

Noise-tolerant Grover's algorithm via success-probability prediction

Jian Leng,¹ Fan Yang,¹ and Xiang-Bin Wang^{1,2,3,4,*}¹State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China²Jinan Institute of Quantum Technology and Jinan branch, Hefei National Laboratory, Jinan, Shandong 250101, China³International Quantum Academy, Shenzhen 518048, China⁴Frontier Science Center for Quantum Information, Beijing 100193, China

(Received 5 October 2023; revised 4 December 2023; accepted 25 December 2024; published 21 January 2025)

We present theoretical and experimental studies on efficient quantum search with noise. We propose a noise-tolerant method that significantly reduces the running time and exponentially improves the error threshold with number of qubits for Grover's search. Experiments are implemented on different quantum computing setups, with all results clearly confirming the advantage of our noise-tolerant method to the original Grover's search. In one setup, our method produces quantum advantages while the original Grover's search does not. In another setup with smaller noise, our method produces a larger quantum advantage than the original Grover's search does.

DOI: [10.1103/PhysRevResearch.7.L012017](https://doi.org/10.1103/PhysRevResearch.7.L012017)

Introduction. Quantum advantage is the heart of quantum computing. Among all existing quantum computing algorithms with quantum advantage [1–4], Grover's search [3] is the only one that has a mathematically proven advantage to classical computing. It has extensive potential applications in many important problems, such as machine learning [5,6], networks [7,8], cryptanalysis [9,10], cryptography [11,12], and so on. In practice, coherently implementing Grover's search is technically difficult since it is sensitive to noise [13–18]. There are lots of excellent studies on reducing noise effects, such as improving the performance of quantum devices [19–29], designing quantum error correction code or quantum error mitigation [30–33], and so on. Recently, better-than-classical results of Grover's search have been experimentally achieved in several-qubits systems [34–38]. However, it is still challenging to coherently implementing Grover's search in a scalable system since the noise effect becomes much more severe with qubit number rise. Noise is still the most serious barrier against the applications of Grover's search. Here we show an approach to overcome this barrier by improving the robustness of Grover's search to tolerate much more severe noise, which is compatible with all existing methods for reducing noise effects [19–27,30–33]. We name it the noise-tolerant method for Grover's search. The key point is to predict the success probability before implementing the Grover circuit. Our method significantly reduces the running time and exponentially improves the error threshold with qubit number rise for Grover's search. Experiments

are implemented on different quantum computing setups with all results strongly confirming the prediction and advantage of our noise-tolerant method. In one setup, our method produces quantum advantages while the original Grover's search does not. In another setup with smaller gate noise, our method produces a larger quantum advantage than the original Grover's search does.

Grover's search under noise. Suppose a search problem has M solutions in total $N = 2^n$ elements. Grover's search [3] begins with the initial state $|\psi_i\rangle = \sum_{x=0}^{N-1} |x\rangle/\sqrt{N}$. Using $|x'\rangle$ to denote a target state and $\{|x''\rangle\}$ to denote other states, we rewrite $|\psi_i\rangle$ in a two-dimensional space [39] $|\psi_i\rangle = \cos\frac{\theta}{2}|R\rangle + \sin\frac{\theta}{2}|T\rangle := \begin{pmatrix} \cos(\theta/2) \\ \sin(\theta/2) \end{pmatrix}$, where $|R\rangle = \frac{1}{\sqrt{N-M}} \sum_{x''} |x''\rangle$, $|T\rangle = \frac{1}{\sqrt{M}} \sum_{x'} |x'\rangle$, and $\sin(\theta/2) = \sqrt{M/N}$. Grover iterate operator S_g can also be written in this two-dimensional subspace [40] $S_g = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. After applying S_g for k iterations, we get the final state

$$|\psi_f\rangle = S_g^k |\psi_0\rangle \\ = \cos[(2k+1)\theta/2]|R\rangle + \sin[(2k+1)\theta/2]|T\rangle.$$

Measuring $|\psi_f\rangle$ we obtain a correct solution with success probability $s = \sin^2[(2k+1)\theta/2]$. The scale of running time is $r = k/s$. Grover's search takes

$$k = k_g = \left\lceil \frac{\pi}{2\theta} - \frac{1}{2} \right\rceil, \quad (1)$$

which gives the optimal success probability for the noiseless case. The above procedure can be illustrated on the Bloch sphere as shown in Fig. 1(a). In a noisy environment, the Bloch sphere is contracted by noise [39]. As shown in Fig. 1(b), the state goes towards the original point step by step because of accumulation of noise effects. Since Grover's search is sensitive to noise [13–18], the final state $|\psi_f\rangle$ is close to the original point at the center of Bloch sphere and

*Contact author: xbwang@mail.tsinghua.edu.cn

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

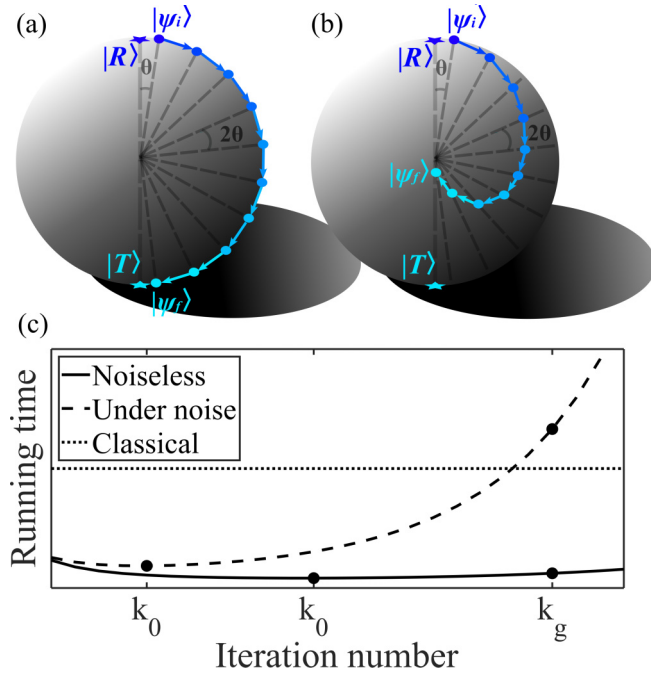


FIG. 1. (a) Grover's search on the Bloch sphere in a noiseless environment. The initial state $|\psi_i\rangle$ is close to the nonsolution state $|R\rangle$. In each iteration, the Grover iteration operator rotates the state by angle 2θ . After $[k_g]$ iterations, we obtain the final state $|\psi_f\rangle$, which is close to the solution state $|T\rangle$. (b) Grover's search in a noisy environment. Since the Bloch sphere is contracted by noise, the state goes not only towards $|T\rangle$, but also towards the original point at the center of the Bloch sphere. (c) The scale of running time changes with iteration number under noiseless and noisy environments. The original Grover's search takes $k = k_g$ and our noise-tolerant method for Grover's search takes $k = k_0 < k_g$. Since the running times of Grover's algorithm are different in noiseless and noisy environment, our method takes different values of k_0 in noiseless and noisy cases.

hence it may lose lots of information for the computing task. In Fig. 1(c), we illustrate the scale of running time r with iteration number k . In a noiseless environment, Grover's search has a quadratic speed advantage compared to classical search. But this quantum computational advantage is weakened or even disappears in a noisy environment, where the performance of Grover's search can be even worse than classical search.

Surely, how to improve the robustness of Grover's search is a very important topic. Inspired by Figs. 1(b) and 1(c), we can apply an iteration number $k_0 \leq k_g$ to reduce the accumulation of noise effects. The main idea of this work is to seek the optimized iteration number k_0 for Grover's search to obtain the optimized performance in a noisy environment. We call this the noise-tolerant method.

Noise-tolerant method for Grover's search. Experimentally, any quantum circuit has to be decomposed into elementary gates that can be realized by quantum devices. We denote the set of elementary gates as $\{G\}$. For example, it can be a universal gates set [41],

$$\{H^1, H^2, \dots, S^1, S^2, \dots, T^1, T^2, \dots, \text{CNOT}^{1,2}, \text{CNOT}^{2,3}, \dots\},$$

where the superscript $\{1, 2, 3, \dots\}$ denotes the index of a qubit. By applying $\{G\}$ we decompose the Grover iteration

operator as $S_g = \dots G''G'G$. Suppose that in the decomposition of S_g each gate G is applied c_G times. However, instead of an ideal gate G , we can only implement a noisy channel $\mathcal{G}$ in practice. *Average fidelity* (or simply, *fidelity*) F_G represents how close an ideal gate G is to a noisy channel $\mathcal{G}$. *Error rate* is defined as $E_G = 1 - F_G$. The fidelity or error rate is a known value for every gate in $\{G\}$ from experiments. In the first part of the Appendix we show that with k iterations the success probability of Grover's search is

$$s(k) \approx \text{SPAM} \times \left[\frac{M}{N} + \left(\sin^2 \frac{(2k+1)\theta}{2} - \frac{M}{N} \right) \times \left(\prod_{G' \in \{G\}} (1 - E_{G'})^{c_{G'}} \right)^k \right], \quad (2)$$

where SPAM is the fidelity of state preparation and measurement. The success probability is predicted before we implement Grover's search. The scale of running time is $r(k) = k/s(k)$. Minimizing $r(k)$, we obtain the optimized iteration number k_0 ,

$$\min_k r(k) = r(k_0). \quad (3)$$

This is the main result of our noise-tolerant method for Grover's search. Our method does not require the noise model, for which the detection method is complicated, but only uses the fidelity or error rate of a quantum gate as the input of Eq. (2). The fidelity or error rate of a quantum gate is basic information available within every quantum computing system. Moreover, our method does not need the exact value of fidelity or error rate of a quantum gate. Even if we only have crude information of fidelity or error rate, our method can still work with an advantageous result, though it is not the optimal result of the method. Applying Eq. (2), we show the performance of Grover's search and our method below.

To quantitatively study the performance, we suppose that (1) the error rate of a single-qubit gate is negligible compared with that of a two-qubit gate; (2) the error rate is the same for every two-qubit gate in $\{G\}$ and is denoted as E_{two} ; (3) $\text{SPAM} = 1$ and $M = 1$. In the decomposition of S_g , we apply two-qubit gates a total of c_{two} times. Equation (2) changes to

$$s(k) \approx \frac{1}{N} + \left(\sin^2 \frac{(2k+1)\theta}{2} - \frac{1}{N} \right) (1 - E_{\text{two}})^{k c_{\text{two}}}. \quad (4)$$

The scale of running time is $r(k) = k/s(k)$. Grover's search takes $k = k_g$ in Eq. (1) and its running time is $r_g = r(k_g)$. Our noise-tolerant method minimizes $r(k)$ to obtain $k = k_0$ and its running time is $r_0 = r(k_0)$. The running time of a classical search is $r_c = (N+1)/2$. Taking $c_{\text{two}} = 16n^2 - 4n + 2$ (this value comes from the circuit in Fig. 3 for numerical simulation), we compare r_c , r_g , and r_0 in Figs. 2(a) and 2(b). *Error threshold* is an error rate such that the scale of the running time of a classical search is the same as that of the quantum search. We obtain the quantum computational advantage when the error rate of the quantum gate is lower than the error threshold. We solve equations $r_g = r_c$ and $r_0 = r_c$ to obtain

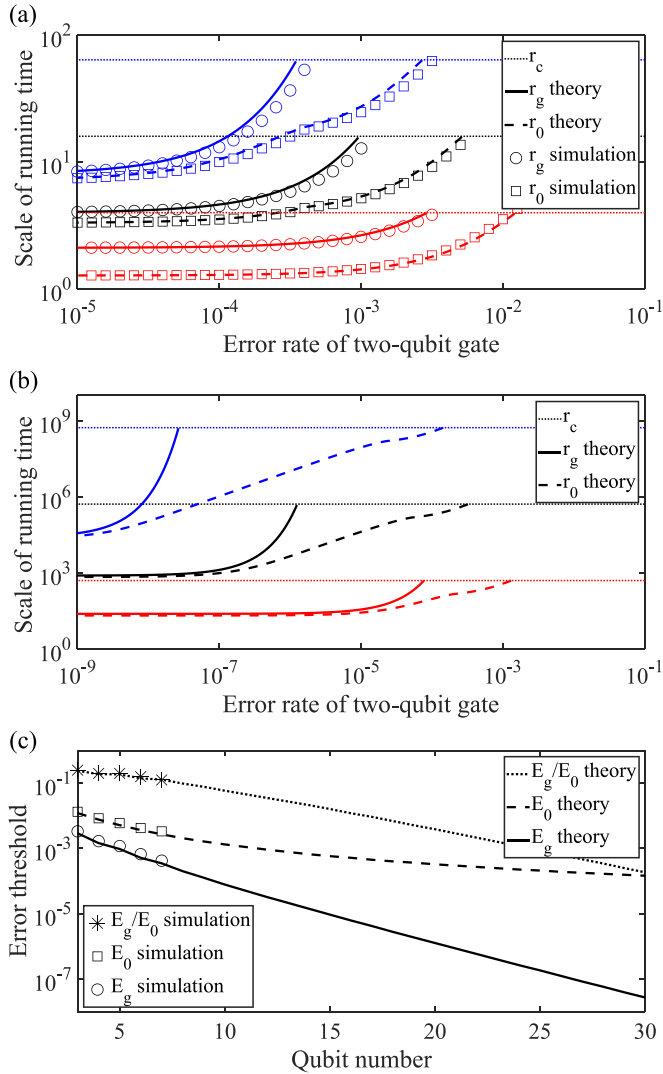


FIG. 2. Performance of theoretical analysis by Eq. (4) and numerical simulation using the circuit of Fig. 3 in exponential coordinates. The comparison between them shows that our Eq. (4) is in agreement with accurate numerical results very well. (a) The scale of running time lengths of classical search, r_c , Grover's search, r_g , and our noise-tolerant method, r_0 . Theoretical curves by Eq. (4): red, $n = 3$; black, $n = 5$; blue, $n = 7$. Numerical simulation: red, $n = 3$, dephasing noise; black, $n = 5$, depolarizing noise; blue, $n = 7$, damping noise. (b) The scale of running time lengths for large numbers of qubits. Red, $n = 10$; black, $n = 20$; blue, $n = 30$. (c) Error thresholds of Grover's search, E_g , and of our noise-tolerant method, E_0 , and their ratio E_g/E_0 .

error thresholds of Grover's search, E_g , and of our method E_0 , respectively. We plot E_g , E_0 , and E_g/E_0 in Fig. 2(c). It shows that E_g exponentially decays with qubit number while E_0 does not. The ratio E_0/E_g (E_g/E_0) exponentially increases (decays) with qubit number rise. Given the data above, we have the following conclusion.

Conclusion. Only using the fidelities or error rates of the quantum gates, our noise-tolerant method predicts the success probability and the scale of running time before implementing the Grover circuit [Eq. (2)]. Our method considerably reduces the running time for Grover's search [Fig. 2(a)] and this

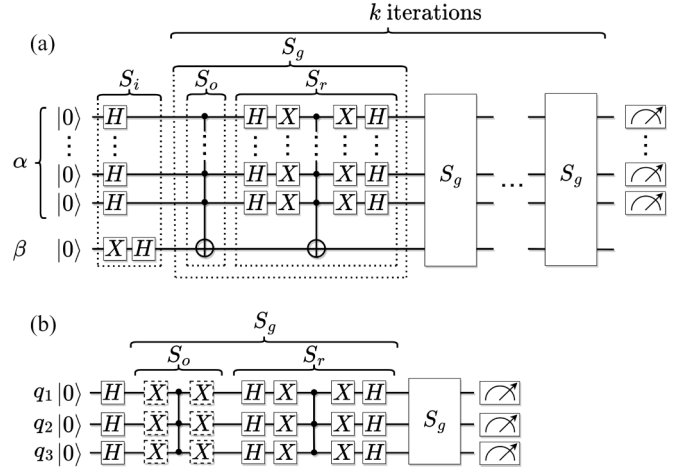


FIG. 3. (a) The circuit of quantum searching, for numerical simulation. The register α consists of n qubits and the ancilla β consists of one qubit. Applying the operator S_i we get the initial state $|\psi_i\rangle$. The Grover iteration operator S_g is constructed by oracle operator S_o and reflection operator S_r . We use the results in Ref. [42] to decompose the $(n + 1)$ -qubit Toffoli gate with $8n^2 - 2n + 1$ CNOT gates. Applying S_g for k iterations we obtain the final state $|\psi_f\rangle$. Measuring $|\psi_f\rangle$ we obtain the success probability $s(k)$. (b) The three-qubit circuit of quantum searching, for experiments. We apply the Grover iteration operator one or two times and measure the final state. We use the results in Refs. [36,43] to decompose the three-qubit controlled-Z gate. By applying or not applying X gates in the oracle operator S_o , we can control the target state to be $\{|000\rangle, |001\rangle, \dots, |111\rangle\}$.

running-time advantage increases with rise of qubit number [Fig. 2(b)]. Moreover, our method exponentially improves the error threshold of Grover's search with qubit number rise [Fig. 2(c)].

To verify our Conclusion, we use a density matrix to numerically simulate Grover's search and our noise-tolerant method under dephasing, depolarizing, and damping noise on a classical computer. The quantum circuit is shown in Fig. 3(a) and the detail for the noise model is given in the second part of the Appendix. Taking $k = k_g$ we obtain the success probability s_g and the scale of running time $r_g = k_g/s_g$ for Grover's search. Taking $k = k_0$ we obtain the success probability s_0 and running time $r_0 = k_0/s_0$ for our noise-tolerant method. The data points $r_g = r_c$ and $r_0 = r_c$ give the error threshold of Grover's search, E_g , and of our method, E_0 , respectively. Simulation results for running time and error threshold are shown in Figs. 2(a) and 2(c). They support our Conclusion.

Note that we have taken specific noise models (dephasing, depolarizing, and damping) as examples to test the correctness of our theoretical results (2) and (3). Surely, our method does not need any information of the noise model in performing quantum computing and of course is not limited by those specific noise models, since Eqs. (2) and (3) do not need any input of the noise model.

Experiments. The experiments were implemented on different quantum computing setups with superconducting processors to verify the prediction and advantage of our noise-tolerant method for Grover's search. In the experiments, a

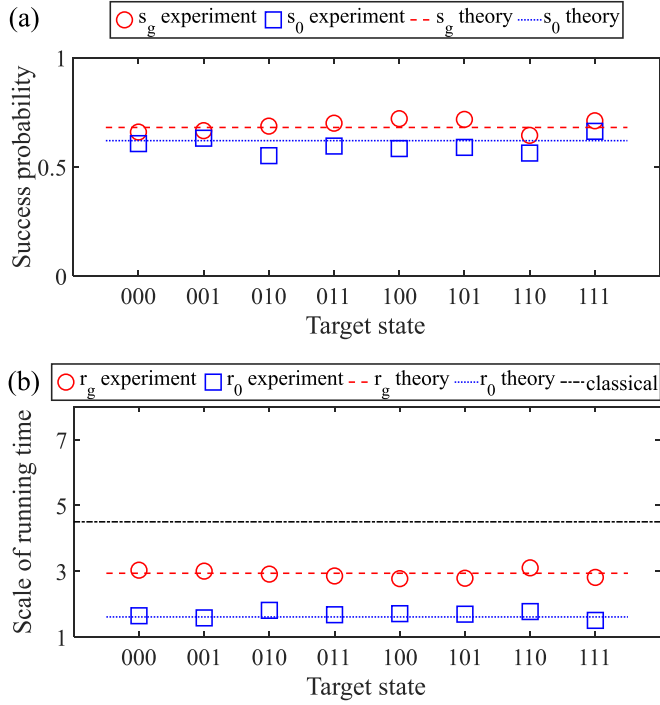


FIG. 4. Experimental results obtained by the VIP service of the superconducting quantum processor of the CCEQ laboratory [26], and theoretically predicted results obtained from Eq. (5). (a) The success probabilities of Grover's search, s_g , and of our noise-tolerant method, s_0 . (b) The scale of running time lengths of Grover's search, r_g , and of our noise-tolerant method, r_0 . The running time of classical search is 4.5. We change the target state from $|000\rangle$ to $|111\rangle$. Each experimental data point is sampled 2×10^4 times.

three-qubit quantum circuit was used, as shown in Fig. 3(b). One experiment was implemented by the VIP service in the laboratory at the CAS Center for Excellence in Quantum Information and Quantum Physics (CCEQ). The information of fidelity is three-bit SPAM, 0.877; single-qubit gate, 0.999; CZ_{1,2}, 0.998; CZ_{2,3}, 0.995. Applying Eq. (2), we obtain

$$\begin{aligned} s(1) &= 0.620, & s(2) &= 0.681, \\ r(1) &= 1.613, & r(2) &= 2.939, \end{aligned} \quad (5)$$

where $s(k)$ and $r(k)$ are the success probability and scale of running time with k iterations predicted by our method. Since $r(1) < r(2)$, we take $k_0 = 1$ for our noise-tolerant method. According to Eq. (1), Grover's search takes $k_g = 2$. Then we compiled our code for both the original Grover's search ($k = 2$) and our noise-tolerant method ($k = 1$) with all possible targets $\{|000\rangle, |001\rangle, \dots, |111\rangle\}$. The code was run in the superconducting quantum processor of the CCEQ laboratory and the experimental output data are shown in Fig. 4. The experimental results have clearly shown the advantage of our noise-tolerant method over that of the original Grover's search. Here the original Grover's search still has a limited quantum advantage to classical computing because the noise of setup in use is too small. As one can see, our noise-tolerant method produces a much better result in the same setup. As shown in Fig. 5, the results of another experiment with a larger

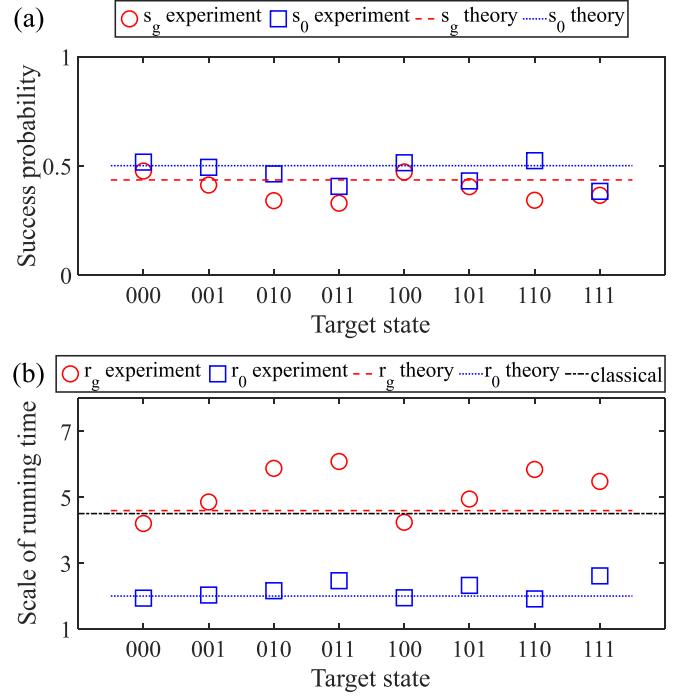


FIG. 5. Experimental results obtained by the standard online service of the superconducting quantum processor of Quafu [27], and theoretically predicted results obtained from Eq. (6). All features are the same as in Fig. 4, but each experimental data point is sampled 10^5 times.

noise, our method produces the quantum advantage while the original Grover's search does not.

The experiment of Fig. 5 was implemented on a superconducting processor through the standard online service of Quafu [44]. The information of fidelity is three-bit SPAM, 0.898; single-qubit gate, 0.997; CZ_{1,2}, 0.984; CZ_{2,3}, 0.986. Similarly to Eq. (5), we calculated the success probability and scale of running time with k iterations predicted by our method:

$$\begin{aligned} s(1) &= 0.501, & s(2) &= 0.436, \\ r(1) &= 1.997, & r(2) &= 4.592. \end{aligned} \quad (6)$$

So our method takes $k_0 = 1$. Grover's search still takes $k_g = 2$. Then we compiled our code of both the original Grover's search ($k = 2$) and our noise-tolerant method ($k = 1$) with all possible targets and sent it to Quafu. We received the experimental output data from Quafu, as shown in Fig. 5. The experimental results not only confirm the theoretical prediction of our noise-tolerant method, but also confirm a powerful improvement in large-noise environment: Our noise-tolerant method can improve Grover's search to realize a quantum computational advantage beyond the classical search for all target states, while no quantum advantage is found without applying our method.

Discussion. We present a noise-tolerant method for Grover's search which significantly reduces the running time and exponentially improves the error threshold with rising qubit amount. Experiments of different searching methods are implemented on different quantum computing setups and

the experimental results have verified the prediction and advantage of our noise-tolerant method. Our method is also compatible with all existing methods for reducing noise effects. Given such advantages in running time, error threshold, and compatibility, our method paves the way for practical applications of Grover's search.

Our method is compatible with all existing methods for reducing noise effects [19,21–27,30–33]. For instance, we can use quantum error correction (QEC) to reduce the noise in future. For both Grover's search and our method, the error rates of logical gates have to be reduced smaller than E_g and E_0 , respectively. QEC codes require $\text{poly}(\log(1/E_g))$ and $\text{poly}(\log(1/E_0))$ numbers of physical gates [39]. From Fig. 2 or Conclusion, we see that E_g exponentially decays with qubit number n while E_0 does not. So the costs of QEC are $\text{poly}(n)$ and $\text{poly}(\log n)$. This means that our method also exponentially reduces the cost of QEC for Grover's search. Given such advantages in running time, error threshold, and compatibility, our method paves the way for practical applications of Grover's search.

Acknowledgments. We thank the laboratory in the CAS Center for Excellence in Quantum Information and Quantum Physics and the Quafu platform for providing us quantum computing services for our experiments. We acknowledge the financial support in part by the National Natural Science Foundation of China, Grants No. 11974204 and No. 12174215, and the Innovation Program for Quantum Science and Technology, Grant No. 2021ZD0300705. This study is also supported by the Taishan Scholars Program.

Appendix: Success-probability prediction for Grover's algorithm. We apply the quantum gate G to a general input state $|\psi_0\rangle$ and obtain the ideal output state $|\psi\rangle = G|\psi_0\rangle$. In the noisy channel, the practical output state is $\mathcal{G}(\psi_0)$. It can always be formulated as

$$\mathcal{G}(\psi_0) = a|\psi\rangle\langle\psi| + (1-a)\rho_\perp,$$

where $\rho_\perp$ satisfies $\langle\psi|\rho_\perp|\psi\rangle = 0$. This means the realistic gate $\mathcal{G}$ presents the ideal output state with probability a . We make the following approximation:

$$\begin{aligned} a &= \langle\psi|\mathcal{G}(\psi_0)|\psi\rangle = \langle\psi_0|G^\dagger\mathcal{G}(\psi_0)G|\psi_0\rangle \\ &\approx \int d\psi_0 \langle\psi_0|G^\dagger\mathcal{G}(\psi_0)G|\psi_0\rangle, \end{aligned}$$

where the integral is over the Haar measure on state space. The integral at the right side of the equation is exactly

the definition of *average fidelity* F_G for quantum gate G . So we have $a = F_G$ and we obtain the ideal output state with the probability F_G . Suppose the Grover iteration operator S_g is decomposed by an elementary gates set $\{G\}$ and each gate G is applied c_g times. We have the probability $\prod_{G \in \{G\}} F_G^{c_g}$ to get the ideal output state. Applying S_g for k iterations, this probability becomes $(\prod_{G \in \{G\}} F_G^{c_g})^k$. So the success probability of Grover's algorithm with k iterations is

$$\begin{aligned} s(k) &\approx \text{probability of getting ideal output state} \\ &\quad \times \text{success probability of measurement results} \\ &\quad + \text{probability of getting nonideal output state} \\ &\quad \times \text{success probability of random sampling} \\ &\approx \left(\prod_{G \in \{G\}} F_G^{c_g} \right)^k \sin^2 \left(\frac{(2k+1)\theta}{2} \right) \\ &\quad + \left(1 - \left(\prod_{G \in \{G\}} F_G^{c_g} \right)^k \right) \frac{M}{N} \\ &= \frac{M}{N} + \left(\sin^2 \frac{(2k+1)\theta}{2} - \frac{M}{N} \right) \left(\prod_{G \in \{G\}} (1 - E_G)^{c_g} \right)^k, \end{aligned}$$

where the error rate is defined as $E_G = 1 - F_G$.

Noise model in numerical simulation. In the numerical simulation, we have applied damping, dephasing, and depolarizing noises [39,45]. Suppose G_a is a single-qubit gate applied on qubit a . The corresponding noisy channel is defined as $\mathcal{G}_a(\rho_a) = \mathcal{E}(G_a \rho_a G_a^\dagger)$, where $\mathcal{E}(\rho_a) = \sum_i E_i \rho_a E_i^\dagger$. We have

$$\text{Damping: } E_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\epsilon} \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & \sqrt{\epsilon} \\ 0 & 0 \end{pmatrix}.$$

$$\text{Dephasing: } E_1 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-\epsilon} \end{pmatrix}, \quad E_2 = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{\epsilon} \end{pmatrix}.$$

$$\text{Depolarizing: } E_1 = \sqrt{1-\epsilon} I, \quad E_2 = \sqrt{\frac{\epsilon}{3}} X,$$

$$E_3 = \sqrt{\frac{\epsilon}{3}} Y, \quad E_4 = \sqrt{\frac{\epsilon}{3}} Z.$$

For two-qubit gate G_{ab} applied on qubits a and b , the corresponding noisy channel is $\mathcal{G}_{ab}(\rho_{ab}) = \mathcal{E} \otimes \mathcal{E}(G_{ab} \rho_{ab} G_{ab}^\dagger)$. The fidelity F_G of the single-qubit gate is $\text{Tr}(\mathcal{G}_a(\rho_a)\rho_a)$ and of the two-qubit gate is $\text{Tr}(\mathcal{G}_{ab}(\rho_{ab})\rho_{ab})$.

-
- [1] D. Deutsch and R. Jozsa, Rapid solution of problems by quantum computation, *Proc. R. Soc. A* **439**, 553 (1992).
 - [2] P. W. Shor, Algorithms for quantum computation: Discrete logarithms and factoring, in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 1994), pp. 124–134.
 - [3] L. K. Grover, A fast quantum mechanical algorithm for database search, in *Proceedings of the Twenty-Eighth Annual*

ACM Symposium on Theory of Computing (ACM, New York, 1996), pp. 212–219.

- [4] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing* (ACM, New York, 2011), pp. 333–342.
- [5] D. Anguita, S. Ridella, F. Riveccio, and R. Zunino, Quantum optimization for training support vector machines, *Neural Netw.* **16**, 763 (2003).

- [6] G. Anikeeva, O. Marković, V. Borish, J. A. Hines, S. V. Rajagopal, E. S. Cooper, A. Periwal, A. Safavi-Naeini, E. J. Davis, and M. Schleier-Smith, Number partitioning with Grover's algorithm in central spin systems, *PRX Quantum* **2**, 020319 (2021).
- [7] Y. Bejerano, S.-J. Han, and A. Kumar, Efficient load-balancing routing for wireless mesh networks, *Comput. Netw.* **51**, 2450 (2007).
- [8] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, Quantum search algorithms for wireless communications, *IEEE Commun. Surv. Tutor.* **21**, 1209 (2018).
- [9] G. Brassard, P. Hoyer, and A. Tapp, in *Quantum cryptanalysis of hash and claw-free functions, LATIN'98: Theoretical Informatics*, Lecture Notes in Computer Science (Springer, Berlin, Heidelberg, 1998), Vol. 1380, pp. 163–169.
- [10] S. Ramos-Calderer, E. Bellini, J. I. Latorre, M. Manzano, and V. Mateu, Quantum search for scaled hash function preimages, *Quantum Inf. Process.* **20**, 180 (2021).
- [11] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, Applying Grover's algorithm to AES: Quantum resource estimates, in *International Workshop on Post-Quantum Cryptography* (Springer, Berlin, 2016), pp. 29–43.
- [12] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, Implementing Grover oracles for quantum key search on AES and LowMC, in *Advances in Cryptology—EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II (Springer, Berlin, 2020), pp. 280–310.
- [13] B. Pablo-Norman and M. Ruiz-Altaba, Robustness of the quantum search algorithm, in *The Eighth Mexican School on Particles and Fields, 20–28 November 1998, Oaxaca de Juarez, Mexico, AIP Conference Proceedings* (AIP, New York, 1999), Vol. 490, pp. 405–408.
- [14] D. Shapira, S. Mozes, and O. Biham, Effect of unitary noise on Grover's quantum search algorithm, *Phys. Rev. A* **67**, 042301 (2003).
- [15] N. Shenvi, K. R. Brown, and K. B. Whaley, Effects of a random noisy oracle on search algorithm complexity, *Phys. Rev. A* **68**, 052313 (2003).
- [16] P. J. Salas, Noise effect on Grover algorithm, *Eur. Phys. J. D* **46**, 365 (2008).
- [17] I. Cohn, A. L. F. De Oliveira, E. Buksman, and J. G. L. De Lacalle, Grover's search with local and total depolarizing channel errors: Complexity analysis, *Int. J. Quantum Inf.* **14**, 1650009 (2016).
- [18] D. Reitzner and M. Hillery, Grover search under localized dephasing, *Phys. Rev. A* **99**, 012339 (2019).
- [19] 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).
- [20] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu *et al.*, Quantum computational advantage using photons, *Science* **370**, 1460 (2020).
- [21] Y. Wu, W.-S. Bao, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan *et al.*, Strong quantum computational advantage using a superconducting quantum processor, *Phys. Rev. Lett.* **127**, 180501 (2021).
- [22] H.-S. Zhong, Y.-H. Deng, J. Qin, H. Wang, M.-C. Chen, L.-C. Peng, Y.-H. Luo, D. Wu, S.-Q. Gong, H. Su *et al.*, Phase-programmable Gaussian boson sampling using stimulated squeezed light, *Phys. Rev. Lett.* **127**, 180502 (2021).
- [23] Y. Zhao, Y. Ye, H.-L. Huang, Y. Zhang, D. Wu, H. Guan, Q. Zhu, Z. Wei, T. He, S. Cao *et al.*, Realization of an error-correcting surface code with superconducting qubits, *Phys. Rev. Lett.* **129**, 030501 (2022).
- [24] R. Acharya, I. Aleiner, R. Allen, T. I. Andersen, M. Ansmann, F. Arute, K. Arya, A. Asfaw, J. Atalaya, R. Babbush *et al.*, Suppressing quantum errors by scaling a surface code logical qubit, *Nature (London)* **614**, 676 (2023).
- [25] Y. Kim, A. Eddins, S. Anand, K. X. Wei, E. Van Den Berg, S. Rosenblatt, H. Nayfeh, Y. Wu, M. Zaletel, K. Temme *et al.*, Evidence for the utility of quantum computing before fault tolerance, *Nature (London)* **618**, 500 (2023).
- [26] S. Cao, B. Wu, F. Chen, M. Gong, Y. Wu, Y. Ye, C. Zha, H. Qian, C. Ying, S. Guo *et al.*, Generation of genuine entanglement up to 51 superconducting qubits, *Nature (London)* **619**, 738 (2023).
- [27] P. Zhao, R. Wang, M.-J. Hu, T. Ma, P. Xu, Y. Jin, and H. Yu, Baseband control of superconducting qubits with shared microwave drives, *Phys. Rev. Appl.* **19**, 054050 (2023).
- [28] B. Pokharel and D. A. Lidar, Demonstration of algorithmic quantum speedup, *Phys. Rev. Lett.* **130**, 210602 (2023).
- [29] T. Roy, L. Jiang, and D. I. Schuster, Deterministic grover search with a restricted oracle, *Phys. Rev. Res.* **4**, L022013 (2022).
- [30] P. W. Shor, Fault-tolerant quantum computation, in *Proceedings of 37th Conference on Foundations of Computer Science* (IEEE, Piscataway, NJ, 1996), pp. 56–65.
- [31] D. Gottesman, Class of quantum error-correcting codes saturating the quantum hamming bound, *Phys. Rev. A* **54**, 1862 (1996).
- [32] D. Poulin, Stabilizer formalism for operator quantum error correction, *Phys. Rev. Lett.* **95**, 230504 (2005).
- [33] J. Preskill, Quantum computing in the NISQ era and beyond, *Quantum* **2**, 79 (2018).
- [34] T. Roy, S. Hazra, S. Kundu, M. Chand, M. P. Patankar, and R. Vijay, Programmable superconducting processor with native three-qubit gates, *Phys. Rev. Appl.* **14**, 014072 (2020).
- [35] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, and C. Monroe, Complete 3-qubit grover search on a programmable quantum computer, *Nat. Commun.* **8**, 1918 (2017).
- [36] K. Zhang, P. Rao, K. Yu, H. Lim, and V. Korepin, Implementation of efficient quantum search algorithms on NISQ computers, *Quantum Inf. Process.* **20**, 233 (2021).
- [37] K. Zhang, K. Yu, and V. Korepin, Quantum search on noisy intermediate-scale quantum devices, *Europhys. Lett.* **140**, 18002 (2022).
- [38] B. Pokharel and D. A. Lidar, Better-than-classical grover search via quantum error detection and suppression, *npj Quantum Inf.* **10**, 23 (2024).
- [39] M. A. Nielsen and I. Chuang, *Quantum Computation and Quantum Information* (AAPT, College Park, MD, 2002).
- [40] J. Leng, F. Yang, and X.-B. Wang, Improving D2p Grover's algorithm to reach performance upper bound under phase noise, *Phys. Rev. Res.* **5**, 023202 (2023).
- [41] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan, On universal and fault-tolerant quantum computing:

- A novel basis and a new constructive proof of universality for Shor's basis, in *40th Annual Symposium on Foundations of Computer Science* (IEEE, Piscataway, NJ, 1999), pp. 486–494.
- [42] J. Leng, F. Yang, and X.-B. Wang, Decomposing $(n + 1)$ -qubit Toffoli gate with shallow circuit depth and no ancilla, *Adv. Quantum Technol.* **7**, 2300370 (2024).
- [43] D. Maslov, Advantages of using relative-phase toffoli gates with an application to multiple control Toffoli optimization, *Phys. Rev. A* **93**, 022311 (2016).
- [44] <https://quafu.baqis.ac.cn>
- [45] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver, A quantum engineer's guide to superconducting qubits, *Appl. Phys. Rev.* **6**, 021318 (2019).