计算机科学
COMPUTER SCIENCE

Camellia密码算法S盒的量子电路优化

吕轶, 罗庆斌, 李强, 郑圆梦

引用本文

吕轶, 罗庆斌, 李强, 郑圆梦. Camellia密码算法S盒的量子电路优化[J]. 计算机科学, 2024, 51(6A): 230900051-6.

LYU Yi, LUO Qingbin, LI Qiang, ZHENG Yuanmeng. Quantum Circuit Optimization of Camellia Cryptographic Algorithm S-box [J]. Computer Science, 2024, 51(6A): 230900051-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230900051

Camellia 密码算法 S 盒的量子电路优化

吕 轶[1] 罗庆斌[1,2] 李 强[1] 郑圆梦[3]
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学院 成都 610054
3 湖北民族大学数学与统计学院 湖北 恩施 445000
(lvzxiong002@gmail.com)

摘 要 S盒是Camellia密码算法重要的非线性组件。使用Toffoli门、CNOT门和NOT门构建Camellia密码算法S盒的量子电路。为了降低计算的复杂度,根据S盒的代数表达式,将有限域$GF(2^8)$中的乘法求逆运算同构到$GF((2^4)^2)$的复合域中的运算,构造出Camellia密码算法S盒的量子电路。在优化方面,将仿射矩阵、同构矩阵以及一组CNOT门对应的矩阵先进行乘法操作,再进行综合,使用DORCIS工具优化$GF(2^4)$中乘法求逆的量子电路,运用W-Type算法优化矩阵运算的量子电路。最终得到的S盒的量子电路只需使用20个量子比特,52个Toffoli门、178个CNOT门和13个NOT门,Toffoli深度为40,电路深度为130。该量子电路的正确性通过IBM公司的Aer模拟器进行验证。相比于已有的结果,文中使用的量子资源有了进一步的减少。

关键词:量子电路;Camellia;S盒;复合域
中图分类号 TP309

Quantum Circuit Optimization of Camellia Cryptographic Algorithm S-box

LYU Yi[1],LUO Qingbin[1,2],LI Qiang[1] and ZHENG Yuanmeng[3]
1 College of Intelligent Science and Engineering,Hubei Minzu University,Enshi,Hubei 445000,China
2 School of Information and Software,University of Electronic Science and Technology of China,Chengdu 610054,China
3 School of Mathematics and Statistics,Hubei Minzu University,Enshi,Hubei 445000,China

Abstract S-box is an important nonlinear component of Camellia cryptographic algorithm. In this paper,Toffoli gate,CNOT gate and NOT gate are used to construct the quantum circuit of Camellia cryptographic algorithm S box. In order to reduce the computational complexity,according to the algebraic expression of the S-box,the multiplication inversion operation in the finite domain $GF(2^8)$isisomorphic to the operation in the complex domain $GF((2^4)^2)$,and finally the quantum circuit diagram of Camellia cipher algorithm S box is synthesized. In optimization,the affine matrix,isomorphic matrix and a group of matrices corresponding to CNOT gates are first multiplied and then synthesized,and the quantum circuit of multiplication inversion in $GF((2^4)^2)$ is optimized using DORCIS tool,and the quantum circuit of matrix operation is optimized using W-Type algorithm. The resulting quantum circuit of the S-box uses only 20 qubits,52 Toffoli gates,178 CNOT gates,and 13 NOT gates,Toffoli-depth is 40,with a circuit depth of 130. The correctness of the quantum circuit is verified by IBM's Aer simulator. Compared with the existing results,the quantum resources used in this paper are further reduced.

Keywords Quantum circuit,Camellia,S-box,Composite field

1 引言

近年来,随着量子计算机的快速发展,量子计算对现代密码学带来了重大的影响。量子计算机利用量子叠加性和量子纠缠等特性,可以快速求解目前传统计算机难以解决的数学困难问题,比如因数分解和离散对数问题,这些困难问题是现代密码学的基础。因此,如何评估密码算法在量子环境下的安全性,引起了密码学界的广泛关注。

研究量子计算对对称密码算法的威胁成为密码学界关注的热点问题之一。为了实施针对对称密码算法的量子攻击,攻击者需要构建一个专用的量子电路来执行特定的量子算法,而加密过程的量子电路往往是这个专用量子电路的重要组成部分。因此,对于攻击者来说,降低加密过程的量子电路的规模可以降低攻击所需要的量子资源;对于设计者来说,掌握该量子电路的最小资源消耗,可以更精确地评估算法抵抗量子攻击的安全强度。此外,由于量子逻辑门是可逆的,使用量子电路构造的密码算法理论上所需要的消耗近零功率,因此可以抵抗与功率分析相关的各种侧信道攻击[1-2]。

基金项目:国家自然科学基金(62262020);湖北省自然科学基金(2020CFB326);湖北民族大学研究生创新项目(MYK2023074)
This work was supported by the National Natural Science Foundation of China(62262020),Hubei Provincial Natural Science Foundation(2020CFB326) and Hubei Minzu University Graduate Innovation Project(MYK2023074).
通信作者:罗庆斌(qingbinluo@126.com)

现有的对称加密算法的量子电路实现主要集中在高级加密标准(AES)[3]上。一些 AES 的量子电路设计,被用来降低量子比特的数量[4-5]。除了优化量子比特的数量之外,还有一些量子电路从电路深度出发进行优化。由于量子电路的深度,特别是 Toffoli 深度[6-8],直接影响了量子计算[9]中电路的运行时间,因此电路深度也是量子电路实现中的一个重要指标。

Camellia 密码[10]是一种对称加密算法,它是日本政府选定的加密标准之一,也是国际标准化组织(ISO)和欧洲电信标准化协会(ETSI)认可的加密算法之一。2000 年,NTT 和 Mitsubishi Electric 公司共同开发出了 Camellia 密码算法,该算法基于 Feistel 网络结构,与 AES(高级加密标准)算法类似,也具有 S 盒和移位操作,同时引入了新的线性变换和置换操作。2003 年,Camellia 密码算法被选为 TLS(传输层安全性)的加密算法之一。2013 年,Camellia 密码算法被选为 TLS 1.3 的加密算法之一。总之,Camellia 密码算法在国际上得到了广泛的认可和使用,其安全性和效率也得到了广泛的验证和测试。在当前的网络安全领域,Camellia 密码算法仍然是一种重要的加密算法。

文献[11]对 Camellia 密码算法做了整体研究,给出了 Camellia 密码算法 S 盒的代数表达式,并对 Camellia 密码的 S 盒完成了量子电路的实现,其中 s_1 盒共使用了 23 个量子比特,67 个 Toffoli 门,308 个 CNOT 门,13 个 NOT 门。Li 等[12]对 Camellia 密码算法的 S 盒的量子电路进行了低成本实现,其中 s_1 盒共使用了 20 个量子比特、54 个 Toffoli 门、196 个 CNOT 门和 13 个 NOT 门。在目前已知的结果中,文献[12]是实现 Camellia 密码算法 S 盒所使用的量子资源最优的结果。

主要研究 Camellia 密码算法 S 盒量子电路的优化。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 S 盒的量子电路;利用一种自动化工具 DORCIS 实现 $GF(2^4)$ 中乘法求逆的量子电路。此外,本文通过 Xiang 等[13]提到的方法对 Camellia 密码的 S 盒仿射变换进行了分解消元,从而得到最优化的量子电路,所使用的量子比特、量子门的数量、Toffoli 深度和量子电路的总深度等量子资源都是目前最少的。

2 预备知识

2.1 常用量子逻辑门

本文主要使用 NCT 库,即 NOT 门、CNOT 门和 Toffoli 门。NOT 门也被叫做 X 门,对应经典的 NOT 操作,反转输入量子位的状态。CNOT 门对应经典的异或操作,该量子门在控制量子比特为 $|1\rangle$ 时反转目标量子比特的状态,即 $CNOT(a,b)=(a,a\oplus b)$。Toffoli 门是三量子比特门,它有两个控制位和一个目标位。当两个控制位都为 $|1\rangle$ 时,目标位才会取反。如果任意一个控制位是 $|0\rangle$,那么目标位不会改变,即 $Toffoli(a,b,c)=(a,b,c\oplus(a\cdot b))$。具体的量子逻辑门设计如图 1 所示。

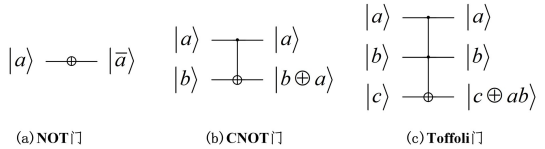

图 1 常用的量子逻辑门

Fig. 1 Common quantum gates

2.2 复合域

复合域[14](Composite Field)是密码学中一个重要的概念,也称为扩域(Extension Field)。它是由有限域(Finite Field)的元素所构成的一个域。在密码学中,复合域中求乘法逆元运算通常用于实现加密算法和数字签名算法。

本文将有限域 $GF(2^8)$ 中的乘法求逆运算同构到复合域 $GF((2^4)^2)$ 中进行运算,文献[15]中给出了在 $GF((2^4)^2)$ 下求乘法逆元的推导过程,取不可约多项式 $p(y)=y^2+y+\lambda$,其中 $\lambda\in GF(2^4)$。设 Y 是 $p(y)$ 的一个根,则对于 $\forall r=r_1Y+r_0\in GF((2^4)^2)$,它的逆元为:

$$r^{-1}=r_1[r_{.0}(r_0+r_1)+r_1^2\lambda]^{-1}Y+(r_0+r_1)[r_{.0}(r_0+r_1)+r_1^2\lambda]^{-1} \tag{1}$$

通过将式(1)中的公式进行展开得到:

$$r^{-1}=r_1[r_{.0}(r_0+r_1)+r_1^2\lambda]^{-1}Y+r_0[r_{.0}(r_0+r_1)+r_1^2\lambda]^{-1}+r_1[r_{.0}(r_0+r_1)+r_1^2\lambda]^{-1} \tag{2}$$

式(2)将在 $GF(2^4)$ 中进行运算。考虑到运算的执行效率,选取不可约多项式 $q(Z)=Z^4+Z+1$。对于 $\forall a\in GF(2^4)$,有:

$$a=\sum_{i=0}^{3}a_iZ^i,a_i\in GF(2) \tag{3}$$

其中,$q(Z)=Z^4+Z+1$ 为 $q(Z)=Z^4+Z+1$ 的一个根。

3 Camellia 密码算法的 S 盒

3.1 S 盒的代数结构

Camellia 密码算法中的 S 盒采用了一种层次结构,由 4 个不同的 S 盒层组成。s_1 盒是第一层 S 盒,其他 S 盒都可以通过 s_1 盒变换得到。它们的代数表达式如下:

$$\begin{cases}s_1:x\to h(g(f(0xc5\oplus x)))\oplus 0x6e\\ s_2:x\to s_1(x)\lll 1\\ s_3:x\to s_1(x)\ggg 1\\ s_4:x\to s_1(x\lll 1)\end{cases} \tag{4}$$

式(4)中的$\lll$($\ggg$)代表循环左移(右移)一个比特,因此在实现了 s_1 盒的量子电路后,其他的 S 盒的量子电路只需要通过移位的操作即可得到,因此后文中的 S 盒就指 s_1。文献[11]给出了一种新的 S 盒代数结构,具体的 Camellia 密码 S 盒的代数结构如下:

$$S(b)=M_2\cdot I\cdot(M_1(b)+C_1)+C_2,b\in GF(2^8) \tag{5}$$

其中,I 是 $GF(2^8)$ 上的乘法逆元,所用到的不可约多项式为:

$$f(x)=x^8+x^6+x^5+x^3+1 \tag{6}$$

M_1,M_2 为 $GF(2)$ 上的 8×8 矩阵,具体值如下:

$$M_1=\begin{bmatrix}0&0&1&0&1&0&0&1\\1&0&1&0&1&0&0&0\\0&0&0&0&0&0&1&1\\0&1&1&0&0&0&0&1\\1&1&1&0&1&1&0&0\\0&1&0&1&0&1&0&1\\0&0&1&1&1&1&1&1\\0&0&0&0&0&1&1&0\end{bmatrix} \tag{7}$$

$$M_2=\begin{bmatrix}0&0&0&1&1&1&0&0\\0&1&1&1&0&0&0&0\\0&1&1&1&0&1&1&0\\1&0&0&0&1&1&0&1\\0&1&0&0&0&0&0&0\\0&0&1&0&0&1&0&1\\0&0&1&0&0&1&0&0\\0&0&0&1&0&0&0&0\end{bmatrix} \tag{8}$$

C_1，C_2 为 $GF(2)$上的常量，值分别为：$C_1=(1,1,1,0,1,1,0,1)$，$C_2=(0,1,1,0,1,1,1,0)$。

3.2　构造同构映射矩阵和 λ 矩阵

S 盒实际上是一个 8 量子比特的逻辑函数。8 量子比特的逻辑函数共有 $2^8!$个，如果直接在 $GF(2^8)$上进行乘法求逆，计算量将十分庞大，目前并没有很好的方法进行求解，所以通过将 $GF(2^8)$同构到 $GF((2^4)^2)$，在 $GF(2^4)$中完成运算。

首先采用文献[15]中构造同构映射类似的方法构造同构映射 δ 和 δ^{-1}，可以求得 Camellia 算法中第一个 S 盒转换基的参数为：$Y=0x7C$，$Z=0x6C$，$\lambda=0x9$。此时，可以得到同构映射 δ 和 δ^{-1} 值分别为：

$$\delta=\begin{bmatrix}1&0&1&1&0&1&1&0\\0&0&0&0&0&0&1&1\\0&0&0&0&1&0&0&1\\0&0&1&1&0&1&1&0\\0&1&1&0&1&1&0&1\\0&0&0&0&0&0&0&1\\0&0&0&0&0&1&1&1\\0&0&0&1&0&0&1&0\end{bmatrix} \tag{9}$$

$$\delta^{-1}=\begin{bmatrix}1&0&0&1&0&0&0&0\\0&0&1&1&1&0&0&1\\0&1&0&1&0&0&1&1\\0&1&0&0&0&1&0&1\\0&0&1&0&0&1&0&0\\0&1&0&0&0&0&1&0\\0&1&0&0&0&1&0&0\\0&0&0&0&0&1&0&0\end{bmatrix} \tag{10}$$

$\lambda=0x9$ 时，计算 $\lambda\cdot a$ 的值等价于计算矩阵 λ 乘 a 的值。λ 可以表示为式如下矩阵形：

$$\lambda=\begin{bmatrix}1&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0\end{bmatrix} \tag{11}$$

3.3　实现 $a^2\times\lambda$ 的量子电路

对于平方运算，因为有限域 $GF(2)$中的特征为 2，所以对于任意元素 $a=\sum_{i=0}^{3}x_iZ^i\in GF(2^4)$有：

$$a^2=(\sum_{i=0}^{3}a_iZ^i)^2=\sum_{i=0}^{3}a_iZ^{2i} \tag{12}$$

因此，对于 $\forall a\in GF(2^4)$，可以得到如下的矩阵 S，使得 $a^2=S\cdot a$，其中：

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

将式(11)和式(13)相乘可以得到 $a^2\times\lambda$ 的矩阵，把 $a^2\times\lambda$ 的矩阵记作 qc。Xiang 等在文献[13]中给出了一种对可逆矩阵优化的一种方式，通过使用交换门来降低所需要的量子资源。通过这种方法，得到 qc 相应的量子电路，如图 2 所示。

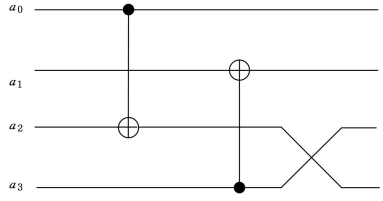

图 2　qc 的量子电路示意图

Fig. 2　Quantum circuit diagram of qc

通过图 2 可以看到实现 $a^2\times\lambda$ 的量子电路，需要 2 个 CNOT 门，电路深度为 1。

3.4　实现乘法的量子电路设计

对于乘法计算，由文献[16]定理可以得出：对于 $\forall f,g,h\in GF(2^4)$，有：

$$f=\sum_{i=0}^{3}f_iZ^i,g=\sum_{i=0}^{3}g_iZ^i,h=\sum_{i=0}^{3}h_iZ^i \tag{14}$$

在 $GF(2)$中，表达式为：

$$h+f\times g=(h_3+(fg)_3)Z^3+(h_2+(fg)_2)Z^2+(h_1+(fg)_1)Z+h_0+(fg)_0 \tag{15}$$

在 $GF(2)$中，表达式为：

$$h+f\times g=(h_3+(fg)_3)Z^3+(h_2+(fg)_2)Z^2+(h_1+(fg)_1)Z+h_0+(fg)_2 \tag{16}$$

在 $(fg)_i$，$i\in0,1,2,3$ 中，i 是 fg 的下标：

$$\begin{aligned}(fg)_0&=(f_1+f_3)(g_1+g_3)+f_0g_0+f_1g_1+f_2g_2+f_3g_3\\(fg)_1&=(f_1+f_3)(g_1+g_3)+(f_0+g_1)(f_0+g_1)+(f_2+f_3)(g_2+g_3)+f_0g_0\\(fg)_2&=(f_0+f_2)(g_0+g_2)+(f_2+f_3)(g_2+g_3)+f_0g_0+f_1g_1\\(fg)_3&=(f_0+f_1+f_2+f_3)(g_0+g_1+g_2+g_3)+f_1g_1+f_2g_2+(f_0+f_2)(g_0+g_2)+(f_2+f_3)(g_2+g_3)+f_0g_0+(f_0+f_1)(g_0+g_1)+(f_1+f_3)(g_1+g_3)\end{aligned} \tag{17}$$

基于以上表达式，文献[16]中提出了一种 W-type 的量子电路设计，即：

$$|f\rangle|g\rangle|h\rangle\rightarrow|f\rangle|g\rangle|h\oplus f\cdot g\rangle \tag{18}$$

通过这种方式可以有效降低所需要的量子资源。根据文献[16]中提到的方法，可以得到乘法计算 A 的量子电路图，如图 3 所示。

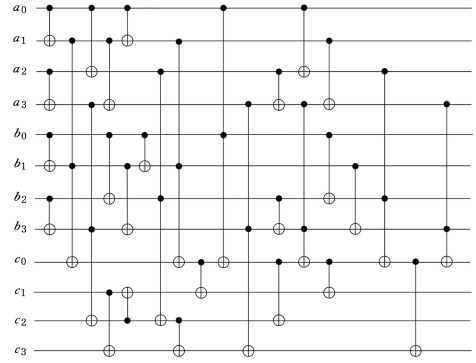

图 3　乘法运算 A 量子电路示意图

Fig. 3　Quantum circuit diagram of multiplication operation A

通过图 3 可知，乘法运算 A 使用了 9 个 Toffoli 门和 23 个 CNOT 门，Toffoli 深度为 6。由于在式(7)中 h 并不一定是全 0 输入，因此，为了保留 h 的输入，需要使用另一种乘法方式。文献[16]中发现只需要在量子输出位 h 上预先执行 CNOT 门的逆电路得到：

$$|f\rangle|g\rangle|h\rangle\rightarrow|f\rangle|g\rangle|h\oplus f\cdot g\rangle \tag{19}$$

然后再执行图 3 中的电路进行还原，即可保留 h 的输入，得到新的乘法运算 B 的量子电路，如图 4 所示。图 4 中的量子电路需要 12 个量子位、9 个 Toffoli 门和 27 个 CNOT 门，Toffoli 深度为 6。因此，与图 3 中的电路相比，图 4 中的电路只增加了 4 个 CNOT 门。

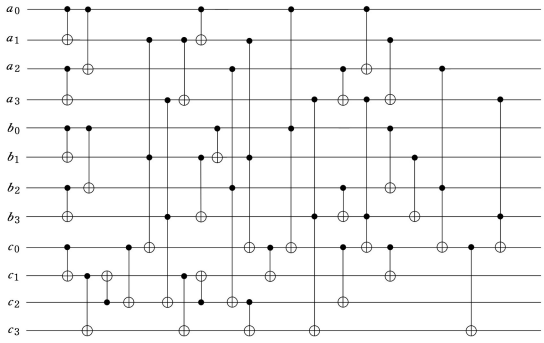

图 4 乘法运算 B 的量子电路示意图

Fig. 4 Quantum circuit diagram of multiplication operation B

3.5 实现 $GF(2^4)$乘法逆的量子电路

如何实现乘法逆电路 I 一直是优化 S 盒量子电路问题的关键。目前已经有了很多方法，Almazrooie 等[17]采用 Itoh-Tsujii 算法得到这种量子电路。Saravanan 等[18]和 Wang 等[19]分别基于一个 $GF(2^4)$与同构的组合域 $GF(2^2)^2$得到这种量子电路。Li 等[16]基于文献[20]中实现 $GF(2^4)$乘法逆的经典电路，给出对应的量子电路。Luo 等[15]采用双向可逆逻辑综合的方式，在 $GF(2^4)$中求解乘法逆电路。Li 等[12]使用 LIGHTER-R 工具[21]辅助实现乘法逆电路。

本文使用 DORCIS[22]实现乘法求逆的量子电路，它是一种自动化工具，可以给出任意 4 比特 S 盒的量子电路。把 $GF(2^4)$乘法逆运算看作一个 4 比特的 S 盒，它的输入和与之对应的逆元如表 1 所列。通过 DORCIS 工具，可以实现 $GF(2^4)$乘法逆的量子电路，如图 5 所示。

表 1 $GF(2^4)$输入和对应逆元

Table 1 Input and corresponding inverse elements of $GF(2^4)$

输入/输出(逆元)	元素															
x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x^{-1}	0	1	9	E	D	B	7	6	F	2	C	5	A	4	3	8

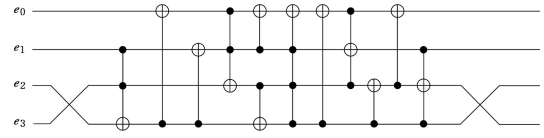

图 5 乘法逆的量子电路示意图

Fig. 5 Schematic diagram ofquantum circuit ofmultiplication inverse

通过 DORCIS 得到的乘法逆的量子电路所需要的量子资源为 4 个 Toffoli 门、7 个 CNOT 门和 1 个三控制位的 CCCNOT 门，将这个 CCCNOT 门等价替换后得到新的乘法逆的量子电路，如图 6 所示。

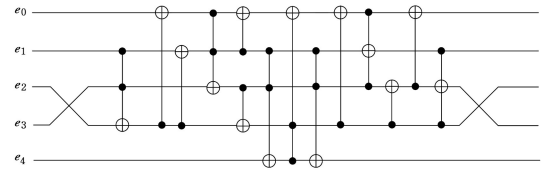

图 6 新的乘法逆的量子电路示意图

Fig. 6 Quantum circuit diagram of new multiplicative inverse

因此，乘法逆量子电路共需要 8 个 Toffoli 门和 7 个 CNOT 门。从表 2 可以看出，相比于其他方法实现的乘法逆电路，本文使用的量子资源最少。

表 2 乘法逆所需资源比较

Table 2 Comparison of resources required for multiplication inverse

文献	# qubits	# CNOT	# Toffoli
[18]	18	22	9
[17]	16	47	48
[19]	8	20	14
[11]	6	22	6
[12]	5	9	9
本文	5	7	8

4 S 盒量子电路的实现

4.1 $M_1 \cdot \delta \cdot cnot$ 乘和 $cnot \cdot \delta^{-1} \cdot M_2$ 乘量子电路的实现

根据式(5)，可以构建出实现 S 盒的整体框架，如图 7 所示。

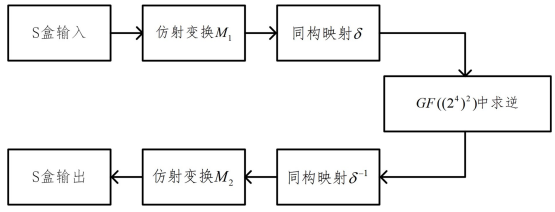

图 7 S 盒复合域实现框架图

Fig. 7 Framework of S-box composite domain implementation

考虑将 $M_1 \cdot \delta$ 相乘后进行运算，先将这两个矩阵相乘后得到一个新的矩阵，再对这个新的矩阵进行量子电路综合，这样可以将两次变换缩减到一次，从而降低量子门数和电路深度。由于在输入 M_1 和 δ 后还会进行一组 CNOT 门操作，将这组 CNOT 门操作也和 $M_1 \cdot \delta$ 相乘得到更优的矩阵 L_1，如图 8 所示。

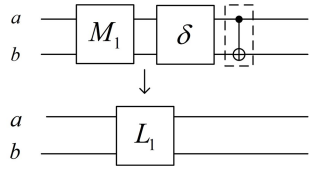

图 8 变化后的矩阵

Fig. 8 Changed matrix

图 8 虚线框内为一组 CNOT 门，其中这组 CNOT 门可以转换为矩阵的形式，即：

$$cnot=\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\1&0&0&0&1&0&0&0\\0&1&0&0&0&1&0&0\\0&0&1&0&0&0&1&0\\0&0&0&1&0&0&0&1\end{bmatrix} \tag{20}$$

通过以上 3 个矩阵相乘后，可以得到新的矩阵为：

$$L_1=\begin{bmatrix}0&0&1&0&1&0&0&0\\1&0&0&0&0&0&0&1\\0&0&0&1&0&0&1&0\\0&1&0&0&1&0&0&0\\1&0&1&0&1&1&0&0\\0&0&0&1&0&1&0&1\\0&1&0&1&0&0&1&1\\0&1&1&0&1&0&1&0\end{bmatrix} \tag{21}$$

使用文献[12]的方法，对矩阵 L_1 进行综合，得到相应的量子电路，如图 9 所示。

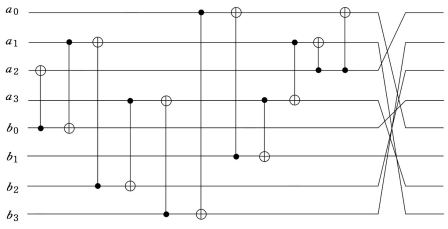

图 9　L_1 的量子电路图

Fig. 9　Quantum circuit diagram of L_1

由图 9 可知，L_1 需要 8 个量子比特和 11 个 CNOT 门。相似地，cnot $\cdot\delta^{-1}\cdot M_2$ 相乘后的矩阵的量子电路如图 10 所示。

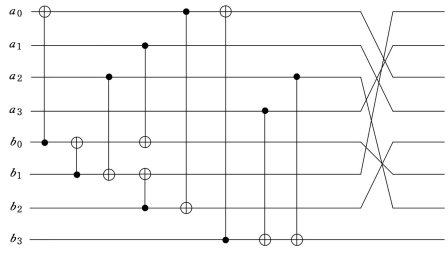

图 10　L_2 的量子电路图

Fig. 10　Quantum circuit diagram of L_2

4.2　实现 Camellia 算法 S 盒的量子电路

有了以上各个量子电路组件，根据式(2)给出的公式可以构造出 Camellia 算法 S 盒的量子电路如图 11 所示，具体的量子电路如图 12 所示。图中量子电路是使用 IBM 公司开发的 qiskit 软件包实现的，子电路中的线路交换采用 SWAP 门实现。

图 11 中，L_1 和 L_2 分别代表 $M_1\cdot\delta\cdot cnot$ 乘和 $cnot\cdot\delta^{-1}\cdot M_2$ 乘，L_1^{-1} 和 L_2^{-1} 分别代表 L_1 和 L_2 的逆运算，M_a 代表乘法运算 A，M_b 代表乘法运算 B，PC 代表 $a^2\times\lambda$，PC^{-1} 表示 PC 的逆运算，I 代表求逆运算，I^{-1} 表示求逆运算的逆运算，图中还用到了 4 组 CNOT 门的加法运算。另外，还需要特别说明的是：在实现 $GF(2^4)$ 中，乘法逆元 I 时借助了寄存器 c 的一个量子比特。

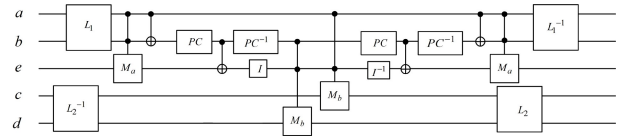

图 11　S 盒的量子电路图

Fig. 11　Quantum circuit diagram o S-box

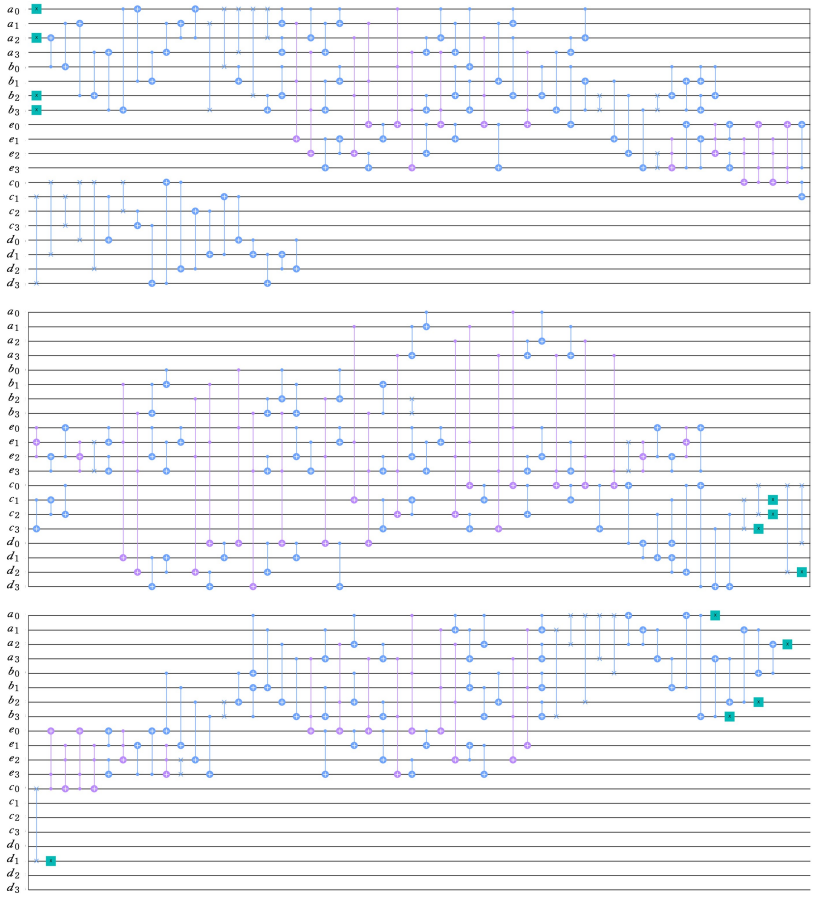

图 12　S 盒的具体量子电路

Fig. 12　Specific quantum circuit of the S-box

5　Camellia 算法 S 盒整体分析

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 盒量子比特数和所使用的量子门的数量以及 Toffoli 门深度刻画电路的复杂度。

在 S 盒实现的量子电路中，a，b，c，d，e 都是 4 量子比特寄存器，所有一共使用了 20 量子比特。现在计算量子门的数量。矩阵 L_1 使用了 11 个 CNOT 门，矩阵 L_2 使用了 9 个 CNOT 门；乘法计算 A 的量子电路共使用了 9 个 Toffoli 门和 23 个 CNOT 门，乘法计算 B 的量子电路共使用了 9 个

Toffoli 门和 27 个 CNOT 门；S 盒的量子电路图中共使用了 2 次乘法计算 A，2 次乘法计算 B；$GF(2^4)$中乘法逆运算的电路图使用了 8 个 Toffoli 门和 7 个 CNOT 门；$a^2\times\lambda$ 的电路图和它的逆电路图都使用了 2 个 CNOT 门，分别使用了 1 次；此外，还使用了 4 组共 16 个 CNOT 门做量子比特的复制。最终实现整个 S 盒所使用的量子资源的对比情况如表 3 所列。

表 3 实现 Camellia S 盒所需资源比较

Table 3 Comparison of resources required to implement Camellia S-box

文献	qubits	Toffoli	CNOT	NOT	T 深度
[11]	23	67	308	13	53
[12]	20	54	196	13	42
本文	20	52	178	13	40

从表 3 可以看出：与文献[10]和文献[11]对比，本文构造 Camellia 算法 S 盒所需的量子资源更少。

结束语 本文使用了更少的量子资源实现了 Camellia 密码算法的 S 盒。根据 S 盒的代数表达式，先将 $GF(2^8)$中乘法逆运算同构到 $GF((2^4)^2)$中实现，然后使用 W-Type 算法对仿射矩阵和同构矩阵以及一组 CNOT 门对应的矩阵相乘后的矩阵进行了优化，使用 DORCIS 工具对 $GF(2^4)$中乘法求逆电路进行了优化，使得所需要的量子资源进一步的减少。最后构造出的 Camellia 算法的 S 盒共需要 20 个量子比特、178 个 CNOT 门、52 个 Toffoli 门和 13 个 NOT 门，Toffoli 门深度为 40。与之前的结论相比，本文使用了更少的量子比特和量子逻辑门，更低的 Toffoli 深度，构造 Camellia 所需要的量子资源和计算复杂度将进一步降低。

随着未来技术的不断发展，量子计算机的研究将对传统密码进行强大的冲击，如何抵抗将要到来的量子计算的攻击成为必须重视的任务，而量子电路对于研究抵抗量子攻击的密码算法有着不可忽视的重要性，对于研究对称密码在量子环境下的安全性分析以及抵抗与功率分析相关的各种侧信道攻击也有很大的意义。

参 考 文 献

[1] BENNETT C H. Logical Reversibility of Computation[J]. IBM Journal of Research and Development, 1973, 17(6): 525-532.

[2] 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.

[3] FIPS 197. Advanced Encryption Standard(AES) [S]. Gaithersburg, NIST, 2001.

[4] LIN D, XIANG Z, XU R, et al. Optimized Quantum Implementation of AES[J]. arXiv: 2109.12354, 2021.

[5] LI Z, GAO F, QIN S, et al. New record in the number of qubits for a quantum implementation of AES[J]. Frontiers in Physics, 2023, 11: 1171753.

[6] JAQUES S. Implementing Grover Oracles for Quantum Key Search on AES and LowMC[J]. arXiv: 1910.01700, 2019.

[7] LI Z, CAI B, SUN H, et al. Novel quantum circuit implementation of Advanced Encryption Standard with low costs[J]. Science China Physics, Mechanics & Astronomy, 2022, 65(9), 290311.

[8] HUANG Z, SUN S. Synthesizing Quantum Circuits of AES with Lower T-depth and Less Qubits[M]// Advances in Cryptology-ASIACRYPT. Cham: Springer, 2022: 614-644.

[9] FOWLER A G. Time-optimal quantum computation[J]. arXiv: 1210.4626, 2013.

[10] AOKI K, ICHIKAWA T, KANDA M, et al. Camel lia: a 128-bit block cipher suitable for multiple platforms-design and analysis [C]// Proceedings of the 7th Annual International Workshop. Waterloo: Springer, 2000: 39-56.

[11] ZOU J, WEI Z, SUN S, et al. Some efficient quantum circuit implementations of Camellia[J]. Quantum Information Processing, 2022, 21(4): 131.

[12] LI Z Q, GAO F, QIN S J, et al. Quantum circuit for implementing Camellia S-box with low costs[J]. Science China Physics, Mechanics & Astronomy, 2023, 53(4): 21-29.

[13] XIANG Z, ZENG X, LIN D, et al. Optimizing Imple mentations of Linear Layers[J]. IACR Trans. Symm. Cryptol., 2020(2): 120-145.

[14] ROMAN S. Field Extensions[M]// Graduate Texts in Mathematics: Field Theory. New York: Springer, 1995: 39-59.

[15] LUO Q B, LI X Y, YAGN G W, et al. Quantum Cir cuit Implementation of S-box for SM4 Cryptographic Algorithm Based on Composite Field Arithmetic[J]. Journal of University of Electronic Science and Technology of China, 2022, 50(6): 820-826.

[16] LI Z Q, CAI B B, SUN H W, et al. Novel quantum circuit implementation of Advanced Encryption Standard with low costs[J]. Chinese Science: Physics, Mechanics and Astronomy, 2022(9): 65.

[17] ALMAZROOIE M, ABDULLAH R, SAMSUDIN A, et al. Quantum Grover Attack on the Simplified-AES[C]// Proceedings of the 2018 7th International Conference on Software and Computer Applications. Kuantan Malaysia: ACM, 2018: 204-211.

[18] 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.

[19] WANG Z G, WEI S J, LONG G L. A quantum circuit design of AES requiring fewer quantumqubits and gate operations[J]. Front Phys, 2022, 17: 41501

[20] BOYAR J, PERALTA R. A New Combinational Logic Minimization Technique with Applications to Cryptology[C]// Experimental Algorithms[M]. Berlin: Springer, 2010: 178-189.

[21] DASU V A, BAKSI A, SARKAR S, et al. LIGHTER-R: Optimized Reversible Circuit Implementation For SBoxes[C]// 2019 32nd IEEE International System-on-Chip Conference (SOCC). Singapore: IEEE, 2019: 260-265.

[22] CHUN M, BAKSI A, CHATTOPADHYAY A. DORCIS: Depth Optimized Quantum Implementation of Substitution Boxes[EB/OL]. (2023-02-25). https://eprint.iacr.org/2023/286.

LYU Yi, born in 1997, postgraduate. His main research interests include quantum circuits and security analysis.

LUO Qingbin, born in 1987, Ph.D. His main research interests include quantum computing and quantum cryptography.