Luo et al. *EPJ Quantum Technology* (2022) 9:24
https://doi.org/10.1140/epjqt/s40507-022-00144-z

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

Quantum reversible circuits for GF(2^8) multiplicative inverse

Qing-bin Luo[1,2*], Guo-wu Yang[3,4*], Xiao-yu Li[2] and Qiang Li[1]

*Correspondence:
qingbinluo@126.com;
guowu@uestc.edu.cn
[1]Department of Computer Science and Technology, School of Information Engineering, Hubei Minzu University, Enshi, 44500, China
[3]Big data research Center & School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu, 611731, China
Full list of author information is available at the end of the article

Abstract

The synthesis of quantum circuits for multiplicative inverse over GF(2^8) are discussed in this paper. We first convert the multiplicative inverse operation in GF(2^8) to arithmetic operations in the composite field GF((2^4)^2), and then discuss the expressions of the square calculation, the inversion calculation and the multiplication calculation separately in the finite field GF(2^4), where the expressions of multiplication calculation in GF(2^4) are given directly in GF(2^4) and given through being transformed into the composite field GF((2^2)^2). Then the quantum circuits of these calculations are realized one by one. Finally, two quantum circuits for multiplicative inverse over GF(2^8) are synthesized. They both use 21 qubits, the first quantum circuit uses 55 Toffoli gates and 107 CNOT gates and the second one uses 37 Toffoli gates and 209 CNOT gates. As an example of the application of multiplication inverse, we apply these quantum circuits to the implementations of the S-box quantum circuit of the AES cryptographic algorithm. Two quantum circuits for implementing the S-box of the AES cryptographic algorithm are presented. The first quantum circuit uses 21 qubits, 55 Toffoli gates, 131 CNOT gates and 4 NOT gates and the second one uses 21 qubits, 37 Toffoli gates, 233 CNOT gates and 4 NOT gates. Through the evaluation of quantum cost, the two quantum circuits of the S-box of AES cryptographic algorithm use less quantum resources than the existing schemes.

Keywords: Quantum circuit; Composite field; Multiplicative inverse; S-box; AES

1 Introduction

The quantum circuit implementations of symmetric cryptographic algorithms have recently received researchers' attention for the following two reasons. On one hand, the security analysis of a cryptographic algorithm in quantum environment needs to estimate the quantum resources used in the cryptographic algorithm. Implementing the cryptographic algorithm with quantum circuits is the most direct way to estimate the quantum resources used. On the other hand, quantum logic gates are all reversible, and cryptographic algorithms implemented by using quantum circuits to consume near zero power theoretically and resist from various side-channel attacks related to power analysis [3, 16].

In the quantum circuit realization schemes of these symmetric cryptographic algorithms, the realization or optimization of the quantum circuit of the S-box is an important research content in these schemes. In 2016, Markus et al. [6] firstly estimated the quantum

Springer

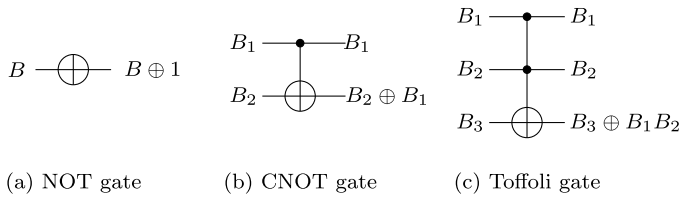
resources required in the S-box in the AES encryption algorithm [5] with two schemes. The Itoh-Tsujii algorithm [7] was mainly used to estimate the resources in the first scheme, which requires a total of 40 qubits, 3584 T gates and 4569 Clifford gates. By computing the short factorizations to estimate the quantum resources in the second scheme, which needs a total of 9 qubits, no more than 9695 T gates and 12631 Clifford gates. However, the authors only estimated the quantum resources required to realize the S-box but did not give the specific quantum circuits. In 2018, Almazrooie et al. [1] implemented the quantum reversible circuit of AES-128. A total of 56 qubits, 448 Toffoli gates, 494 CNOT gates and 4 NOT gates are used in the quantum circuit of S-box. By optimizing the Boolean expressions of each output in the S-box of the AES encryption algorithm, the quantum circuit given by Langenberg et al. [8] uses a total of 32 qubits, 55 Toffoli gates, 314 CNOT gates and 4 NOT gates. By further optimizing the output Boolean expressions in the S-box of the AES encryption algorithm, the quantum circuit designed by Zou et al. [23] uses a total of 26 qubits, 46 Toffoli gates, 304 CNOT gates and 4 NOT gates. In addition to AES block cipher algorithm, Luo et al. [11] also implemented the quantum circuit of S-box of SM4 cipher algorithm [13], which uses a total of 48 qubits and 592 quantum logic gates. Soon after, Luo et al. [12] used only 21 qubits, 55 Toffoli gates, 176 CNOT gates and 10 NOT gates to realize the quantum circuit of S-box of SM4 cryptographic algorithm.

By analyzing the algebraic expressions of S-boxes of AES [5], SM4 [10] and Camellia [2] etc., it can be seen that the outputs of S-boxes of these algorithms are almost obtained by multiplicative inverse operations and affine transformations of the inputs over the finite field GF(2^8). The quantum circuit of affine transformation is easy to implement. The matrix in the affine transformation can be realized in a manner similar to Gaussian elimination, that is, the matrix is transformed into a unit matrix through row transformation, and a CNOT gate is added to the corresponding qubits when the row transformation is performed. And then these CNOT gates are arranged in reverse order, the quantum circuit of the matrix is constructed. For the column vector, it can be realized by adding NOT gates at the corresponding qubits where "1" appears. The difficulty of the problem is how to realize the quantum circuit of the multiplicative inverse over the finite field GF(2^8). In fact, Wang et al. [21] showed that the inverse of α is $\alpha^{-1} = \alpha^{2^m-2}$ for any α in the finite field GF(2^m). This formula was used in Ref. [1, 11] to construct the quantum circuits of the multiplicative inverse in the S-boxes. However, the quantum circuits constructed in this way used too much quantum resources. In this paper, we will discuss that the quantum reversible circuits over GF(2^8) multiplicative inverse based on composite field arithmetic, which has been applied to S-box optimization using CMOS standard cell library [4, 17]. It is also helpful for constructing the quantum circuits of multiplicative inverse in finite field GF(2^m).

The rest of this paper is organized as follows. We will introduce the preliminaries in Sect. 2. In Sect. 3, the arithmetic operations over finite fields and composite fields are described. In Sect. 4, all the quantum circuits are synthesised in details. Finally, a short discussion and conclusion is given in Sect. 5.

2 Preliminaries

Let $f(x) \in \mathrm{GF}(2)[x]$ be an irreducible polynomial over binary finite field GF(2) of degree 8 and let X be a root of $f(x)$, then any element $\alpha \in \mathrm{GF}(2^8)$ can be represented in the polynomial basis $\{1, X, X^2, \ldots, X^7\}$ as $\alpha = \sum_{i=0}^{7} a_i X^i$ with $a_i \in \mathrm{GF}(2)$. For any $\alpha \in \mathrm{GF}(2^8)$, its inverse is the element α^{-1} such that $\alpha \cdot \alpha^{-1} \equiv 1 \bmod f(x)$.



(a) NOT gate (b) CNOT gate (c) Toffoli gate

Figure 1 The elementary quantum gates in NCT gate library

The main work in this paper is to construct the quantum circuits of the inverse for any given $\alpha \in \mathrm{GF}(2^8)$ by using quantum gates. The elementary quantum gates are used to manipulate quantum information in quantum computation [14]. Quantum gates are reversible, that is, they can be regarded as bijection. Three types of elementary quantum gates, which are quantum NOT gate, CNOT gate and Toffoli gate, will be used in this paper. The quantum NOT gate maps one qubit $|B\rangle$ as $|B\rangle \longrightarrow |B \oplus 1\rangle$ as shown in Fig. 1(a), where $\oplus$ is the GF(2) addition (XOR). 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 literatures. The CNOT gate maps two qubits $|B_1\rangle$ and $|B_2\rangle$ as $|B_1\rangle|B_2\rangle \longrightarrow |B_1\rangle|B_2 \oplus B_1\rangle$ as shown in Fig. 1(b), where $|B_1\rangle$ is control qubit and $|B_2\rangle$ is target qubit. A CNOT gate has a quantum cost of 1 [20]. The Toffoli gate maps three qubits $|B_1\rangle$, $|B_2\rangle$ and $|B_3\rangle$ as $|B_1\rangle|B_2\rangle|B_3\rangle \longrightarrow |B_1\rangle|B_2\rangle|B_3 \oplus B_1B_2\rangle$ as shown in Fig. 1 (c), where $|B_1\rangle$ and $|B_2\rangle$ are control qubits and $|B_3\rangle$ is target qubit. The quantum cost of Toffoli gate is 5 as it needs 5 2-qubit gates to implement it [20].

In fact, 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 [19].

3 Composite field arithmetic

The idea is to transform the calculation in the finite field $\mathrm{GF}(2^8)$ into the composite field arithmetic, and gradually realize the quantum circuits calculated in the composite field, so as to construct the quantum circuits for multiplicative inverse in the finite field $\mathrm{GF}(2^8)$.

3.1 Multiplicative inverse over GF($(2^4)^2$)

Let $g(y) = y^2 + \mu y + \lambda$ be an irreducible polynomial over $\mathrm{GF}((2^4)^2)$ and let Y be a root of $g(y)$, where $\mu, \lambda \in \mathrm{GF}(2^4)$, then for any $\mathbf{r} \in \mathrm{GF}((2^4)^2)$ we have $\mathbf{r} = r_1 Y + r_0$, where $r_1, r_0 \in \mathrm{GF}(2^4)$. For any $\mathbf{r} = r_1 Y + r_0 \in \mathrm{GF}((2^4)^2)$, we can compute its inverse as

$$\mathbf{r}^{-1} = r_1\left(r_0^2 + r_0 r_1 \mu + r_1^2 \lambda\right)^{-1} Y + (r_0 + \mu r_1)\left(r_0^2 + r_0 r_1 \mu + r_1^2 \lambda\right)^{-1}. \tag{1}$$

We enforce the $\mu = 1$ so as to simplify arithmetic operations, then $g(y) = y^2 + y + \lambda$ and the formula (1) become

$$\mathbf{r}^{-1} = r_1\left(r_0^2 + r_0 r_1 + r_1^2 \lambda\right)^{-1} Y + (r_0 + r_1)\left(r_0^2 + r_0 r_1 + r_1^2 \lambda\right)^{-1}. \tag{2}$$

We next discuss the arithmetic operations in finite field $\mathrm{GF}(2^4)$ because $r_1, r_0, \lambda \in \mathrm{GF}(2^4)$ in formula (2).

3.2 GF(2^4) arithmetic

Let $h(z)$ be an irreducible polynomial over GF(2) of degree 4 and let Z be a root of $h(z)$, then any element $\mathbf{a} \in \mathrm{GF}(2^4)$ can be represented as $\mathbf{a} = \sum_{i=0}^{3} a_i Z^i$ with $a_i \in \mathrm{GF}(2)$. Because the characteristic of the finite field GF(2^4) is 2, for any $\mathbf{a} = \sum_{i=0}^{3} a_i Z^i \in \mathrm{GF}(2^4)$ we have

$$\mathbf{a}^2 = \left(\sum_{i=0}^{3} a_i Z^i\right)^2 = \sum_{i=0}^{3} a_i Z^{2i}. \tag{3}$$

Therefore, for any $\mathbf{a} \in \mathrm{GF}(2^4)$, there exists a matrix $\mathbf{S} \equiv [1, Z^2, Z^4, Z^6] \bmod h(z)$ over GF(2) such that

$$\mathbf{a}^2 \equiv \mathbf{S}\mathbf{a} \bmod h. \tag{4}$$

For multiplication calculation, we can get the following results from Theorem 1 in Ref. [15]: for $\mathbf{a},\mathbf{b} \in \mathrm{GF}(2^4)$, note that $\mathbf{c} = \mathbf{a} \cdot \mathbf{b}$ we have

$$\mathbf{c} = \mathbf{d} + \mathbf{Q}^T \cdot \mathbf{e}, \tag{5}$$

where

$$\mathbf{d} = \begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{pmatrix} = \mathbf{L} \cdot \mathbf{b} = \begin{pmatrix} a_0 & 0 & 0 & 0 \\ a_1 & a_0 & 0 & 0 \\ a_2 & a_1 & a_0 & 0 \\ a_3 & a_2 & a_1 & a_0 \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}, \tag{6}$$

$$\mathbf{e} = \begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \end{pmatrix} = \mathbf{U} \cdot \mathbf{b} = \begin{pmatrix} 0 & a_3 & a_2 & a_1 \\ 0 & 0 & a_3 & a_2 \\ 0 & 0 & 0 & a_3 \end{pmatrix} \cdot \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix}, \tag{7}$$

and $\mathbf{Q}^T$ is the transpose matrix of $\mathbf{Q}$ over GF(2) such that

$$\begin{pmatrix} Z^4 \\ Z^5 \\ Z^6 \end{pmatrix} \equiv \mathbf{Q} \cdot \begin{pmatrix} 1 \\ Z \\ Z^2 \\ Z^3 \end{pmatrix} \bmod h(z). \tag{8}$$

For the multiplicative inverse in finite field GF(2^4), it is actually to construct a quantum circuit that maps any element $\mathbf{a} \in \mathrm{GF}(2^4)$ to its inverse $\mathbf{a}^{-1}$, i.e. $\sigma(\mathbf{a}) = \mathbf{a}^{-1}$. Obviously, the mapping σ is a bijection, so it can be regarded as a 4-qubit reversible logic function. Although all 4-qubit logic functions cannot been synthesized with existing logic synthesis methods [9, 22], we can fortunately synthesize the quantum circuit for the multiplicative inverse mapping σ for some specific irreducible polynomial $h(z)$.

Next, we discuss whether the arithmetic in GF(2^4) need to be transformed into the composite field GF($(2^2)^2$), so as to further optimize the quantum circuits to be constructed? In fact, for a given invertible matrix over GF(2), we can effectively construct its quantum circuit with CNOT gates, so the quantum circuit of square operation in GF(2^4) can

be easily constructed by using formula (4). Because the quantum circuit that synthesizes multiplicative inverse in GF($(2^2)^2$) has to use additional auxiliary qubits compared with in GF(2^4), we don't have to convert the arithmetic to GF($(2^2)^2$) to construct it. However, it is not immediately obvious whether the quantum circuit of multiplication in GF(2^4) through arithemetic in GF($(2^2)^2$) can reduce the use of quantum resources, we discuss this next.

3.3 Multiplication over GF($(2^2)^2$)

Let $p(w) = w^2 + w + \eta$ be an irreducible polynomial over GF(2^2) and let W be a root of $p(w)$, where $\eta \in \mathrm{GF}(2^2)$, then for two elements $\mathbf{s} = s_1 W + s_0$, $\mathbf{t} = t_1 W + t_0 \in \mathrm{GF}((2^2)^2)$, we may compute the product $\mathbf{s} \times \mathbf{t}$ as follows:

$$\begin{aligned}
\mathbf{s} \times \mathbf{t} &= (s_1 W + s_0)(t_1 W + t_0) \\
&= s_1 t_1 W^2 + s_1 t_0 W + s_0 t_1 W + s_0 t_0 \\
&= s_1 t_1 W + s_1 t_1 \eta + s_1 t_0 W + s_0 t_1 W + s_0 t_0 \\
&= (s_1 t_1 + s_1 t_0 + s_0 t_1) W + (s_1 t_1 \eta + s_0 t_0) \\
&= \big(s_0 t_0 + (s_1 + s_0)(t_1 + t_0)\big) W + (s_1 t_1 \eta + s_0 t_0).
\end{aligned} \tag{9}$$

Formula (9) requires us to do multiplication in finite field GF(2^2). There is only one irreducible polynomial $q(v) = v^2 + v + 1$ over GF(2). Let V be a root of $q(v)$, then for two elements $\mathbf{i} = i_1 V + i_0$, $\mathbf{j} = j_1 V + j_0 \in \mathrm{GF}(2^2)$, we have

$$\mathbf{i} \times \mathbf{j} = \big(i_0 j_0 + (i_1 + i_0)(j_1 + j_0)\big) V + (i_1 j_1 + i_0 j_0). \tag{10}$$

3.4 Change of basis representations

Before constructing the quantum circuits, we need to discuss the isomorphic mappings of basis transformations. Let ϕ be the isomorphic mapping from the finite field GF(2^8) to the composite field GF($(2^4)^2$), that is, $\phi : \mathrm{GF}(2^8) \longmapsto \mathrm{GF}((2^4)^2)$, then its inverse mapping ϕ^{-1} is the isomorphic mapping from the composite field GF($(2^4)^2$) to the finite field GF(2^8). Using the fact that GF(2^8) contains a subfield isomorphic to GF($(2^4)^2$) as well as a subfield isomorphic to GF(2^4), we may represent both Y and Z as elements in GF(2^8). Then, the basis change mapping ϕ^{-1} can be computed as follows:

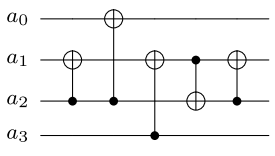
$$\phi^{-1} = \big[1, Z, Z^2, Z^3, Y, YZ, YZ^2, YZ^3\big]. \tag{11}$$

Using the fact that $(\phi^{-1})^{-1} = \phi$, the isomorphic mapping ϕ can be computed. Similarly, the isomorphic mapping ψ^{-1} from the composite field GF($(2^2)^2$) to the finite field GF(2^4) can be computed as follows:

$$\psi^{-1} = [1, V, W, VW]. \tag{12}$$

And the isomorphic mapping ψ from GF(2^4) to GF($(2^2)^2$) can be computed by using the fact that $\psi = (\psi^{-1})^{-1}$.

Figure 2 The quantum circuit of square over GF(2^4)



4 Quantum circuits

The quantum circuits are mainly implemented by Python language and qiskit software package developed by IBM Corporation. We specify $f(x) = x^8 + x^4 + x^3 + x + 1$ because it is also used in the algebraic expression of the S-box of AES cryptographic algorithm and $h(z) = z^4 + z + 1$ because less quantum resources are used to synthesize the quantum circuit of multiplicative inverse in GF(2^4) by using the bidirectional synthesis method [22]. Of course, our implementation methods are also applicable for other irreducible polynomials.

4.1 Quantum circuit of square over GF(2^4)

After $h(z) = z^4 + z + 1$ is specified, the value of $\mathbf{S}$ in formula (4) can be computed as

$$\mathbf{S} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{13}$$

The quantum circuit of $\mathbf{S}$ can be synthesised by using Gaussian elimination method as Fig. 2.

4.2 Quantum circuit of multiplication over GF(2^4)

The value of $\mathbf{Q}^T$ can be computed by using formula (8) as

$$\mathbf{Q}^T = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \tag{14}$$

The quantum circuit of multiplication over GF(2^4) can be synthesised with formula (5) as Fig. 3. As we discussed in Sect. 3.3, the quantum circuit of multiplication in GF(2^4) can also be synthesised by using the operations in the composite field GF((2^2)^2). Here, we first calculate the isomorphic mappings ψ and ψ^{-1} between finite field GF(2^4) and composite field GF((2^2)^2). There are 2 irreducible polynomials in the form of $p(w) = w^2 + w + \eta$ in GF((2^2)^2) and each polynomial has 2 roots and the irreducible polynomial $q(\nu) = \nu^2 + \nu + 1$ has 2 roots. Therefore, there are 8 pairs of isomorphic mappings ψ and ψ^{-1}. In order to minimize the use of quantum gates in realizing the isomorphic mappings, we select the pair with the least number of elements "1". By doing so, we can get $\eta = V$ and

$$\psi^{-1} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \psi = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{15}$$

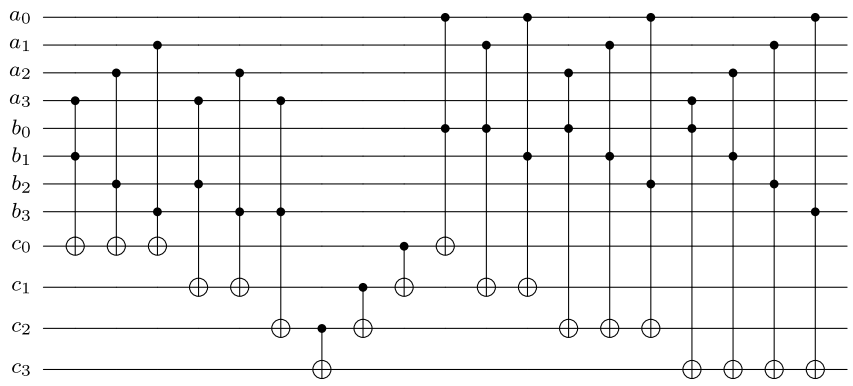
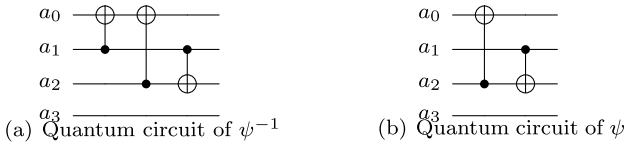


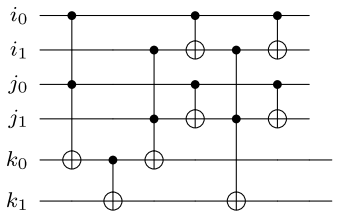
Figure 3 The quantum circuit of multiplication over GF(2^4)



(a) Quantum circuit of ψ^{-1} (b) Quantum circuit of ψ

Figure 4 Quantum circuits of isomorphic mappings between GF(2^4) and GF((2^2)^2)

Figure 5 The quantum circuit of multiplication over GF(2^2)



Then the quantum circuit of isomorphic mapping ψ^{-1} can be synthesised as Fig. 4(a) and ψ as Fig. 4(b).

According to Eq. (10), the quantum circuit of multiplication over GF(2^2) can be synthesised as Fig. 5. If the initial quantum state on wire k_0 is not $|0\rangle$ before executing the quantum circuit, we have to change the second quantum gate CNOT($k_0; k_1$) to Toffoli($i_0, j_0; k_1$).

Then, we can synthesis the quantum circuit of multiplication over GF(2^4) according to Eq. (9) and the isomorphic mappings between GF(2^4) and GF((2^2)^2) as Fig. 6.

Both Fig. 3 and Fig. 6 implement the quantum circuits of multiplication over GF(2^4), but they use different quantum resources. We analyze the quantum resources by comparing the number of CNOT gates, the number of Toffoli gates and quantum cost used in the two methods as shown in Table 1. As can be seen from Table 1, the quantum circuit in Fig. 6 uses more CNOT gates and more quantum cost than those in Fig. 3, but less Toffoli gates than that in Fig. 3. However, a circuit consisting of CNOT gates and one-qubit gates which implements the 3-qubit Toffoli gate without ancillae requires at least 6 CNOT gates [18]. According to this metric, the quantum circuit in Fig. 6 use less quantum resources than the quantum circuit in Fig. 3

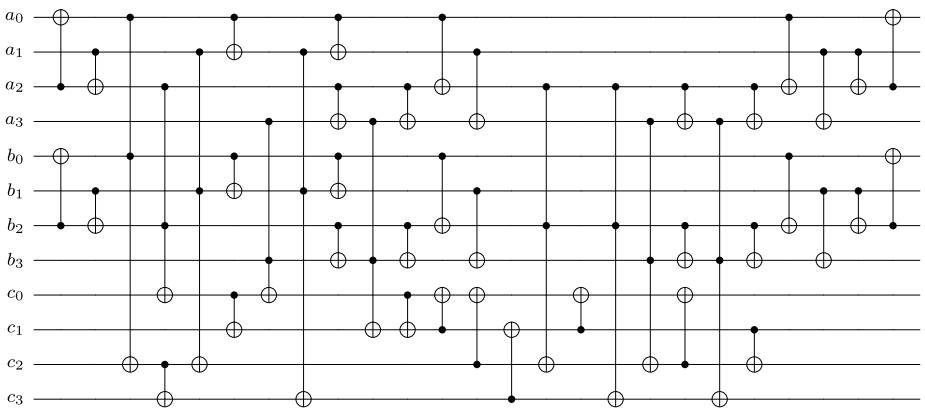


Figure 6 The quantum circuit of multiplication over GF(2^4) using arithmetic in GF((2^2)^2)

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

Schemes	Qubits	Toffoli gates	CNOT gates	Quantum cost	Depth
Fig. 3	12	16	3	83	15
Fig. 6	12	10	37	87	18

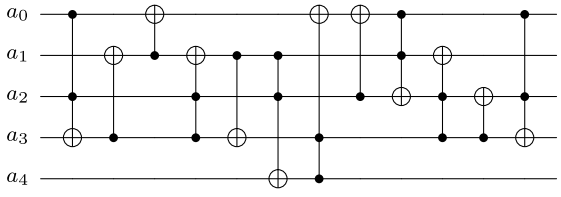


Figure 7 The quantum circuit of multiplicative inverse over GF(2^4)

4.3 Quantum circuit of multiplicative inverse over GF(2^4)

After $h(z) = z^4 + z + 1$ is specified, we can express the mapping σ that maps any element $\mathbf{a} \in \mathrm{GF}(2^4)$ to its inverse as the permutation as $(2,9)(3,14)(4,13)(5,11)(6,7)(8,15)(10,12)$. Obviously, this is an odd permutation consisting of 7 transpositions. But the NOT gates, CNOT gates and Toffoli gates in the 4-qubit circuit are all even permutations, which means that the 4-qubit quantum circuit synthesized only by using the logic gates in the NCT library cannot realize the multiplicative inverse over GF(2^4). Our strategy is to add an auxiliary qubit and synthesize an odd permutation first. Here we first use two Toffoli gates to synthesize the permutation $(14, 15)$ with the help of auxiliary qubits, and then use the bidirectional synthesis algorithm in Ref. [22] to realize the quantum circuit of multiplicative inverse over GF(2^4) as shown in Fig. 7.

4.4 Quantum circuits of the isomorphic mappings ϕ and ϕ^{-1}

There are 8 irreducible polynomials in the form of $g(y) = y^2 + y + \lambda$ in GF((2^4)^2) and each polynomial has 2 roots and the irreducible polynomial $h(z) = z^4 + z + 1$ has 4 roots. Therefore, there are 64 pairs of isomorphic mappings ϕ and ϕ^{-1}. In order to minimize the use of quantum gates in realizing the isomorphic mappings, we select the pair with the least

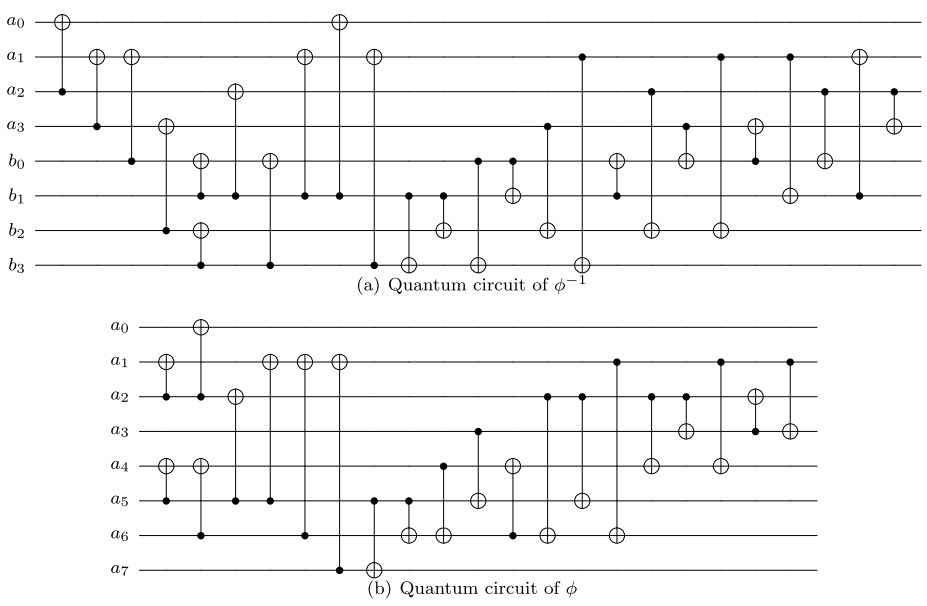


Figure 8 Quantum circuits of isomorphic mappings between GF(2^8) and GF((2^4)^2)

number of elements "1". By doing so, we can get $\lambda = Z^3 + Z^2$ and

$$\phi^{-1} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \phi = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} \tag{16}$$

then the quantum circuit of isomorphic mapping ϕ^{-1} can be synthesised as Fig. 8(a) and ϕ as Fig. 8(b).

After $\lambda = Z^3 + Z^2$ is determined, for any $\mathbf{a} \in \mathrm{GF}(2^4)$, calculating the value of $\lambda \cdot \mathbf{a}$ is equivalent to calculating the value of the matrix λ multiplied by $\mathbf{a}$, where the matrix

$$\lambda = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}. \tag{17}$$

The quantum circuit of the matrix λ can be synthesised as Fig. 9.

4.5 Quantum circuit of multiplicative inverse over GF(2^8)

For the convenience of description, denote S as the quantum circuit for realizing the square over GF(2^4) in Fig. 2. In the quantum circuit of multiplication over GF(2^4) in Fig. 3, denote the two multipliers as two solid circles and the result as M. Denote the symbol I as

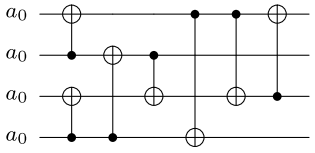


Figure 9 The quantum circuit of the matrix λ

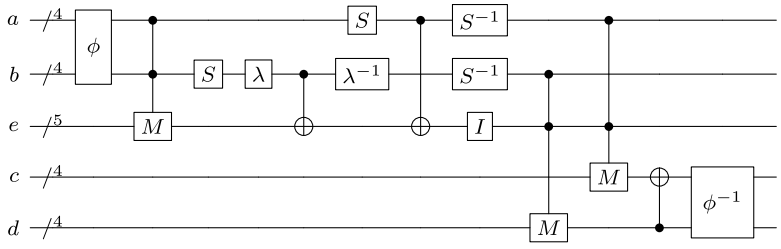


Figure 10 The logic diagram of the quantum circuit for multiplicative inverse over GF(2^8)

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

Schemes	Qubits	Toffoli gates	CNOT gates	Quantum cost	Depth
Appendix A	21	55	107	382	95
Appendix B	21	37	209	394	103

the multiplicative inverse in Fig. 7. The quantum circuits in Fig. 8(a) and Fig. 8(b) for realizing isomorphic mappings are denoted as ϕ^{-1} and ϕ respectively. The quantum circuit in Fig. 9 is denoted as λ. In addition, in order to use as few auxiliary qubits as possible, we need to restore some registers. At this time, we only need to add the original quantum circuit in reverse order. The inverse quantum circuit in Fig. 2 is recorded as S^{-1} and the inverse circuit in Fig. 9 is recorded as λ^{-1}. According to Eq. (2), the logic diagram of the quantum circuit for multiplicative inverse over GF(2^8) can be obtained as shown in Fig. 10 and the specific quantum circuit diagrams are shown in the appendixes.

In this diagram, a, b, c and d are all 4-qubit registers, and e is a 5-qubit register. Except that the multiplicative inverse over GF(2^4) needs to use the 5th qubit of register e, other operations only use the first 4 qubits. During initialization, the value of register a is the lower 4 qubits of the input, b is the upper 4 qubits of the input, and the value of each qubit of c, d, and e is $|0\rangle$. After the operation of this circuit diagram, register c is the lower 4 qubits of the output, and d is the upper 4 qubits of the output. The quantum circuit in Fig. 10, which is verified by the Aer simulator of the IBM quantum platform, is completely correct. If we want to use fewer Toffoli gates, the quantum circuit of the multiplication over GF(2^4) in Appendix A can be replaced with Fig. 6, see Appendix B for the specific quantum circuit. We can analyze the quantum resources used by them as shown in Table 2.

4.6 Quantum circuit of S-box of AES cryptographic algorithm

As an example of the application of quantum circuit for GF(2^8) multiplicative inverse, we will apply them to the implementations of quantum circuit of the S-box of AES cryptographic algorithm. The S-box function of an input α is defined as

$$\mathrm{Sbox}(a) = A\left(\alpha^{-1}\right) = \mathbf{F}\alpha^{-1} \oplus \nu, \tag{18}$$

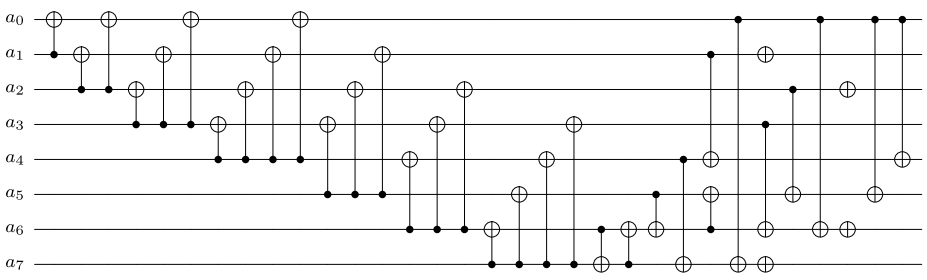


Figure 11 The quantum circuit of the affine transformation A

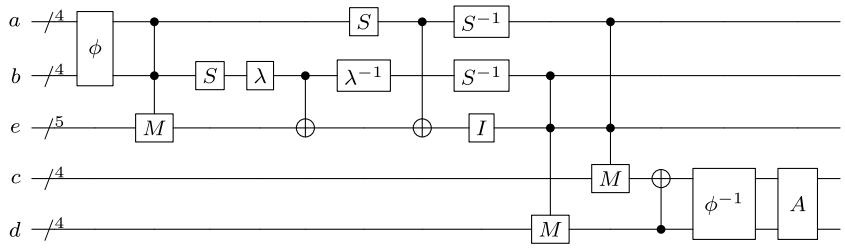


Figure 12 The logic diagram of the quantum circuit for S-box of AES cryptographic algorithm

where α^{-1} is the multiplicative inverse in GF(2^8) with the irreducible polynomial $f(x) = x^8 + x^4 + x^3 + x + 1$, ν is the column vector over GF(2), that is, $\nu = (0, 1, 1, 0, 0, 0, 1, 1)^T$, and

$$\mathbf{F} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{19}$$

Then the quantum circuit of the affine transformation A can be synthesised as Fig. 11.

After the quantum circuit of the affine transformation A is realized, we only need to add it to the output of the inverse quantum circuit in Fig. 10 to synthesize the quantum circuit of the S-box. We denote the quantum circuit of the affine transformation A in Fig. 11 as A for the convenience of description, the logic diagram of the quantum circuit for S-box of AES cryptographic algorithm as shown in Fig. 12.

When synthesizing the quantum circuit of S-box, if the value of $F \cdot \phi^{-1}$ is calculated first and then their calculation results are synthesized, the quantum circuit will use fewer CNOT gates than by synthesizing the two matrices respectively. Therefore, this strategy is adopted in our specific implementation scheme. The quantum circuit in Appendix A is used as the multiplicative inverse over GF(2^8) to realize the specific quantum circuit of the S-box of AES, see Appendix C, and the quantum circuit in Appendix B as the multiplicative inverse to realize the specific quantum circuit of the S-box of AES, see Appendix D. Next,

Table 3 The quantum resources for quantum circuits of S-box of AES cryptographic algorithm

Schemes	Qubits	Toffoli gates	CNOT gates	NOT gates	Quantum cost
Ref. [1]	56	448	494	4	2738
Ref. [8]	32	55	314	4	593
Ref. [23]	26	46	304	4	538
Appendix C	21	55	131	4	410
Appendix D	21	37	233	4	422

we compare the quantum resources used by our works and the existing quantum circuits that implement the S-box of the AES cryptographic algorithm, as shown in Table 3.

As can be seen from Table 3, 4 NOT gates need to be used in all the quantum circuits to realize the S-box of AES. We only need 21 qubits in both the two schemes, which is less than the existing schemes. The quantum circuit in Appendix C uses the lowest CNOT gates and quantum cost among the existing schemes. The Toffoli gates used in the quantum circuit in Appendix D is the lowest among the existing schemes. It uses only slightly more quantum cost than the quantum circuit in Appendix C, and less than other existing schemes.

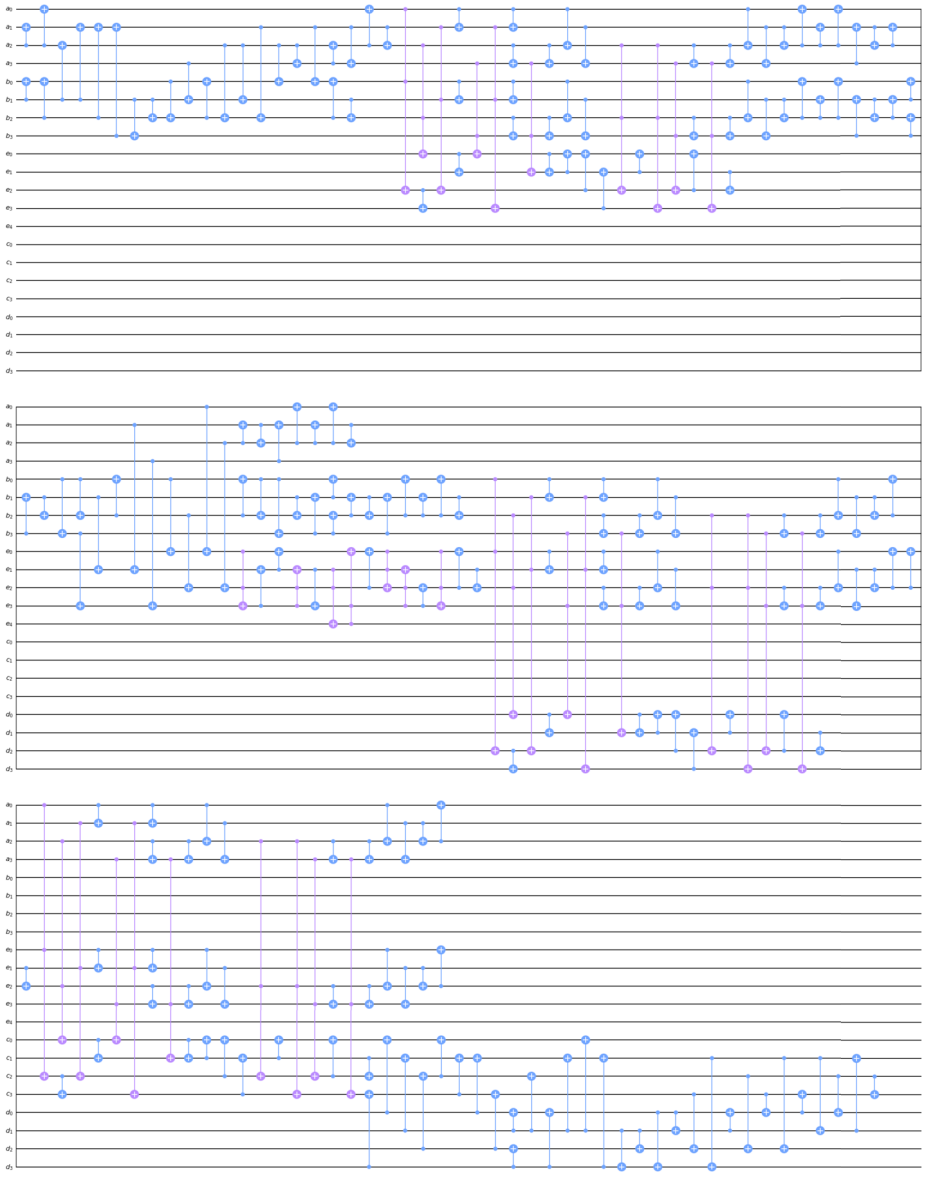
5 Discussion and conclusion

Among the basic arithmetic operations over finite fields, the computation of multiplicative inverse is the most time consuming operation. In this paper, we mainly discuss the synthesis of quantum circuits for multiplicative inverse over GF(2^8). We first convert the multiplicative inverse operation in GF(2^8) to arithmetic operations in the composite field GF((2^4)^2), and then discuss the expressions of the square calculation, the inversion calculation and the multiplication calculation separately in the finite field GF(2^4), where the expressions of multiplication calculation in GF(2^4) are given directly in GF(2^4) and given through being transformed into the composite field GF((2^2)^2). Then the quantum circuits of these calculations are realized one by one. Finally, two quantum circuits for multiplicative inverse over GF(2^8) are synthesized. They both use 21 qubits, the first quantum circuit uses 55 Toffoli gates and 107 CNOT gates and the second one uses 37 Toffoli gates and 209 CNOT gates. As an example of the application of multiplication inverse, we apply these quantum circuits to the implementations of the S-box quantum circuit of the AES cryptographic algorithm. Two quantum circuits for implementing the S-box of the AES cryptographic algorithm are presented. The first quantum circuit uses 21 qubits, 55 Toffoli gates, 131 CNOT gates and 4 NOT gates and the second one uses 21 qubits, 37 Toffoli gates, 233 CNOT gates and 4 NOT gates. Through the evaluation of quantum cost, the two quantum circuits of the S-box of AES cryptographic algorithm use less quantum resources than the existing schemes.

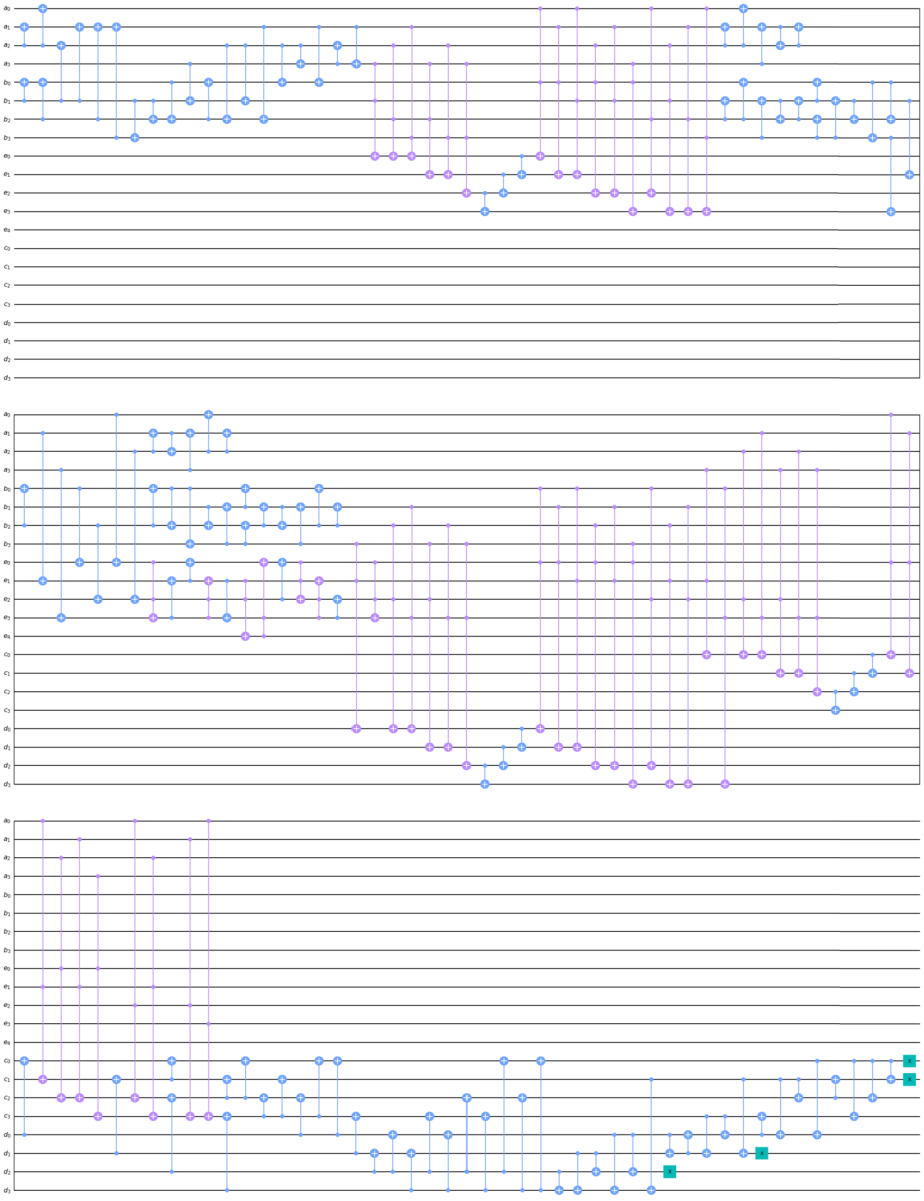
The work that can be done next: on one hand, the optimization of the implementation method of the linear transformation quantum circuit represented by a matrix, we use the Gaussian elimination method in this paper to achieve it, and whether there are other better methods is worth discussing. On the other hand, whether the normal basis representation can reduce the use of quantum resources? In this paper, all the elements in finite fields are represented by polynomial basis. The normal basis representation can indeed optimize the classical circuit of S-box [4], and it is also worth investigating whether this representation can optimize quantum circuit of S-box.

Appendix A: The quantum circuit of multiplicative inverse over GF(2^8) where multiplication in GF(2^4) realized by using Fig. 3

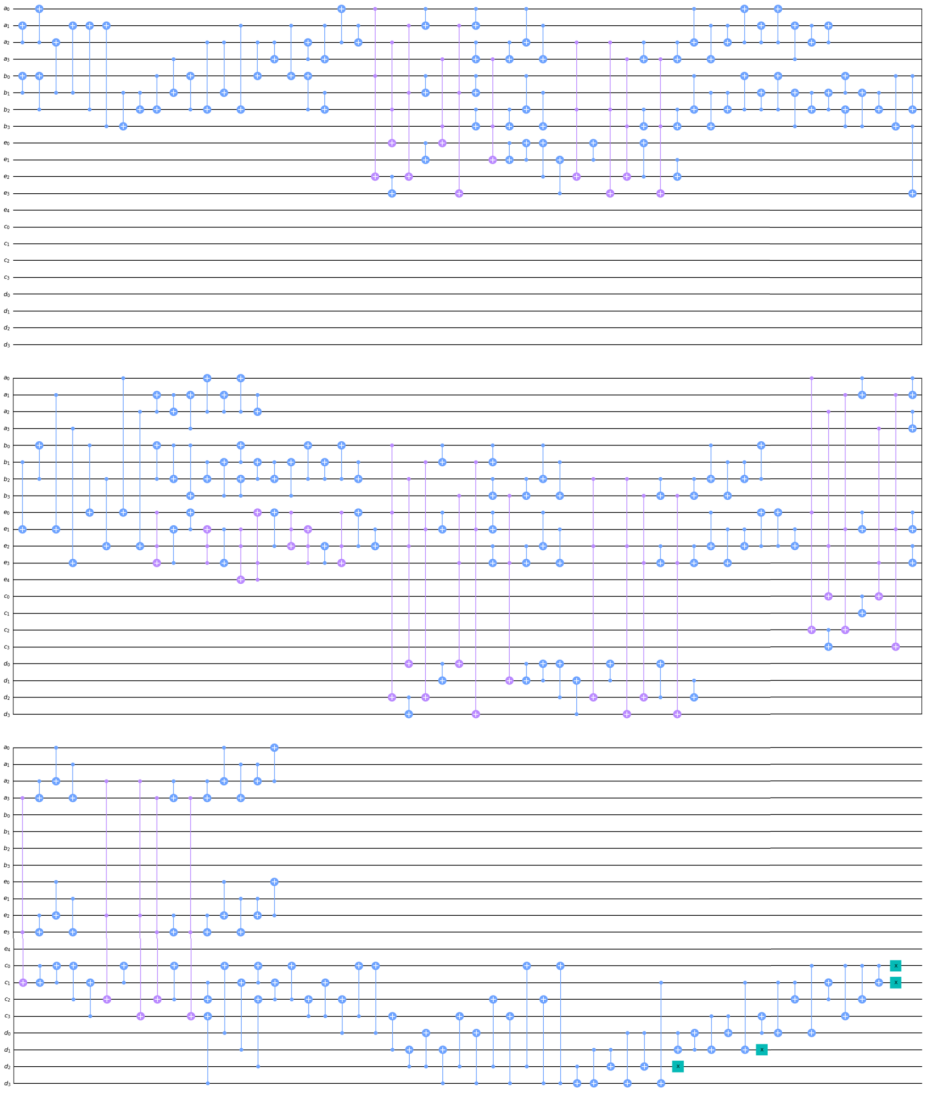
Appendix B: The quantum circuit of multiplicative inverse over GF(2^8) where multiplication in GF(2^4) realized by using Fig. 6



Appendix C: The quantum circuit of the S-box of AES cryptographic algorithm where multiplicative inverse over GF(2^8) realized by using Appendix A



Appendix D: The quantum circuit of the S-box of AES cryptographic algorithm where multiplicative inverse over GF(2^8) realized by using Appendix B



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.

Funding
This work is supported by the Natural Sciences Foundation of Hubei Province (Grant No. 2020CFB326), the Natural Science Foundation of Fujian Province (Grant No. 2020J01812),the National Key R&D Program of China (Grant No. 2018YFA0306703), Chengdu Innovation and Technology Project(Grant No.2021-YF05-02414-GX), and the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (Grant No. SKLACSS-202105).

Abbreviations
Not applicable.

Availability of data and materials
All data generated or analysed during this study are included in this published article.

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

Author details
[1]Department of Computer Science and Technology, School of Information 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. [4]Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu University of Information Technology, Chengdu, Sichuan 610225, China.

Publisher's Note

Received: 10 February 2022 Accepted: 21 September 2022 Published online: 07 October 2022

References

1. Almazrooie M, Samsudin A, Abdullah R et al. Quantum reversible circuit of AES-128. Quantum Inf Process. 2018;17(5):1–30.
2. Aoki K, Ichikawa T, Kanda M et al. Camellia: a 128-bit block cipher suitable for multiple platforms—design andanalysis. In: International workshop on selected areas in cryptography. Berlin: Springer; 2000. p. 39–56.
3. Bennett C. Logical reversibility of computation. IBM J Res Dev. 1973;17(6):525–32.
4. Canright D. A very compact S-box for AES. In: International workshop on cryptographic hardware and embedded systems. Berlin: Springer; 2005. p. 441–55.
5. FIPS Pub. 197: specification for the AES. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (2001).
6. 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.
7. Itoh T, Tsujii S. A fast algorithm for computing multiplicative inverses in GF(2m) using normal bases. Inf Comput. 1988;78(3):171–7.
8. 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.
9. Li Z, Chen H, Xu B et al. Fast algorithm for 4-qubit reversible logic circuits synthesis. In: 2008 IEEE congress on evolutionary computation. 2008. p. 2202–7.
10. Liu F, Ji W, Hu L et al. Analysis of the SMS4 block cipher. In: Information security and privacy. Berlin: Springer; 2007. p. 158–70.
11. 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.
12. Luo QB, Li XY, Yang GW, et al. Quantum Circuit Implementation of S-box for SM4 Cryptographic Algorithm Based on Composite Field Arithmetic. J Univ Electron Sci Tech China. (2022). To appear.
13. Lv SW, Su BZ, Wang P et al. Overview on SM4 algorithm. J Infor Sec Res. 2016;2(11):995–1007.
14. Nielsen MA, Chuang I. Quantum computation and quantum information. Cambridge: Cambridge University Press; 2002.
15. Reyhani-Masoleh A, Hasan MA. Low complexity bit parallel architectures for polynomial basis multiplication over GF(2m). IEEE Trans Comput. 2004;53(8):945–59.
16. Saravanan P, Kalpana P. Novel reversible design of advanced encryption standard cryptographic algorithm for wireless sensor networks. Wirel Pers Commun. 2018;100(4):1427–58.
17. Satoh A, Morioka S, Takano K et al. A compact Rijndael hardware architecture with S-box optimization. In: International conference on the theory and application of cryptology and information security. Berlin: Springer; 2001. p. 239–54.
18. Shende VV, Markov IL. On the CNOT-cost of TOFFOLI gates. arXiv:0803.2316 (2008).
19. 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.
20. Thapliyal H, Ranganathan N. Design of reversible latches optimized for quantum cost, delay and garbage outputs. In: 2010 23rd international conference on VLSI design. 2010. p. 235–40.
21. Wang CC, Truong TK, Shao HM et al. VLSI architectures for computing multiplications and inverses in GF(2m). IEEE Trans Comput. 1985;100(8):709–17.
22. Yang G, Song X, Hung WN et al. Bi-directional synthesis of 4-bit reversible circuits. Comput J. 2008;51(2):207–15.
23. Zou J, Liu Y, Dong C et al. Observations on the Quantum Circuit of the SBox of AES. IACR Cryptol. ePrint Arch. 2019;1245.