中国科学 : 物理学 力学 天文学 2024 年 第 54 卷 第 4 期 : 240314
SCIENTIA SINICA Physica, Mechanica & Astronomica physcn.scichina.com
《中国科学》杂志社 SCIENCE CHINA PRESS
论 文

SM4算法S盒的高效量子电路实现

刘嘉宏, 谭晓青*, 李明, 包戴鹏伟

暨南大学信息科学技术学院, 广州 510632
*联系人, E-mail: ttanxq@jnu.edu.cn

收稿日期: 2023-10-26; 接受日期: 2023-12-07; 网络出版日期: 2024-03-21
广东省基础与应用基础研究基金(编号: 2024A151501306)资助项目

摘要 近年来, 对称密码的量子实现受到了广泛关注. SM4分组密码算法是我国首个商用密码标准, 在2021年成为ISO/IEC国际标准. S盒作为SM4算法中最复杂的组件, 其量子电路实现对整个SM4算法的量子电路有重大影响. 本文依据SM4算法S盒的代数结构, 使用塔域分解技术实现其量子电路. 本文提出的SM4算法S盒的量子电路, 基于NCT门集分析, 需要的量子资源为20个量子比特、52个Toffoli门、196个CNOT门、13个X门, Toffoli深度为36; 基于Clifford+T门集分析, 需要量子资源为20个量子比特、334个T门、548个CNOT门、129个1qCliff门, T深度为108. 与已有文献相比, 本文提出的量子电路需要的量子资源更少.

关键词 SM4算法, S盒, 量子电路, 塔域分解

PACS: 03.67.Lx, 03.67.Dd, 03.67.Pp

1 引言

随着量子计算机的出现与量子计算的发展, 人们提出了可以攻击现有加密标准的量子算法. 其中, Shor算法[1]能够在多项式时间内对整数进行因子分解, 威胁RSA, ECDSA, ECDH等公钥密码系统. Simon算法[2]可以找到由密码结构导出的周期函数的隐藏周期, 从而进行密码分析攻击. Grover搜索算法[3]通过搜索与少量明文-密文对匹配的密钥来对分组密码进行量子攻击, 与经典算法相比, Grover算法在搜索无序集合时能够实现二次加速. 尽管当前处于含噪中型量子(NISQ)时代, 量子计算机的规模尚不足以攻破现行密码体制, 但随着技术的发展, 这些量子算法在将来总会被实现. 为确保网络安全, 需要准确估计量子威胁的实际到来时间, 故而需要对Shor算法、Simon算法和Grover算法进行资源评估. 其中Grover算法的实现需要设计分组密码的量子电路. 高效实现分组密码算法的量子电路这一研究领域引起了许多学者的兴趣.

已经有许多学者讨论了各种分组密码算法的量子电路实现, 重点关注其S盒实现, 因为它是分组密码中最复杂的组件、唯一的非线性组件、唯一的T门来源, 需要消耗的资源多, 可优化空间大, 所以其量子电路高效实现成为减少整个分组密码量子资源消耗的关键. 自2016年Grassl等人[4]设计了AES算法[5]的量子电路以来, AES算法S盒的量

引用格式: 刘嘉宏, 谭晓青, 李明, 等. SM4算法S盒的高效量子电路实现. 中国科学: 物理学 力学 天文学, 2024, 54: 240314
Liu JH, Tan X Q, Li M, et al. Efficient quantum circuit implementation of the SM4 S-box (in Chinese). Sci Sin-Phys Mech Astron, 2024, 54: 240314, doi: 10.1360/SSPMA-2023-0386

© 2024 《中国科学》杂志社

子电路实现成为了热门的研究对象[6–12], 而关于SM4算法[1)]S盒的量子电路实现则研究得比较少[13–17]. SM4分组密码是我国首个商用密码标准, 在2021年6月正式成为ISO/IEC国际标准[18], 对我国商用密码产业的发展有重大影响. 本文基于塔域分解技术研究SM4算法S盒的高效量子电路实现.

塔域分解技术最早由Itoh等人[19]提出, 用于实现有限域中的乘法逆运算. 这可以应用到S盒的紧凑硬件实现中. 2000年, Rijmen[20]提出使用子域$GF(2^4)$上的运算完成有限域$GF(2^8)$上的求逆运算方法, 降低实现AES算法S盒的代数复杂度. 但是实际上, 他们并没有给出AES算法S盒的具体实现. 2001年, Rudra等人[21]使用塔域分解技术经典实现AES算法的S盒. Wolkerstorfer等人[22]、Canright[23,24]和Boyar等人[25,26]都基于塔域分解技术完成了当时最紧凑的AES算法S盒经典硬件实现. 2022年, Li等人[9]利用塔域分解技术实现了当时最紧凑的AES算法S盒的量子电路. 2023年, Li等人[12]继续对AES算法S盒的量子电路进行改进. 2007年, Liu等人[27]对SM4算法的S盒进行分析, 给出了S盒的代数结构. Wei等人[28]根据S盒的代数结构, 使用塔域分解技术完成了AES, Camellia和SM4算法S盒的经典实现. 2021年, 林达等人[13]分析Wei等人[28]的SM4算法S盒的经典实现的预印版[2)], 结合启发式算法设计了SM4算法S盒的量子电路. 2022年, Zou等人[17]与罗庆斌等人[14]各自利用塔域分解技术实现了比林达等人[13]更紧凑的SM4算法S盒的量子电路. 但是罗庆斌等人[14]的量子电路的辅助量子比特利用率极低. 2023年, Lin等人[15]和Luo等人[16]进一步改进了SM4算法S盒的量子电路. 本文基于塔域分解技术实现了比现有文献更高效的SM4算法S盒的量子电路.

量子电路是用可逆量子门实现的. 其中X门、CNOT门和Toffoli门是通用的逻辑门, 构成了所谓的NCT门集. 其中Toffoli门比其他两个门需要更多的资源. 故而本文以NCT门集分析量子资源开销时, 额外统计Toffoli深度. 然而, 当前的量子设备容易出现噪音, 因此需要进行纠错. 作为一种通用的容错门集, Clifford+T门集已广泛应用于可逆电路的合成. Clifford+T门集合包含Hadamard门、S门、X门、CNOT门和T门. 其中Hadamard门、S门、X门都是作用在单个量子比特上, 本文与文献[7, 15, 17]一样, 将其统称为1qCliff门. T门不是Clifford门, 其实现比Clifford+T门集合中的其他门要昂贵得多. 根据文献[29], T门的实现成本是CNOT门的46–350倍. 因此本文在使用Clifford+T门集分析量子资源时, 除了统计Clifford门数以及T门数, 额外统计了T深度.

2 预备知识

Toffoli门可以实现两个单比特的量子乘法运算: $|a\rangle|b\rangle|c\rangle \to |a\rangle|b\rangle|c\oplus a\cdot b\rangle$. 2013年, Amy等人[30]提出可以把Toffoli门分解为7个T门、7个CNOT门和2个H门组成的量子电路, T深度为3. 具体分解如图1所示.

使用Toffoli门实现乘法运算, 成本比较高. 为了节省Toffoli门的使用, 2020年, Jaques等人[7]提出T深度为1的QAND门用于实现$|a\rangle|b\rangle|0\rangle|0\rangle \to |a\rangle|b\rangle|a\cdot b\rangle|0\rangle$与T深度为0的QAND†门用于实现$|a\rangle|b\rangle|a\cdot b\rangle \to |a\rangle|b\rangle|0\rangle$. QAND门与QAND†门在特定情况下可以取代Toffoli门, 其量子电路分别如图2和3所示.

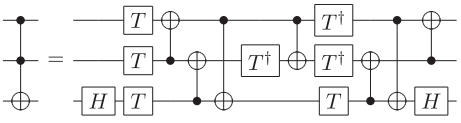


图 1 Toffoli门分解

Figure 1 Decompose of Toffoli gate.

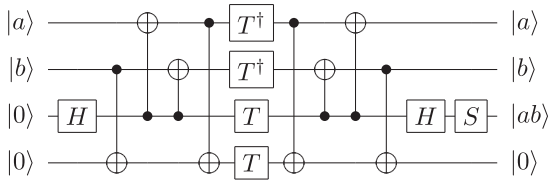


图 2 QAND门

Figure 2 QAND gate.

1) GB/T 32907-2016, 信息安全技术 SM4分组密码算法.

2) Wei Z H, Sun S W, Hu L, et al. Scrutinizing the tower field implementation of the $\mathbb{F}_{2^8}$ inverter—With applications to AES, Camellia, and SM4. IACR Cryptology ePrint Archive, 2019: 2019/738 (https://eprint.iacr.org/2019/738).

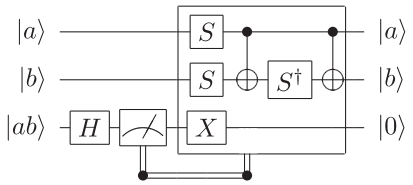


图 3 QAND†门
Figure 3 QAND† gate.

3 SM4算法S盒的量子实现

S盒是SM4算法唯一的非线性结构, 其实现效率影响整个算法的性能. 本节基于SM4算法S盒的代数结构, 使用塔域分解技术实现其高效的量子电路, 并与已有的文献做比较.

3.1 S盒的代数结构

根据文献[31], SM4算法的S盒可以表示为有限域$GF(2^8)$上的运算, 表达式为

$$S(x) = A \cdot I_{\mathcal{PB}}(A \cdot x \oplus c) \oplus c, \tag{1}$$

其中, $I_{\mathcal{PB}}$表示有限域$GF(2^8)$上的逆运算, 其不可约多项式为$f(x) = x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$, 且

$$A = \begin{pmatrix} 1&1&0&1&0&0&1&1\\ 1&1&1&0&1&0&0&1\\ 1&1&1&1&0&1&0&0\\ 0&1&1&1&1&0&1&0\\ 0&0&1&1&1&1&0&1\\ 1&0&0&1&1&1&1&0\\ 0&1&0&0&1&1&1&1\\ 1&0&1&0&0&1&1&1 \end{pmatrix}, \quad c = \begin{pmatrix} 1\\1\\0\\1\\0\\0\\1\\1 \end{pmatrix}.$$

因此可以使用式(1)实现S盒替换, 但是实现有限域$GF(2^8)$上的逆运算需要较多的资源. 为节省资源开销, 本文使用塔域分解技术, 借助有限域$GF(2^4)$完成有限域$GF(2^8)$上的求逆运算, 这个方法包含3个关键步骤: 构建有限域$GF((2^4)^2)$、寻找有限域$GF(2^8)$与$GF((2^4)^2)$之间的同构映射、实现有限域$GF((2^4)^2)$上的逆运算.

首先构建有限域$GF((2^4)^2)$. 陈晨等人[18]根据莫比乌斯函数计算出$GF(2)$上的四次不可约多项式有3个, 分别为$y^4 + y + 1$, $y^4 + y^3 + 1$和$y^4 + y^3 + y^2 + y + 1$. 而$GF(2^4)$上的二次不可约多项式有120个. 本文选取复合域为

$$\begin{cases} GF((2^4)^2) : P(x) = x^2 + x + \lambda, \\ GF(2^4) : Q(y) = y^4 + y^3 + 1, \end{cases} \tag{2}$$

其中, $\lambda = y^2 \in GF(2^4)$. 接着构造有限域间的同构映射, 根据陈晨等人[18]提出的方法构造从有限域$GF(2^8)$到$GF((2^4)^2)$的同构映射. 找到的同构映射一共有8种, 选择其中一种, 其映射矩阵记为M, 逆映射矩阵记为M^{-1}, M和M^{-1}分别为

$$M = \begin{pmatrix} 0&1&1&1&1&1&0&0\\ 1&1&1&1&0&0&1&0\\ 1&1&0&1&0&0&0&0\\ 0&1&1&1&0&0&1&0\\ 1&0&1&1&0&0&1&0\\ 0&0&0&1&1&0&0&0\\ 1&1&0&1&1&0&1&0\\ 1&0&1&1&1&1&1&1 \end{pmatrix}, \quad M^{-1} = \begin{pmatrix} 0&1&0&1&0&0&0&0\\ 0&1&0&0&1&0&0&0\\ 0&1&1&1&1&1&1&0\\ 0&0&1&1&1&0&0&0\\ 0&0&1&1&1&1&0&0\\ 1&0&1&1&0&0&1&0\\ 0&0&0&1&1&1&1&0\\ 1&0&0&0&0&1&1&1 \end{pmatrix}.$$

于是得到式(1)的等价公式为

$$\begin{aligned} S(x) &= A \cdot I_{\mathcal{PB}}(A \cdot x \oplus c) \oplus c \\ &= A \cdot I_{\mathcal{PB}}(M^{-1} \cdot M \cdot (A \cdot x \oplus c)) \oplus c \\ &= A \cdot M^{-1} \cdot I'_{\mathcal{PB}}(M \cdot A \cdot x \oplus M \cdot c) \oplus c, \end{aligned} \tag{3}$$

其中, $I'_{\mathcal{PB}}$表示有限域$GF((2^4)^2)$上的逆运算. 本文根据式(3)实现SM4算法S盒的量子电路, 这主要分为3步. 首先, 实现式(3)中线性部分的量子电路, 包括$M \cdot A$, $M \cdot c$和$A \cdot M^{-1}$; 其次, 实现非线性部分, 即$GF((2^4)^2)$中求逆运算的量子电路; 最后, 将这两部分合并起来得到S盒的量子电路.

3.2 S盒线性部分的量子电路

本节实现S盒线性部分的量子电路. 直接计算式(3)

中的$M\cdot A$, $M\cdot c$和$A\cdot M^{-1}$得

$$MA=\begin{pmatrix}1&1&0&0&0&1&0&0\\1&1&1&1&1&0&1&1\\0&1&0&0&0&0&0&0\\0&0&1&0&1&0&0&0\\0&0&0&1&0&0&1&0\\0&1&0&0&0&1&1&1\\0&0&1&1&0&0&1&0\\0&0&0&1&0&1&1&0\end{pmatrix},\ Mc=\begin{pmatrix}0\\0\\1\\1\\1\\1\\0\\0\end{pmatrix},$$

$$AM^{-1}=\begin{pmatrix}1&0&1&1&1&0&0&1\\1&1&0&1&1&1&0&1\\1&1&1&0&1&1&0&0\\0&0&1&0&1&1&0&0\\0&1&0&0&1&1&1&1\\1&1&1&1&1&0&0&0\\0&1&0&1&1&1&1&1\\0&0&0&0&0&1&0&1\end{pmatrix}.$$

为实现MA和AM^{-1}的量子电路, 普遍的做法是使用PLU分解, 将原矩阵分解为一个上三角矩阵、一个下三角矩阵和一个置换矩阵, 然后应用CNOT门实现上三角矩阵和下三角矩阵的量子电路. 置换矩阵则可以通过改写输入输出位的下标实现, 因此其量子资源开销可以视作0. Chung等人[8]、Li等人[9,12]和李振强等人[29]都采用了PLU分解的方法. 但是此方法可能会导致较多的CNOT门数. 2020年, Xiang等人[32]基于矩阵分解理论提出了一套搜索矩阵优化实现的启发式算法, 该方法能够搜索$GF(2)$上二元矩阵的优化实现. 使用该方法得到的量子电路与PLU分解相比, 在CNOT门数方面有一定的优势. 因此本文应用Xiang等人[32]提出的算法实现MA和AM^{-1}的量子电路如图 4和5所示, 各需要8个量子比特以及12或14个CNOT门. 而式(3)中的异或Mc可由4个X门完成, 异或c可由5个X门完成.

3.3 S盒非线性部分的量子电路

本节实现S盒非线性部分, 即$GF((2^4)^2)$中求逆运算的量子电路. $GF((2^4)^2)$中任意元素可表示为 $p=p_1x+p_0$, 设其逆元为$p^{-1}=(p^{-1})_1x+(p^{-1})_0$, 根据文献[9,29]可得$(p^{-1})_0$和$(p^{-1})_1$分别为

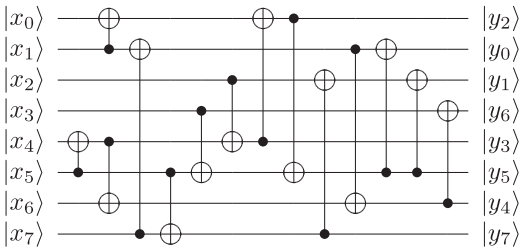


图 4 线性变换AM^{-1}的量子电路

Figure 4 Quantum circuit of linear transformation AM^{-1}.

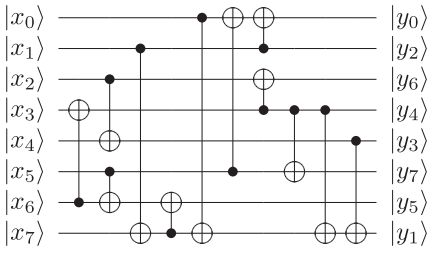


图 5 线性变换MA的量子电路

Figure 5 Quantum circuit of linear transformation MA.

$$\begin{cases}(p^{-1})_0=t^{-1}(p_0+p_1),\\(p^{-1})_1=t^{-1}p_1,\end{cases}\tag{4}$$

其中, $t=p_1^2\cdot\lambda+(p_0+p_1)p_0$, $\lambda=y^2\in GF(2^4)$. 根据式(4), 不难看出, 要实现有限域$GF((2^4)^2)$中的逆运算, 只需要实现$GF(2^4)$中的乘法运算和逆运算.

下面介绍有限域$GF(2^4)$中的乘法运算及其量子实现. 在$GF(2^4)$中, 任意两元素a和b可表示为

$$\begin{cases}a=a_0+a_1y+a_2y^2+a_3y^3,\\b=b_0+b_1y+b_2y^2+b_3y^3.\end{cases}\tag{5}$$

直接计算可得$a\cdot b$为

$$a\cdot b=(ab)_0+(ab)_1y+(ab)_2y^2+(ab)_3y^3,\tag{6}$$

其中, $(ab)_0$, $(ab)_1$, $(ab)_2$和$(ab)_3$分别为

$$\begin{aligned}(ab)_0&=(a_1+a_3)(b_1+b_3)+(a_2+a_3)(b_2+b_3)+a_0b_0\\&\quad+a_1b_1+a_3b_3,\\(ab)_1&=(a_0+a_1)(b_0+b_1)+(a_2+a_3)(b_2+b_3)+a_0b_0\\&\quad+a_1b_1+a_2b_2,\end{aligned}$$

$$(ab)_2 = (a_0 + a_2)(b_0 + b_2) + a_0b_0 + a_1b_1 + a_2b_2 + a_3b_3,$$

$$(ab)_3 = (a_0 + a_1 + a_2 + a_3)(b_0 + b_1 + b_2 + b_3) + a_0b_0 + (a_0 + a_2)(b_0 + b_2) + (a_0 + a_1)(b_0 + b_1) + a_2b_2.$$

根据式(6)给出$GF(2^4)$中乘法的量子电路如图 6所示, 需要12个量子比特、9个Toffoli门、25个CNOT门, Toffoli深度为5.

有限域$GF((2^4)^2)$中的逆运算$I'_{\mathcal{PB}}$需要将有限域$GF(2^4)$中两个数的乘法结果加上第三个数. 为此, 本文参考Li等人[9]的方法, 在不需要辅助比特的情况下实现有限域$GF(2^4)$中的三元运算$c+a\cdot b$. 该方法只需要在图 6量子电路前面添加一个量子电路, 具体如图 7所示, 其中m_1表示图 6的量子电路. 图 7所示的量子电路需要12个量子比特、9个Toffoli门、31个CNOT门, Toffoli深度为5.

接着实现$a^2\cdot\lambda$的量子电路, 其中$\lambda = y^2 \in GF(2^4)$, 设$a = a_0 + a_1y + a_2y^2 + a_3y^3$. 直接计算可得

$$a^2\cdot\lambda = a_1 + a_2 + (a_2 + a_3)y + (a_0 + a_2 + a_3)y^2 + (a_1 + a_2 + a_3)y^3. \tag{7}$$

根据式(7)实现$a^2\cdot\lambda$的量子电路如图 8所示, 需要4个量子比特和4个CNOT门.

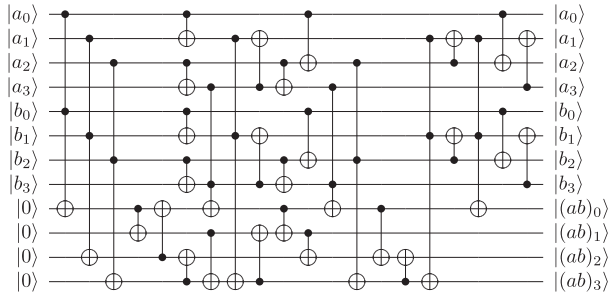


图 6 $GF(2^4)$中乘法量子电路

Figure 6 Quantum circuit of implementation the multiplication in $GF(2^4)$.

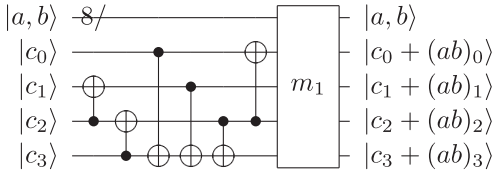


图 7 $GF(2^4)$中计算$c + a\cdot b$的量子电路

Figure 7 Quantum circuit of calculate $c + a\cdot b$ in $GF(2^4)$.

下面介绍如何实现有限域$GF(2^4)$中的逆运算的量子电路. 实际上这个工作已经有很多人做过了, 例如Saravanan等人[6]、Chung 等人[8]、Wang 等人[11]和Li等人[9]使用塔域分解技术, 将$GF(2^4)$中的元素映射到复合域$GF((2^2)^2)$中求逆元, 再映射回有限域$GF(2^4)$, 最终完成$GF(2^4)$中的求逆运算. 而Li等人[12]和李振强等人[29]则把$GF(2^4)$中的逆运算看成是一个4 × 4的S盒替换, 使用一个自动化工具LIGHTER-R[33]搜索其量子电路实现. 本文同样把$GF(2^4)$中的逆运算看作4×4的S盒替换, 但是使用一个比LIGHTER-R工具更为先进的DORCIS工具[3)]实现其量子电路. DORCIS工具[3)]可以4 × 4或3 × 3的S盒的量子电路, 并且电路深度或T深度比LIGHTER-R工具给出的电路更低或至少同等水平. 把$GF(2^4)$中的逆运算看作4 × 4的S盒, 其输入与输出如表 1所示.

根据表 1, 直接应用DORCIS工具[3)]搜索, 得到实现有限域$GF(2^4)$中逆运算的量子电路如图 9所示. 图 9所示的量子电路中包含1个CCCNOT门, 根据Li等人[12]和李振强等人[29], CCCNOT门可由如图 10所示电路实现. 因此实现图 9所示的电路需要5个量子比特、8个Toffoli门、7个CNOT门, Toffoli深度为8.

接下来实现$GF((2^4)^2)$中逆运算量子电路. 本文参考Li等人[9]的电路并对其进一步改进, 减少2个模块以节省8个CNOT门, 最终构造的实现有限域$GF((2^4)^2)$中逆运算量子电路如图 11所示. 其中, m_1为图 6的电

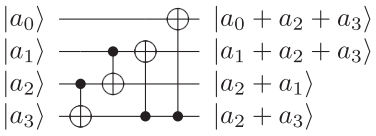


图 8 $GF(2^4)$中计算$a^2\cdot\lambda$的量子电路

Figure 8 Quantum circuit of calculate $a^2\cdot\lambda$ in $GF(2^4)$.

表 1 $GF(2^4)$中乘法逆的查找表

Table 1 Lookup table of the multiplicative inversion in $GF(2^4)$

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

3) Chun M, Baksi A, Chattopadhyay A. DORCIS: Depth optimized quantum implementation of substitution boxes. Cryptology ePrint Archive, 2023.

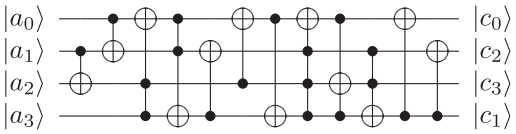


图 9 $GF(2^4)$中求逆运算的量子电路

Figure 9 Quantum circuit of implementation the inversion in $GF(2^4)$.

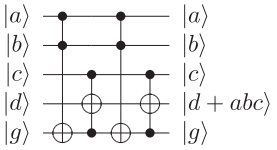


图 10 CCCNOT门的分解

Figure 10 Decomposition of CCCNOT gate.

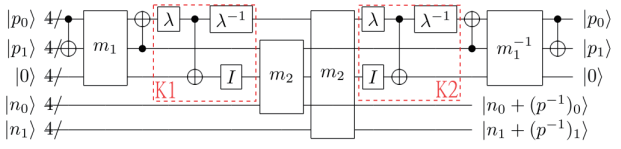


图 11 (网络版彩图) $GF((2^4)^2)$中求逆运算的量子电路

Figure 11 (Color online) Quantum circuit of implementation the inversion in $GF((2^4)^2)$.

路, 其作用为实现$|a\rangle|b\rangle|0^{\otimes 4}\rangle \to |a\rangle|b\rangle|a\cdot b\rangle$; m_1^{-1}为图6所示电路的逆电路, 其作用为实现$|a\rangle|b\rangle|a\cdot b\rangle \to |a\rangle|b\rangle|0^{\otimes 4}\rangle$; m_2为图7所示的电路, 其作用为实现$|a\rangle|b\rangle|c\rangle \to |a\rangle|b\rangle|c\oplus a\cdot b\rangle$; λ为图8所示的电路, 其作用为实现$|a\rangle \to |a^2\cdot\lambda\rangle$; λ^{-1}为图8所示电路的逆电路, 其作用为实现$|a^2\cdot\lambda\rangle \to |a\rangle$; I为图9所示的电路, 其作用为实现$|a\rangle \to |a^{-1}\rangle$. 此电路需要20个量子比特、52个Toffoli门、166个CNOT门, Toffoli深度为36.

图11所示的实现有限域$GF((2^4)^2)$中逆运算量子电路还可以进一步优化. 将图11中红色虚线框起来的部分分别记为电路K1和K2, 对这两部分电路做进一步优化, 得到的结果如图12和13所示, 与原电路相比, 各减少4个CNOT门. 用图12和13的量子电路替换图11中红色虚线框K1和K2, 可以得到新的实现$GF((2^4)^2)$中逆运算的量子电路, 需要20个量子比特、52个Toffoli门、158个CNOT门, Toffoli深度为36. 由于不可约多项式不同, 本文实现$GF((2^4)^2)$中逆运算的量子电路比李振强等人[29]的量子电路少2个Toffoli门和16个CNOT门, Toffoli深度减少6.

3.4 S盒的量子电路

本节根据式(3), 结合第3.2和3.3节的量子电路, 构造SM4算法S盒的量子电路如图14所示. 读者可通过我们提供的代码[4)]验证电路的正确性.

在图14所示的电路中, MA为图5的电路, 其作用为实现$|x\rangle \to |(MA)x\rangle$; AM^{-1}为图4的电路, 其作用为实现$|x\rangle \to |(AM^{-1})x\rangle$; $I'_{\mathcal{PB}}$为红色虚线框被图12和13替换后的图11的电路, 其作用为实现$|x\rangle|y\rangle|0^{\otimes 4}\rangle \to |x\rangle|y+x^{-1}\rangle|0^{\otimes 4}\rangle$, 异或$Mc$可以通过4个X门实现, 异或$c$可以通过5个X门实现. 图14所示的电路需要20个量子比特、52个Toffoli门、196个CNOT门、13个X门,

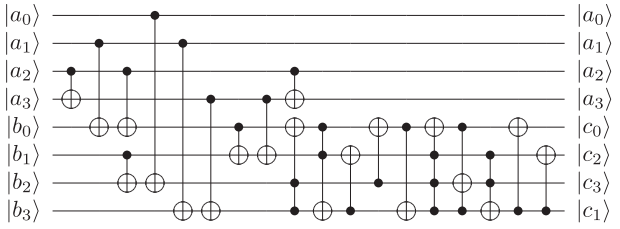


图 12 K1的量子电路

Figure 12 Quantum circuit of K1.

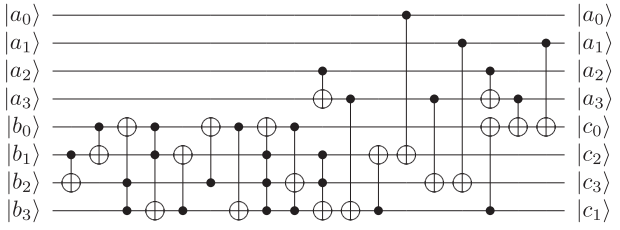


图 13 K2的量子电路

Figure 13 Quantum circuit of K2.

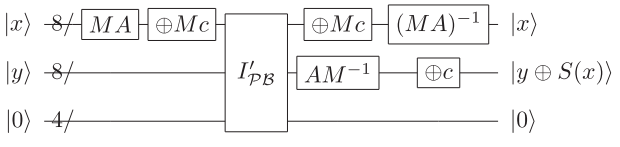


图 14 SM4算法S盒的量子电路

Figure 14 Quantum circuit of SM4's S-box.

4) https://github.com/hongmerly/Efficient-quantum-circuit-implementation-of-SM4-S-box.

Toffoli深度为36. 本文的SM4算法S盒量子电路与已有的SM4算法S盒电路比较如表 2所示.

从表 2可知, 与林达等人[13]的电路对比, 本文的量子电路所有指标都更好, 其中量子比特数少了2, Toffoli门数减少了30, CNOT门数减少了314, X门数减少了74, Toffoli深度减少了32. 与Lin等人[15]的电路相比, 本文的电路除了Toffoli深度略高之外, 其他的指标都比较好. 与Luo等人[16]的电路相比, 本文的量子电路多了2个CNOT门, 但是少了2个X门, Toffoli深度也减少了4.

罗庆斌等人[14]的量子电路比本文的电路少20个CNOT门, 但是多3个Toffoli门. 根据图 1所示的Toffoli门分解, 1个Toffoli门需要通过7个T门、7个CNOT门和2个H门实现, 并且T门的实现成本为CNOT门的46–350倍[29], 这意味着本文提出的电路量子门成本更低. 同时本文的Toffoli深度也更浅. 除此之外, 罗庆斌等人[14]的量子电路在执行结束后没有把辅助比特回收. 他们的电路每执行一次, 就需要消耗5个辅助量子比特. 这对于SM4算法来说代价是巨大的, 因为整个SM4需要执行256次S盒, 这意味着需要消耗$256\times5=1240$个辅助量子比特.

表 2基于NCT门集分析量子资源, 而在量子计算领域还有另一种通用量子门集也经常被拿来分析量子资源, 那就是Clifford+T门集. 本文也可用Clifford+T门集分析量子资源, 但需要指出, 本文图 11所示电路中的前3个Toffoli门可以更换为QAND门, 而最后3个Toffoli门可以更换为QAND†门, 于是得到本文新的统计开销为20个量子比特、46个Toffoli门、3个QAND门、3个QAND†门、196个CNOT门和13个X门, T深度为$3\times36=108$. 转换为Clifford+T门集计算, 则需要334个T门、548个CNOT门、129个1qCliff门. 本文的量子电路基于Clifford+T门集统计的开销与其他文献的比较如表 3所示.

由表 3可知, 本文提出的SM4算法S盒的量子电路除了T深度比较高之外, 无论是量子比特数、T门数、CNOT门数还是1qCliff门数都是最少的. Lin等人[15]的电路, 虽然T深度最少, 但是T门数却是最多的. 而Zou等人[17]的电路看似在T深度与T门数之间取得了一个平衡, 但是需要的量子比特数、CNOT门数和1qCliff门数都是最多的. 因此如果从量子比特数和量子门开销方面分析, 忽略T深度略高这个因素, 本文的量子电路在以上三者中是最好的.

表 2 S盒电路与其他文献比较(基于NCT门集)

Table 2 Comparsion of our S-box circuit with other studies (based on NCT gate)

S盒	#qubits	#Toffoli	#CNOT	#X	Toffoli深度
[本文]	20	52	196	13	36
林达等人[13]	22	82	510	87	68
罗庆斌等人[14]	21	55	176	10	46
Lin等人[15]	21	59	203	13	24
Luo等人[16]	20	52	194	15	40

表 3 S盒电路与其他文献比较(基于Clifford+T门集)

Table 3 Comparsion of our S-box circuit with other studies (based on Clifford+T gate)

S盒	#qubits	#T	#CNOT	#1qCliff	T深度
[本文]	20	334	548	129	108
Lin等人[15]	21	413	616	131	72
Zou等人[17]	23	338	680	223	86

4 结论

本文使用塔域分解技术实现了高效的SM4算法S盒的量子电路. 与已有的文献对比, 本文设计的SM4算法S盒的量子电路需要的量子比特数最少, Toffoli门数和T门数最少. 因此本文的SM4算法S盒的量子电路与已有文献相比, 在量子比特数和量子门开销方面有一定的优势.

参考文献

1 Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev, 1999, 41: 303–332

2 Simon D R. On the power of quantum computation. SIAM J Comput, 1997, 26: 1474–1483

3 Grover L K. A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing. Philadelphia, 1996. 212–219

4 Grassl M, Langenberg B, Roetteler M, et al. Applying Grover's algorithm to AES: Quantum resource estimates. In: Proceedings of the 7th International Workshop on Post-Quantum Cryptography. Cham: Springer, 2016. 29–43

5 Daemen J, Rijmen V. Announcing the advanced encryption standard (AES). Federal Information Processing Standards Publication, 2001, 197: 1–51

6 Saravanan P, Kalpana P. Novel reversible design of advanced encryption standard cryptographic algorithm for wireless sensor networks. Wireless Pers Commun, 2018, 100: 1427–1458

7 Jaques S, Naehrig M, Roetteler M, et al. Implementing Grover oracles for quantum key search on AES and LowMC. In: Advances in Cryptology-EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30. Cham: Springer International Publishing, 2020. 280–310

8 Chung D, Lee S, Choi D, et al. Alternative tower field construction for quantum implementation of the AES S-box. IEEE Trans Comput, 2021, 71: 2553–2564

9 Li Z Q, Cai B B, Sun H W, et al. Novel quantum circuit implementation of Advanced Encryption Standard with low costs. Sci China-Phys Mech Astron, 2022, 65: 290311

10 Huang Z, Sun S. Synthesizing quantum circuits of AES with lower T-depth and less qubits. In: International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer Nature Switzerland, 2022. 614–644

11 Wang Z G, Wei S J, Long G L. A quantum circuit design of AES requiring fewer quantum qubits and gate operations. Front Phys, 2022, 17: 41501

12 Li Z, Gao F, Qin S, et al. New record in the number of qubits for a quantum implementation of AES. Front Phys, 2023, 11: 1171753

13 Lin D, Xiang Z J, Zhang R L, et al. Quantum implementation of SM4 (in Chinese). J Cryptol Res, 2021, 8: 999–1018 [林达, 向泽军, 张若琳, 等. SM4算法的量子实现. 密码学报, 2021, 8: 999–1018]

14 Luo Q B, Li X Y, Yang G W, et al. Quantum circuit implementation of S-box for SM4 cryptographic algorithm based on composite field arithmetic (in Chinese). J Univ Electron Sci Technol China, 2022, 51: 812–818 [罗庆斌, 李晓瑜, 杨国武, 等. 基于复合域SM4密码算法S盒的量子电路实现. 电子科技大学学报, 2022, 51: 812–818]

15 Lin D, Xiang Z, Xu R, et al. Quantum circuit implementations of SM4 block cipher based on different gate sets. Quantum Inf Process, 2023, 22: 282

16 Luo Q B, Li Q, Li X Y, et al. Quantum implementaion of SM4 block cipher with less qubits. 2023, PREPRINT (Version 1) available at Research Square

17 Zou J, Li L, Wei Z, et al. New quantum circuit implementations of SM4 and SM3. Quantum Inf Process, 2022, 21: 181

18 Chen C, Guo H, Wang C, et al. A fast software implementation of SM4 based on composite fields (in Chinese). J Cryptol Res, 2023, 10: 289–305 [陈晨, 郭华, 王闯, 等. 一种基于复合域的国密SM4算法快速软件实现方法. 密码学报. 2023, 10: 289–305]

19 Itoh T, Tsujii S. A fast algorithm for computing multiplicative inverses in GF(2^m) using normal bases. Inf Computat, 1988, 78: 171–177

20 Rijmen V. Efficient implementation of the Rijndael S-box. Technical Report. Belgium: Katholieke Universiteit Leuven, Dept. ESAT. 2000

21 Rudra A, Dubey P K, Jutla C S, et al. Efficient Rijndael encryption implementation with composite field arithmetic. In: Cryptographic Hardware and Embedded Systems-CHES 2001: Third International Workshop. Berlin, Heidelberg: Springer, 2001. 171–184

22 Wolkerstorfer J, Oswald E, Lamberger M. An ASIC implementation of the AES SBoxes. In: Topics in Cryptology-CT-RSA 2002: The Cryptographers' Track at the RSA Conference. Berlin, Heidelberg: Springer, 2002. 67–78

23 Canright D. A very compact Rijndael S-box. Technical Report. Monterey: Naval Postgraduate School, 2004

24 Canright D. A very compact S-box for AES. In: International Workshop on Cryptographic Hardware and Embedded Systems. Berlin, Heidelberg: Springer, 2005. 441–455

25 Boyar J, Peralta R. A new combinational logic minimization technique with applications to cryptology. In: Festa P, ed. Experimental Algorithms. SEA 2010. Lecture Notes in Computer Science, vol 6049. Berlin, Heidelberg: Springer, 2010. 178–189

26 Boyar J, Peralta R. A small depth-16 circuit for the AES S-box. In: IFIP International Information Security Conference. Berlin, Heidelberg: Springer, 2012. 287–298

27 Liu F, Ji W, Hu L, et al. Analysis of the SMS4 block cipher. In: Information Security and Privacy: 12th Australasian Conference, ACISP 2007. Berlin, Heidelberg: Springer, 2007. 158–170

28 Wei Z, Sun S, Hu L, et al. Searching the space of tower field implementations of the $\mathbb{F}_{2^8}$ inverter-with applications to AES, Camellia and SM4. Int J Inform Comput Secur, 2023, 20: 1–26

29 Li Z Q, Gao F, Qin S J, et al. Quantum circuit for implementing Camellia S-box with low costs (in Chinese). Sci Sin-Phys Mech Astron, 2023, 53: 240313 [李振强, 高飞, 秦素娟, 等. 以低成本实现Camellia算法S盒的量子电路. 中国科学: 物理学 力学 天文学, 2023, 53: 240313]

30 Amy M, Maslov D, Mosca M, et al. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. IEEE Trans Comput-Aided Des Integr Circuits Syst, 2013, 32: 818–830
31 Wang L, Gong Z, Liu Z, et al. Fast software implementation of SM4 based on tower field (in Chinese). J Cryptol Res, 2022, 9: 1081–1098 [王磊, 龚征, 刘哲, 等. 基于塔域的SM4算法快速软件实现. 密码学报. 2022, 9: 1081–1098]
32 Xiang Z, Zeng X, Lin D, et al. Optimizing implementations of linear layers. In: IACR Transactions on Symmetric Cryptology, 2020. 120–145
33 Dasu V A, Baksi A, Sarkar S, et al. LIGHTER-R: Optimized reversible circuit implementation for sboxes. In: 2019 32nd IEEE International System-on-Chip Conference (SOCC). IEEE, 2019. 260–265

Efficient quantum circuit implementation of the SM4 S-box

LIU JiaHong, TAN XiaoQing*, LI Ming & BAO DaiPengWei

College of Information Science and Technology, Jinan University, Guangzhou 510632, China
**Corresponding author (email: ttanxq@jnu.edu.cn)*

In recent years, the quantum circuit implementation in symmetric cryptography has attracted widespread attention. The SM4 block cipher algorithm is China's first commercial cipher standard and was accepted as an ISO/IEC international standard in 2021. S-box is the most complex component in the SM4 block cipher algorithm. This study investigates the quantum circuit implementation of the SM4 S-box. Based on the algebraic structure, using tower filed decomposition technology, the quantum circuit of the SM4 S-box is built. Based on the number of NCT gate sets, our quantum circuit requires 20 qubits, 52 Toffoli gates, 196 CNOT gates, and 13 X gates. The Toffoli depth of our circuit is 36. Compared with previous literature, the quantum circuit proposed herein requires fewer quantum resources.

SM4 algorithm, S-box, quantum circuit, tower filed decomposition

PACS: 03.67.Lx, 03.67.Dd, 03.67.Pp

doi: 10.1360/SSPMA-2023-0386