基于复合域 SM4 密码算法 S 盒的量子电路实现

罗庆斌[1,2]，李晓瑜[2*]，杨国武[3]，牛伟纳[3]，李 强[1]

(1. 湖北民族大学智能科学与工程学院 湖北 恩施 445000；2. 电子科技大学信息与软件工程学院 成都 610054；
3. 电子科技大学计算机科学与工程学院 成都 611731)

【摘要】S 盒是 SM4 分组密码算法中重要的非线性组件。使用 Toffoli 门、CNOT 门和 NOT 门构建 S 盒的量子电路。首先，基于 S 盒的代数表达式，通过同构映射矩阵，将有限域GF(2^8)中的求逆运算转化到有限域GF((2^4)^2)中的运算；其次，在GF(2^4)中分别给出了平方计算、乘法计算和求逆运算的量子电路；再次，通过最小化同构矩阵中“1”元素的个数，求出最优的同构映射矩阵，并给出相应的量子电路；然后，通过高斯消元法给出 S 盒表达式中仿射变换的量子电路；最后，综合出 SM4 密码算法 S 盒的量子电路。该量子电路的正确性通过 IBM 量子平台的 Aer 模拟器进行了验证。复杂度分析表明：所给出 S 盒的量子电路一共使用了 21 个量子比特，55 个 Toffoli 门、176 个 CNOT 门和 10 个 NOT 门，电路深度为 151。相比于已有结果，所使用的量子资源进一步减少，效率进一步提高。

关 键 词 代数运算； 复合域； 量子电路； S 盒； SM4

中图分类号 TP309 **文献标志码** A doi:10.12178/1001-0548.2022033

Quantum Circuit Implementation of S-box for SM4 Cryptographic Algorithm Based on Composite Field Arithmetic

LUO Qingbin[1,2], LI Xiaoyu[2*], YANG Guowu[3], NIU Weina[3], and LI Qiang[1]

(1. College of Intelligent Systems Science and Engineering, Hubei Minzu University Enshi Hubei 445000;
2. School of Information and Software Engineering, University of Electronic Science and Technology of China Chengdu 610054;
3. School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract The S-box is an important nonlinear component in SM4 block cipher algorithm. In this paper, Toffoli gates, CNOT gates and NOT gates are used to construct the quantum circuit of the S-box. Based on the algebraic expression of the S-box, the inverse operation in finite field GF(2^8) is transformed into operations in finite field GF((2^4)^2) through isomorphic mapping matrices. The quantum circuits of square calculation, multiplication calculation and inversion operation in GF(2^4) are given respectively. By minimizing the number of "1" elements in the isomorphic matrices, the optimal isomorphic mapping matrices are obtained, and the corresponding quantum circuits are given. Then, the quantum circuit of affine transformation in S-box expression is given by Gaussian elimination method; Finally, the quantum circuit of S-box in SM4 cryptographic algorithm is synthesized. The correctness of the quantum circuit is verified by the Aer simulator of IBM quantum platform. The complexity analysis shows that the given quantum circuit of the S-box uses 21 qubits, 55 Toffoli gates, 176 CNOT gates and 10 NOT gates, and the circuit depth is 151. Compared with the existing results, the quantum resources used are further reduced and the efficiency is further improved.

Key words algebraic operation; composite field; quantum circuit; S box; SM4

自从 Shor 算法[1] 提出以来，利用量子技术对现代密码算法的分析便受到研究者们的关注。在对称密码算法的分析中，文献 [2] 首先分析了量子技术对对称密码算法的影响，如 Grover 算法[3] 可以平方加速密钥搜索速度，建议把密钥长度至少增加一倍以达到非量子环境下的安全强度。文献 [4] 利

收稿日期：2022－01－22；修回日期：2022－03－28
基金项目：国家自然科学基金 (61772006)；国家重点研发计划 (2018YFA0306703)；湖北省自然科学基金 (2020CFB326)；广西省自然科学基金 (2019GXNSFAA185033)；福建省自然科学基金 (2020J01812)
作者简介：罗庆斌 (1987－)，男，博士，主要从事量子计算和量子密码方面的研究.
*通信作者：李晓瑜，E-mail：xiaoyuuestc@uestc.edu.cn

用 Simon 算法[5] 可以快速寻找碰撞周期的特性分析对称密码系统的安全性，大幅提升了查询效率。随后，结合 Grover 算法和 Simon 算法对具有不同结构或不同加密方式的对称密码算法分析方案被提出[6-8]。

这些安全分析大多需要对对称密码算法量子电路实现的资源进行评估，因此对称密码算法的量子电路实现近几年也得到了大量关注。此外，量子逻辑门都是可逆的，使用量子电路实现的密码算法在执行过程中不会有能量的耗散，因此可以抵抗各种和能量分析相关的侧信道分析攻击[9]，这是对称密码算法量子电路实现受到关注的另一原因。

在现有的对称密码算法量子电路实现方案中，S 盒作为密码组件的非线性结构，一直是研究的重点。文献 [10] 首先对 AES 密码算法中综合 S 盒所需的量子电路资源用两种方案进行了评估：方案一主要采用 Itoh-Tsujii 算法[11] 进行评估，一共需要使用 40 个量子比特，3 584 个 T 门和 4 569 个 Clifford 门；方案二主要使用稳定子链技术[12] 进行评估，一共使用 9 个量子比特，不超过 9 695 个 T 门和 12 631 个 Clifford 门。但这两种方案中只评估了实现 S 盒时所需的量子资源，并没有给出具体的量子线路。文献 [13] 主要使用 Itoh-Tsujii 算法[11] 具体实现了 AES 密码算法 S 盒的量子电路，一共使用了 56 个量子比特，448 个 Toffoli 门，494 个 CNOT 门和 4 个 NOT 门。通过优化 AES 密码算法 S 盒中每个输出的布尔表达式，文献 [14] 给出的量子电路一共使用了 32 个量子比特，55 个 Toffoli 门，314 个 CNOT 门和 4 个 NOT 门。通过对 S 盒中输出布尔表达式的进一步优化，文献 [15] 设计的 AES 密码算法 S 盒的量子电路一共使用 26 个量子比特，46 个 Toffoli 门，304 个 CNOT 门和 4 个 NOT 门。

本文主要研究 SM4 密码算法 S 盒的量子电路实现。SM4 密码算法是用于 WAPI 的分组密码算法，2006 年由我国国家密码管理局公开发布[16]，2021 年 6 月发布成为国际标准[17](标准号为 ISO/IEC 18033-3：2010/AMD1：2021)。目前对于 SM4 密码算法量子电路实现的研究较少。文献 [18] 实现了 SM4 密码算法的 S 盒，一共使用了 48 个量子比特，592 个量子门，电路深度为 289。文献 [19] 实现的 SM4 密码算法的 S 盒中添加了 14 个辅助量子比特，加上输入和输出的量子比特，一共需要 30 个量子比特，82 个 Toffoli 门，510 个 CNOT 门和 87 个 X 门。X 门和 NOT 门是等价的，所以本文中不区分 X 门和 NOT 门。本文主要通过把 $GF(2^8)$中的运算同构到$GF((2^4)^2)$中，使用 NOT 门、CNOT 门和 Toffoli 门构建实现 S 盒的量子电路。所使用的量子比特，量子门的数量，量子电路的深度等量子资源相比于文献 [19] 都有较大的减少。

1　SM4 密码算法的 S 盒

1.1　S 盒的代数结构

SM4 密码算法的加解密过程可以参看文献 [20]，这里不再赘述。S 盒是 SM4 密码算法中唯一的非线性变换，是保证算法安全性的关键组件，通常由 256 个元素构成的查询表进行描述。文献 [21] 研究了 S 盒的代数结构，并给出了具体表达式：

$$S(\boldsymbol{\alpha}) = A_2 \cdot I \cdot A_1(\boldsymbol{\alpha}) \quad \forall \boldsymbol{\alpha} \in \mathrm{GF}(2^8) \tag{1}$$

式中，I是$GF(2^8)$上的乘法逆元，所用到的不可约多项式为：

$$f(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1 \tag{2}$$

A_1和A_2是如下的仿射变换：

$$A_1 = A_2 = \boldsymbol{\alpha} \cdot \boldsymbol{F} + \boldsymbol{\nu} \tag{3}$$

式中，$\boldsymbol{F}$是$GF(2)$上8×8的矩阵，具体值如下：

$$\boldsymbol{F} = \begin{pmatrix} 1&1&1&0&0&1&0&1 \\ 1&1&1&1&0&0&1&0 \\ 0&1&1&1&1&0&0&1 \\ 1&0&1&1&1&1&0&0 \\ 0&1&0&1&1&1&1&0 \\ 0&0&1&0&1&1&1&1 \\ 1&0&0&1&0&1&1&1 \\ 1&1&0&0&1&0&1&1 \end{pmatrix} \tag{4}$$

$\boldsymbol{\nu}$是$GF(2)$上的向量，$\boldsymbol{\nu} = (1,1,0,0,1,0,1,1)$。

1.2　S 盒的分解

S 盒事实上是一个 8 量子比特的逻辑函数，8 量子比特的逻辑函数一共有$2^8!$个。对于任意给定的 8 量子比特的逻辑函数，目前还没有有效的算法对其综合。在式 (1) 中，仿射变换式 (3) 可以通过高斯消元法先综合出矩阵$\boldsymbol{F}$，再通过在对应位置添加 NOT 门的方式综合出$\boldsymbol{\nu}$的方式完成。接下来主要是综合出$GF(2^8)$上的乘法逆元运算$\boldsymbol{I}$，虽然它可以看成是由对换构成的置换，但依然没有有效的综合算法。本文策略是将$GF(2^8)$上的求逆运算同构到$GF((2^4)^2)$上的运算。当然，对于$GF(2^4)$上的运算可以进一步同构到$GF((2^2)^2)$中的运算，从而将$GF(2^8)$中的求逆运算同构到 $GF(((2^2)^2)^2)$中的运算。

但在GF((2²)²)上实现GF(2⁴)上的求逆等运算时不得不添加更多的辅助量子比特。另外，对于大多数4量子比特逻辑函数，可以采用双向综合[22]等方法实现。因此，只需将GF(2⁸)上的求逆运算同构到GF((2⁴)²)上的运算。实现S盒的整体框架如图1所示。

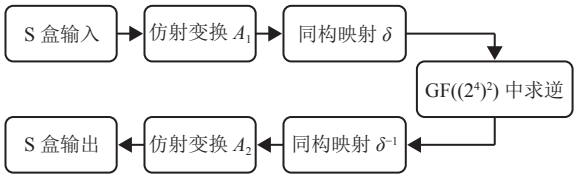

图1 SM4密码算法S盒复合域实现框架图

2 复合域中的运算

由文献[21]可知，SM4密码算法求逆运算用到的不可约多项式为式(2)中的$f(x)$，即运算中用到的有限域$\mathrm{GF}(2^8)\cong\mathrm{GF}(2)[x]/(f(x))$。因为同构关系，所以当给定$n$次不可约多项式$g(x)$时，文中不再区分$\mathrm{GF}(2^n)$和$\mathrm{GF}(2)[x]/(g(x))$。设$X$为$f(x)$的一个根，对于$\forall\boldsymbol{\alpha}\in\mathrm{GF}(2^8)$有：

$$\boldsymbol{\alpha}=\sum_{i=0}^{7}\alpha_i X^i\quad \alpha_i\in\mathrm{GF}(2) \tag{5}$$

同理，取不可约多项式$p(y)=y^2+\mu y+\lambda$，其中$\mu,\lambda\in\mathrm{GF}(2^4)$，设$Y$是$p(y)$的一个根，则对于$\forall\boldsymbol{r}\in\mathrm{GF}((2^4)^2)$有：

$$\boldsymbol{r}=r_1Y+r_0\ r_1,r_0\in\mathrm{GF}(2^4) \tag{6}$$

对于任意元素$\boldsymbol{r}\in\mathrm{GF}((2^4)^2)$，求得其逆元为：

$$\begin{aligned}\boldsymbol{r}^{-1}=&r_1(r_0^2+r_0r_1\mu+r_1^2\lambda)^{-1}Y+\\&(r_0+\mu r_1)(r_0^2+r_0r_1\mu+r_1^2\lambda)^{-1}\end{aligned} \tag{7}$$

为了计算简便，取$\mu=1$，则不可约多项式$p(y)=y^2+y+\lambda$，式(7)变为：

$$\begin{aligned}\boldsymbol{r}^{-1}=&r_1(r_0^2+r_0r_1+r_1^2\lambda)^{-1}Y+\\&(r_0+r_1)(r_0^2+r_0r_1+r_1^2\lambda)^{-1}\end{aligned} \tag{8}$$

从式(8)可知，为了求$\boldsymbol{r}^{-1}$，需要在$\mathrm{GF}(2^4)$中进行运算，因此需要在$\mathrm{GF}(2^4)$中选取一个不可约多项式。考虑到这些运算的执行效率，在3个4次不可约多项式中选取$q(z)=z^4+z+1$。设Z是$q(z)$的一个根，则对于$\forall\boldsymbol{a}\in\mathrm{GF}(2^4)$有：

$$\boldsymbol{a}=\sum_{i=0}^{3}a_iZ^i\quad a_i\in\mathrm{GF}(2) \tag{9}$$

3 基本组件的量子电路

由图1所示，为了实现SM4密码算法的S盒，需要分别实现$\mathrm{GF}((2^4)^2)$中的求逆运算，同构映射δ和同构映射δ^{-1}，以及仿射变换A_1和A_2。下面分别描述它们的量子电路，文中的量子电路主要使用python语言并利用qiskit软件包实现。

3.1 $\mathrm{GF}((2^4)^2)$求逆的基本量子电路

从式(8)可知，为了求$\boldsymbol{r}^{-1}$，需要在$\mathrm{GF}(2^4)$做加法、平方、乘法和求逆运算。加法运算可以直接通过在对应位置添加CNOT门完成，这里不再讨论。下面先讨论平方运算。因为有限域$\mathrm{GF}(2^4)$的特征为2，所以，对于任意元素$\boldsymbol{a}=\sum_{i=0}^{3}a_iZ^i\in\mathrm{GF}(2^4)$有：

$$\boldsymbol{a}^2=\left(\sum_{i=0}^{3}a_ix^i\right)^2=\sum_{i=0}^{3}a_ix^{2i} \tag{10}$$

因此，对于$\forall\boldsymbol{a}\in\mathrm{GF}(2^4)$，可以找到如下的矩阵$\boldsymbol{S}$使得$\boldsymbol{a}^2=\boldsymbol{S}\cdot\boldsymbol{a}$，其中，

$$\boldsymbol{S}=\begin{pmatrix}1&0&1&0\\0&0&1&0\\0&1&0&1\\0&0&0&1\end{pmatrix} \tag{11}$$

利用高斯消元法，可以实现其量子电路如图2所示。

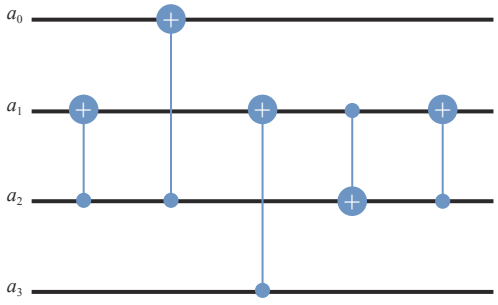

图2 实现式(10)平方计算的量子电路图

对于乘法计算，由文献[23]定理1可以得出：对于$\forall\boldsymbol{a},\boldsymbol{b}\in\mathrm{GF}(2^4)$，记$\boldsymbol{c}=\boldsymbol{a}\cdot\boldsymbol{b}$，有：

$$\boldsymbol{c}=\boldsymbol{d}+\boldsymbol{Q}^{\mathrm{T}}\cdot\boldsymbol{e} \tag{12}$$

其中，

$$\boldsymbol{d}=\begin{pmatrix}d_0\\d_1\\d_2\\d_3\end{pmatrix}=\boldsymbol{L}\cdot\boldsymbol{b}=\begin{pmatrix}a_0&0&0&0\\a_1&a_0&0&0\\a_2&a_1&a_0&0\\a_3&a_2&a_1&a_0\end{pmatrix}\cdot\begin{pmatrix}b_0\\b_1\\b_2\\b_3\end{pmatrix} \tag{13}$$

$$\boldsymbol{e}=\begin{pmatrix}e_0\\e_1\\e_2\\e_3\end{pmatrix}=\boldsymbol{U}\cdot\boldsymbol{b}=\begin{pmatrix}0&a_3&a_2&a_1\\0&0&a_3&a_2\\0&0&0&a_3\end{pmatrix}\cdot\begin{pmatrix}b_0\\b_1\\b_2\\b_3\end{pmatrix} \tag{14}$$

式中，a_i和b_i分别是$\boldsymbol{a}$和$\boldsymbol{b}$和对应位置上的元素，可以计算出：

$$\boldsymbol{Q}^{\mathrm{T}}=\begin{pmatrix}1&0&0&0\\1&1&0&0\\0&1&1&0\\0&0&1&0\end{pmatrix} \tag{15}$$

于是，可以实现$\boldsymbol{a}$和$\boldsymbol{b}$乘积的量子电路如图 3 所示。

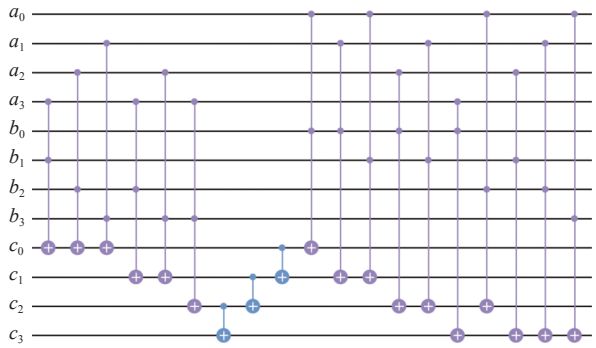

图 3　式 (12) 中乘法计算的量子电路图

对于乘法求逆运算，首先将其表示成如下置换：

$$(2,9)(3,14)(4,13)(5,11)(6,7)(8,15)(10,12) \tag{16}$$

显然，这是由 7 个对换构成的奇置换。但 4 量子比特中的 NOT 门，CNOT 门和 Toffoli 门全都是偶置换，这意味着仅使用 NCT 库中的逻辑门综合出的 4 量子比特量子电路不能实现GF(2^4)中的求逆运算。本文策略是添加一个辅助量子比特，先综合出一个奇置换。这里先用两个 Toffoli 门，借助辅助量子比特综合出置换(14,15)，然后使用文献[22] 中的双向综合算法实现出求逆运算的量子电路如图 4 所示。图中a_4是辅助量子比特。

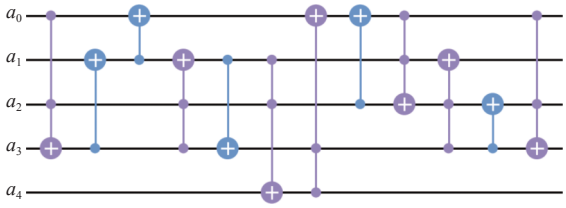

图 4　实现乘法求逆运算的量子电路图

有了这些基本量子电路图，便可以非常容易地实现式 (8) 中GF($(2^4)^2$)内的求逆运算。

3.2　同构映射的量子电路图

在讨论同构映射δ和δ^{-1}的量子电路之前，先讨论它们的构造。事实上，GF(2^8)中含有与GF(2^4)同构的子域，也含有GF($(2^4)^2$)同构的子域，可以把Y和Z用GF(2^8)中的元素表示，则GF($(2^4)^2$)的基也可以用GF(2^8)中的元素表示，于是有：

$$\delta^{-1}=[1,Z,Z^2,Z^3,Y,YZ,YZ^2,YZ^3] \tag{17}$$

由$(\delta^{-1})^{-1}=\delta$可以求出同构映射$\delta$。

接下来，讨论同构映射的选取。GF($(2^4)^2$)中，形如$p(y)=y^2+y+\lambda$的不可约多项式共有 8 个，每个多项式都有 2 个根。$q(z)$共有 4 个根。因此，一共有 64 组同构映射。为了在实现同构映射时尽可能少地使用量子门，选取元素“1”的个数最少的一组。经计算，这 64 组中δ和δ^{-1}最少共有 44 个“1”。此时，$Y=0\mathrm{xC5}$，$Z=0\mathrm{x50}$，$\lambda=0\mathrm{xF}$。同构映射为：

$$\delta=\begin{pmatrix}1&0&1&0&0&0&0&0\\0&1&0&0&1&0&0&0\\0&0&1&0&0&0&0&1\\0&0&0&0&1&1&1&1\\0&0&0&0&0&0&0&1\\0&1&0&0&0&1&0&0\\0&0&0&0&1&0&1&1\\0&1&1&1&1&0&1&0\end{pmatrix} \tag{18}$$

$$\delta^{-1}=\begin{pmatrix}1&0&1&0&1&0&0&0\\0&0&0&1&0&1&1&0\\0&0&1&0&1&0&0&0\\0&0&1&1&0&1&0&1\\0&1&0&1&0&1&1&0\\0&0&0&1&0&0&1&0\\0&1&0&1&1&1&0&0\\0&0&0&0&1&0&0&0\end{pmatrix} \tag{19}$$

利用高斯消元法可以综合出δ和δ^{-1}的量子电路分别如图 5 和图 6 所示。

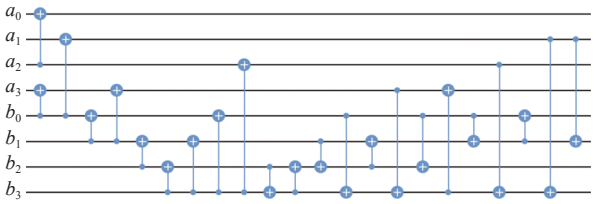

图 5　同构映射δ的量子电路图

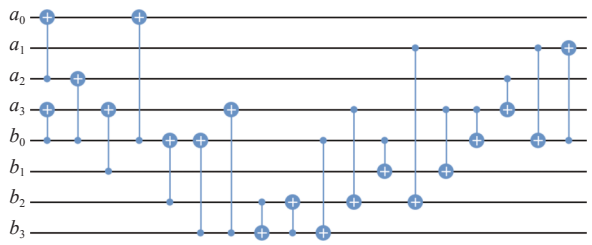

图 6　同构映射δ^{-1}的量子电路图

当$\lambda=0\mathrm{xF}$时，对于$\forall\boldsymbol{a}\in\mathrm{GF}(2^4)$，计算$\lambda\cdot\boldsymbol{a}$的值等价于计算矩阵$\boldsymbol{\lambda}$乘以$\boldsymbol{a}$的值，其中，

$$\boldsymbol{\lambda}=\begin{pmatrix}1&1&1&1\\1&0&0&0\\1&1&0&0\\1&1&1&0\end{pmatrix} \tag{20}$$

其量子电路如图 7 所示。

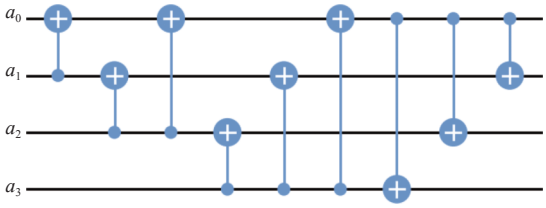

图 7 乘以常数λ的量子电路

3.3 仿射变换的量子电路图

仿射变换式 (3) 中$\boldsymbol{F}$和$\boldsymbol{\nu}$的值都已经给出，所以可以综合出其量子电路如图 8 所示。

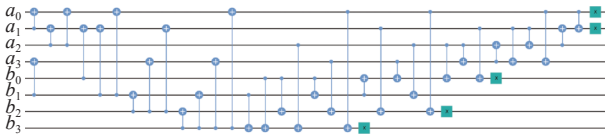

图 8 式 (3) 中仿射变换的量子电路图

4 S 盒的量子电路图

4.1 量子电路图

为了描述方便，记S为图 2 中实现平方计算的电路图，图 3 中实现乘法计算量子电路的乘数分别记为两个实心圆点，结果记为M。I为图 4 中求逆运算的量子电路图，图 5 和图 6 中实现同构映射的电路图分别记为δ和δ^{-1}，图 7 中的量子电路记为λ，A_1和A_2为图 8 中仿射变换的量子电路图。此外，为了尽可能少地使用辅助量子比特，需要把一些寄存器还原，此时只需逆序添加原来的量子电路即可，图 2 的逆电路记为S^{-1}，图 7 的逆电路记为λ^{-1}。根据图 1 和式 (8) 可以得出 SM4 密码算法的量子电路逻辑图如图 9 所示，具体的量子电路图如图 10 所示。图 9 中 a,b,c,d 都是 4 量子比特寄存器，e 是 5 量子比特寄存器。除了求逆操作需要用到寄存器 e 的第 5 位外，其他操作都只用到前面的 4 位。初始化时，寄存器 a 的值为 S 盒输入的低 4 位，b 为 S 盒输入的高 4 位，c,d,e 每一位上的值都为$|0\rangle$。经过该电路图运算后，寄存器 c 输出 S 盒输出的低 4 位，d 输出 S 盒输出的高 4 位。通过 IBM 量子平台的 Aer 模拟器验证，该量子电路图是完全正确的。

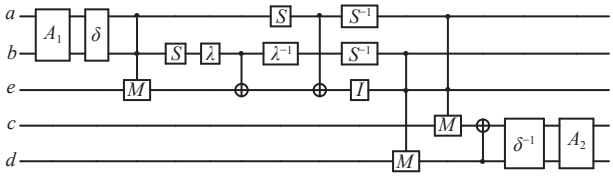

图 9 S 盒的量子电路示意图

4.2 量子电路复杂度分析

文中的量子电路是通过 NOT 门、CNOT 门和 Toffoli 门实现的。通过计算 S 盒量子电路的比特数和所使用的量子门的数量刻画电路的复杂度。在 S 盒实现的量子电路中，a,b,c,d 都是 4 量子比特寄存器，e 是 5 量子比特寄存器，所有一共使用了 21 量子比特。现在计算量子门的数量，仿射变换A_1和A_2其实是一样的，它们的电路图都使用了 35 个 CNOT 门，和 5 个 NOT 门；同构映射δ的电路图共使用了 23 个 CNOT 门；δ^{-1}的电路图共使用 19 个 CNOT 门；平方计算S的电路图和它的逆电路图都使用了 5 个 CNOT 门，它们在 S 盒的量子电路图中都使用了 2 次；乘以常数λ的量子电路和它的逆电路都使用了 9 个 CNOT 门；乘法计算的量子电路共使用了 16 个 Toffoli 门和 3 个 CNOT 门，S 盒的量子电路图中共使用了 3 次乘法计算；乘法逆运算的电路图共使用了 7 个 Toffoli 门和 5 个 CNOT 门；此外还使用了 3 组共 12 个 CNOT 门做量子比特的复制。最终本文实现整个 S 盒所使用的量子资源，和文献 [19] 使用量子资源的对比情况如表 1 所示。

表 1 文献 [19] 与本文综合 S 盒所用量子资源对比表

个

量子资源	文献[19]	本文
量子比特	30	21
Toffoli门	82	55
CNOT门	510	176
NOT门	87	10

由表 1 可以看出，实现 SM4 密码算法 S 盒文献 [19] 需要使用 30 个量子比特，82 个 Toffoli 门，510 个 CNOT 门和 87 个 NOT 门。采用本文提出的方法只需要使用 21 个量子比特，55 个 Toffoli 门，176 个 CNOT 门和 10 个 NOT 门。此外，还计算出本文中实现的 SM4 算法 S 盒量子电路的深度为 151。由此可以看出：本文实现的方法的效率在文献 [19] 的基础上有显著提高。

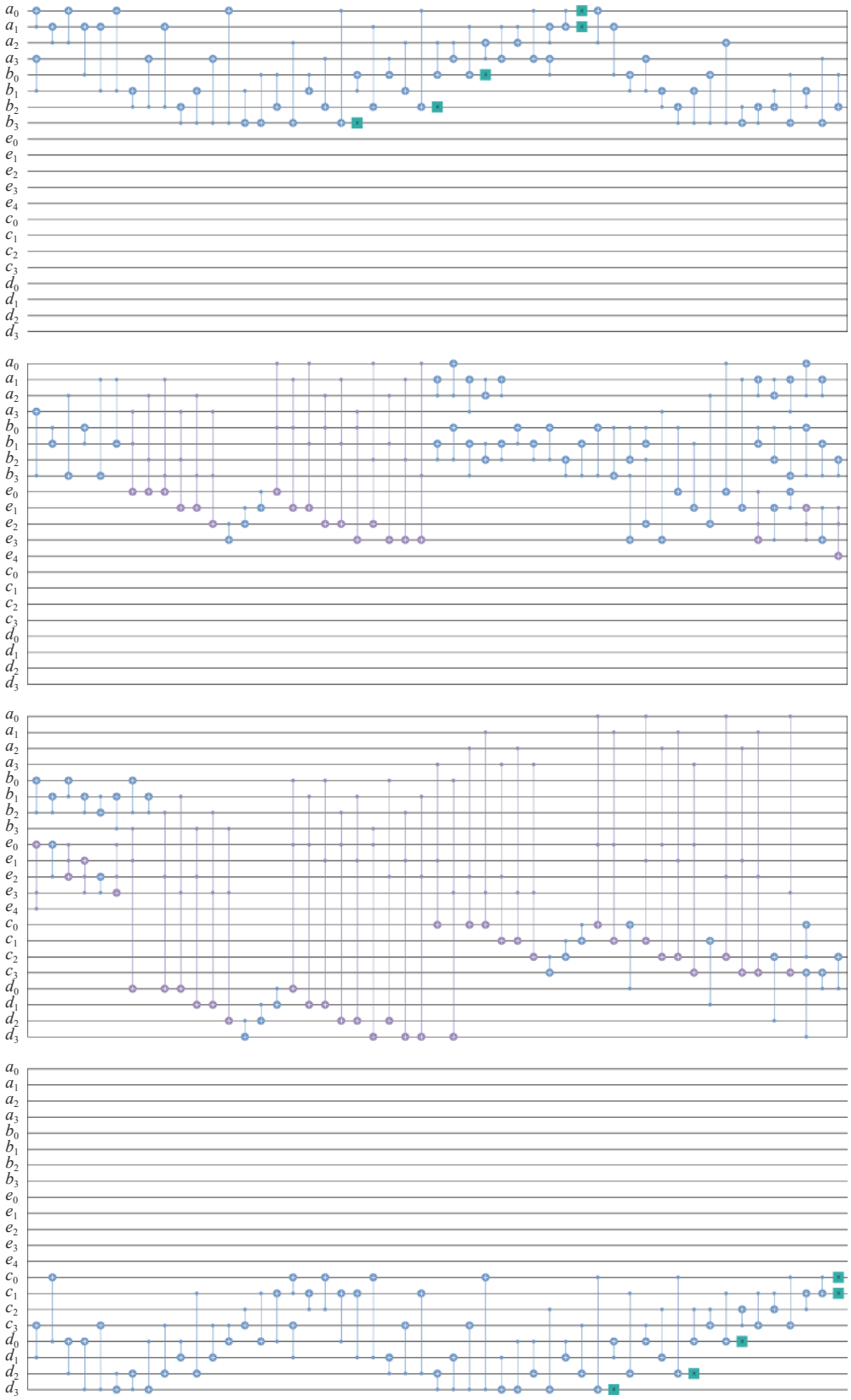

图 10　SM4 密码算法 S 盒的具体量子电路图

5　结 束 语

本文采用 NOT 门、CNOT 门和 Toffoli 门实现 SM4 密码算法 S 盒的量子电路图。根据 S 盒的代数结构，首先将$GF(2^8)$中的求逆运算同构到GF

$((2^4)^2)$求逆，其次根据GF$((2^4)^2)$中求逆运算的表达式分别给出了GF(2^4)中平方计算、乘法计算和求逆运算的量子电路，再次根据最小化基转换矩阵中“1”元素个数的原则求出了基转化矩阵的量子电路，然后利用高斯消元法给出了仿射变换的量子电路，最后综合出 SM4 密码算法 S 盒的量子电路。整个量子电路一共使用了 21 个量子比特，55 个 Toffoli 门，176 个 CNOT 门和 10 个 NOT 门。和现有方法相比，所使用的量子资源进一步减少，效率进一步提高。

参 考 文 献

[1] PETER W. Shor polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM J Comput, 1997, 26(5): 1484-1509.

[2] YAMAMURA A, ISHIZUKA H. Quantum cryptanalysis of block ciphers (Algebraic systems, formal languages and computations)[J]. RIMS Kokyuroku, 2000(1166): 235-243.

[3] GROVER L K. A fast quantum mechanical algorithm for database search[C]//Proc of the 28th Annual ACM Symposium on Theory of Computing (STOC). [S.l.]: ACM, 1996: 212-219.

[4] KAPLAN M, LEURENT G, LEVERRIER A, et al. Breaking symmetric cryptosystems using quantum period finding[C]//Annual International Cryptology Conference. Berlin, Heidelberg: Springer, 2016: 207-237.

[5] SIMON D. On the power of quantum computation [C]//Proceedings of the 35th IEEE Symposium on the Foundations of Computer Science (FOCS). [S.l.]: IEEE, 1994: 116-123.

[6] LEANDER G, MAY A. Grover meets Simon-quantumly attacking the FX-construction[C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2017: 161-178.

[7] DONG X Y, WANG X Y. Quantum key-recovery attack on feistel structures[J]. Science China Information Sciences, 2018, 61(10): 1-7.

[8] SAMIR H, LARS R K. A quantum distinguisher for 7/8-round SMS4 block cipher[J]. Quantum Information Processing, 2020, 19(11): 1-22.

[9] SARAVANAN P, KALPANA P. Novel reversible design of advanced encryption standard cryptographic algorithm for wireless sensor networks[J]. Wireless Personal Communications, 2018, 100(4): 1427-1458.

[10] GRASSL M. LANGENBERG B. ROETTELER M. et al. Applying grover’s algorithm to AES: Quantum resource estimates[EB/OL]. (2015-12-15). https://arxiv.org/abs/1512.04965.

[11] ITOH T, TSUJII S. A fast algorithm for computing multiplicative inverses in GF (2m) using normal bases[J]. Information and Computation, 1988, 78(3): 171-177.

[12] EGNER S, PUSCHEL M. Solving puzzles related to permutations groups[C]//Proc International Symposium on Symbolic and Algebraic Computation (ISSAC’98). [S.l.]: ACM, 1998: 186-193.

[13] ALMAZROOIE M, SAMSUDIN A, ABDULLAH R, et al. Quantum reversible circuit of AES-128[J]. Quantum Information Processing, 2018, 17(5): 1-30.

[14] LANGENBERG B, PHAM H, STEINWANDT R. Reducing the cost of implementing the advanced encryption standard as a quantum circuit[J]. IEEE Transactions on Quantum Engineering, 2020(1): 1-12.

[15] ZOU J, LIU Y, DONG C. et al. Observations on the quantum circuit of the SBox of AES[EB/OL]. (2019-10-24).https://eprint.iacr.org/2019/1245.

[16] 国家密码管理局. 国家密码管理局关于发布无线局域网产品密码事宜公告[EB/OL]. (2006-01-06). https//sca.gov. cn/sca/xwdt/2006-01/06/content_1002355. shtml.
State Cryptography Administration. Announcement of the state cryptography administration on issuing ciphers for WLAN products[EB/OL]. (2006-01-06). https//sca. gov.cn/sca/xwdt/2006-01/06/content_1002355. shtml.

[17] 国家密码管理局. 我国 SM4 分组密码算法正式成为 ISO/IEC 国际标准[EB/OL]. (2021-07-08). https//www.oscca.gov.cn/sca/xwdt/2021-07/08/content_1060866.shtml.
State Cryptography Administration. China's SM4 block cipher algorithm has officially become an ISO/IEC international standard[EB/OL]. (2021-07-08). https//www.oscca.gov.cn/sca/xwdt/2021-07/08/content_1060866.shtml.

[18] 罗庆斌, 李晓瑜, 杨国武. SM4 密码算法 S 盒的量子电路实现[J]. 电子科技大学学报, 2021, 50(6): 820-826.
LUO Q B, LI X Y, YANG G W. Quantum circuit implementation of S-box for SM4 cryptographic algorithm[J]. Journal of University of Electronic Science and Technology of China, 2021, 50(6): 820-826.

[19] 林达, 向泽军, 张若琳, 等. SM4 算法的量子实现[J]. 密码学报, 2021, 8(6): 999-1018.
LIN D, XIANG Z J, ZHANG R L, et al. Quantum implementation of SM4[J]. Journal of Cryptologic Research, 2021, 8(6): 999-1018.

[20] 中国标准化委员会. GB/T 32907-2016 信息安全技术 SM4 分组密码算法[S]. 北京: 中国质检出版社, 2016.
China Standardization Commission. GB/T 32907-2016 information security technology: SM4 block cipher algorithm[S]. Beijing: China Quality Inspection Press, 2016.

[21] LIU F, JI W, HU L, et al. Analysis of the SMS4 block cipher[C]//Information Security and Privacy. Berlin, Heidelberg: Springer, 2007: 158-170.

[22] YANG G, SONG X, HUNG W, et al. Bi-directional synthesis of 4-bit reversible circuits[J]. The Computer Journal, 2008, 51(2): 207-215.

[23] REYHANI-MASOLEH A, HASAN M A. Low complexity bit parallel architectures for polynomial basis multiplication over GF (2m)[J]. IEEE Transactions on Computers, 2004, 53(8): 945-959.

编 辑 蒋 晓