Luo et al. *EPJ Quantum Technology* (2025) 12:14
https://doi.org/10.1140/epjqt/s40507-025-00317-6

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

Analysis of converting $\mathfrak{C}^{o}$-circuit into $\mathfrak{C}^{*}$-circuit

Qing-bin Luo[1,2*], Lang Ding[1], Guo-wu Yang[3] and Xiao-yu Li[2]

*Correspondence:
qingbinluo@126.com
[1]College of Intelligent Systems Science and Engineering, Hubei Minzu University, Enshi, 44500, China
[2]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, China
Full list of author information is available at the end of the article

Abstract

A $\mathfrak{C}^{*}$-circuit, which was proposed in Asiacypt 2022 by Huang and Sun (Advances in cryptology – ASIACRYPT 2022, pp. 614–644, 2022), can directly perform calculations with the existing quantum states, thereby reducing the use of quantum resources in quantum logic synthesis. We theoretically prove how to convert a $\mathfrak{C}^{o}$-circuit into the corresponding $\mathfrak{C}^{*}$-circuit through two lemmas and one theorem. The first lemma proves the interchangeability of CNOT gates and NOT gates by using the equivalence of quantum circuits. The second lemma proves that adding CNOT gates to the front of a quantum circuit whose initial states are all $|0\rangle$s will not change the output states of the circuit. The theorem is used to describe what kind of $\mathfrak{C}^{o}$-circuit can be transformed into $\mathfrak{C}^{*}$-circuit, and the correctness of this transformation is proved. Our work will provide a theoretical basis for converting $\mathfrak{C}^{o}$-circuit to $\mathfrak{C}^{*}$-circuit. Then applying the theoretical analysis results to the multiplication over GF(2^8), the constructed quantum circuit needs 27 Toffoli gates and 118 CNOT gates, which is 15 fewer Toffoli gates and 43 CNOT gates than the current best result. This shows that the method of constructing quantum circuits by using the conversion of $\mathfrak{C}^{o}$-circuit to $\mathfrak{C}^{*}$-circuit is very efficient.

Keywords: Quantum circuit; Quantum logic synthesis; $\mathfrak{C}^{*}$-circuit; Multiplication

1 Introduction

In quantum computation, when it is necessary to calculate the value of the output $f(x)$ based on the input x, it is generally necessary to encode x on a quantum register a to obtain the quantum state $|x\rangle_a$, and initialize a register b whose inputs are all $|0\rangle$s, and then construct a quantum circuit through quantum logic gates to perform operations, and finally the quantum state $|x\rangle$ is still output on the register a, and the calculated result $f(x)$ is output on the register b. This process or quantum circuit can be denoted as $|x\rangle_a|0\rangle_b \longrightarrow |x\rangle_a|f(x)\rangle_b$. Sometimes it is necessary to use an auxiliary quantum register c whose initial quantum states are all $|0\rangle$s, and restore the output states in register c to $|0\rangle$s after the calculation, i.e. $|x\rangle_a|0\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|f(x)\rangle_b|0\rangle_c$. This quantum circuit is denoted as $\mathfrak{C}^{o}$-circuit [1]. Meanwhile, Huang et al. [1] also defined the $\mathfrak{C}^{*}$-circuit as $|x\rangle_a|y\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|y \oplus f(x)\rangle_b|0\rangle_c$, which is used to construct a quantum circuit for an S-box that can be iterated in place within the AES cryptographic algorithm's round

Springer

function. Then Huang et al. [1] discussed that if the quantum circuit of $|x\rangle_a|y\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|A(y) \oplus f(x)\rangle_b|0\rangle_c$ can be constructed, the inverse circuit of linear transformation A can be added in front of the output qubits to construct the corresponding $\mathfrak{C}^*$-circuit $|x\rangle_a|y\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|y \oplus f(x)\rangle_b|0\rangle_c$. However, in our view, there are still two issues that need to be addressed in Huang et al.'s work [1]. Firstly, they did not discuss how to construct a quantum circuit $|x\rangle_a|y\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|A(y) \oplus f(x)\rangle_b|0\rangle_c$ from the quantum circuit $|x\rangle_a|0\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|f(x)\rangle_b|0\rangle_c$. In other words, they did not discuss how to construct the linear transformation A. Secondly, they pointed out that by adding a quantum circuit for the inverse transformation A^{-1} of A at the front end of the register b of the quantum circuit $|x\rangle_a|y\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|A(y) \oplus f(x)\rangle_b|0\rangle_c$, the corresponding $\mathfrak{C}^*$-circuit can be realized. However, this result is not obvious, because there are other quantum gates among the quantum gates that realizes the transformation A. They did not demonstrate why it is sufficient to add only the quantum circuit for the inverse transformation A^{-1}, without the need to add the quantum circuit for the inverse transformation of other quantum gates. For the first issue, We will point out in Theorem 1 that the linear transformation A is actually the linear transformation composed of all (f)-type CNOT gates, that is, the CNOT gates whose control qubit and target qubit are on register b. For the second issue, we will provide a detailed proof, utilizing two lemmas and one theorem, to demonstrate why merely adding (f)-type CNOT gates in reverse order at the front of register b is sufficient to convert the $\mathfrak{C}^\circ$-circuit into the corresponding $\mathfrak{C}^*$-circuit, although there are quantum gates of types (e), (g), and (i) among these (f)-type CNOT gates.

Besides the work by Huang et al. [1], there are other studies that involve converting $\mathfrak{C}^\circ$-circuit into $\mathfrak{C}^*$-circuit. However, they fail to provide specific definitions and detailed discussions. These studies primarily concentrate on the quantum circuit design of block cipher algorithms. In 2020, Zou et al. [2] implemented the quantum circuit of $|x\rangle_a|y\rangle_b|0^{n-8}\rangle_c \longrightarrow |x\rangle_a|y \oplus S(x)\rangle_b|0^{n-8}\rangle_c$ based on the quantum circuit of $|x\rangle_a|0^n\rangle_{bc} \longrightarrow |x\rangle_a|S(x)\rangle_b|0^{n-8}\rangle_c$ by using an additional auxiliary quantum register while constructing the S-box of AES block cipher. Because previous research [3–5] only implemented the quantum circuit of $|x\rangle_a|0^n\rangle_{bc} \longrightarrow |x\rangle_a|S(x)\rangle_b|0^{n-8}\rangle_c$, the quantum circuit of the AES block cipher algorithm constructed by Zou et al. can save a lot of quantum resources. In 2022, Wang et al. [6] constructed the quantum circuit of $|x\rangle_a|y\rangle_b|0^{16}\rangle_c \longrightarrow |x\rangle_a|y \oplus S(x)\rangle_b|0^{16}\rangle_c$ by adding an affine transformation quantum circuit composed of 8 CNOT gates to the output of the quantum circuit the AES block cipher S-box $|x\rangle_a|0^{24}\rangle_{bc} \longrightarrow |x\rangle_a|S(x)\rangle_b|0^{16}\rangle_c$ of constructed by Langenberg et al. [5], and further optimized the quantum circuit of the AES block cipher algorithm. By adding linear transformation quantum circuits at the front of the output circuits, Li et al. [7] realized the quantum circuit $|f\rangle_a|g\rangle_b|h\rangle_c \longrightarrow |f\rangle_a|g\rangle_b|h \oplus fg\rangle_c$ of the multiplication in finite field GF(2^4) by using the quantum circuit $|f\rangle_a|g\rangle_v|0^4\rangle_c \longrightarrow |f\rangle_a|g\rangle_b|fg\rangle_c$ and the quantum circuit $|x\rangle_a|y\rangle_b|0^6\rangle_c \longrightarrow |x\rangle_a|y \oplus S(x)\rangle_b|0^6\rangle_c$ of AES block cipher S-box by using the quantum circuit $|x\rangle_a|0^{14}\rangle_{bc} \longrightarrow |x\rangle_a|S(x)\rangle_b|0^6\rangle_c$. However, why adding the quantum circuits of linear transformations is feasible has not been proven or explained in Ref. [6, 7]. Therefore, the complete theoretical analysis of how to construct $\mathfrak{C}^*$-circuit from $\mathfrak{C}^\circ$-circuit is missing, we will complete this work in this paper.

As an application of the theoretical analysis, we will improve the quantum circuit of multiplication over GF(2^8) based on the work of Luo et al. [8]. The multiplication arithmetic over GF(2^8) has important applications in cryptography, such as Almazrooie [4] and

Luo et al. [9] based on Fermat's little theorem using the quantum circuit of multiplication arithmetic over GF GF(2^8) to realize the quantum circuits of the S-boxes of AES and SM4 cipher algorithms respectively.

The finite field GF(2^m) is very important in modern cryptography. For example, the encryption and decryption processes of cryptographic algorithms such as AES [10], SM4 [11], and Camellia [12] are realized through arithmetic operations in finite field GF(2^m) generated by an irreducible pentanomial with degree m = 8 using polynomial basis representation. For quantum circuit realizations of multiplication, the number of qubits, the number of Toffoli gates, and the number of CNOT gates of the circuits are mainly considered as optimization objectives. In this paper, the irreducible polynomial over GF(2^8) considered is $f(x) = x^8 + x^4 + x^3 + x + 1$. When the finite field GF(2^8) generated by the irreducible pentanomial $f(x) = x^8 + x^4 + x^3 + x + 1$, the quantum circuit of multiplication in Ref. [3] requires 64 Toffoli gates, 21 CNOT gates and 24 qubits (no ancillas), the quantum circuit in Ref. [4] requires 64 Toffoli gates, 17 CNOT gates, and 24 qubits, the quantum circuit in Ref. [13] requires 64 Toffoli gates, 15 CNOT gates, and 24 qubits, and the quantum circuit in Ref. [8] requires 42 Toffoli gates, 161 CNOT gates, and 24 qubits. In physical implementations, a Toffoli gate needs much more quantum resources than a CNOT gate. Therefore, reducing the number of Toffoli gates in the quantum circuits of multiplication over GF(2^8) makes sense in terms of reducing the use of quantum resources. When constructing the quantum circuit of multiplication over GF(2^8), we will first optimize the number of Toffoli gates and then optimize the number of CNOT gates, without adding any auxiliary qubits.

The rest of this paper is organized as follows. We will introduce the preliminaries of quantum logic gates and related composite field arithmetic in Sect. 2. In Sect. 3, we will use two lemmas and one theorem to gradually describe how to construct $\mathfrak{C}^*$-circuit from $\mathfrak{C}^\circ$-circuit. In Sect. 4, we discuss the improved quantum circuits of multiplication over GF(2^8). Finally, a short conclusion is given in Sect. 5.

2 Preliminaries

2.1 Quantum logic gates

In quantum computation, the elementary quantum gates are used to manipulate quantum information [14]. Because the NCT gate library composed only of NOT gates, CNOT gates and Toffoli gates is universal, that is, for all m and all permutations $\pi \in S_{2^m}$, there exists some n such that some circuit composed of gates from NCT gate library computes π using n qubits of temporary storage [15], the quantum circuits composed of these three quantum gates have been extensively studied [16]. The definitions of these three quantum gates are as follows (also see Fig. 1).

NOT gate: maps one qubit $|B\rangle$ as $|B\rangle \longrightarrow |B \oplus 1\rangle$, i.e. $NOT|B\rangle = |B \oplus 1\rangle = |\bar{B}\rangle$.

CNOT gate: maps two qubits $|B_1\rangle$ and $|B_2\rangle$ as $|B_1\rangle|B_2\rangle \longrightarrow |B_1\rangle|B_2 \oplus B_1\rangle$, i.e. $CNOT|B_1\rangle|B_2\rangle = |B_1\rangle|B_2 \oplus B_1\rangle$, where $|B_1\rangle$ is control qubit and $|B_2\rangle$ is target qubit.

Toffoli gate: maps three qubits $|B_1\rangle$, $|B_2\rangle$ and $|B_3\rangle$ as $|B_1\rangle|B_2\rangle|B_3\rangle \longrightarrow |B_1\rangle|B_2\rangle|B_3 \oplus B_1B_2\rangle$, i.e. $Toffoli|B_1\rangle|B_2\rangle|B_3\rangle = |B_1\rangle|B_2\rangle|B_3 \oplus B_1B_2\rangle$, where $|B_1\rangle$ and $|B_2\rangle$ are control qubits and $|B_3\rangle$ is target qubit.

Since the matrix form of the quantum NOT gate is equal to the Pauli X matrix, the notation "X" for the quantum NOT gate is used for historical reasons in some literature. The quantum CNOT gate is sometimes called as the CX gate and the quantum Toffoli gate is called as the CCNOT gate or CCX gate.

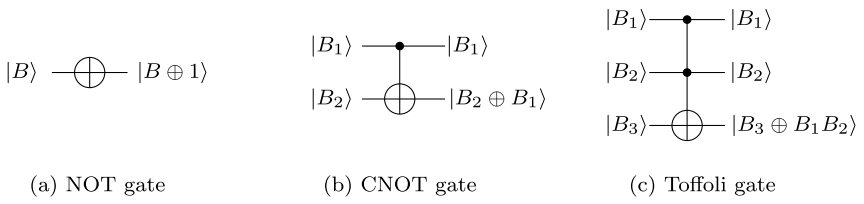


Figure 1 The elementary quantum gates in NCT gate library

2.2 Composite field arithmetic

As an application of theoretical analysis, we will implement the quantum circuit of multiplication over GF(2^8) based on composite field arithmetic operations. Although the methods will be applicable to any irreducible polynomial over GF(2^8), in order to construct the specific quantum circuit, we concretize the irreducible polynomial as follows

$$f(x) = x^8 + x^4 + x^3 + x + 1 \tag{1}$$

It is difficult to directly construct a quantum circuit for multiplication over GF(2^8), so we will use the method similar to Ref. [8] to construct the quantum circuit for multiplication over GF(2^8) based on composite field theory. Let $g(y) = y^2 + y + \lambda$ be an irreducible polynomial over GF(2^4) and Y be a root of $g(y)$, where $\lambda \in$ GF(2^4), then for any $\mathbf{a,b} \in$ GF((2^4)^2) we have $\mathbf{a} = a_1Y + a_0$ and $\mathbf{b} = b_1Y + b_0$, where $a_1, a_0, b_1, b_0 \in$ GF(2^4). The product $\mathbf{a} \times \mathbf{b}$ can be computed as follows:

$$\mathbf{a} \times \mathbf{b} = (a_0b_0 + (a_1 + a_0)(b_1 + b_0))Y + (a_1b_1\lambda + a_0b_0) \tag{2}$$

According to the method of calculating the isomorphic mapping [8], we can construct the isomorphic mapping ϕ^{-1} from the composite field GF((2^4)^2) to the finite field GF(2^8) as follows:

$$\phi^{-1} = \left[1, Z, Z^2, Z^3, Y, YZ, YZ^2, YZ^3\right] \tag{3}$$

Where Z is a root of the irreducible polynomial $h(z) = z^4 + z + 1$ over GF(2). Using the fact that $(\phi^{-1})^{-1} = \phi$, the isomorphic mapping ϕ can be computed. In order to use as little quantum resources as possible during implementations, a pair of specific values of ϕ and ϕ^{-1} can be given as follows:

$$\phi = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \phi^{-1} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{4}$$

After ϕ and ϕ^{-1} are specified, we can get $\lambda = Z^3 + Z^2 \in \mathrm{GF}(2^4)$ and the corresponding matrix is

$$\lambda = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \tag{5}$$

3 Theoretical analysis

In order to make the description more concise, we continue to use the symbols in Ref. [1], and denote the quantum circuit $|x\rangle_a|0\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|f(x)\rangle_b|0\rangle_c$ as $\mathfrak{C}^{\mathrm{o}}$-circuit, and the quantum circuit $|x\rangle_a|y\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|y \oplus f(x)\rangle_b|0\rangle_c$ as $\mathfrak{C}^{*}$-circuit. Next, we will use two lemmas and one theorem to show how to convert a $\mathfrak{C}^{\mathrm{o}}$-circuit into its corresponding $\mathfrak{C}^{*}$-circuit.

Lemma 1 *For a quantum circuit composed only of NOT gates and CNOT gates, all NOT gates can be moved together while maintaining the CNOT gates in the original circuit by using equivalent subcircuit substitution.*

Proof Without loss of generality, suppose our goal is to move the NOT gates to the right of the CONT gates. For a fixed CNOT gate, there are only 4 cases of the NOT gates on its left. These four cases and their equivalent quantum circuits are shown in Fig. 2.

From Fig. 2, it can be seen that for a fixed CNOT gate, the NOT gates on its left can be moved to the right without any changes to its control and target qubits. This means that for a quantum circuit composed only of NOT gates and CNOT gates, keeping all CNOT gates in the circuit unchanged, all NOT gates can be moved to the right side of the circuit according to the equivalent subcircuit in Fig. 2.

In fact, the four circuits of the right side of the equal sign in Fig. 2 are four cases where the NOT gates are on the right of a fixed CNOT gate. This means that using the equivalent subcircuit in Fig. 2, all NOT gates can also be moved to the left of all CNOT gates. The proof of Lemma 1 is completed. □

Lemma 2 *For a quantum circuit composed only of NOT gates and CNOT gates, if the initial state of each qubit input is* $|0\rangle$*, adding any number of CNOT gates at the front end of this quantum circuit will not change the value of the quantum circuit output.*

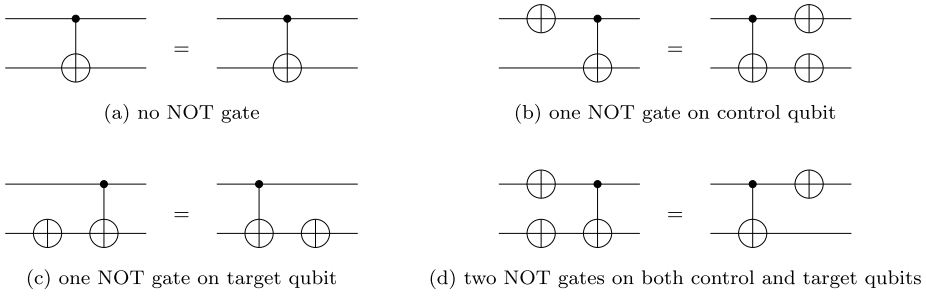


Figure 2 Four cases of a fixed CNOT gate with NOT gates on its left and the corresponding equivalent quantum circuits

Proof Because these CNOT gates are added to the front end of the quantum circuit, the inputs of these CNOT gates are all $|0\rangle$s, and the outputs after the added CNOT gates are all $|0\rangle$s. This is the same effect as not adding these CNOT gates, so the output value of the original quantum circuit will not change. The proof of Lemma 2 is completed. □

For a quantum circuit composed only of NOT gates and CNOT gates, obviously this quantum circuit can be represented by a unitary matrix U', and the input and output of this quantum circuit are denoted as $|x\rangle$ and $|f(x)\rangle$, i.e. $|f(x)\rangle = U'|x\rangle$. Because the non-zero input states are realized by adding NOT gates, the NOT gates of realizing the quantum state $|x\rangle$ can also be regarded as a part of the quantum circuit, denote the unitary matrix corresponding to the quantum circuit at this time as U, and the input states will all be $|0\rangle$, i.e. $|f(x)\rangle = U|0\rangle$. According to Lemma 1, it can be obtained that $U = U_2 * U_1$, where U_1 and U_2 are respectively the matrices corresponding to the subcircuits composed of all CNOTs and all NOT gates after moving according to the method in Lemma 1, then the quantum circuit is $|f(x)\rangle = U_2 * U_1|0\rangle$. According to Lemma 2, adding the corresponding CNOT gates in U_1 in reverse order at the front end of the circuit to achieve the unitary matrix U_1^{-1} will not change the output $|f(x)\rangle$ of the original quantum circuit, i.e. $|f(x)\rangle = U_2 * U_1 * U_1^{-1}|0\rangle = U_2|0\rangle$. At this time, only the NOT gates corresponding to U_2 are left in the quantum circuit for operation. If an input state $|y\rangle$ is prepared by adding NOT gates at the input end, the output of the quantum circuit will become $|f(x) \oplus y\rangle$, i.e. $|f(x) \oplus y\rangle = U_2|y\rangle = U_2 * U_1 * U_1^{-1}|y\rangle = U * U_1^{-1}|y\rangle$. Because the CNOT gates corresponding to U and U_1 are the same, the quantum circuit of U_1^{-1} can be constructed directly through U to get the output $|f(x) \oplus y\rangle$.

Now, we return to the discussion of $\mathfrak{C}^{\circ}$-circuit and $\mathfrak{C}^{*}$-circuit. Because the difference between $\mathfrak{C}^{\circ}$-circuit and $\mathfrak{C}^{*}$-circuit is that the input and output on register b are different, it is only necessary to analyze the operations involving register b. The set of wires on register b is denoted as β, while the sets of wires on registers a and c are denoted as α, there are 9 types of operations involving register b, as shown in Fig. 3.

Theorem 1 *If a $\mathfrak{C}^{\circ}$-circuit is composed of only four types of quantum logic gates* (*e*), (*f*), (*h*), *and* (*i*) *in Fig.* 3, *the corresponding $\mathfrak{C}^{*}$-circuit can be achieved by adding* (*f*)*-type CNOT gates in reverse order at the front end of register b.*

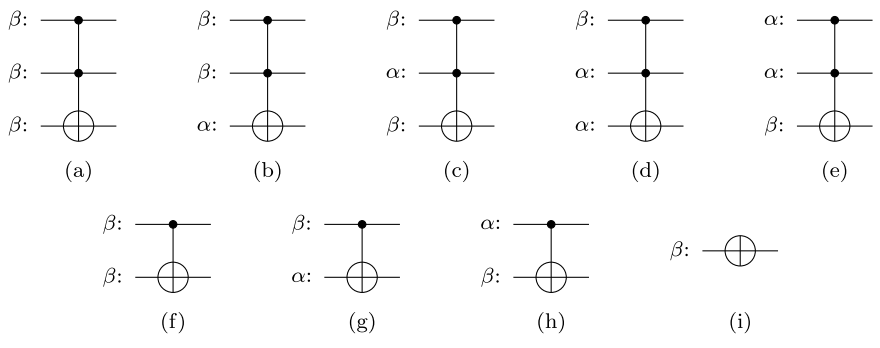


Figure 3 9 types of quantum logic gates with register b participating in calculations

Proof If a $\mathfrak{C}^o$-circuit $|x\rangle_a|0\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|f(x)\rangle_b|0\rangle_c$ is composed of only four types of quantum logic gates (e), (f), (h), and (i) in Fig. 3, then the quantum subcircuit on the output register b can be abstractly viewed as a quantum circuit consisting of only CNOT gates and NOT gates, and Theorem 1 can be proved using Lemma 1 and Lemma 2. We will prove this fact below. The target qubits of the (e) and (h)-type quantum gates act on register b, and the control qubits are not on register b, so there are only two results for the operations of the qubits on register b: the first is that the target qubit is flipped, which is equivalent to adding a NOT gate to the corresponding qubit; the second is that the qubit on the target qubit is not flipped, which is equivalent to not doing any operation. The (f)-type quantum logic gates actually perform CNOT gate operations on register b and the (i)-type quantum logic gates actually perform the NOT gate operations on the register b. Therefore, if a $\mathfrak{C}^o$-circuit is only composed of four types of quantum logic gates (e), (f), (h), and (i) in Fig. 3, it is equivalent to only performing CNOT gates and NOT gates on register b. According to Lemma 1, we can keep all (f)-type CNOT gates unchanged, and imagine moving the (e), (h), and (i)-type quantum gates to the right end of all (f)-type CNOT gates according to the equivalent circuit in Fig. 2. In order to eliminate the impact on $f(x)$ when the initial input on register b is changed from $|0\rangle_b$ to $|y\rangle_b$, we add all (f)-type CNOT gates in reverse at the front end of register b according to Lemma 2, and then the corresponding $\mathfrak{C}^*$-circuit is constructed. Finally, we imagine moving all the (e), (h), and (i)-type quantum gates that have been moved to the right end back to their original positions according to the equivalent circuit in Fig. 2. In fact, we just add all (f)-type CNOT gates in reverse order at the front end of register b, and the original $\mathfrak{C}^o$-circuit has not changed. The proof of Theorem 1 is completed. □

For Theorem 1, there are two points that need to be clarified.

(1) Because there are other logic gates between the CNOT gates on register b, the CNOT gates added in reverse order are most likely not optimal. Therefore, all the (f)-type quantum logic gates can be extracted and simplified and then added in reverse order. Another optimization method is to express all the extracted CNOT gates as a linear transformation matrix A, synthesize the quantum circuit of the inverse matrix of A with an efficient method, and then add the synthesized CNOT gates to the front end of register b.

(2) When there are the other 5 operations in Fig. 3 in a $\mathfrak{C}^o$-circuit, the method in Theorem 1 cannot convert the $\mathfrak{C}^o$-circuit into $\mathfrak{C}^*$-circuit.

As an application of the theoretical analysis, we will improve the quantum circuit of multiplication over GF(2^8) in the next section.

4 Improved quantum circuit of multiplication over GF(2^8)

In order to construct the quantum circuit of multiplication over GF(2^8) according to Formula (2), the quantum circuit of multiplication over GF(2^4) have to been constructed firstly.

4.1 Quantum circuits of multiplication over GF(2^4)

In Ref. [8], the quantum circuit of multiplication over GF(2^4) when the initial quantum states on the output register t are all $|0\rangle$s has been constructed as shown in Fig. 4.

When the initial qubits of the quantum circuit of multiplication over GF(2^4) on register t are not all $|0\rangle$s, Ref. [8] have to replace the CNOT gates whose target qubit are on register

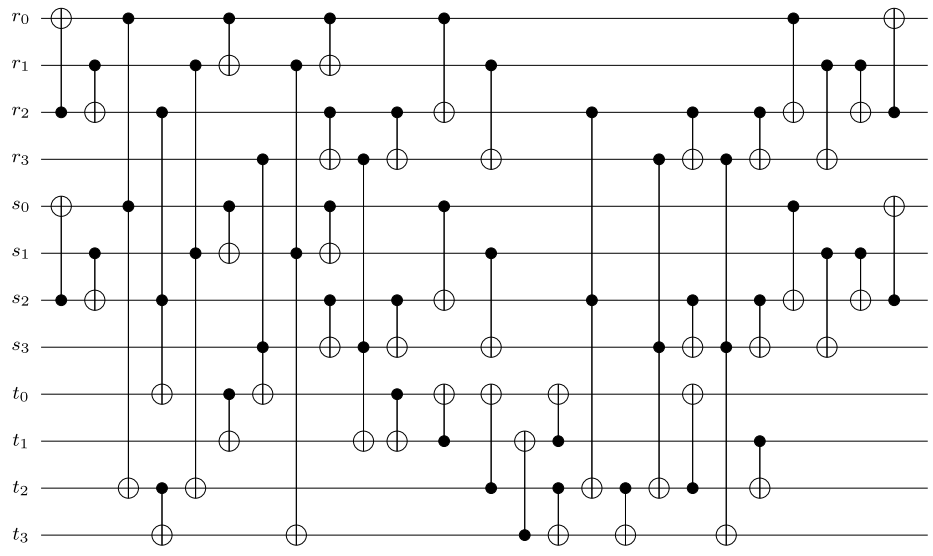


Figure 4 The quantum circuit of multiplication over GF(2^4) in Ref. [8]

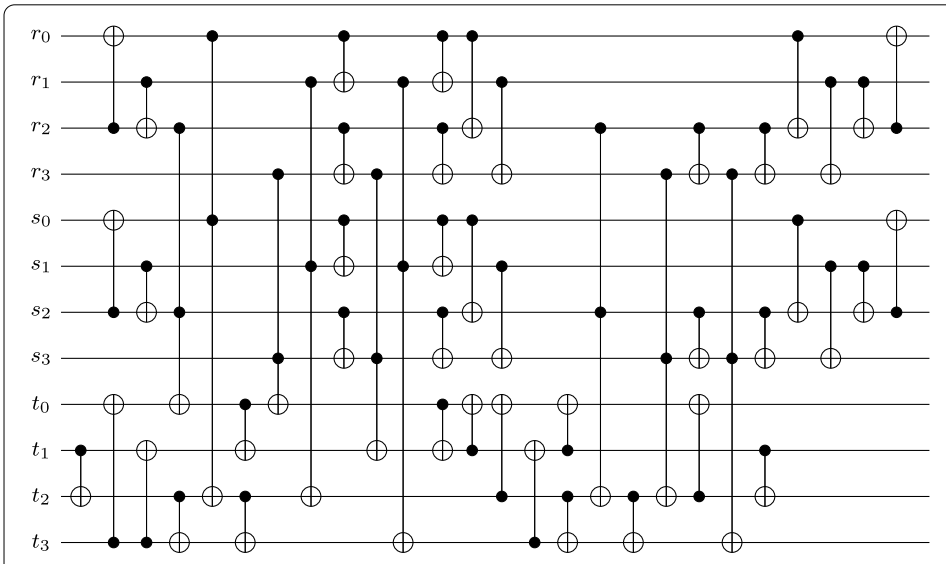


Figure 5 the $\mathfrak{C}^*$-circuit of multiplication over GF(2^4) based on $\mathfrak{C}^o$-circuit in Ref. [8]

t with the equivalent Toffoli gates. However, based on Fig. 4 and the theoretical analysis in Sect. 3, we can add the corresponding 11 CNOT gates on the register t in reverse order to gain the $\mathfrak{C}^*$-circuit of Fig. 4. Then we use the DORCIS [17] tool to optimize the 11 CNOT gates added in reverse order, and additional quantum resource is reduced from 11 CNOT gates to 4 CNOT gates. the improved $\mathfrak{C}^*$-circuit of multiplication over GF(2^4) is shown in Fig. 5.

In fact, Li et al. [7] directly construct a $\mathfrak{C}^o$-circuit of multiplication over GF(2^4) by observing and simplifying the calculations in the irreducible polynomial $x^4 + x + 1$. This $\mathfrak{C}^o$-circuit as shown in Fig. 6 uses fewer qauntum resources than Fig. 4.

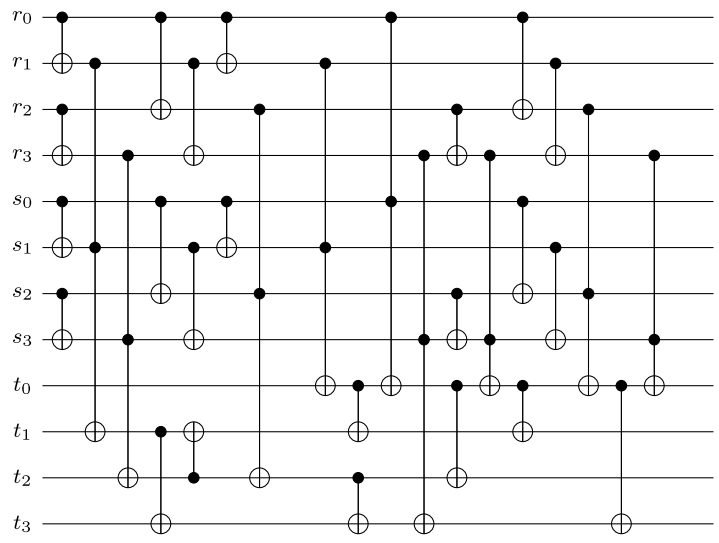


Figure 6 The $\mathfrak{C}^{\circ}$-circuit of multiplication over GF(2^4) in Ref. [7]

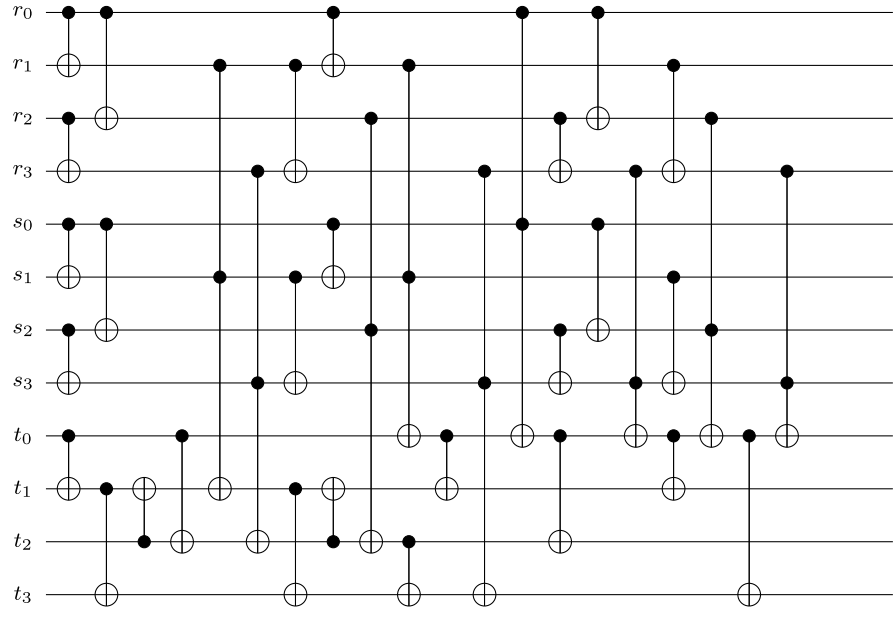


Figure 7 The improved $\mathfrak{C}^{*}$-circuit of multiplication over GF(2^4) based on $\mathfrak{C}^{\circ}$-circuit in Ref. [7]

According to the theoretical analysis in Sect. 3 and Fig. 6, the improved $\mathfrak{C}^{*}$-circuit of multiplication over GF(2^4) can be constructed as shown in Fig. 7.

The quantum circuits of multiplication over GF(2^4) can be implemented in Figs. 4, 5, 6 and 7, but they use different quantum resources. We analyze the quantum resources by comparing the number of CNOT gates and the number of Toffoli gates used in the four methods as shown in Table 1. As can be seen from Table 1, Figs. 4 and 5 require more CNOT gates than Figs. 6 and 7, but they need the same number of Toffoli gates. Therefore, from the perspective of optimizing the quantum resources, when constructing the

Table 1 The quantum resources for quantum circuits of multiplication over GF(2^4)

Schemes	Fig. 4	Fig. 5	Fig. 6	Fig. 7
qubits	12	12	12	12
CNOT gates	39	43	23	27
Toffoli gates	9	9	9	9

quantum circuits of multiplication over GF(2^8), we will preferentially use Figs. 6 and 7 as the quantum circuit of multiplication over GF(2^4). In addition, these four quantum circuits have been verified to be correct.

4.2 Improved quantum circuits of ϕ, ϕ^{-1} and λ

In order to implement the quantum circuit of multiplication over GF(2^8), in addition to implementing the quantum circuit of multiplication over GF(2^4), it is also necessary to implement the quantum circuit of the isomorphic matrices ϕ and ϕ^{-1}, as well as the matrix λ. We will adopt the method proposed by Xiang et al. [18] to reduce the number of CNOT gates. Then the improved quantum circuit of isomorphic mapping ϕ^{-1} can be realized as Fig. 8a and ϕ as Fig. 8b.

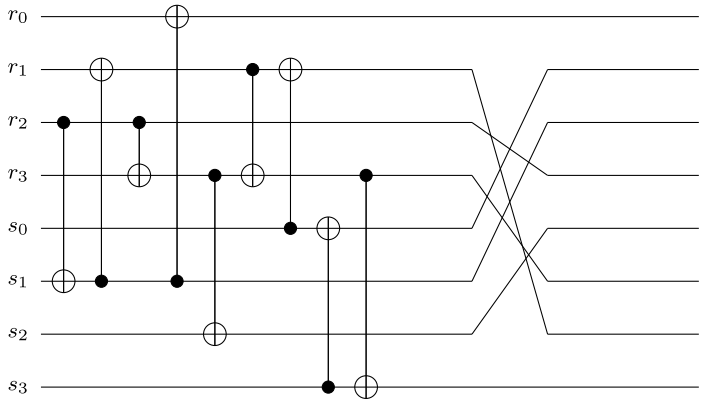
Similarly, the improved quantum circuit of the matrix λ can be implemented as Fig. 9.

4.3 Improved quantum circuit of multiplication over GF(2^8)

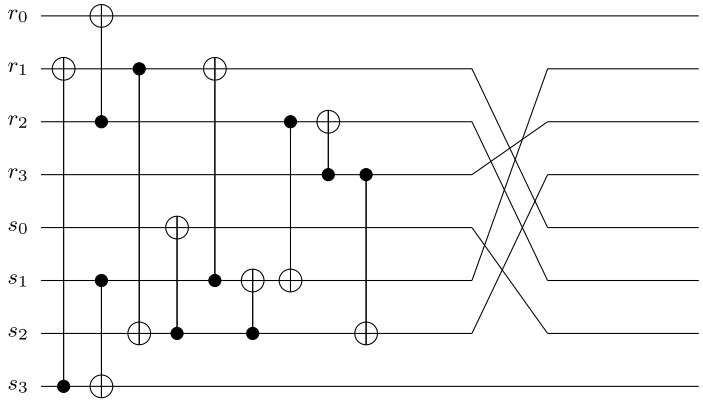
After the quantum circuits of ϕ, ϕ^{-1} and λ are implemented, we can construct the quantum circuit of multiplication over GF(2^8) with the irreducible polynomial $f(x) = x^8 + x^4 + x^3 + x + 1$. For the convenience of description, the quantum circuits corresponding to ϕ, ϕ^{-1} and λ are represented by their symbols in the logic diagram. For the quantum circuits in Figs. 6 and 7 that implement multiplication over GF(2^4), denote the two multipliers as two solid circles, the result in Fig. 6 as M1 and the result in Fig. 7 as M2. The logic diagram of the quantum circuit for multiplication over GF(2^8) as shown in Fig. 10 according to Formula (2). And the specific quantum circuit is shown in the Appendix. The correctness of this circuit, and each quantum circuit in this paper, is verified using the Aer simulator on the IBM quantum computing cloud platform.

Although the logic diagram of the quantum circuit for multiplication over GF(2^8) in Fig. 10 is the same as that in Ref. [8], we use fewer quantum resources than ones in Ref. [8]. This is mainly due to three improvements. Firstly, we use the quantum circuit for multiplication over GF(2^4) in Ref. [7], which has fewer CNOT gates compared to Ref. [8]. Secondly, we use the method of converting $\mathfrak{C}^{\circ}$-circuit into $\mathfrak{C}^{*}$-circuit in Theorem 1 to further reduce the quantum resources of $\mathfrak{C}^{*}$-circuit for multiplication over GF(2^4) in Fig. 7. Thirdly, we use the method of implementing the quantum circuit of the matrix in Ref. [18], thereby optimizing the quantum circuits of matrices ϕ, ϕ^{-1} and λ. The quantum resources used in our work with the existing quantum circuits that implement multiplication over GF(2^8) are shown in Table 2.

As can be seen from Table 2, all five schemes in this table use only 24 qubits without auxiliary qubits. Our scheme uses a total of 118 CNOT gates, which is more than that in Ref. [3, 4, 13]. However, Ref. [3, 4, 13] all have to use 64 Toffoli gates, and Ref. [8] has to use 42 Toffoli gates, while our scheme only uses 27 Toffoli gates, which is the least in all schemes. According to the method in Ref. [19], we convert the number of CNOT gates and Toffoli gates into quantum cost. It can be seen that the quantum cost in our scheme is 253, which is the smallest among all schemes.



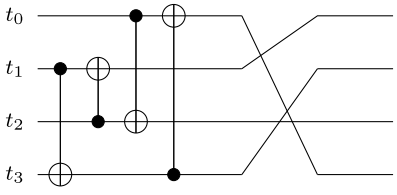
(a) Improved quantum circuit of ϕ^{-1}



(b) Improved quantum circuit of ϕ

Figure 8 Improved quantum circuits of isomorphic mappings between GF(2^8) and GF((2^4)^2)

Figure 9 The improved quantum circuit of the matrix λ



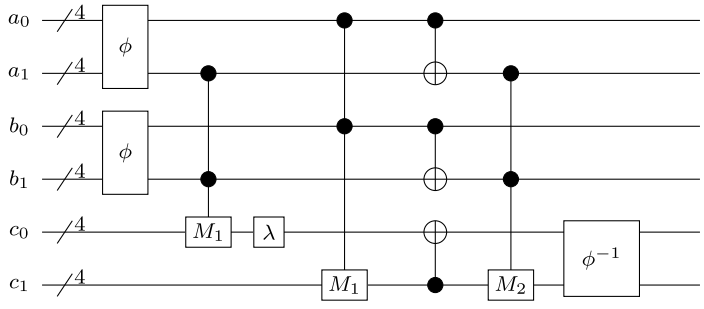


Figure 10 The logic diagram of the quantum circuit for multiplication over GF(2^8)

Table 2 The quantum resources for quantum circuits of multiplication over GF(2^8)

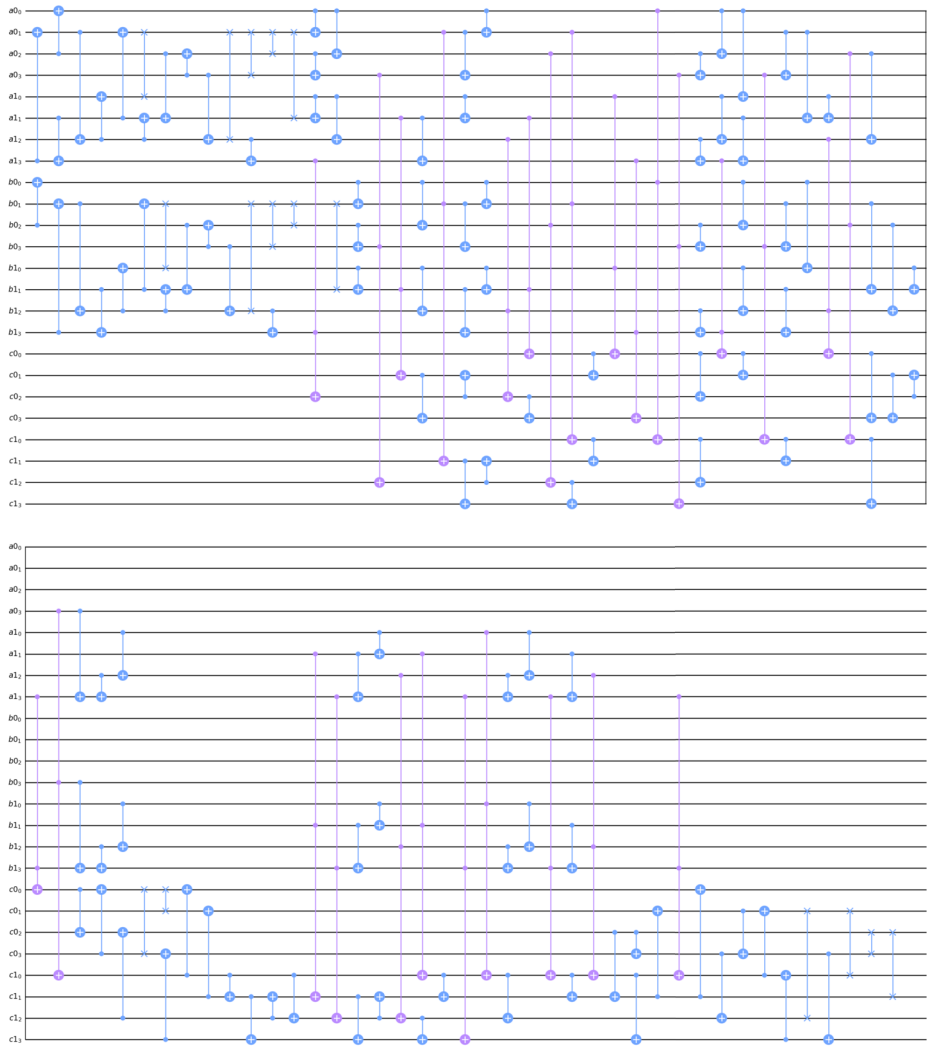
Quantum resources	Ref. [3]	Ref. [4]	Ref. [13]	Ref. [8]	This work
qubits	24	24	24	24	24
CNOT gates	21	17	15	161	118
Toffoli gates	64	64	64	42	27
quantum cost	341	337	335	371	253

5 Conclusion

A $\mathfrak{C}^{\circ}$-circuit is easy to construct in quantum logic synthesis, but iteratively constructing more complex quantum circuits with $\mathfrak{C}^{\circ}$-circuit needs to continuously add quantum resources such as qubits. A $\mathfrak{C}^{*}$-circuit can directly perform calculations with existing quantum states, reducing the use of quantum resources in quantum logic synthesis. Huang et al. [1] provided the definitions for the $\mathfrak{C}^{\circ}$-circuit and the $\mathfrak{C}^{*}$-circuit, and observed that the corresponding $\mathfrak{C}^{*}$-circuit can be derived from the quantum circuit $|x\rangle_a|y\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|A(y) \oplus f(x)\rangle_b|0\rangle_c$. However, they did not discuss how to obtain the quantum circuit $|x\rangle_a|y\rangle_b|0\rangle_c \longrightarrow |x\rangle_a|A(y) \oplus f(x)\rangle_b|0\rangle_c$ from the corresponding $\mathfrak{C}^{\circ}$-circuit, nor the correctness of this derivation. We theoretically proved how to transform from $\mathfrak{C}^{\circ}$-circuit to $\mathfrak{C}^{*}$-circuit through two lemmas and one theorem. The first lemma proves the interchangeability of CNOT gates and NOT gates by using the equivalence of quantum circuits. The second lemma proves that adding CNOT gates to the front of a quantum circuit whose initial states are all $|0\rangle$s will not change the output state of the circuit. The theorem is used to describe what kind of $\mathfrak{C}^{\circ}$-circuit can be transformed into $\mathfrak{C}^{*}$-circuit, and the correctness of this transformation is proved. Our work will provide a theoretical basis for the conversion of $\mathfrak{C}^{\circ}$-circuit to $\mathfrak{C}^{*}$-circuit.

As an application of the theoretical analysis, we improve the quantum circuit of multiplication over GF(2^8). And multiplication over GF(2^8) has many applications in modern cryptography, we mainly discuss the quantum circuit implementations of multiplication over GF(2^8) with the irreducible polynomial $f(x) = x^8 + x^4 + x^3 + x + 1$, which can be used to estimate quantum resources in security analysis. In addition, Toffoli gates need a lot of quantum resources in physical implementation. In this paper, we try to construct quantum circuits with as few Toffoli gates as possible, based on the theoretical basis of the proof. By discussing the case of whether the initial output qubits of the product are all $|0\rangle$s, we give the quantum circuit of multiplication over GF (2^4) in this case according to the principle of minimizing the number of Toffoli gates. Finally, the constructed quantum circuit of multiplication over GF(2^8) needs a total of 24 qubits, 118 CNOT gates, and 27 Toffoli gates. Compared to the previous conclusion, the constructed quantum circuit without auxiliary qubits require only 27 Toffoli gates, 15 fewer than quantum circuits achieved by existing methods, and the quantum resources and computational complexity required to construct the quantum circuits of multiplication over GF(2^8) are further reduced. In addition to applying the method of converting $\mathfrak{C}^{\circ}$-circuit to $\mathfrak{C}^{*}$-circuit to the quantum circuits for multiplication in binary field and block cipher S-box, this method may also be applied to quantum error correction and fault-tolerant computing, which is a direction worth studying in the future.

Appendix: The specific quantum circuit of multiplication over GF(2^8)



Abbreviations
Not applicable.

Acknowledgements
The authors would like to thank the editor and the referees for carefully reading the paper, and for their useful comments which helped improve the paper.

Author contributions
The original idea to this paper came from Qingbin Luo. All authors contributed to the preparation of the manuscript. All authors read and approved the final manuscript.

Funding
This work is supported by Hubei Provincial Natural Science Foundation Joint Fund Project (Grant No. 2024AFD066), the Campus Research Project of Hubei Minzu University (Grant No. XN2304), the National Natural Science Foundation of China (Grant Nos. 62262020, 12164037, 62172075), the National Key R&D Program of China (Grant No.2018YFA0306703).

Data availability
All data generated or analysed during this study are included in this manuscript.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
We give our consent for the publication of identifiable details within the text to be published in EPJ Quantum Technology.

Competing interests
The authors declare no competing interests.

Author details
[1]College of Intelligent Systems Science and Engineering, Hubei Minzu University, Enshi, 44500, China. [2]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, 610054, China. [3]Big data research Center & School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China.

Received: 5 June 2024 Accepted: 16 January 2025 Published online: 28 January 2025

References

1. Huang Z, Sun S. Synthesizing quantum circuits of AES with lower T-depth and less qubits. In: Advances in cryptology – ASIACRYPT 2022. Lecture notes in computer science. vol. 13793. 2022. p. 614–44.
2. Zou J, Wei Z, Sun S, et al. Quantum circuit implementations of AES with fewer qubits. In: Advances in cryptology – ASIACRYPT 2020. Lecture notes in computer science. vol. 12492. Cham: Springer; 2020. p. 697–926.
3. Grassl M, Langenberg B, Roetteler M, et al. Applying Grover's algorithm to AES: quantum resource estimates. In: Post-quantum cryptography. Cham: Springer; 2016. p. 29–43.
4. Almazrooie M, Samsudin A, Abdullah R, et al. Quantum reversible circuit of AES-128. Quantum Inf Process. 2018;17(5):1–30.
5. Langenberg B, Pham H, Steinwandt R. Reducing the cost of implementing the advanced encryption standard as a quantum circuit. IEEE Trans Quantum Eng. 2020;1:1–12.
6. Wang ZG, Wei SJ, Long GL. A quantum circuit design of AES requiring fewer quantum qubits and gate operations. Front Phys. 2022;17(4):41501.
7. Li Z, Cai B, Sun H, et al. Novel quantum circuit implementation of advanced encryption standard with low costs. Sci China, Phys Mech Astron. 2022;65(9):290311.
8. Luo Q-B, Li X-Y, Yang G-W, et al. Quantum reversible circuits for $\mathbf{GF}(2^8)$ multiplication based on composite field arithmetic operations. Quantum Inf Process. 2023;22:58.
9. Luo QB, Li XY, Yang GW. Quantum circuit implementation of S-box for SM4 cryptographic algorithm. J Univ Electron Sci Tech China. 2021;50(6):820–6. https://doi.org/10.12178/1001-0548.2021252.
10. FIPS Pub. 197: Specification for the AES, Nov. 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
11. Lv SW, Su BZ, Wang P, et al. Overview on SM4 algorithm. J Inf Secur Res. 2016;2(11):995–1007.
12. Aoki K, Ichikawa T, Kanda M, et al. Camellia: a 128-bit block cipher suitable for multiple platforms-design and analysis. In: International workshop on selected areas in cryptography. Berlin: Springer; 2000. p. 39–56.
13. Imana JL. Optimized reversible quantum circuits for F28 multiplication. Quantum Inf Process. 2021;20(1):1–15.
14. Nielsen MA, Chuang I. Quantum computation and quantum information. Cambridge: Cambridge University Press; 2002.
15. Shende VV, Prasad AK, Markov IL, et al. Synthesis of reversible logic circuits. IEEE Trans Comput-Aided Des Integr Circuits Syst. 2003;22(6):710–22.
16. Saeedi M, Markov IL. Synthesis and optimization of reversible circuits—a survey. ACM Comput Surv. 2013;45(2):1–34.
17. Chun M, et al. DORCIS: depth optimized quantum implementation of substitution boxes. IACR Cryptol. ePrint Arch. 2023 (2023): 286.
18. Xiang Z, Zeng X, Lin D, Bao Z, Zhang S. Optimizing implementations of linear layers. IACR Trans Symmetric Cryptol. 2020;2020(2):120–45. https://doi.org/10.13154/tosc.v2020.i2.120-145.
19. Luo QB, Yang GW, Li XY, et al. Quantum reversible circuits for multiplicative inverse. EPJ Quantum Technol. 2022;9(1):24.

Publisher's Note