


# Iterative quantum optimization with an adaptive problem Hamiltonian for the shortest vector problem

Yifeng Rocky Zhu <sup>1</sup>, David Joseph,<sup>2</sup> Cong Ling,<sup>3</sup> and Florian Mintert<sup>1,4</sup>

<sup>1</sup>*Physics Department, Blackett Laboratory, Imperial College London, Prince Consort Road, SW7 2AZ, United Kingdom*

<sup>2</sup>*SandboxAQ, Palo Alto, California, USA*

<sup>3</sup>*Electrical and Electronic Engineering Department, Imperial College London*

<sup>4</sup>*Helmholtz-Zentrum Dresden-Rossendorf, Bautzner Landstraße 400, 01328 Dresden, Germany*



(Received 29 April 2022; accepted 16 August 2022; published 29 August 2022)

Quantum optimization algorithms hold the promise of solving classically hard, discrete optimization problems in practice. The requirement of encoding such problems in a Hamiltonian realized with a finite (and currently small) number of qubits, however, poses the risk of finding only the optimum within the restricted space supported by this Hamiltonian. We describe an iterative algorithm in which a solution obtained with such a restricted problem Hamiltonian is used to define a new problem Hamiltonian that is better suited than the previous one. In numerical examples of the shortest vector problem, we show that the algorithm with a sequence of improved problem Hamiltonians converges to the desired solution.

DOI: [10.1103/PhysRevA.106.022435](https://doi.org/10.1103/PhysRevA.106.022435)

## I. INTRODUCTION

The currently available hardware for quantum information processing is getting close to the specifications that are required for the solution of real-world problems [1]. As a result of the anticipated ability of quantum computers to break popular cryptographic protocols, a new generation of protocols has been developed [2]. These postquantum cryptographic protocols are expected to be secure even if an eavesdropper had access to a fully functioning quantum computer. There is a variety of such protocols, and the assessment of their security either in terms of security proof or explicit counterattack is a central goal of the community.

A large class of postquantum cryptographic protocols is based on the shortest vector problem (SVP) of lattices. Similar to the prime-factorization problem that Rivest-Shamir-Adleman (RSA) [3] is built upon, SVP is also a seemingly simple problem that turns out to be computationally difficult to solve [4]. It is a discrete optimization problem, defined in terms of a basis of a finite-dimensional vector space. Lattice vectors are obtained by forming linear combinations of the basis vectors with integer expansion coefficients. Usually, the security of lattice-based cryptography can be reduced to the problem of finding the shortest, nonzero vector of a lattice (in the following simply referred to as the *shortest vector*).

The computational effort required to find the shortest vector depends on the properties of a basis; with a *good basis* of short vectors that are close-to-orthogonal to each other, the shortest vector can typically be found efficiently in practice, but with a *bad basis* of long and close-to-parallel vectors finding the shortest vector is computationally intractable, even with the largest currently existing classical high-performance computers for lattices with a dimension in the hundreds. A

cryptographic protocol can, therefore, be based on a publicly known bad basis [4].

Since the shortest-vector problem can be mapped onto a quantum Ising Hamiltonian [5], such that its eigenvectors and eigenvalues correspond to lattice vectors and their squared lengths, it can readily be formulated as a quantum mechanical algorithm such as an adiabatic algorithm [6,7], variational quantum eigensolver [8–11], or a quantum approximate optimization algorithm (QAOA) [12,13].

A crucial issue in all these implementations is that any finite number of qubits allows only for an optimization over a finite range of values of the expansion coefficients. Even though there is a minimal number of qubits that guarantees that the shortest vector can be found [5,11], this number [ $O(d \log d)$  where  $d$  is the dimension] is far out of reach for current and foreseeable technology. Even in the absence of any imperfections, such as limited gate fidelities or decoherence, realistic sizes of a qubit register would thus result in the risk of finding the shortest vector within a subset of vectors that is not the actual shortest vector.

As we will show here, the qubit requirement to realize a problem Hamiltonian in a sufficiently large Hilbert space based on a bad basis is indeed very stringent. Finding a reasonably short, but not necessarily the shortest vector within a subset of vectors, however, helps to construct a better basis than the originally used one, as also exploited in independent, concurrent work [11]. A quantum algorithm with a problem Hamiltonian based on this improved basis then gives access to shorter vectors than the one based on the original problem Hamiltonian. The resultant iterative improvement of basis and corresponding problem Hamiltonian enables the search for the actual shortest vector even under stringent limitations of the available qubits.

## II. QUANTUM OPTIMIZATION FOR THE SHORTEST VECTOR PROBLEM

A lattice is the collection of points in a  $d$ -dimensional space given by the linear superpositions  $\sum_{i=1}^d n_i \mathbf{b}_i$  of basis vectors  $\mathbf{b}_i$  with integer expansion coefficients  $n_i$ . Any lattice [14] can be represented by infinitely many bases; given one basis  $\{\mathbf{b}_i\}$ , any other basis  $\{\mathbf{a}_i\}$  can be formed in terms of linear combinations

$$\mathbf{a}_i = \sum_j V_{ij} \mathbf{b}_j, \quad (1)$$

where the matrix  $V$  has integer elements  $V_{ij}$  and determinant  $\pm 1$ , i.e., it is unimodular.

A quantum mechanical Hamiltonian  $H_P$  representing a lattice can be defined as [15]

$$H_P = \sum_{ij=1}^d (\mathbf{b}_i \mathbf{b}_j) \hat{Q}_i \hat{Q}_j, \quad (2)$$

where the scalar factors  $\mathbf{b}_i \mathbf{b}_j$  determine the structure of the lattice and each of the mutually commuting operators  $\hat{Q}_i$  has an integer spectrum. Any state that is a mutual eigenvector of all the operators  $\hat{Q}_i$  with corresponding eigenvalues  $n_i$  corresponds to a lattice vector  $\sum_i n_i \mathbf{b}_i$ , and the associated eigenvalue of  $H_P$  is given by the squared length  $\sum_{ij=1}^d \mathbf{b}_i \mathbf{b}_j n_i n_j$  of this lattice vector.

In practice, the operators  $\hat{Q}_i$  act on a Hilbert space that is the tensor product of  $d$  smaller factors and the indices  $i$  indicate the factor that the respective operator acts on nontrivially. Each of the operators  $\hat{Q}_i$  can be realized in terms of several qubits and the encoding

$$\hat{Q}_i = \frac{1}{2} \left( \sum_{j=1}^k 2^{j-1} \hat{Z}_{ij} + \mathbb{1} \right), \quad (3)$$

with the Pauli  $\hat{Z}$  operator achieves a nondegenerate spectrum in the range  $[-2^{k-1} + 1, 2^{k-1}]$  in terms of  $k$  qubits. With this encoding, the problem Hamiltonian for a  $d$ -dimensional lattice is an Ising Hamiltonian with  $dk$  qubits interacting via a  $\hat{Z}\hat{Z}$  interaction [5].

Deterministically finding the first excited state of this problem Hamiltonian corresponding to the shortest vector is typically not possible with quantum hardware of the limited, currently available specifications, but a QAOA algorithm

$$|\Psi\rangle = \exp(-i\beta H_D) \exp(-i\gamma H_P) |\Psi_0\rangle \quad (4)$$

of lowest depth [16] can realize a state  $|\Psi\rangle$  that results in high probabilities to project onto a low-lying eigenstate of  $H_P$  upon measurement of the observables  $\hat{Q}_i$  if the initial state  $|\Psi_0\rangle$ , Rabi-angles  $\beta$  and  $\gamma$ , and driver Hamiltonian  $H_D$  are chosen suitably [13, 17].

## III. LIMITED PARAMETER RANGE

The problem Hamiltonian in Eq. (2) is defined in terms of a basis of the lattice and different choices for this basis will generally result in different Hamiltonians. Even

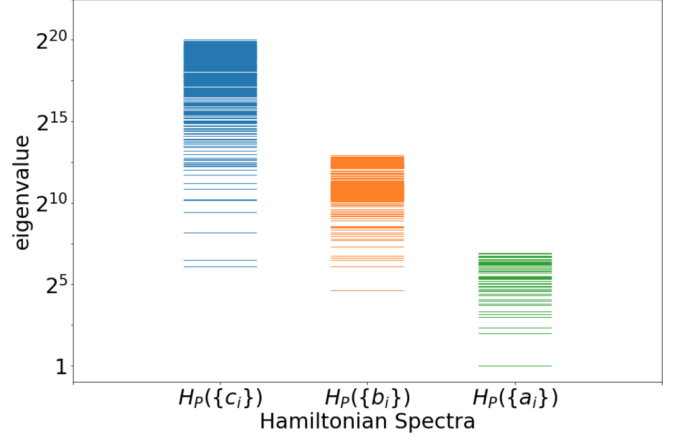


FIG. 1. The blue (left), orange (middle), and green (right) level sets depict the spectra of finite-dimensional problem Hamiltonians [Eq. (2)] for the lattice defined in terms of the bases in Eqs. (7), (6), and (5) respectively; each of the four operators  $\hat{Q}_i$  [Eq. (3)] is comprised of  $k = 2$  qubits. The green (right) spectrum corresponds to the problem Hamiltonian defined in terms of the shortest basis and it contains the eigenvalue corresponding to the shortest vector of length 1. The orange (middle) and blue (left) spectra correspond to the problem Hamiltonians defined in terms of the increasingly bad bases, and their lowest eigenvalues lie significantly above the eigenvalue corresponding to the actual shortest vector.

though any such problem Hamiltonian has the same spectrum (given by the squared lengths of all the lattice vectors) the problem Hamiltonians defined with different lattice bases have different physical properties, encoded in the scalar factors  $\mathbf{b}_i \mathbf{b}_j$ .

In any practical implementation with the operators  $\hat{Q}_i$  realized in terms of several qubits, such as the construction given in Eq. (3), the resulting problem Hamiltonians are truncated and their spectra are only subsets of the spectrum of the full problem Hamiltonian. This truncation also breaks the equivalence of different problem Hamiltonians, and the spectrum of any truncated problem Hamiltonian depends on the underlying lattice basis.

A problem Hamiltonian constructed in terms of a good basis will be such that the shortest vector is associated with eigenvalues of the operators  $\hat{Q}_i$  that have a small magnitude because the expansion of the shortest vector in terms of a good basis requires only small expansion coefficients. Since, however, the expansion of the shortest vector in terms of a bad basis typically requires large expansion coefficients, the operators  $\hat{Q}_i$  need a broad spectrum to ensure that the spectrum of the problem Hamiltonian contains the eigenvalue associated with the shortest vector.

This is exemplified for the case of a four-dimensional lattice  $\mathcal{L}$  in Fig. 1. A basis  $\{\mathbf{a}_i\}$  of  $\mathcal{L}$  with vectors of minimal lengths is given by

$$\mathbf{a}_1 = [1, 0, 0, 0], \quad (5a)$$

$$\mathbf{a}_2 = [0, 2, 0, 0], \quad (5b)$$

$$\mathbf{a}_3 = [0, 0, 3, 0], \quad (5c)$$

$$\mathbf{a}_4 = [0, 0, 0, 4]. \quad (5d)$$

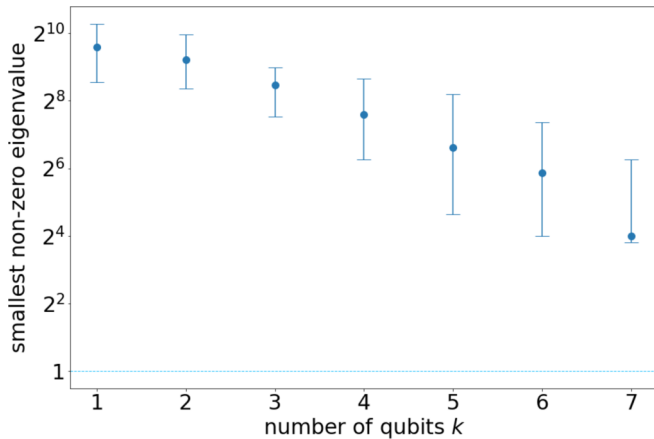


FIG. 2. Lowest nonzero eigenvalues of problem Hamiltonians for the four-dimensional lattice defined in Eq. (5) as a function of the number of qubits  $k$  used in the realization of the operators  $\hat{Q}_i$  in Eq. (3). The dots depict the medians over 100 problem Hamiltonians constructed in terms of randomly chosen unimodular matrices and the error bars depict the corresponding 75th percentiles.

Two exemplary bases with longer basis vectors are given by

$$\mathbf{b}_1 = [3, 0, 15, -12], \quad (6a)$$

$$\mathbf{b}_2 = [0, 4, 3, 8], \quad (6b)$$

$$\mathbf{b}_3 = [28, -18, 9, 8], \quad (6c)$$

$$\mathbf{b}_4 = [0, 0, 3, -4], \quad (6d)$$

and

$$\mathbf{c}_1 = [25, 78, 105, 160], \quad (7a)$$

$$\mathbf{c}_2 = [-3, 32, 18, 64], \quad (7b)$$

$$\mathbf{c}_3 = [53, 128, 195, 264], \quad (7c)$$

$$\mathbf{c}_4 = [0, 8, 9, 12]. \quad (7d)$$

All three bases represent the same lattice  $\mathcal{L}$ . The basis  $\{\mathbf{a}_i\}$  qualifies as a good basis, while  $\{\mathbf{c}_i\}$  is a bad basis, and the basis  $\{\mathbf{b}_i\}$  is clearly better than  $\{\mathbf{c}_i\}$ , but substantially worse than  $\{\mathbf{a}_i\}$ .

Figure 1 depicts the spectra of the problem Hamiltonians constructed with either of these three bases and each operator  $\hat{Q}_i$  realized in terms of  $k = 2$  qubits. Whereas the spectrum of the problem Hamiltonian constructed with the basis  $\{\mathbf{a}_i\}$  (green) covers mostly low-lying states of the spectrum of the full problem Hamiltonian, the spectra of the problem Hamiltonians constructed with the basis  $\{\mathbf{b}_i\}$  (orange) and  $\{\mathbf{c}_i\}$  (blue) cover substantially more high-lying states. In particular, the lowest nonzero states encoded in these two Hamiltonians are substantially higher than the actual shortest vector.

A problem Hamiltonian constructed with a bad basis that does include the eigenstate of the shortest vector would thus require substantially more qubits per lattice dimension. Figure 2 depicts the smallest nonzero eigenvalue of problem Hamiltonians realized with different numbers of qubits per lattice dimension as a function of the qubit number  $k$ . The dots depict the medians over 100 bases constructed with randomly chosen unimodular matrices  $W = LU$  obtained as a product

of a lower triangular matrix  $L$  and an upper triangular matrix  $U$  with unit diagonal elements, and all other nonvanishing elements are chosen randomly from a uniform distribution within the range  $[-10, 10]$ ; the error bars depict the 75th percentiles.

The smallest nonzero eigenvalues clearly decrease with the number of qubits, but even with seven qubits, the median is still larger than the shortest vector length (indicated by a light-blue line). Extrapolating from Fig. 2 suggests that about ten qubits per lattice dimension are required to ensure that the eigenvector associated with the shortest lattice vector is contained in the explicit realization of the problem Hamiltonian.

Since this qubit requirement seems far out of reach with near-future technology [18,19], we will present in the following an adaptive algorithm that is based on a gradual improvement of bases and the corresponding implementation of the problem Hamiltonian.

#### IV. ADAPTIVE PROBLEM HAMILTONIAN

The iterative quantum optimization with adaptive problem Hamiltonian (IQOAP) algorithm is initialized with the problem Hamiltonian constructed with the bad basis that is publicly available in a cryptographic protocol. An algorithm such as QAOA that can find a low-lying state in the spectrum of this problem Hamiltonian, at least probabilistically, produces a lattice vector. If it is possible to replace one of the basis vectors with this newly obtained vector while maintaining a basis [i.e., a set of vectors that spans the complete lattice, or, equivalently a set of vectors related to the original basis via Eq. (1) by a unimodular matrix  $V$ ], the basis is updated provided that the new basis vector is shorter than the basis vector that is being dropped. Independently of whether the basis is updated or not, the algorithm continues with the above quantum optimization using the problem Hamiltonian constructed with the current basis.

The central advantage of this strategy is that the number of qubits required to run the quantum optimization is significantly reduced. Even a realization with too few qubits to encode the actual shortest vector can help to find a better basis, which in turn will help to find short vectors at the available qubit count. One may certainly expect that the rate of convergence depends on the number of utilized qubits, but as we will show in the following, even an implementation with few qubits does typically result in reliable convergence to the actual shortest vector.

In the following discussion, the quantum mechanical part of IQOAP is performed in terms of QAOA with a single step in terms of problem Hamiltonian and driver Hamiltonian each, as given in Eq. (4). The driver Hamiltonian  $H_D = \sum_j \hat{X}_j$  is given by the collective Pauli  $\hat{X}$ . A single-step QAOA typically results in a high chance of observing the ground state of the problem Hamiltonian if  $\beta$  [in Eq. (4)] is chosen to adopt the value of  $\pi/4$ , and the value  $\gamma$  is chosen such that the expectation value is minimized [13,20]. Since in the present case the interest lies in the lowest excited eigenstate, it is indeed favorable to choose the values for the Rabi angles  $\beta$  and  $\gamma$  such that  $\langle \Psi | H_P | \Psi \rangle$  is minimized under the constraint  $\beta = \gamma$ . Since  $\langle \Psi | H_P | \Psi \rangle$  can be classically evaluated without explicit construction of the state  $|\Psi\rangle$  in Eq. (4) [13,21],

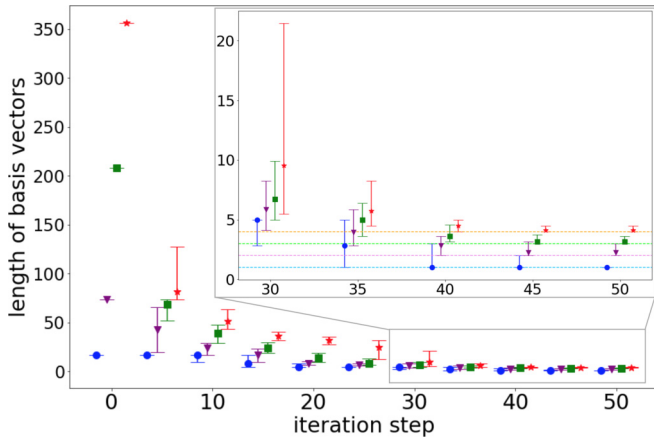


FIG. 3. Convergence of the basis during an IQOAP algorithm for the four-dimensional basis defined through Eq. (7). The y axis shows the lengths of the four basis vectors. The medians of the shortest, second shortest, second longest, and longest vectors over 50 iterations of the algorithm are denoted by blue circle, purple triangle, green square, and red star symbols, respectively. The error bars depict the 80th percentiles. The fluctuations result from the probabilistic nature of QAOA. The inset depicts a zoom in to the later stage of the algorithm and the horizontal lines depict the lengths of the basis vectors given in Eq. (5).

this minimization can be performed classically without using quantum mechanical computational resources.

Each run of QAOA yields a lattice vector  $\mathbf{v}$ . This is substituted into the basis if the following criteria are met.

- (1)  $\mathbf{v}$  is shorter than some basis vector  $\mathbf{b}$ .
- (2) Replacing  $\mathbf{b}$  with  $\mathbf{v}$  preserves the lattice.
- (3) If there are multiple eligible vectors to replace, then the longest eligible basis vector is replaced by  $\mathbf{v}$ .

If the above criteria are not met, then the QAOA circuit is repeated with the same problem Hamiltonian. Figure 3 depicts an example of how the basis vectors of the four-dimensional lattice defined through Eq. (7) decrease as the algorithm progresses. The problem Hamiltonian is encoded with  $k = 2$  qubits for each operator  $\hat{Q}_i$  in Eq. (3).

The dots depict the medians over 50 independent executions of the algorithm and the error bars indicate the 80th percentiles. For reasons of visibility only data for every fifth iteration step is depicted and the four data sets are depicted with different offsets on the  $x$  axis to avoid overlapping symbols. Typically it is possible to update the basis after two to ten repetitions of QAOA, and indeed, the lengths of all the four basis vectors decrease rapidly as the algorithm progresses.

The inset shows a zoom in to the later stage of the algorithm with the convergence towards the shortest basis. After 50 iterations, the actual shortest vector is found with high probability (82%) and also the other obtained basis vectors coincide with the shortest vectors [Eq. (5)] in the vast majority of cases.

These convergence properties are indeed not specific to this particular lattice, as shown in Fig. 4 which depicts the convergence of the algorithm for different four-dimensional lattices. The rate of convergence is very similar to that shown in Fig. 3; only the fluctuations around the medians (depicted

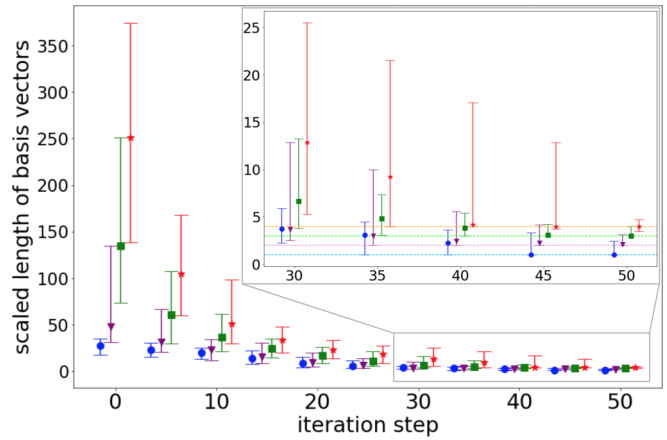


FIG. 4. Convergence of the IQOAP algorithm with 50 randomly chosen four-dimensional lattices. Since the lengths of the shortest vectors are different for different lattices, the y axis depicts the lengths of the basis vectors normalized to the lengths of the shortest basis vectors with a scaling factor of  $j = 1, 2, 3, 4$ . The medians of the scaled shortest, second shortest, second longest, and longest vectors over 50 iterations of the algorithm are denoted by blue circle, purple triangle, green square, and red star symbols, respectively. The error bars depict the 80th percentiles.

by the error bars) are a bit larger. Also here, the actual shortest vector is found within 50 iterations in the vast majority of cases, highlighting that the algorithm converges reliably independent of the properties of the underlying lattice.

## V. CONCLUSION

The ability to update the problem Hamiltonian during the progress of the algorithm opens up a new avenue of combining classical and quantum mechanical elements in an algorithm. Whereas many current hybrid algorithms such as the variational quantum eigensolver [8–11] have quantum and classical components (the quantum mechanical evaluation of a function and its classical minimization) that are independent of each other, the classical and quantum mechanical aspects in IQOAP are closely intertwined in that extracting classical information from QAOA [12,13] (or a similar algorithm) and classically updating the basis and corresponding problem Hamiltonian creates a modified problem to be solved by quantum mechanical means. The updated problem, in turn, gives access to classical information of increased relevance and this interplay of quantum and classical elements then results in the algorithm's convergence.

The weight of classical and quantum mechanical components in the algorithm can be readily shifted to either side. An increasing number of available qubits gives access to broader spectra of the truncated problem Hamiltonians, which reduces the number of classical basis-updates before the shortest vector is found. The effort on the quantum mechanical side of the algorithm can be reduced if classical lattice reduction algorithms [4] are employed together with the basis updates.

While certainly beyond the capabilities of current quantum technologies, one can also envision a more coherent version of this algorithm, in which there is no classical readout during the algorithm, but a problem Hamiltonian conditioned on the

current state of the algorithm executed so far is being implemented.

The present algorithm also does not need to be understood as a stand-alone solution, but can also be combined with classical basis reduction algorithms [22,23]. Depending on the progress in the development of coherent quantum devices, it might be advisable to start with a classical basis reduction until a treatment with a device with limited qubit number becomes actually helpful; but if devices with large qubit numbers but insufficient coherence time to solve the full problem are available, one can also consider using the present algorithm as an initial step for further classical processing.

The multiple possibilities to expand the present algorithm in terms of classical or quantum mechanical components make this algorithm sufficiently versatile for applications also beyond the presently discussed lattice problems, such as the closest vector problem (CVP) [4] and learning with errors (LWE) [24].

While the scaling of the number of qubits required to represent the shortest vector is already rigorously bounded [11], very little is known about the scaling of the computational time of quantum algorithms with increasing dimension of the underlying lattice. Since the problems that can be simulated by classical means are so much smaller than problems of interest in cryptography, extrapolation from classical simulations is not likely to provide a meaningful estimate. The reduction in qubit numbers, however, will allow us to explore quantum algorithms for high-dimensional lattice problems even if hardware to directly solve the full problem is not yet available. As such, the present or similar techniques [11] can also help to estimate the quantum complexity of lattice problems.

#### ACKNOWLEDGMENT

This work was supported, in part, by the Engineering and Physical Sciences Research Council (EPSRC) under Grant No. EP/S021043/1.

- 
- [1] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell *et al.*, Quantum supremacy using a programmable superconducting processor, *Nature (London)* **574**, 505 (2019).
  - [2] D. J. Bernstein, Introduction to post-quantum cryptography, in *Post-Quantum Cryptography*, edited by D. J. Bernstein, J. Buchmann, and E. Dahmen (Springer, Berlin, Heidelberg, 2009), pp. 1–14.
  - [3] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM* **26**, 96 (1983).
  - [4] *The LLL Algorithm: Survey and Applications*, edited by P. Q. Nguyen and B. Vallée, (Springer, New York, 2010).
  - [5] D. Joseph, A. Callison, C. Ling, and F. Mintert, Two quantum Ising algorithms for the shortest-vector problem, *Phys. Rev. A* **103**, 032433 (2021).
  - [6] D. Aharonov, W. Van Dam, J. Kempe, Z. Landau, S. Lloyd, and O. Regev, Adiabatic quantum computation is equivalent to standard quantum computation, *SIAM Rev.* **37** (2004).
  - [7] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, Quantum computation by adiabatic evolution, [arXiv:quant-ph/0001106](https://arxiv.org/abs/quant-ph/0001106).
  - [8] A. Peruzzo, J. McClean, P. Shadbolt, M.-H. Yung, X.-Q. Zhou, P. J. Love, A. Aspuru-Guzik, and J. L. O’Brien, A variational eigenvalue solver on a photonic quantum processor, *Nat. Commun.* **5**, 4213 (2014).
  - [9] J. R. McClean, J. Romero, R. Babbush, and A. Aspuru-Guzik, The theory of variational hybrid quantum-classical algorithms, *New J. Phys.* **18**, 023023 (2016).
  - [10] D. Wecker, M. B. Hastings, and M. Troyer, Progress towards practical quantum variational algorithms, *Phys. Rev. A* **92**, 042303 (2015).
  - [11] M. R. Albrecht, M. Prokop, Y. Shen, and P. Wallden, Variational quantum solutions to the shortest vector problem, *IACR Cryptol. ePrint Arch.* **2022**, 233 (2022).
  - [12] E. Farhi, J. Goldstone, and S. Gutmann, A quantum approximate optimization algorithm, [arXiv:1411.4028](https://arxiv.org/abs/1411.4028).
  - [13] D. Joseph, A. J. Martinez, C. Ling, and F. Mintert, Quantum mean-value approximator for hard integer-value problems, *Phys. Rev. A* **105**, 052419 (2022).
  - [14] Apart from the case of one-dimensional lattices. There are only two one-dimensional unimodular matrices (+1 and -1), so each one-dimensional lattice can only be represented by two bases.
  - [15] D. Joseph, A. Ghionis, C. Ling, and F. Mintert, Not-so-adiabatic quantum computation for the shortest vector problem, *Phys. Rev. Res.* **2**, 013361 (2020).
  - [16] E. Farhi, D. Gamarnik, and S. Gutmann, The quantum approximate optimization algorithm needs to see the whole graph: A typical case, [arXiv:2004.09002](https://arxiv.org/abs/2004.09002).
  - [17] L. Bittel and M. Kliesch, Training Variational Quantum Algorithms is NP-Hard, *Phys. Rev. Lett.* **127**, 120502 (2021).
  - [18] J. Preskill, Quantum computing in the nisq era and beyond, *Quantum* **2**, 79 (2018).
  - [19] K. Bharti, A. Cervera-Lierta, T. Kyaw, T. Haug, S. Alperin-Lea, A. Anand, M. Degroote, H. Heimonen, J. S. Kottmann, T. Menke *et al.*, Noisy intermediate-scale quantum algorithms, *Rev. Mod. Phys.* **94**, 015004 (2022).
  - [20] E. Farhi, J. Goldstone, and S. Gutmann, A quantum approximate optimization algorithm applied to a bounded occurrence constraint problem [arXiv:1412.6062](https://arxiv.org/abs/1412.6062).
  - [21] E. Farhi and A. W. Harrow, Quantum supremacy through the quantum approximate optimization algorithm, [arXiv:1602.07674](https://arxiv.org/abs/1602.07674).
  - [22] A. K. Lenstra, Jr., H. Lenstra, and L. László, Factoring polynomials with rational coefficients, *Math. Ann.* **261**, 515 (1982).
  - [23] C. Schnorr, A hierarchy of polynomial time lattice basis reduction algorithms, *Theor. Comput. Sci.* **53**, 201 (1987).
  - [24] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, *J. ACM* **56**, 1 (2009).