Y. Fei, Factoring integers with sublinear resources on a superconducting quantum processor, https://arxiv.org/abs/2212.12372, 2022.

[7] Z. Pei, C. Hong, F. Xia, and C. Wang, An innovative algorithm for attacking symmetric ciphers using D-Wave quantum annealing, *Tsinghua Sci. Technol.*, vol. 30, no. 5, pp. 2184–2194, 2025.

[8] C. Wang, J. Yu, Z. Pei, Q. Wang, and C. Hong, A first successful factorization of RSA-2048 integer by d-wave quantum computer, *Tsinghua Sci. Technol.*, vol. 30, no. 3, pp. 1270–1282, 2024.

[9] C. Hong, Z. Pei, Q. Wang, S. Yang, J. Yu, and C. Wang, Quantum attack on RSA by D-Wave Advantage: a first break of 80-bit RSA, *Sci. China Inf. Sci.*, vol. 68, no. 2, p. 129501, 2025.

[10] D. J. Bernstein and T. Lange, Post-quantum cryptography, *Nature*, vol. 549, pp. 188–194, 2017.

[11] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, CRYSTALS-Kyber, https://pq-crystals.org/kyber/, 2017.

[12] B. Shi, D. Leo, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé, Crystals-dilithium, https://pq-crystals.org/dilithium/index.shtml, 2020.

[13] T. Prest, P. A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. Whyte, and Z. Zhang, Falcon, https://falcon-sign.info/, 2020.

[14] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, *J. ACM*, vol. 56, no. 6, pp. 1–40, 2009.

[15] A. Esser, F. Heuer, R. Kübler, A. May, and C. Sohler, Dissection-bkw, in *Proc. Annu. Int. Cryptology Conf.*, Santa Barbara, CA, USA, 2018, pp. 638–666.

[16] M. R. Albrecht and Y. Shen, Quantum augmented dual attack, https://arxiv.org/abs/2205.13983, 2022.

[17] H. Liu and Y. Yu, A non-heuristic approach to time-space tradeoffs and optimizations for BKW, in *Proc. Int. Conf. Theory Appl. Cryptology Inf. Security*, Taipei, Taiwan, 2022, pp. 741–770.

[18] J. Cao, H. Jiang, and Q. Cheng, Refined Attack on LWE with Hints: Constructing Lattice via Gaussian Elimination, in *Proc. Annu. Int. Cryptology Conf.*, Santa Barbara, CA, USA, 2025, pp. 385–416.

[19] E. Wenger, E. Saxena, M. Malhou, E. Thieu, and K. Lauter, Benchmarking attacks on learning with errors, in *Proc. 2025 IEEE Symp. Security Privacy (SP)*, San Francisco, CA, USA, 2025, pp. 279–297.

[20] A. Qayyum, Advancing LWE cryptanalysis: An updated MIP model and QUBO formulation for quantum annealing, *Prikl. Diskr. Mat. Suppl.*, no. 18, pp. 194–200, 2025.

[21] A. Chailloux and P. Hermouet, On the quantum equivalence between $S|\mathrm{LWE}\rangle$ and ISIS, in *Proc. Annu. Int. Cryptology Conf.*, Santa Barbara, CA, USA, 2026, pp. 391–428.

[22] L. Lv, B. Yan, H. Wang, Z. Ma, Y. Fei, X. Meng, and Q. Duan, Using variational quantum algorithm to solve the LWE problem, *Entropy*, vol. 24, no. 10, p. 1428, 2022.

[23] M. Zheng, J. Zeng, W. Yang, P. J. Chang, Q. Lu, B. Yan, H. Zhang, M. Wang, S. Wei, and G. L. Long, Quantum-classical hybrid algorithm for solving the learning-with-errors problem on NISQ devices, *Commun. Phys.*, vol. 8, no. 1, p. 208, 2025.

[24] E. Farhi, J. Goldstone, and S. Gutmann, A Quantum Approximate Optimization Algorithm, https://arxiv.org/abs/1411.4028, 2014.

[25] M. R. Albrecht, R. Player, and S. Scott, On the concrete hardness of learning with errors, *J. Math. Cryptol.*, vol. 9, no. 3, pp. 169–203, 2015.

[26] A. K. Lenstra, H. W. Lenstra, and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.*, vol. 261, pp. 515–534, 1982.

[27] L. Babai, On Lovász' lattice reduction and the nearest lattice point problem, *Combinatorica*, vol. 6, pp. 1–13, 1986.

[28] A. B. Finnila, M. A. Gomez, C. Sebenik, C. Stenson, and J. D. Doll, Quantum annealing: A new method for minimizing multidimensional functions, *Chem. Phys. Lett.*, vol. 219, no. 5-6, pp. 343–348, 1994.

[29] K. Ohno and N. Togawa, Mitigating precision errors in quantum annealing via coefficient reduction of embedded Hamiltonians, *IEEE Trans. Quantum Eng.*, vol. 7, Art. no. 3102522, 2026.

[30] M. Ohkuwa, H. Nishimori, and D. A. Lidar, Reverse annealing for the fully connected p-spin model, *Phys. Rev. A*, vol. 98, no. 2, p. 022314, 2018.

Author biography



Chunlei Hong received the MS degree from Hubei University, Wuhan, China, in 2022. He is currently a PhD candidate at Shanghai University, Shanghai, China. His main research interests include cyberspace security and quantum computing cryptography.

Just Accepted



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

Just Accepted