scientific reports

Check for updates

OPEN

Improved circuit implementation of the HHL algorithm and its simulations on QISKIT

Meng Zhang[1], Lihua Dong[1]✉, Yong Zeng[2] & Ning Cao[1]

In 2019, Yonghae Lee et al. combined the circuit implementation of the Harrow–Hassidim–Lloyd (HHL) algorithm with a classical computer, and designed a hybrid HHL algorithm to reduce experimental errors caused by decoherence and so on. However, the improvement is achieved only in the auxiliary quantum coding phase, and no quantum resource reduction is done on the quantum phase estimation and inverse quantum phase estimation stages. At the same time, the circuit improvement illustration on a 2 × 2 linear system just has the result and no specific process. In this paper, based on the idea of the hybrid HHL algorithm and a generic circuit of HHL algorithm, an improved circuit implementation of the HHL algorithm is proposed. The feasibility of the improved circuit implementation of the HHL algorithm is verified by IBM's qiskit. The improved circuit illustrations on a 4 × 4 linear system show that the improved circuit implementation of the HHL algorithm can effectively reduce quantum resources without losing the fidelity of the results. Thus the improved circuit implementation of the HHL algorithm can further avoid some result errors than the existing implementation methods.

Quantum computing is an operation method that follows the operating laws of quantum mechanics. Compared with traditional classical computing, quantum computing achieves an exponential speedup on some problems. For example, the Shor quantum algorithm[1] is famous for factoring large integers in polynomial time. Grover algorithm[2] achieves an exponential speedup in searching data. While the HHL algorithm[3] for solving linear systems of equations with exponential speedup over the best known classical algorithms.

However, during the operation of quantum circuits, due to the limitations of current technology, the errors of quantum gates, experimental errors and decoherence will introduce errors in the experimental process[4–6]. Therefore, it is necessary to reduce the number of gates and the overall running time of the algorithm. In view of this, the realization and improvement of quantum circuits has attracted the attention of various fields.

Among them, in terms of quantum circuit implementation and improvement of cryptographic algorithms, Langenberg et al. proposed the quantum circuit implementation and improvement of AES cryptographic algorithm[7], and many scholars have made further improvements on it[8,9].

In circuit synthesis of quantum algorithms, Monz et al. implemented the use of Shor's algorithm to factorize numbers 15[10] using 7 qubits and 4 cache qubits with efficient control. Diao et al. proposed the quantum circuit composition of Grover algorithm[11]. Markus Grassl successfully used the Grover algorithm to realize the exhaustive key search for AES[12]. The quantum circuit implementation and improvement of the HHL algorithm also attracted a lot of attention. Among them, by introducing the variable time amplitude amplification algorithm into the HHL algorithm, Ambainis et al. reduced the number of repeated runs required to obtain the correct answer, thereby reducing the running time of the algorithm[13], but did not give a specific quantum circuit implementation. Yudong Cao et al. proposed a generic circuit of HHL algorithm[14]. Yonghae Lee et al. gave a hybrid HHL quantum algorithm[6] by combining with classical computers, which effectively reduces the quantum gate resources used in the auxiliary qubit rotation part of the HHL algorithm. Compared with the generic circuit of HHL algorithm proposed by Cao et al., the hybrid HHL algorithm uses smaller quantum resources in the auxiliary qubit rotation stage. However, the improvement has only limited to the auxiliary quantum encoding stage, and no quantum resource can be reduced on the quantum phase estimation and inverse quantum phase estimation stages. Meanwhile, in the circuit improvement verification, there is only improvement result on a 2×2 linear system and no specific realization process is given.

In view of this, inspired by the idea of combining with classical computers and the generic circuit of HHL algorithm, we provide an improved circuit implementation of the HHL algorithm to further reducing the number of quantum gates, thus further avoiding some result errors caused by quantum gate errors. The experimental

[1]School of Communication Engineering, Xidian University, Xi'an 710071, China. [2]School of Network and Information Security, Xidian University, Xi'an 710071, China. ✉email: lih_dong@mail.xidian.edu.cn

results show that our improved circuit implementation of the HHL algorithm effectively reduces the consumption of quantum resources without losing the fidelity of the results.

Basic definitions.

- *k-fixed*[6]: Suppose $\lambda_j,\ j = 1, \ldots, l$, is all non-zero eigenvalues of the Hermitian matrix A, b_k^j is the kth bit of the binary representation of the eigenvalues λ_j, $j = 1, \ldots, l$, defined $\overline{m}_k$, $k \in N$, as follows

$$\overline{m}_k = \frac{1}{l}\left(\sum_{j=1}^{l} b_k^j\right) \tag{1}$$

  Hermitian matrix A is said to be *k-fixed* if it is $\overline{m}_k$ fixed at 0 or 1.
- *n-estimated*[6]: Denoted λ as the eigenvalue of the matrix, if it can be represented λ by no more than n binary number, it is called *n-estimated.*
- *fidelity f*[15]: In the experiment in this paper, fidelity can be understood as the inner product of two vectors:

$$f = (x_{theory}, x_{simulation}) \tag{2}$$

  where x_{theory} and $x_{simulation}$ are normalized values.

HHL algorithm.

The definition of general linear equations satisfies the following conditions:

$$A\overrightarrow{x} = \overrightarrow{b}$$

where **A** is m × n matrix:

The above mentioned is a system of linear equations in the classical algorithm, which is expressed in quantum computation as follows:

$$A|x\rangle = |b\rangle$$

where $|x\rangle$ and $|b\rangle$ are quantum states.

The HHL algorithm is used to solve quantum equations. However, when using HHL algorithm to solve the problem, some specific conditions still need to be met. Matrix **A** must be an $n \times n$ square matrix, and **A** must be a Hermitian operator. If not, **A** needs to be transformed into a Hermitian matrix in some way. The core idea of HHL algorithm includes phase estimation, controlled rotation and inverse phase estimation.

The general steps of the HHL algorithm are:

(1) First, initialize the quantum state $|b\rangle$.
(2) The quantum phase estimation method is used to decompose $|b\rangle$, into the superposition of the linear combination of eigenvectors of **A**.
(3) After inverting the matrix **A**, we get the quantum state $A^{-1}|x\rangle = |b\rangle$.
(4) Canceling the eigenvalues stored in the register by using the inverse quantum phase estimation method.

Quantum circuit implementation of HHL algorithm.

The quantum circuit implementation of the HHL algorithm requires the use of three quantum registers, denoted as *Ancilla*, *Reg.C* and *Reg.B*, where

- *Ancilla* is used to store auxiliary qubits;
- *Reg.C* is used to store the binary representation of the eigenvalues of the coefficient matrix A;
- *Reg.B* is used to store the vector solution of a system of linear equations when the measurement of the contents of the *Ancilla* quantum register is 1.
- Initially, all three quantum registers are set to $|0\rangle$ state.

As shown in Fig. 1, the quantum circuit implementation process of the HHL algorithm is mainly composed of three stages, namely: quantum phase estimation (Quantum Phase Estimation, QPE), auxiliary quantum encoding (Ancilla quantum encoding, AQE) and inverse quantum phase estimation (Inverse Quantum Phase Estimation, Inverse QPE) of which

(a) QPE, that is, Quantum Phase Estimation. In the HHL algorithm, if the quantum register is measured after the QPE stage, then the binary representation of the eigenvalues of the linear equation system will be obtained, denoted as $|\theta_0\theta_1 \ldots \theta_{n-1}\rangle$.

  Firstly, in the preparation phase, the first n qubits are initialized to 0, and the last m qubits are initialized to the quantum state $|u\rangle$, so the initial state of the register is $|0\rangle^{\otimes n}|u\rangle$, then apply the H gate to n qubits.

$$\begin{aligned}|\varphi_1\rangle &= \left(H^{\otimes n} \otimes I\right)|0\rangle^{\otimes n}|u\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x_0x_1\ldots x_{n-1} \in \{0,1\}^n} |x_0x_1 \ldots x_{n-1}\rangle|u\rangle, \quad x_i \in \{0, 1\}\end{aligned} \tag{3}$$

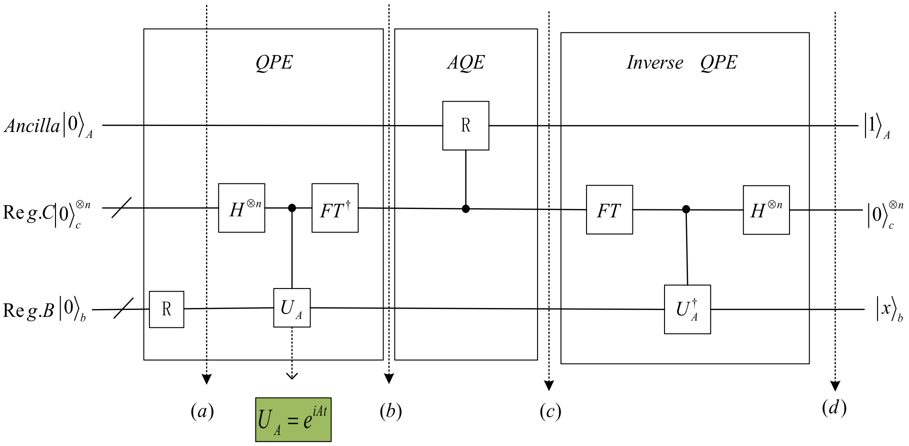


Figure 1. Circuit overview diagram of HHL algorithm.

Secondly, using n controlled U gates, add the phase $e^{2\pi i\theta}$ to the probability amplitude.

$$|\varphi_2\rangle = \frac{1}{2^{\frac{n}{2}}} \underbrace{|0\rangle + e^{2\pi i 2^{n-1}(0.\theta_0\theta_2,...,\theta_{n-1})}|1\rangle}_{1\text{st } qubit} \otimes ... \otimes \underbrace{|0\rangle + e^{2\pi i 2^{1}(0.\theta_0\theta_1,...,\theta_{n-1})}|1\rangle}_{n-1\text{st } qubit} \\ \otimes \underbrace{|0\rangle + e^{2\pi i 2^{0}(0.\theta_0\theta_1,...,\theta_{n-1})}|1\rangle}_{n\text{st } qubit} |u\rangle \tag{4}$$

Finally, the inverse QFT (quantum Fourier transform) is performed on the $|\varphi_2\rangle$ quantum state. This step extracts the target value θ from the probability amplitude to the ground state. For qubits $|x_k\rangle, k = 1, 2, \ldots n$.

$$|x_k\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{\theta_k} e^{\frac{1}{2}\pi i\theta_{k+1}} ... e^{\frac{1}{2^{n-1}}\pi i\theta_{n-1}}|1\rangle\right). \tag{5}$$

To extract θ_k into the quantum state, it is necessary to perform phase rotation on the qubit $|x_k\rangle$ before applying the H gate to the qubit $|x_k\rangle$, and the phase selection angle is $e^{\frac{1}{2}\pi i\theta_{k+1}} ... e^{\frac{1}{2^{n-1}}\pi i\theta_{n-1}}$.

$$H \otimes CU(e^{\frac{1}{2}\pi i\theta_{k+1}} ... e^{\frac{1}{2^{n-1}}\pi i\theta_{n-1}})|\theta_0\rangle|x_k\rangle = |\theta_0\rangle|\theta_k\rangle \tag{6}$$

Extract all $|\theta_0\theta_1...\theta_{n-1}\rangle$ into qubits to get the binary representation of the eigenvalues of the matrix

$$|\varphi_3\rangle = |\theta_0\theta_1...\theta_{n-1}\rangle|u\rangle \tag{7}$$

Measure the result to get $|\theta_0\theta_1...\theta_{n-1}\rangle$, which is the binary representation of the eigenvalues of the desired matrix.

In the entire HHL algorithm, the unitary operator $U = U_A = e^{iAt} = \sum_{j=0}^{N-1} e^{i\lambda_j t}|u_j\rangle\langle u_j|$, $|b\rangle = \sum_{j=0}^{N-1} b_j|u_j\rangle$, where t is a constant that can be set by itself. Therefore, in the entire HHL algorithm, the state of time, that is, the moment in Fig. 1 is (b):

$$|0\rangle_A \otimes \sum_{j=0}^{N-1} b_j|\lambda_j\rangle_{nl} \otimes |u_j\rangle \\ |u\rangle = \sum_{j=0}^{N-1} b_j|u_j\rangle, \quad |\lambda_j\rangle_{nl} = \frac{1}{\sqrt{2^n}}\sum_{i=0}^{n-1}|\theta_i\rangle \tag{8}$$

Here $|\lambda_j\rangle_{nl}$ is the n-bit binary representation of "λ_j".

(b) In the AQE stage, a controlled rotation operation on auxiliary qubits is performed as follows:

$$|0\rangle_A \otimes |\lambda_j\rangle_{nl} \rightarrow \left(\sqrt{1 - \frac{c^2}{\lambda_j^2}}|0\rangle_A + \frac{c}{\lambda_j}|1\rangle_A\right) \otimes |\lambda_j\rangle_{nl} \tag{9}$$

Here c is a normalizing constant.

After the AQE part, the state of the system at moment Fig. 1c is:

$$\sum_{j=0}^{N-1} b_j|\lambda_j\rangle_{nl}|u_j\rangle\left(\sqrt{1 - \frac{c^2}{\lambda_j^2}}|0\rangle_A + \frac{c}{\lambda_j}|1\rangle_A\right) \tag{10}$$

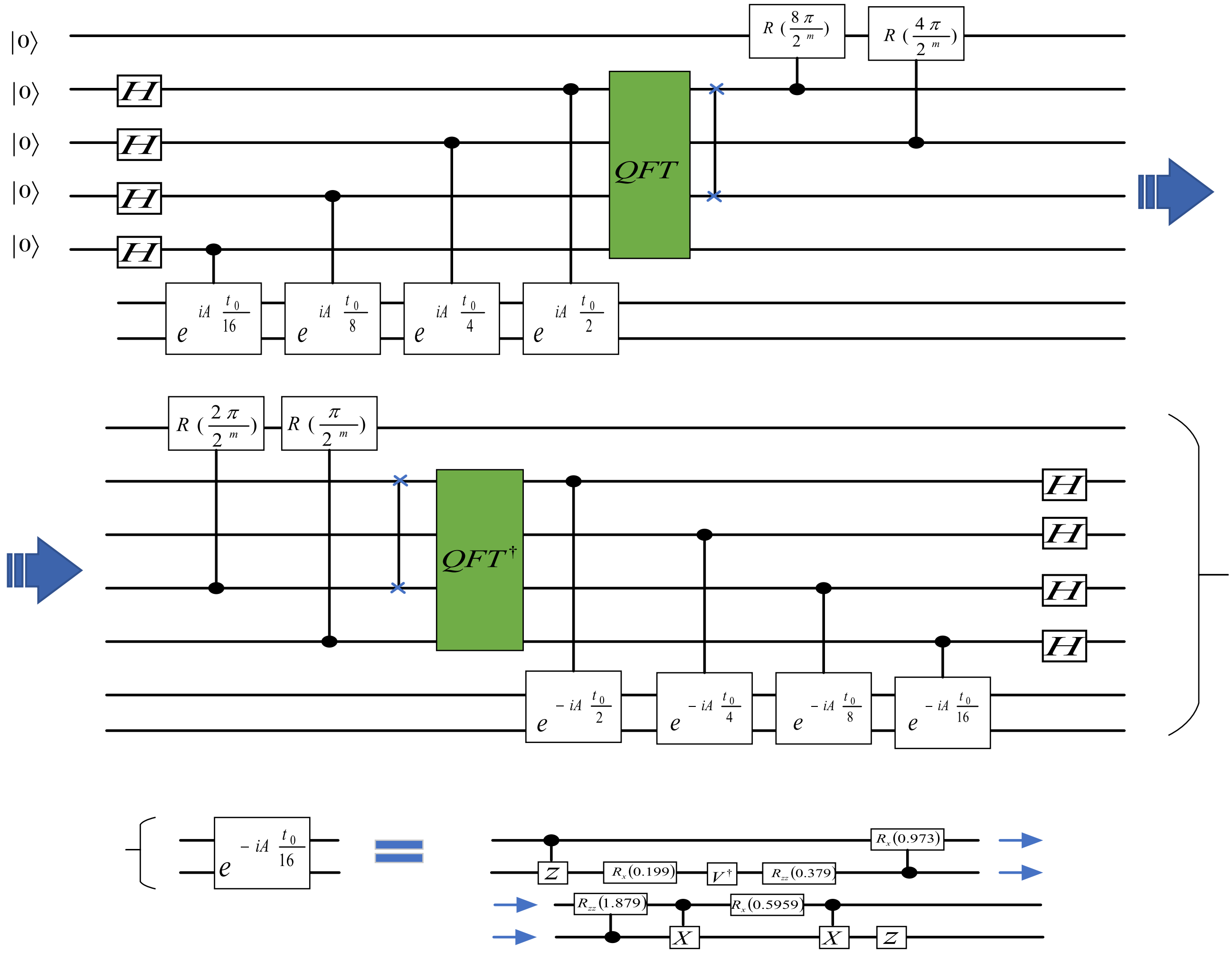


Figure 2. Generic circuit of HHL algorithm.

(c) Inverse QPE stage is the inverse operation of the QPE stage. After the Inverse QPE stage, the $|\lambda_j\rangle$ in the superposition state in the *Reg.C* register will become $|0\rangle$, at this time, the state of the entire quantum system is Fig. 1 (*d*):

$$\sum_{j=0}^{N-1} b_j |0\rangle_{nl} |u_j\rangle \left(\sqrt{1 - \frac{c^2}{\lambda_j^2}} |0\rangle_A + \frac{c}{\lambda_j} |1\rangle_A \right) \tag{11}$$

After the above three stages are completed, the status in the *Reg.C* register changes to the $|0\rangle^{\otimes n}$ state, and the auxiliary qubit is measured on the Z-axis. If the outcome is 1, the register is in the post-measurement state:

$$|x\rangle = \left(\sqrt{\frac{1}{\sum_{j=0}^{N-1} |b_j|^2 / |\lambda_j|^2}} \right) \sum_{j=0}^{N-1} \frac{b_j}{\lambda_j} |0\rangle_{nl} |u_j\rangle. \tag{12}$$

which up to a normalisation factor corresponds to the solution.

Generic circuit of HHL algorithm. In 2012, Yudong Cao et al. proposed an efficient and generic circuit of HHL algorithm[14]. In this design, the Group Leader Optimization Algorithm was used to find the circuit decomposition of the Hamiltonian analog operator exp[iA(2π/16)][16,17]. Then simply multiply the offset angles of all the revolving gates in the circuit by a factor of 2, 4, and 8 to get the operators $exp[iA(2\pi/8)]$, $exp[iA(2\pi/4)]$ and $exp[iA(2\pi/2)]$. They show a 4 × 4 linear system as shown in Fig. 2 below.

Hybrid HHL algorithm. Yonghae Lee et al. proposed a hybrid HHL algorithm in 2019[6]. The implementation of the algorithm is based on the following two characteristics given in the paper:

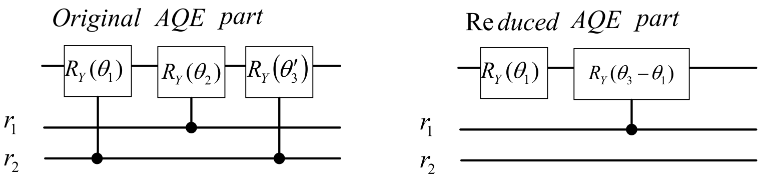


Figure 3. The quantum circuits before and after the improvement of the AQE stage in the hybrid HHL algorithm.

Characteristic 1. The fidelity of HHL algorithm results can reach 1 only when all eigenvalues of the matrix can perfectly *n-estimated*.

For example, for a 2 × 2 matrix, at that time $\lambda_{n=2} = 1, 2$ or 3, its eigenvalues are *2-estimated*. Using 2-bit quantum registers, its fidelity can reach 1, but if its eigenvalues exceed 3 or are decimals, it is not perfectly *2-estimated*, so the fidelity cannot reach 1 when using 2-bit quantum registers.

Characteristic 2. If the eigenvalues of the matrix are not perfectly *n-estimated*, then the fidelity of the algorithm's results will be positively related to the number of extra quantum registers used.

This is because for matrices with non-perfect *n-estimated* eigenvalues, additional qubit registers are needed to represent the eigenvalues of the matrix and to control the phase rotation. In other words, additional quantum are required to improve the fidelity of the results. For example, the eigenvalues of a 2 × 2 matrix $\lambda_{n=2} = 4$ are not perfectly represented by *2-estimated*. In this case, in order to make the fidelity close to 1, it is necessary to use 3 qubits to store the eigenvalue information of the matrix.

From Characteristic 1 and Characteristic 2 we note that once the eigenvalues of the matrix are not perfectly *n-estimated*, the number of qubits in quantum registers that need to be used to achieve high fidelity increases dramatically.When all eigenvalues can be perfectly *n-estimated*, n—scale quantum registers are also required to ensure high fidelity. Therefore, in the implementation process of the HHL algorithm, in order to reduce the circuit complexity, it is necessary to choose a matrix with perfect *n-estimated* as much as possible. At the same time, the literature[6] pointed out the following conclusion.

Conclusion. In the execution of the HHL algorithm, for a perfect *n-estimated* matrix, if it has *k-fixed* eigenvalues, it can be implemented with a smaller depth quantum circuit, and compared with the original HHL algorithm, the circuit complexity is reduced, and the smaller depth quantum circuit of HHL algorithm has higher fidelity.

Reference[6] uses the above conclusion to improve the quantum circuit of the AQE stage of the HHL algorithm, and gives the improved quantum circuit of the 2 × 2 matrix as shown in Fig. 3. In the hybrid HHL algorithm, the feedforward combined with the information obtained by classical calculation after quantum phase estimation effectively reduces the number of quantum gates of the original HHL algorithm.

However, the implementation details of the improvement of the AQE stage of the HHL algorithm are not described in this algorithm, and the quantum circuits in the QPE and inverse QPE stages are not improved.

This paper will take the generic circuit of HHL algorithm proposed by Yudong Cao et al. as the framework, and use the design idea of the hybrid HHL algorithm proposed by Yonghae Lee et al. to improve the implementation circuit of the HHL algorithm as a whole.

Result

Preparation before implementation.

QPE is repeatedly performed to obtain the information of the eigenvalues: in the quantum phase estimation part, the binary representation of the eigenvalues has been stored in $Reg.B$ each qubit of the quantum register after the phase estimation. If the $Reg.B$ quantum register is measured on the Z-axis, then the $Reg.B$ quantum register can be collapsed to an eigenvalue of the matrix, and the measurement process can be repeated[6].

Secondly, the prior information is obtained by combining probability statistics with classical computers: whether the information of the matrix eigenvalues obtained in the QPE stage is statistically observed to be *k-fixed*. If the *k-fixed* characteristic is not observed in the statistical eigenvalue information, more qubit registers need to be used to store the matrix eigenvalues in order to discover the *k-fixed* characteristic.

Simplification of quantum circuits.

In this subsection, according to the *k-fixed* property of the matrix, we give a specific implementation method to reduce the number of quantum gates required to realize the HHL quantum circuit, and compare it with the generic circuit of HHL algorithm.

(1) Quantum phase estimation stage

When the eigenvalue of the matrix, that is, λ is k-fixed, the kth binary value $\overline{m}_k$ of all eigenvalues of the matrix is either 0 or 1.

Firstly, when $\overline{m}_k = 0$, in the first part of the QPE, n – 1 H gates are used to add to the qubit except the kth qubit.

$$|\varphi_1\rangle = \left(H^{\otimes n-1} \otimes I\right)|0\rangle^{\otimes n}|u\rangle = \frac{1}{\sqrt{2^n}} \sum_{x_0x_1...x_{n-1}\in\{0,1\}^n} |0\rangle\left|x_0x_1...x_{k-1}x_{k+1}...x_n\right\rangle|u\rangle \tag{13}$$

According to our definition of $\overline{m}_k$, the state of Eq. (13) is the same as the state of Eq. (3) at this time.

Secondly, when using n – 1 controlled gate to add phase $e^{2\pi i\theta}$ to the probability amplitude, it does not have to act on the kth qubit.

$$\begin{aligned}|\varphi_2\rangle = \frac{1}{2^{\frac{n}{2}}} &\underbrace{|0\rangle + e^{2\pi i 2^{n-1}(0.\theta_0\theta_1,...,\theta_{n-1})}|1\rangle}_{1\text{st } qubit} \otimes ... \underbrace{|0\rangle}_{k\text{st } qubit} ... \otimes \underbrace{|0\rangle + e^{2\pi i 2^{1}(0.\theta_0\theta_1,...,\theta_{n-1})}|1\rangle}_{n-1\text{st } qubit} \\ &\otimes \underbrace{|0\rangle + e^{2\pi i 2^{0}(0.\theta_0\theta_1,...,\theta_{n-1})}|1\rangle}_{n\text{st } qubit} |u\rangle\end{aligned} \tag{14}$$

The state of Eq. (14) is the same as the state of Eq. (4) at this time.

Finally, $|\varphi_2\rangle$ quantum state performs inverse quantum Fourier transform, which extracts the target value θ from the probability amplitude into the ground state.

For qubits $|x_k\rangle, k = 1, 2, ...n$. We already know that the matrix is *k-fixed* and $\overline{m}_k = 0$, so there is no need to adjust $|x_k\rangle$ perform phase rotation and directly measure $|x_k\rangle$, we can get $|0\rangle$.

$$|\varphi_3\rangle = \left|\theta_0\theta_1...\theta_{k-1}0\theta_{k+1}...\theta_{n-1}\right\rangle|u\rangle \tag{15}$$

The state of Eq. (15) is also the same as the state of Eq. (7) at this time.

When the matrix is *k-fixed* and $\overline{m}_k = 0$. According to the definition of $\overline{m}_k$, the QPE part of the improved circuit implementation of the HHL algorithm is the same as the QPE part of the original HHL algorithm. For $\overline{m}_k = 1$, it is similar to the process of $\overline{m}_k = 0$, except that in the first stage of QPE, the initialization state of the kth qubit is changed to $|1\rangle$.

For example, when the eigenvalue of a perfect *4-estimated* matrix is λ_j *2-fixed*, one can get

$$\begin{aligned}|\varphi\rangle_{\theta_1=0} = &\frac{\left(|0\rangle + e^{2\pi i\left(\frac{1}{2}\theta_3\right)}|1\rangle\right)\left(|0\rangle + e^{2\pi i\left(\frac{1}{2}\theta_2+\frac{1}{4}\theta_3\right)}|1\rangle\right)}{4} \\ &\cdot \frac{\left(|0\rangle + e^{2\pi i\left(\frac{1}{4}\theta_2+\frac{1}{8}\theta_3\right)}|1\rangle\right)\left(|0\rangle + e^{2\pi i\left(\frac{1}{2}\theta_0+\frac{1}{8}\theta_2+\frac{1}{16}\theta_3\right)}|1\rangle\right)}{4}|\mu\rangle \rightarrow |\theta_0\theta_2\theta_3\rangle|0\rangle|\mu\rangle.\end{aligned} \tag{16}$$

$$\begin{aligned}|\varphi\rangle_{\theta_1=1} = &\frac{\left(|0\rangle + e^{2\pi i\left(\frac{1}{2}\theta_3\right)}|1\rangle\right)\left(|0\rangle + e^{2\pi i\left(\frac{1}{2}\theta_2+\frac{1}{4}\theta_3\right)}|1\rangle\right)}{4} \\ &\cdot \frac{\left(|0\rangle + e^{2\pi i\left(\frac{1}{4}\theta_2+\frac{1}{8}\theta_3\right)}|1\rangle\right)\left(|0\rangle + e^{2\pi i\left(\frac{1}{2}\theta_0+\frac{1}{8}\theta_2+\frac{1}{16}\theta_3\right)}|1\rangle\right)}{4}|\mu\rangle \rightarrow |\theta_0\theta_2\theta_3\rangle|1\rangle|\mu\rangle.\end{aligned} \tag{17}$$

According to the above formula, the comparison diagram shown in Fig. 4 can be obtained.

Thus, if the eigenvalues of a perfect *n-estimated* matrix satisfy *k-fixed*. For a qubit representing λ_k in quantum register $Reg.C$, the applied quantum gate can be roughly reduced by a factor of $\frac{n-1}{n}$.

(2) Auxiliary quantum encoding phase

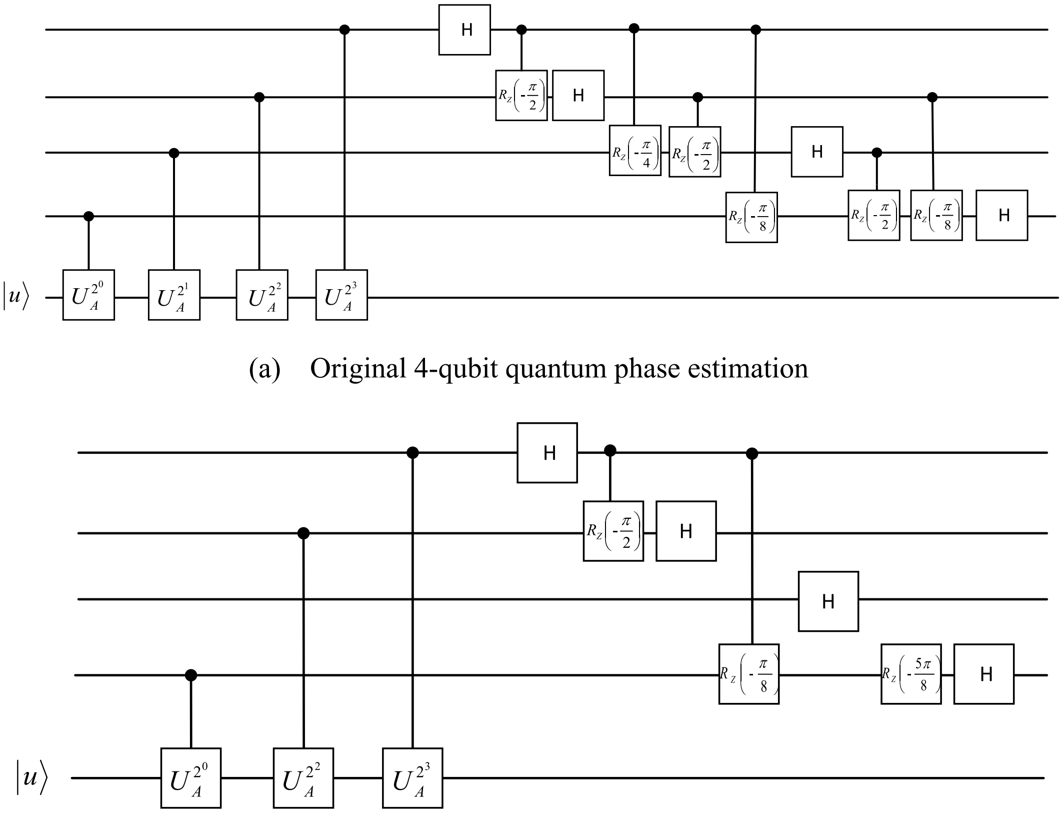
After phase estimation, quantum register $Reg.C$ stores a series of binary superposition states of eigenvalues. The control rotation part is to control the auxiliary qubit according to the superposition state in the quantum register at this time, as shown in Fig. 5 below. Figure 5a is the quantum circuit under the generic circuit of HHL algorithm. Figure 5b is *2-fixed* and $\overline{m}_1 = 0$ improved quantum circuit implementation. Figure 5c is the improved quantum circuit implementation of 2-fixed and $\overline{m}_1 = 1$.

After the AQE section, we can get the system status as follows:

$$|0\rangle_A|\theta_0\theta_2\theta_3\rangle|1\rangle|\mu\rangle \rightarrow \left(\left(\sqrt{1-\left(\frac{c}{\lambda_{\theta_1=1}}\right)^2}\right)|0\rangle_A + \frac{c}{\lambda_{\theta_1=1}}|1\rangle_A\right)|\theta_0\theta_2\theta_3\rangle|1\rangle|\mu\rangle. \tag{18}$$

$$|0\rangle_A|\theta_0\theta_2\theta_3\rangle|0\rangle|\mu\rangle \rightarrow \left(\left(\sqrt{1-\left(\frac{c}{\lambda_{\theta_1=0}}\right)^2}\right)|0\rangle_A + \frac{c}{\lambda_{\theta_1=0}}|1\rangle_A\right)|\theta_0\theta_2\theta_3\rangle|0\rangle|\mu\rangle. \tag{19}$$

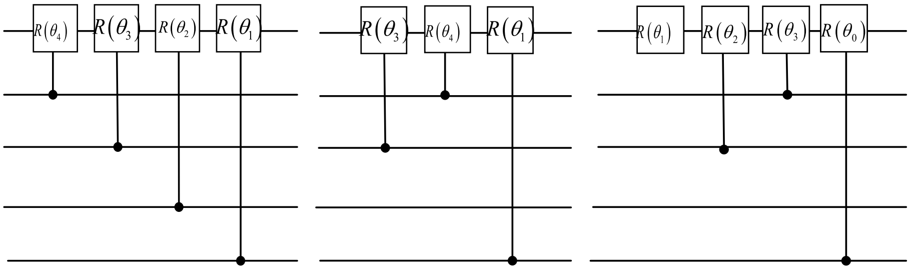
(3) Inverse quantum phase estimation


H
$R_Z\left(-\frac{\pi}{2}\right)$
H
$R_Z\left(-\frac{\pi}{4}\right)$
$R_Z\left(-\frac{\pi}{2}\right)$
H
$R_Z\left(-\frac{\pi}{8}\right)$
$R_Z\left(-\frac{\pi}{2}\right)$
$R_Z\left(-\frac{\pi}{8}\right)$
H
$|u\rangle$
$U_A^{2^0}$
$U_A^{2^1}$
$U_A^{2^2}$
$U_A^{2^3}$
H
$R_Z\left(-\frac{\pi}{2}\right)$
H
H
$R_Z\left(-\frac{\pi}{8}\right)$
$R_Z\left(-\frac{5\pi}{8}\right)$
H
$|u\rangle$
$U_A^{2^0}$
$U_A^{2^2}$
$U_A^{2^3}$

(a) Original 4-qubit quantum phase estimation

(b) Quantum Phase Estimation with *2-fixed* Properties

Figure 4. Comparison of quantum phase estimation with and without *4-estimated* and *2-fixed* properties.



(a) HHL Quantum of 4×4 linear system quantum circuit

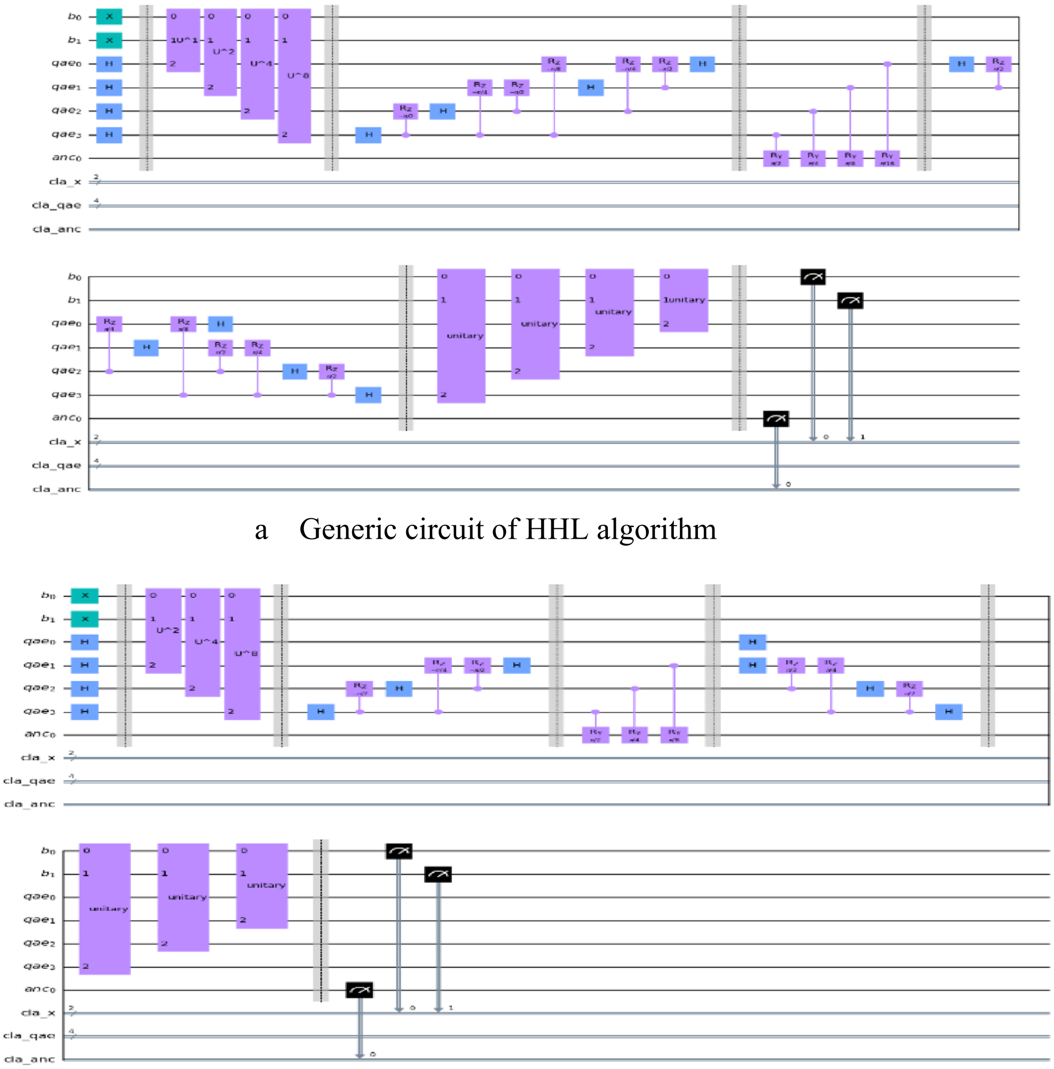
(b) *2-fixed* and $\overline{m}_1 = 0$ improved quantum circuit

(c) *2-fixed* and $\overline{m}_1 = 1$ improved quantum circuit

Figure 5. AQE part of the original circuit and the improved circuit.

After the AQE part, the inverse quantum phase estimation and quantum phase estimation have the same simplified circuit implementation, and will not be repeated here. The applied quantum gates can likewise be roughly reduced to the original $\frac{n-1}{n}$.

Quantum circuit implementation example. IBM Q provides a Qiskit library based on the Python programming environment that can be used for remote access or emulation with classics. In this section, the Qiskit library is used to simulate a linear system $Ax = b$, where A is a randomly chosen 4×4 matrix that is 4-estimated and 1-fixed, $A = \begin{bmatrix} 11 & 5 & -1 & -1 \\ 5 & 11 & 1 & 1 \\ -1 & 1 & 11 & -5 \\ -1 & 1 & -5 & 11 \end{bmatrix}$, $b = (0, 0, 0, 1)^T$, with the generic circuit of HHL algorithm and the improved



a Generic circuit of HHL algorithm

b Improved circuit implementation of the HHL algorithm

Figure 6. Comparison of the generic circuit of HHL algorithm and improved circuit implementation of the HHL algorithm.

circuit implementation of the HHL algorithm. To obtain the result we run the simulation 1024 times. Here the eigenvalues of matrix A can be accurately stored using four qubits.

The quantum circuit is shown in Fig. 6 below.

It can be seen from Fig. 6 that the improved circuit implementation of the HHL algorithm uses less quantum gates than the generic circuit of HHL algorithm. On the other hand, the quantum resources and fidelity used to obtain the simulation solution using the generic circuit of HHL algorithm and the simulation solution obtained through the improved circuit implementation of the HHL algorithm are compared as shown in Table 1 below.

Experimental results show that when using improved circuit to solve linear equations, the fidelity of the experimental solution is higher than that of the original HHL general purpose quantum circuit, and it uses less quantum resources.

Discussion

In general, for linear systems, if the prior condition is satisfied, that is, the eigenvalues of the matrix of the linear equation system have *k-fixed* characteristics, the quantum resources consumption can be reduced without reducing the fidelity of the experimental results. For an n-dimensional linear equation system, in the case of satisfying *k-fixed*, the quantum gate applied to the qubit representing λ_k in the quantum register $Reg.C$ can be roughly reduced to the original $\frac{n-1}{n}$. If we observe more *k-fixed* information in the first step, and record the number of *k-fixed* as k_{num}, $0 < k_{num} <= n$, the applied quantum gates can be roughly reduced to the original $\frac{n-k_{num}}{n}$, and the reduced circuit depth of the quantum circuit is about 2n.

Algorithm	Solution	Fidelity	Depth	Width	Total quantum gate
Theoretical solution	$\begin{pmatrix} \sqrt{0.0455} \\ \sqrt{0.0455} \\ \sqrt{0.1818} \\ \sqrt{0.7272} \end{pmatrix}$	1	–	–	–
Generic circuit	$\begin{pmatrix} \sqrt{0.0412} \\ \sqrt{0.0450} \\ \sqrt{0.2450} \\ \sqrt{0.6687} \end{pmatrix}$	0.993	28	14	39
Improved circuit	$\begin{pmatrix} \sqrt{0.0371} \\ \sqrt{0.0358} \\ \sqrt{0.1687} \\ \sqrt{0.7583} \end{pmatrix}$	0.998	21	14	28

Table 1. Comparison of simulative and theoretical solutions of 4×4 linear system. When using quantum circuits to implement the HHL algorithm to solve the linear equation system, the fidelity of the experimental solution cannot reach 1 due to current technical limitations.

Methods

Improved circuit implementation of the HHL algorithm is the same as the generic circuit of HHL algorithm in the initialization part, the difference is that the improved circuit implementation of the HHL algorithm uses the generic circuit of HHL algorithm to achieve the QPE part, and further uses the measured *Reg*.*B* quantum register. The information of some matrix eigenvalues is used to assist the construction of the following circuit.

(1) Generic circuit of HHL algorithm

```
Initialize:
  $Anc: q\ [0] \leftarrow |0\rangle$
    $Re\ g\ .C: q\ [0]q[1]q[2]q[3] \leftarrow |0000\rangle$
    $Re\ g\ .B: q\ [0]q[1] \leftarrow \big(U_3(\theta,0{,}0)\big) \otimes U_3(\theta,0{,}0)|00\rangle$
   Different $|b\rangle$ can be achieved by changing the $\theta$ value.
QPEA:
   $for\ i = 0\ to\ 3\ do$
         $Re\ g\ .C: q\ [i] \leftarrow U_A^{2^j} \otimes (Re\ g\ .B: q\ [0]q[1], Re\ g\ .C: q\ [i])$
   $end$
   $Re\ g\ .C: q\ [0] \leftarrow H \otimes \left(c - U_3\left(0{,}0,-\frac{7}{8}\pi\right)(Re\ g\ .C: q\ [3]q[2]q[1], Re\ g\ .C: q\ [0])\right)$
   $Re\ g\ .C: q\ [1] \leftarrow H \otimes \left(c - U_3\left(0{,}0,-\frac{3}{4}\pi\right)(Re\ g\ .C: q\ [3]q[2], Re\ g\ .C: q\ [1])\right)$
   $Re\ g\ .C: q\ [2] \leftarrow H \otimes \left(c - U_3\left(0{,}0,-\frac{1}{2}\pi\right)(Re\ g\ .C: q\ [3], Re\ g\ .C: q\ [2])\right)$
   $Re\ g\ .C$:q[3] $\leftarrow H \otimes Re\ g\ .C: q\ [3]$
          $c - U_3\left(0{,}0,-\frac{7}{8}\pi\right)$ is composed of three qubits that control different rotation angles for
   $Re\ g\ .C: q\ [3]q[2]q[1]$ respectively. $c - U_3(0{,}0,-\frac{3}{4}\pi)$ is composed of two qubits that control
   different rotation angles for the control bits $Re\ g\ .C: q\ [3]q[2]$ respectively.
AQE:
  $anc\_q\ [0] \leftarrow c - U_3(\frac{1}{2}\pi, 0{,}0)(Re\ g\ .C: q\ [3], anc\_q\ [0])$
   $anc\_q\ [0] \leftarrow c - U_3(\frac{1}{4}\pi, 0{,}0)(Re\ g\ .C: q\ [2], anc\_q\ [0])$
   $anc\_q\ [0] \leftarrow c - U_3(\frac{1}{8}\pi, 0{,}0)(Re\ g\ .C: q\ [1], anc\_q\ [0])$
   $anc\_q\ [0] \leftarrow c - U_3(\frac{1}{16}\pi, 0{,}0)(Re\ g\ .C: q\ [0], anc\_q\ [0])$
$Inverse\_AQE$:
   $Reg.C: q[0]q[1]q[2]q[3] \leftarrow q\_f\ t(Reg.C: q[0]q[1]q[2]q[3])$
   $for\ i = 0\ to\ 3\ do$
         $Reg.C: q[i] \leftarrow inverse\ \_U_A^{2^i} \otimes (Reg.B: q[0]q[1], Reg.C: q[i])$
   $end$
Measure:
  $Do\ measure\ anc\_q\ [0]$
    $if\ anc\_q\ [0] = |1\rangle$then
      $return\ Reg.B: q[0]q[1]$
    $end$
```

(2) Improved circuit implementation of the HHL algorithm

```
Initialization:
    $Anc : q\,[0] \leftarrow |0\rangle$
    $Re\,g\,.C : q\,[0]q[1]q[2]q[3] \leftarrow |0000\rangle$
    $Re\,g\,.B : q\,[0]q[1] \leftarrow \big(U_3(\theta, 0{,}0)\big) \otimes U_3(\theta, 0{,}0)|00\rangle$
QPEA:
    $for\ i = 1\ to\ \ 3\ \ do$
        $Re\,g\,.C : q\,[i] \leftarrow U_A^{2^j} \otimes (Re\,g\,.B : q\,[0]q[1], Re\,g\,.C : q\,[i])$
    $end$
    $Re\,g\,.C : q\,[1] \leftarrow H \otimes \left(c - U_3\left(0{,}0, -\frac{3}{4}\pi\right)(Re\,g\,.C : q\,[3]q[2], Re\,g\,.C : q\,[1])\right)$
    $Re\,g\,.C : q\,[2] \leftarrow H \otimes \left(c - U_3\left(0{,}0, -\frac{1}{2}\pi\right)(Re\,g\,.C : q\,[3], Re\,g\,.C : q\,[2])\right)$
    $Re\,g\,.C$: q[3] $\leftarrow H \otimes Re\,g\,.C : q\,[3]$
AQE:
    $anc\,\_\,q\,[0] \leftarrow c - U_3(\frac{1}{2}\pi, 0{,}0)(Re\,g\,.C : q\,[3], anc\,\_\,q\,[0])$
    $anc\,\_\,q\,[0] \leftarrow c - U_3(\frac{1}{4}\pi, 0{,}0)(Re\,g\,.C : q\,[2], anc\,\_\,q\,[0])$
    $anc\,\_\,q\,[0] \leftarrow c - U_3(\frac{1}{8}\pi, 0{,}0)(Re\,g\,.C : q\,[1], anc\,\_\,q\,[0])$
$\boldsymbol{Inverse\,\_\,AQE}$:
    $Reg.C: q[0]q[1]q[2]q[3] \leftarrow q\,\_\,f\ t(Reg.C: q[0]q[1]q[2]q[3])$
    $for\ i = 1\ to\ \ 3\ \ do$
        $Reg.C: q[i] \leftarrow inverse\ \_U_A^{2^i} \otimes (Reg.B: q[0]q[1], Reg.C: q[i])$
    $end$
Measure:
        $Do\ measure\ anc\,\_\,q\,[0]$
          $if\ anc\,\_\,q\,[0] = |1\rangle$then
            $return\ Reg.B: q[0]q[1]$
          $end$
```

Data availability

The datasets used and/or analysed during the current study available from the corresponding author on reasonable request.

Received: 30 March 2022; Accepted: 28 July 2022
Published online: 02 August 2022

References

1. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **41**(2), 303–332 (1999).
2. Grover, L. K. Quantum mechanics helps in searching for a needle in a Haystack. *Phys. Rev. Lett.* **79**(2), 325 (1997).
3. Harrow, A. W., Hassidim, A. & Lloyd, S. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.* **103**(15), 150502–150502 (2009).
4. Maslov, D. *et al.* Quantum circuit simplification and level compaction. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.* **27**(3), 436–444 (2008).
5. Cory, D. G. *et al.* ChemInform Abstract: NMR based quantum information processing: Achievements and prospects. *ChemInform* **32**(7), 875–907 (2001).
6. Lee, Y., Joo, J. & Lee, S. Hybrid quantum linear equation algorithm and its experimental test on IBM Quantum Experience. *Sci. Rep.* **9**(1), 1–12 (2019).
7. Langenberg, B., Pham, H. & Steinwandt, R. Reducing the cost of implementing the advanced encryption standard as a quantum circuit. *IEEE Trans. Quantum Eng.* **1**, 1–12 (2020).
8. Zou, J. *et al.* Quantum circuit implementations of AES with fewer qubits. In *International Conference on the Theory and Application of Cryptology and Information Security* 697–726 (Springer, 2020).
9. Jaques, S. *et al.* Implementing Grover oracles for quantum key search on AES and LowMC. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* 280–310 (Springer, 2020).
10. Monz, T. *et al.* Realization of a scalable Shor algorithm. *Science* **351**(6277), 1068–1070 (2016).
11. Diao, Z., Zubairy, M. S. & Chen, G. A quantum circuit design for Grover's algorithm. *Zeitschrift fur Naturforschung A* **57**(8), 701–708 (2002).

12. Grassl, M. *et al.* Applying Grover's algorithm to AES: quantum resource estimates. In *Post-Quantum Cryptography* (ed. Takagi, T.) 29–43 (Springer, 2016).
13. Ambainis, A. Variable time amplitude amplification and a faster quantum algorithm for solving systems of linear equations. In *Computer Science* (2010).
14. Cao, Y. *et al.* Quantum circuit design for solving linear systems of equations. *Mol. Phys.* **110**(15–16), 1675–1680 (2012).
15. Ji, W. & Meng, X. Demonstration of quantum linear equation solver on the IBM qiskit platform. In *2020 19th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)* (2020).
16. Storme, L., Vos, A. D. & Jacobs, G. Group theoretical aspects of reversible logic gates. *J. Univ. Comput. Sci.* **5**(5), 307–321 (1999).
17. He, X., Guan, Z. & Ding, F. The mapping and optimization method of quantum circuits for Clifford + T gate. *Appl. Math. Appl. Phys. (English)* **7**(11), 15 (2019).

Acknowledgements

The authors would like to thank for the support from the National Science Foundation of China (No. 61941105). We sincerely thank all the reviewers and editors for their very professional comments that made us aware of the inadequacies in our paper. We acknowledge use of the qiskit for this work. Te views expressed are those of the authors and do not refect the ofcial policy or position of IBM or the qiskit team.

Author contributions

M.Z., L.D. and Y.Z. conceived the experimental test on IBM Quantum Experience, and M.Z. conducted the experimental test. M.Z. and L.D. wrote the manuscript. Y.Z. and N.C. supervised the work and revised the manuscript. All authors discussed the results, and reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to L.D.

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

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