SM3 杂凑函数低 T 深度量子线路实现

邹剑[1,2]，李俊康[1,2]，郭楠生[1,2]，孙莹[3]，李子臣[4]
（1.福州大学计算机与大数据学院，福建 福州 350108；2.福州大学网络系统信息安全福建省高校重点实验室，福建 福州 350108；
3.北京电子科技学院密码科学与技术系，北京 100070；4.北京印刷学院信息工程学院，北京 102600）

摘要：针对 SM3 杂凑函数量子线路因“原地计算”导致 T 深度过高的问题，提出了一种低 T 深度架构。通过引入基于 Wallace 树的量子保留进位加法器与低深度全/半加器，将多操作数模加路径压缩至常数级；并分配额外量子比特存储中间状态，免除了回收辅助量子比特产生的高 T 深度操作。实验表明，在消耗 5 453 个量子比特的前提下，线路 T 深度从 4 528 压缩至 1 712，T 门总数从 965 632 降至 314 11。该方案为对称密码的后量子安全性评估提供了高效途径。

关键词：量子线路；SM3；量子保留进位加法器；T 深度优化
中图分类号：TP309.7
文献标志码：A
doi：10.11959/j.issn.1000–436x.TXXB260224

Low T-depth quantum circuit implementation of SM3 hash function

Zou Jian[1,2], Li Junkang[1,2], Guo Nansheng[1,2], Sun Ying[3], Li Zichen[4]
1. College of Computer and Data Science, Fuzhou University, Fuzhou 350108, China
2. Key Laboratory of Network Systems and Information Security, Fuzhou University, Fuzhou 350108, China
3. Department of Cryptography Science and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China
4. School of Information Engineering, Beijing Institute of Graphic Communication, Beijing 102600, China

Abstract: To address the high T-depth issue in SM3 hash function quantum circuits caused by in-place computation, a low T-depth architecture was proposed. By introducing Wallace tree-based quantum carry-save adders and low-depth full/half adders, the multi-operand modular addition path was compressed to a constant level. Furthermore, allocating extra qubits to store intermediate states eliminated the high T-depth operations required for uncomputing ancilla qubits. Experiments demonstrate that using 5 453 qubits reduced the circuit T-depth from 4 528 to 1 712 and decreased the total T-gate count from 965 632 to 314 112. The proposed scheme provides an efficient approach for evaluating the post-quantum security of symmetric cryptography.

Key words: quantum circuit, SM3, quantum carry-save adder, T-depth optimization

0 引言

随着量子科学和计算机技术的飞速演进[1]，研究人员发现利用量子并行性能够高效求解现有部分主流密码算法所采用的数学难题，从而对当前全球信息安全密码体系的安全性构成系统性的潜在威胁。例如，Shor 算法[2]能够在多项式时间内破解基于大整数分解和离散对数求解难题的公钥加密方法如 RSA（Rivest, Shamir, Adleman）密码体制[3]和椭圆曲线密码体制（ECC）[4]。此外，Grover 算法[5]能对传统搜索问题实现穷举搜索效率的平方倍加

收稿日期：2026–04–24；修回日期：2026–07–01
通信作者：孙莹，sunybesti@foxmail.com
基金项目：国家密码科学基金资助项目（No.2025NCSF02012）
Foundation Item：The National Cryptologic Science Fund of China (No.2025NCSF02012)

速，对高级加密标准（AES）[6]、SHA-2[7]以及SHA-3[8]等对称密码和杂凑算法的抗穷举攻击能力提出了新的挑战。另外，Simon 算法[9]能高效解决特定的周期问题，对相关算法的设计提出了新的挑战。

为了应对量子计算带来的明确挑战，美国国家标准与技术研究院（National Institute of Standards and Technology, NIST）启动了后量子密码（PQC）标准算法的全球征集工作[10]。NIST 在制定新的算法安全等级时指出，现有量子算法的复杂度评估较为困难，可以用量子线路的实现代价作为对应量子攻击的复杂度评价指标，因而学界迫切需要对密码算法建立高效的量子线路实现方案。目前，对于量子线路优化的研究主要围绕量子比特数与线路 T 深度这两个核心指标展开。

在量子线路优化方面，研究者主要聚焦于减少量子比特的数量（即降低线路宽度）。例如，Grassl 等[11]对 AES 算法首次构建了仅需 40 个量子比特的 S 盒。此后，Almazrooie 等[12]与 Langenberg 等[13]分别通过优化乘法逆元和塔域分解技术，将 AES-128 的总量子比特数压缩至 976 个和 864 个。2020 年，Zou 等[14]利用改进的 zig-zag 结构，仅用 512 个量子比特便实现了 AES-128。2022 年，Wang 等[15]提出了一种新颖的“线性密钥扩展”方法，在不增加过多深度的情况下，成功将 AES-128 的量子比特消耗量进一步降至 400 个。同年，Li 等[16]创新性地设计了仅需 20 个量子比特的原地（in-place）S 盒实现，从而将 AES-128 整体线路的极限宽度下探至 270 个量子比特。2023 年，Lin 等[17]对 AES 算法 S 盒的经典实现进行了重新划分，进一步设计了该算法的 S 盒及其逆的低宽度量子实现。在 Eurocrypt 2025 上，Huang 等[18]基于向量布尔函数最小宽度理论，实现了仅需 9 个量子比特的 AES 算法 S 盒。

在优化线路 T 深度方面，研究焦点开始转向“以量子比特数换 T 深度”。Jaques 等[19]首次引入基于测量的极低深度量子与（QAND）门，从底层门级组件上为对称密码的极低 T 深度优化确立了全新的基础。Li 等[20]提出了 T 深度仅为 4 的 S 盒线路，将 AES-128 整体 T 深度减至 80； Huang 和 Sun[21]在 Asiacrypt 2022 上提出了 T 深度为 3 的 S 盒，成功构建了 T 深度为 60 的 AES-128 线路。Liu 等[22]提出了基于“共享思想”的组合管道架构，在不增加 T 深度的前提下将 S 盒辅助比特降至 83 个。Shi 等[23]提出压缩流水线新架构，进一步将 AES-128 的 T 深度极限压缩至 33。在 Eurocrypt 2025 上，Huang 等[18]从代数结构理论出发，提出了一种构建最小 T 深度量子线路的系统化方法，成功设计出了 T 深度仅为 3 且 Clifford 门数量显著优化的极紧凑 AES 算法 S 盒线路。这种“量子比特数与 T 深度权衡”的优化理念也迅速扩展至其他对称密码和流密码体系，如针对 Camellia[24-25]、SM4[26-28]，以及 ZUC[29-30]的低宽度构造和低 T 深度构造。

此外，在容错量子计算（fault-tolerant quantum computing, FTQC）环境中，量子态极易受环境噪声的影响而导致退相干，NIST 在制定后量子安全标准时引入了最大相干运行深度（MaxDepth）的约束[10]，即单次量子程序的执行时间不能超过设备量子态退相干的极限。当针对密码杂凑函数的单一 Grover 搜索线路深度超出该硬件限制时，攻击者将被迫采用并行 Grover 算法以缩短执行时间。然而，Grover 算法的并行化面临着严苛的平方级空间惩罚，即深度每降低一半，需付出平方级的量子比特代价[19]。基于这一特性，简单的深度与宽度乘积（T-DW cost = T-depth×Width）不足以真实评估在量子计算机上使用 Grover 算法的攻击代价，因此 Jang 等[31]在探讨 NIST 后量子安全强度时指出，在考量 MaxDepth 约束与并行 Grover 模型时，深度应当被赋予更高的权重，综合资源评估指标应转换为 TD^2-M cost（即 $T\text{-depth}^2\times\text{Width}$）。该指标已经成为当前衡量量子密码算法硬件实现成本的更科学的标尺。因此，将单一线路的 T 深度压缩至极限水平，不仅能够提升执行效率，更是为了在 MaxDepth 的约束下，降低对 Grover 并行化的依赖，进而从根本上削减综合资源代价。

作为我国的杂凑函数标准，SM3 的量子线路的优化研究正逐步逼近极限。早期的研究主要聚焦于降低量子比特数。2021 年，Song 等[32]首先提出了一种实现方案，其消耗了 2 721 个量子比特，且 T 深度高达 117 120。2022 年，Zou 等[27]通过复用机制构建了仅需 33 个可复用辅助量子位的 SM3 线路，其整体消耗量子比特数为 970，T 深度为 25 344。随着容错量子计算对执行效率要求的提升，研究方向开始转向降低线路的 T 深度。2026 年，杨婷玉等[33]通过常数与变量的分组模加优化，提出了仅消耗 779 个量子比特的低宽度实现，而且提出了两

种低T深度方案，将T深度成功压缩至7 040和7 136，同时消耗约1 130和1 098个量子比特。邹剑等[34]引入基于QAND门优化的低T深度量子加法器，并探索了量子组件的重新排列优化整体线路，对SM3提出了一种新型低T深度方案，将T深度极致压缩至4 528，同时消耗1 369个量子比特。然而，本文发现现有的SM3量子线路研究在优化T深度时，大多受限于原地计算的范式，即将计算结果直接覆盖于原输入寄存器的状态空间内。为了维持低宽度水平，这些方案必须在每一轮更新后执行复杂的反计算以清空量子比特，限制了T深度的下降空间。

针对SM3杂凑函数量子线路因“原地计算”导致T深度高的问题，本文提出了一种高效量子线路架构。本文的主要贡献如下。

（1）通过使用非原地（out-of-place）的方式计算轮间状态，即分配全新的干净辅助量子比特以存储计算结果，本文打破了之前线路设计中对轮函数状态寄存器原地更新的依赖，并提出了一种新型SM3量子线路设计，实现了更低的T深度。

（2）针对SM3轮函数中密集的多操作数连加需求，本文引入基于Wallace树的量子保留进位加法器（quantum carry-save adder, QCSA），并结合低深度的量子全加器（quantum full adder, QFA）与量子半加器（quantum half adder, QHA），成功将多操作数模加的路径压缩至常数级别。

（3）刷新了SM3量子线路资源的纪录。表1展示了SM3量子线路的资源消耗对比，其中，#T表示T门总数，#CNOT表示受控非（controlled-NOT, CNOT）门（lqClifford门）总数，#1qcliff为单量子比特的Clifford门总数，包括Hadamard门、X门等。为了合理对比相关资源实现代价，本文引入了TD^2-M cost指标进行资源消耗的量化评估。需要注意的是，文献[27,33-34]未统计TD^2-M cost，表1中相关方案的TD^2-M cost均由本文依据其公开的基础数据统一推算得出，以便在同一基准下进行对比。结果表明，本文方案尽管增加了量子比特数，但实现了CNOT门数与T深度的大幅下降，本文方案在T深度、CNOT门数和TD^2-M cost等值上显著优于对比方案。

1　相关工作

在SM3等密码杂凑函数的量子线路实现中，模2^n加法器是调用频繁且消耗资源最多的核心非线性组件。随着FTQC中对于降低T深度的要求增加，量子模加器的设计经历了从降低辅助量子比特到追求极低T深度的演进。

2004年，Cuccaro等[35]提出了一种经典的量子串行进位加法器（quantum ripple-carry adder, QRCA）。该结构的最大优势在于极致的空间效率，对于n比特的模加运算，仅需消耗一个辅助量子比特用于存储初始进位。但其采用逐位传递进位信号的串行逻辑，Toffoli深度与操作数位宽n成正比，这在对时间敏感的量子密码分析中将导致不可接受的执行时延。

为了突破QRCA的深度瓶颈，Draper等[36]于2006年引入经典计算中的超前进位逻辑，设计出了量子超前进位加法器（quantum carry-lookahead adder, QCLA）。该设计定义了两个核心的基础信号：进位生成信号g与传播信号p。具体而言，信号g表示当前操作数位是否能够独立产生向高位的进位，而信号p则表示当前位是否会将来自低位的进位继续向高位传递。在此逻辑基础上，Draper等[36]创新性地构建了基于二叉树结构的区间生成信号G_{ij}与区间传播信号P_{ij}，使从最低位到任意高位的进位均可通过并行计算提前得出，而不需要等待低位的逐位传递。这一设计成功将Toffoli深度从线性级压缩至对数级$O(\log n)$，大幅提升了量子加法器的运算速度，为后续密码算法的并行化奠定了基础。

随着对低深度量子线路需求的不断增加，

表1　SM3量子线路资源消耗对比

方案	T深度	量子比特数	#T	#CNOT	#1qcliff	TD^2-M cost
本文方案	1 712	5 453	314 112	857 792	297 280	1.59×10^{10}
文献[34]方案	4 528	1 369	965 632	2 310 528	905 984	2.80×10^{10}
文献[33]方案	7 040	1 130	662 528	1 782 656	1 201 216	5.60×10^{10}
文献[27]方案	25 344	970	1 187 072	1 370 432	420 160	6.23×10^{11}

Wang 等[37]在 Draper 工作的基础上对数种量子前缀树架构进行了系统性探索，指出 Draper 等[36]的 QCLA 所使用的 Brent-Kung 树由于逻辑层级较深，并非低深度的最优选择，同时提出了一种基于 Sklansky 并行前缀树结构的最优深度量子加法器。在具体的量子实现上，Wang 等[37]的设计引入了大量可复零的辅助量子比特，利用 CNOT 门将关键的 p 信号和 g 信号进行状态复制以支持高度并行的区间信号传播。此外，该加法器采用了完全非原地的架构，并利用逻辑与门结构替代部分成对 Toffoli 门以减少深度。虽然该加法器消耗了较多的量子比特数，但成功将 32 位模加器的 Toffoli 深度压缩至 $\log n + 1$ 水平，相比经典的 Draper QCLA 实现了近 50% 的深度缩减，达到当前量子模加器的最优深度。

纵观上述密码算法与量子加法器的演进历程可以发现，通过引入大量辅助比特来实现非原地计算与高度并行化，已成为突破 T 深度下界的必然途径。但现有的加法器均是针对双操作数设计的。面对 SM3 轮函数中高频出现的 4～5 个操作数连加，若直接采用双操作数加法器进行串行级联，深度的线性累加将成为限制整体线路执行速度的瓶颈。因此，探索适用于多操作数并行压缩的底层加法架构，是本文进一步突破 SM3 时间复杂度的重要切入点。

2　预备知识

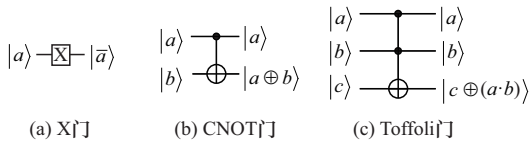
2.1　量子线路与量子门

量子计算以量子位（qubit）作为基本信息单元，通过量子逻辑门的序列（即量子线路）实现信息的演化。评估用于密码分析的量子线路的性能时，通常采用 Clifford+T 门集。该门集由 Clifford 门（如 X 门、CNOT 门、Hadamard 门等）和非 Clifford 门（T 门）组成。

（1）量子非门（X 门）作用于单量子比特，实现逻辑非操作，将状态 $|a\rangle$ 映射为 $|a\oplus 1\rangle$，其线路如图 1(a)所示。

（2）CNOT 门作用于两个量子比特，当控制位为 $|1\rangle$ 时，目标位执行异或操作，映射关系为 $|a,b\rangle \to |a,a\oplus b\rangle$，其线路如图 1(b)所示。

（3）Toffoli 门，也称控控非（CCNOT）门，是经典逻辑与运算对应的量子运算，映射关系为 $|a,b,c\rangle \to |a,b,c\oplus(a\cdot b)\rangle$，其线路如图 1(c)所示。



(a) X门　(b) CNOT门　(c) Toffoli门

图 1　基础量子门线路

对 Toffoli 门的分解方案有很多种，Amy 等[38]实现了 T 深度为 3、宽度为 3 的 Toffoli 门分解方案，具体实现如图 2 所示。

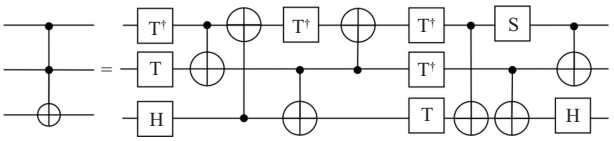


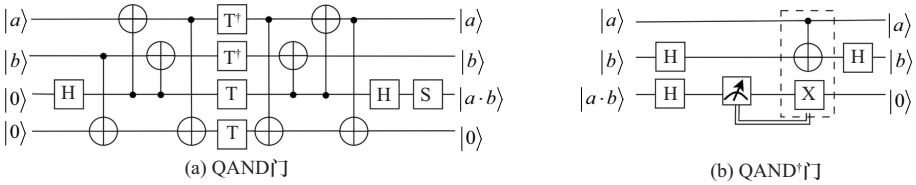
图 2　T 深度为 3、宽度为 3 的 Toffoli 门实现

文献[19]中提出的 QAND 门仅需 4 个 T 门且 T 深度为 1，由于该设计所消耗的 T 门数量最小并且深度最低，因此本文引入 QAND 门来实现 Toffoli 门的功能。QAND† 门的 T 深度为 0。文献[19]的 QAND 门与 QAND† 门如图 3 所示。

2.2　SM3 杂凑函数

SM3 是我国自主设计的杂凑函数标准[39]，其输入为长度 l（$l < 2^{64}$）比特的消息 m，经过消息填充、分组与扩展和迭代压缩，最终生成 256 比特的杂凑值。其具体算法流程说明如下。

（1）消息填充。为了使填充后的消息长度为 512 比特的整数倍，需要进行消息填充。首先在原始消息 m 末尾添加一个比特“1”；然后添加 k 个比特“0”，其中 k 是满足 $l + 1 + k \equiv 448 \pmod{512}$ 的



(a) QAND门　(b) QAND†门

图 3　文献[19]的 QAND 门与 QAND† 门

最小非负整数；最后，添加一个64比特的位串，该位串为原始消息长度l的二进制表示。填充后的消息m'长度为$n \times 512$比特。

（2）消息分组与扩展。将填充后的消息m'按512比特进行分组：$m' = B^{(0)}B^{(1)}\cdots B^{(n-1)}$。对于每个消息分组$B^{(i)}$，通过消息扩展算法生成132个32比特的字，用于后续压缩运算，包括$W_0,W_1,\cdots,W_{67}$和$W_0',W_1',\cdots,W_{63}'$。首先将$B^{(i)}$划分为16个字$W_0,W_1,\cdots,W_{15}$。对于$j = 16,\cdots,67$，W_j的计算式为：

$$W_j = P_1\left(W_{j-16}\oplus W_{j-9}\oplus\left(W_{j-3}\lll 15\right)\right)\oplus\left(W_{j-13}\lll 7\right)\oplus W_{j-6} \tag{1}$$

其中，$P_1(X) = X\oplus(X\lll 15)\oplus(X\lll 23)$为置换函数，$\oplus$表示按位异或，$\lll$表示循环左移。对于$j = 0,\cdots,63$所需的$W_j'$消息扩展为：

$$W_j' = W_j\oplus W_{j+4} \tag{2}$$

（3）迭代压缩。SM3算法使用迭代压缩结构，其压缩函数为CF。设IV为256比特的初始向量，迭代过程$V^{(i+1)} = \mathrm{CF}(V^{(i)},B^{(i)})\oplus V^{(i)}, 0 \leqslant i \leqslant n-1$。其中，$V^{(0)} = \mathrm{IV}$，$V^{(n)}$为最终杂凑值。压缩函数CF将$V^{(n)}$载入$A\sim H$共8个32比特寄存器中，执行64轮迭代。每轮迭代的计算方式如算法1所示。

算法1 迭代压缩算法

输入 $V_0,W_0,W_1,\cdots,W_{67},W_0',W_1',\cdots,W_{63}'$

输出 V_n

1)for $j = 0$ to 63 do

2) $\mathrm{SS}_1 = ((A\lll 12) + E + (T_j\lll j))\lll 7$

3) $\mathrm{SS}_2 = \mathrm{SS}_1\oplus(A\lll 12)$

4) $\mathrm{TT}_1 = \mathrm{FF}_j(A,B,C) + D + \mathrm{SS}_2 + W_j'$

5) $\mathrm{TT}_2 = \mathrm{GG}_j(E,F,G) + H + \mathrm{SS}_1 + W_j$

6) $D = C$

7) $C = B\lll 9$

8) $B = A$

9) $A = \mathrm{TT}_1$

10) $H = G$

11) $G = F\lll 19$

12) $F = E$

13) $E = P_0(\mathrm{TT}_2)$

14)end for

算法1中，加号代表模2^{32}的加法运算，步骤13)中$P_0(X) = X\oplus(X\lll 9)\oplus(X\lll 17)$，$T_j$为算法常量，$\mathrm{FF}_j$和$\mathrm{GG}_j$为布尔函数，定义如下：

$$\mathrm{FF}_j(X,Y,Z) = \begin{cases} X\oplus Y\oplus Z, & 0 \leqslant j \leqslant 15 \\ (X\wedge Y)\vee(X\wedge Z)\vee(Y\wedge Z), & 16 \leqslant j \leqslant 63 \end{cases} \tag{3}$$

$$\mathrm{GG}_j(X,Y,Z) = \begin{cases} X\oplus Y\oplus Z, & 0 \leqslant j \leqslant 15 \\ (X\wedge Y)\vee(\neg X\wedge Z), & 16 \leqslant j \leqslant 63 \end{cases} \tag{4}$$

2.3 并行前缀加法与保留进位算术基础

在大数模加运算中，传统的串行进位加法器由于进位信号的逐位横向传递，存在线性深度瓶颈。为了实现时间复杂度的对数级加速，计算体系结构中通常引入并行前缀树架构。该架构首先对所有操作数位并行预计算出进位生成信号g和传播信号p，随后利用树状网络在lb$n$层内并行结合得出所有位的进位信号，最终实现高速双操作数求和。

然而，在面对3个或更多操作数连加的场景时，仅依靠双操作数前缀树的串行级联仍会导致深度成倍增加。为此，经典算术逻辑中引入了保留进位加法器（carry-save adder, CSA）。其核心机制在于延迟进位传播，即在多操作数相加时，采用位级并行的纵向压缩机制，将本位的部分和与向高位的进位独立保存为两个全新向量，而不进行横向传递。由于切断了横向依赖，CSA单层压缩的路径为常数级别。

上述宏观架构在经典数字电路中的算术逻辑设计中应用广泛，但在容错量子计算环境中，受限于量子不可克隆定理以及非Clifford门（如Toffoli门）极高的物理代价，如何将这些理论架构转化为底层的极低深度量子逻辑门网络，并适配具体密码算法（如SM3杂凑函数）的多模加操作，仍是极其复杂的工程挑战。本文将详细探讨面向SM3算法定制化的底层组件重构与线路映射方法。

3 低T深度量子线路实现组件

3.1 基于Sklansky并行前缀树结构的量子加法器

下面以两个n比特操作数$A = a_n\cdots a_1$与$B = b_n\cdots b_1$为例，详细介绍Wang等[37]的基于Sklansky并行前缀树结构的最优深度量子加法器的计算流程。

（1）初始传播与生成信号的预计算。对每一位 i（$1 \leqslant i \leqslant n$），并行计算初始的进位传播信号 p_i 与进位生成信号 g_i，$p_i = a_i \oplus b_i$，$g_i = a_i \cdot b_i$。

（2）基于 Sklansky 树的区间信号传播。定义区间生成信号 $G_{i:j}$ 与区间传播信号 $P_{i:j}$，两个相邻区间信号的结合操作为 $(G_{i:j},P_{i:j}) = (g_i,p_i) \circ (G_{i-1:j},P_{i-1:j}) = (g_i \oplus (p_i \cdot G_{i-1:j}),p_i \cdot P_{i-1:j})$。在经典的 Sklansky 树中，低位的进位信号需要向多个高位分支传递。为了在量子线路中实现这一步骤，Wang 等[37]利用 CNOT 门将低位的 $G_{i:j}$ 信号的状态复制到全新的辅助比特上。通过 lb$n$ 层的并行计算，将输出所有的进位信号 $c_i = G_{i:1}$。

（3）区间传播信号 $P_{i:j}$ 的反计算。在所有进位信号 c_i 均计算得出后，逆序执行 Sklansky 树中用于计算区间传播信号 $P_{i:j}$ 及其复制状态的逻辑门。该步骤使大量辅助量子比特被重置为初始态，可以在后续过程中复用，优化了整体的空间开销。

（4）求和与初始 p_i 的反计算。获得所有进位信号 c_i 后，最终的加法和 s_i 可通过完全并行的 CNOT 门生成，即 $s_i = p_i \oplus c_i$。同时，利用 $b_i = p_i \oplus a_i$ 的操作，将步骤（1）中产生的初始进位传播信号 p_i 反计算清零。最终，除了承载进位与和的必要量子比特外，其余辅助比特均被完美复原。

为直观展示基于 Sklansky 树的并行区间信号传播机制，图 4 展示了 $n = 4$ 时的量子 Sklansky 前缀树结构。第 1 层首先进行初始进位传播信号与进位生成信号的预计算过程得到 (p_i,g_i)，其中 $1 \leqslant i \leqslant 4$。第 2 层进行进位传播过程，相邻的 (p_1,g_1) 与 (p_2,g_2) 结合生成 $(G_{2:1},P_{2:1})$，同时 (p_3,g_3) 与 (p_4,g_4) 结合。在关键的第 3 层中，低位生成的进位信息 $G_{2:1}$ 需要同时传递给高位的第 3 位和第 4 位，量子线路利用 CNOT 门引入干净的辅助比特对 $G_{2:1}$ 进行复制，从而并行地计算出 $c_3 = G_{3:1}$ 与 $c_4 = G_{4:1}$。这种结构确保了加法器的 Toffoli 深度严格受限于树的高度，接下来只需要进行反计算步骤清空辅助比特。

为了计算 SM3 轮函数中间状态，本文需要构建低深度的双操作数模加器。Wang 等[37]提出了 Sklansky 加法器的基础架构，在此基础上，本文对其底层门级实现进行了重构，具体而言，将加法器中的 Toffoli 门替换为 QAND 门，基于此策略，具体资源消耗如表 2 所示。

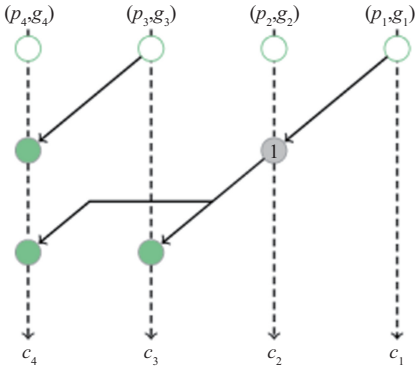


图 4　$n = 4$ 时的量子 Sklansky 前缀树结构

表 2　基于 Sklansky 结构的 2ⁿ 量子模加器资源消耗

操作数位宽 n	T 深度	量子比特数	#T	#CNOT	#1qcliff
31	8	259	1 024	2 321	806
30	8	246	972	2 202	765

3.2　量子保留进位加法器

尽管基于并行前缀树的加法器[37]已将双操作数模加的 T 深度压缩至极低水平，但 SM3 与 SHA-2 等杂凑函数的轮函数中往往包含密集的多操作数连加运算（例如 SM3 中 TT_1 和 TT_2 的计算需将 4 个 32 位字相加）。如果仅使用双操作数加法器进行串行级联或普通的二叉树型级联，其每次加法都需要等待进位信号的传播，这一传播过程的 T 深度将随操作数的宽度增加。而多个加法器深度的累加将限制整体线路的 T 深度。为了打破这一限制，本文参考 Kim 等[40]提出的 QCSA，将多模加问题转化为基于 QFA 与 QHA 的位级并行压缩问题。

量子保留进位的概念最早由 Gossett[41]于 1998 年提出。在将 3 个操作数（A,B,C）相加时，不直接计算并传播进位求出最终和，而是通过一层并行的 QFA 与 QHA 将它们压缩为和与进位 2 个部分。该步骤彻底避免了进位信号在寄存器中的横向传播，使单层压缩的 T 深度与操作数位宽无关，进而降低为常数级别。在此后的十余年中，QCSA 架构被广泛应用于低深度的量子乘法器设计中，用于压缩乘法计算时产生的多个部分[42]。然而，由于每一次压缩都会产生新的中间状态，需要使用辅助比特来接收，这种巨大的量子比特消耗使它在早期空间受限的量子线路设计中鲜有应用。

随着量子线路的容错要求发展，线路设计的 T 深度愈发重要。2025 年，Jang 等[31]采用 Kim 等[40]的设计，首次在 SHA-2 的极低深度量子线路中引

入了 Wallace 树结构的 QCSA，通过并行的 QFA 层，成功将 SHA-2 轮函数中的多操作数模加步骤压缩至极低层级，直到最后一级才使用低深度的双操作数加法器合并结果。Jang 等[31]的实验数据表明，为了实现极致的时间优化，其 SHA-256 量子线路虽然在线路宽度上消耗了高达 5 715 个量子比特，但成功将整体 Toffoli 深度大幅压缩至 1 332，创造了该领域的历史纪录。

3.3 QCSA 多操作数加法的纵向压缩约简过程

在 QCSA 的设计思想中，M 个 n 位操作数被视为一个 $M \times n$ 的布尔矩阵，QCSA 的多操作数相加流程并不直接进行进位的链式传播，而需要先经过约简将多操作数模加转换为双操作数模加。约简阶段的核心目标是通过并行压缩，将 M 个操作数逐步减少至 2 个操作数。该过程按位权重对所有操作数的比特进行分组，并进行相互独立的纵向压缩，采用 QFA 计算 3 比特操作数至 2 比特的和与进位的纵向压缩（3-to-2 压缩），QHA 计算 2 比特操作数至 2 比特的和与进位计算（2-to-2 压缩）。当某列需压缩两个输入比特 a 和 b 时，调用 QHA 进行 2-to-2 压缩，分别计算本位的部分和与向高位的进位，将部分和 $S = a \oplus b$ 的计算结果原地留在 b 上，进位 $K = a \cdot b$ 使用辅助比特存储。当某列需压缩 3 个输入比特 a,b,c 时，调用 QFA 进行 3-to-2 压缩，同样计算本位的部分和与进位，将部分和 $S = a \oplus b \oplus c$ 原地留在 c 上，进位 $K = (a \cdot b) \oplus (a \cdot c) \oplus (b \cdot c)$ 使用辅助比特存储，QHA 和 QFA 的线路实现如图 5 所示。

在一轮约简中，由于所有 QFA 和 QHA 产生的进位都被“保留”并直接传递给下一轮的高位，而不需要在当前轮的列与列之间横向传播。因此，对于 n 位宽的操作数，这一轮的 n 个列压缩操作是在量子线路上绝对并行执行的。单轮 3-to-2 压缩的 T 深度严格等于单个 QFA 的 T 深度。经过对数级轮次的并行约简后，M 个操作数将被最终压缩为 2 个操作数。之后调用一次传统的双操作数进位传播加法器将它们相加，即可得出多模加的和。为直观说明多操作数并行压缩机制，图 6 展示了基于 Wallace 树的 5 操作数（2 比特宽）并行约简流程的比特状态和对应的线路实现。

图 6 中，每个操作数比特用黑色圆点表示。在第一层（Lv1）对第一列和第二列各自的 3 个比特调用 QFA 进行压缩（图 6 中虚线框部分），部分和原地存储，进位使用辅助比特存储。第二层同样调用 QFA 进行压缩，压缩后第一列仅剩 1 个留在原地的比特，第二列有 3 个比特，而第三列有 2 个进位比特，因此在第三层，对第二列调用 QFA 进行压缩，对第三列调用 QHA 进行压缩。压缩后每一列的比特数都不大于 2，约简过程完成。接下来进行最终的进位传播双操作数加法，调用进位传播加法器计算多操作数加法的最终结果。

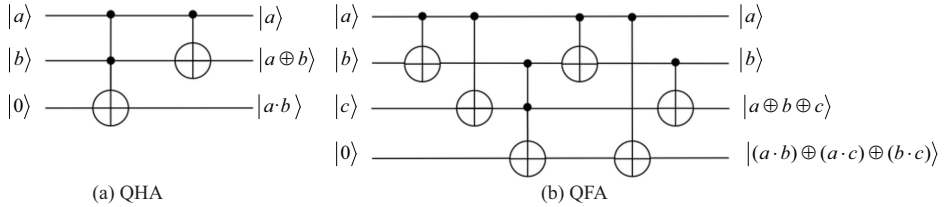
4 SM3 量子线路整体实现

4.1 SM3 轮函数的基础组件实现与消耗

在 SM3 的每一轮迭代压缩中，首先需要完成当前轮扩展字 W_j 与 W_j' 的计算，然后并行执行布尔函数 $\mathrm{FF}_j(A,B,C)$ 与 $\mathrm{GG}_j(E,F,G)$，在迭代压缩中还需要使用 QHA 与 QFA 进行纵向压缩。本文在这些组件的实现中，充分借鉴了现有最优的低深度架构，具体资源开销与线路设计如下。

（1）消息扩展线路。每一轮的扩展字 W_j 和 W_j' 分别如式(1)和式(2)所示。其中，针对置换函数 P_1 的量子实现，本文直接采用了 Zou 等[27]提出的原地优化结构，该结构仅消耗 68 个 CNOT 门。除 P_1 之外的消息扩展操作中，需额外执行 4 次 32 位的异或运算，共消耗 $4 \times 32 = 128$ 个 CNOT 门。对于全部 64 轮的消息扩展，线路仅需维护一个滑动窗口内的 16 个 32 比特消息字。通过这一轮间比特复用策略，整个消息扩展仅占用 $16 \times 32 = 512$ 个量子比特。

（2）布尔函数 FF_j 与 GG_j 的非原地线路。在生成 W_j 的同时，需并行计算当前轮的布尔函数 FF_j 与



(a) QHA (b) QFA

图 5 QHA 和 QFA 的线路实现

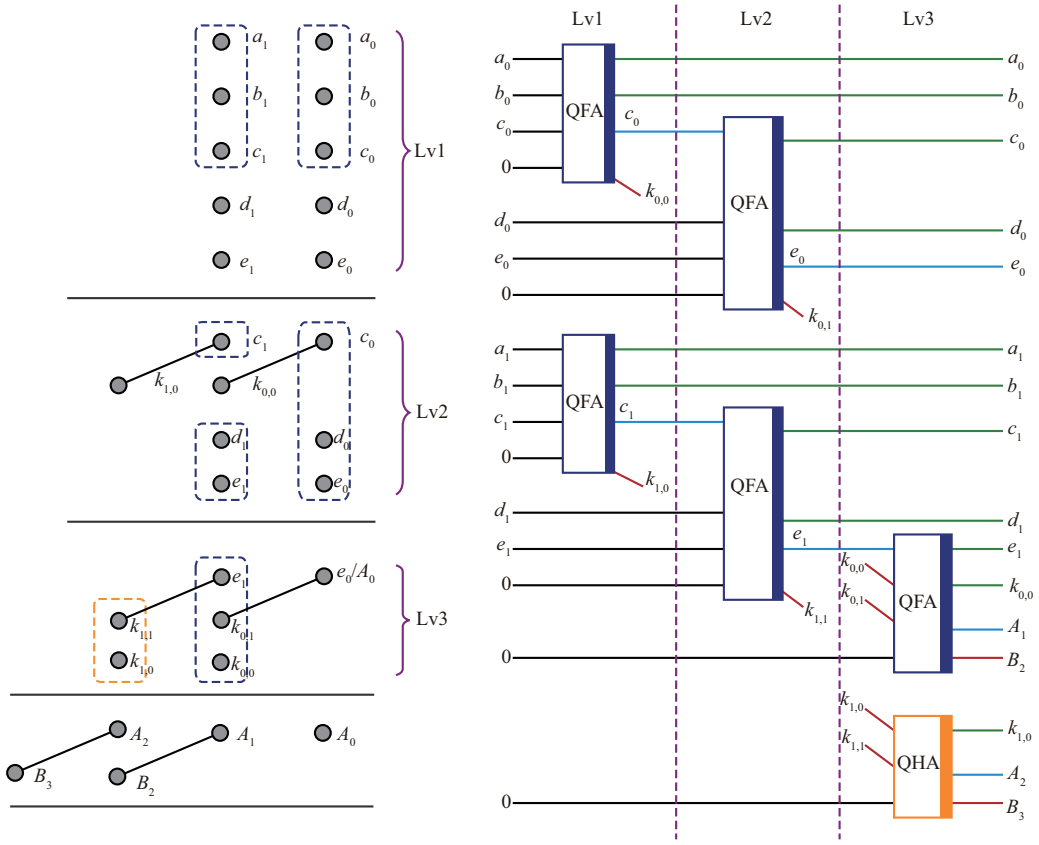


图 6　基于 Wallace 树的 5 操作数(2 比特宽)并行约简流程的比特状态和对应的线路实现

GG_j，具体如式(3)和式(4)所示。根据轮数 j 的不同，其量子实现策略分为以下两种情况。

① $0 \leqslant j \leqslant 15$ 时，FF_j 与 GG_j 均为纯线性异或（XOR）操作，不需要消耗任何 T 门资源。每个函数的 32 位操作消耗 $3 \times 32 = 96$ 个 CNOT 门。因此，并行执行 FF_j 与 GG_j 总计仅消耗 192 个 CNOT 门。

② $16 \leqslant j \leqslant 63$ 时，FF_j 与 GG_j 分别对应非线性函数 MAJ 与 CH。为了将 T 深度压缩至理论下界，本文采用基于 QAND 门的非原地结构。对于 MAJ 函数实现，采用 Yang 等[33]设计的非原地 MAJ 线路（FF_j）及其逆线路（$FF_j^{\dagger}$），其中，FF_j 的 T 深度仅为 1，消耗 1 个辅助比特；$FF_j^{\dagger}$ 的 T 深度为 0，且释放辅助比特。对于 CH 函数实现，采用 Zou 等[27]提出的非原地 CH 线路（GG_j）及其逆线路（$GG_j^{\dagger}$），其中，GG_j 的 T 深度为 1，消耗 1 个辅助比特；$GG_j^{\dagger}$ 的 T 深度为 0。

这两种非原地设计在 32 位宽的并发执行下，FF_j 与 GG_j 各需消耗 4×32=128 个 T 门（含 $T^{\dagger}$ 门），在此过程中仅消耗 1 个 T 深度。在 CNOT 开销方面，MAJ 与 CH 分别消耗 11 个和 10 个 CNOT 门，因此 FF_j 与 GG_j 并行执行共消耗(11+10)×32=672 个 CNOT 门。

（3）QFA 与 QHA 的量子线路。SM3 迭代压缩中计算中间变量 TT_1 与 TT_2 的过程，本文使用了 QCSA 进行纵向压缩约简。其中，QHA 与 QFA 实现借鉴 Jaques 等[34]的 QAND 门方案，在分配 1 个辅助量子比特作为目标位的前提下，将进位 K 的计算 T 深度压缩至 1。单个 QHA 消耗 4 个非 Clifford 门（包含 2 个 T 门与 2 个 $T^{\dagger}$ 门）、9 个 CNOT 门，以及 3 个 1qClifford 门（2 个 H 门和 1 个 S 门）。在反计算阶段释放辅助比特时，得益于基于测量的 $QAND^{\dagger}$ 线路，单个 $QHA^{\dagger}$ 彻底免除了 T 门的使用，其 T 深度为 0，因而仅需消耗 2 个 CNOT 门、4 个 1qClifford 门（3 个 H 门和 1 个 X 门），以及 1 次测量操作（Measurement）。单个 QFA 消耗 4 个非 Clifford 门（2 个 T 门和 2 个 $T^{\dagger}$ 门）、13 个 CNOT 门及 3 个 1qClifford 门（2 个 H 门和 1 个 S 门）。$QFA^{\dagger}$ 与 $QHA^{\dagger}$ 类似，其反计算线路 T 深度同样为 0。单个 $QFA^{\dagger}$ 仅消耗 6 个 CNOT 门、4 个单比特门（3 个 H 门和 1 个 X 门）及 1 次测量操作。在多模加法器的设计中，由于不需

要最高位的进位计算，只需计算部分和，因此在最高位使用简化的QFA，这只需要消耗3个CNOT门，不消耗T门等其他资源。简化的QFA†的消耗与简化的QFA的消耗相同。

4.2 SM3轮函数量子实现

SM3的核心难点在于高效计算具有多操作数连加特征的TT_1与TT_2。为了打破双操作数加法器串行级联带来的深度瓶颈，本文采用Kim等[40]的基于Wallace树的QCSA，结合低深度的QFA与QHA组件，将整个轮函数的计算与反计算过程划分为7个逻辑执行层。

树状并行压缩阶段（第1层～第3层），旨在通过延迟进位传播，将多操作数并行压缩为双操作数，为计算TT_1与TT_2做准备。

在第1层，并行处理3个独立的多操作数模加分支：$W'_{j-4}+\mathrm{FF}+H_{j-4}$、$E_{j-4}+(A_{j-4}\lll 12)+(T_{j-4}\lll(j-4))$、$W_{j-4}+\mathrm{GG}+D_{j-4}$。3个多模加分支的比特状态如图7所示，针对32位宽的数据，本层共调用31×3=93个标准QFA与3个简化QFA（仅计算最高位的和）。QFA将部分和原地输出于原有寄存器上，而进位则输出至31×3=93个干净的辅助量子比特上（记为$k_{0,0}$、$k_{0,1}$、$k_{0,2}$）。第1层的T深度为1，消耗372个T门、1 218个CNOT门、279个1qClifford门，辅助量子比特增加93个。

第2层的处理和第1层不同。在理想的多操作数相加场景下，最优策略是利用QCSA将所有操作数一直压缩至最后，仅在末尾调用一次双操作数模加器以最小化T深度。然而，观察SM3轮函数计算式可以发现：在计算TT_1与TT_2之前，必须先计算中间变量$SS_1=((A\lll 12)+E+(T\lll(j \bmod 32)))\lll 7$。由于QCSA的并行压缩机制输出的是未聚合的部分和与进位，而模加运算与循环移位操作在数学上并不满足分配律，不能进行顺序的互换，即$(S+C)\lll 7\neq(S\lll 7)+(C\lll 7)$。因此，必须在执行$\lll 7$之前，将QCSA第1层的压缩结果进行一次聚合。在第2层，针对第1层E_{j-4}分支产生的高31位QFA结果，调用3.1节提到的量子模加器进行合并。将结果左移7位得到核心变量SS_1。随后，利用32个CNOT门将SS_1复制至提前备好的$A_{j-4}\lll 12$寄存器上生成SS_2。第2层具有1个模加器深度（T深度为8），消耗1 024个T门、2 353个CNOT门、806个1qClifford门，额外消耗166个辅助比特。

第3层的思路类似第1层，利用生成的SS_1和SS_2，并行计算$SS_1+(W_{j-4}+k_{0,2})$与$SS_2+(W_j+k_{0,0})$。第3层共调用60个QFA、2个简化QFA和2个QHA。部分和原地覆盖SS_1和SS_2（记为SS'_1、SS'_2），进位则再次输出至62个全新的辅助量子比特上（记为$k_{1,0}$、$k_{1,1}$）。第3层的T深度为1，消耗248个T门、804个CNOT门、186个1qClifford门，额外消耗62个辅助比特。

第4层为TT_1与TT_2结果计算阶段，调用2个并行的31位量子模加器，将第3层产生的SS'_1、SS'_2分别与其对应的进位向量合并，最终生成输出态TT_1和TT_2。为解耦轮间数据依赖，生成的64位结果将直接存储于下一轮的独立缓存比特中，不参与后续的反计算释放。第4层的T深度为8，消耗2 048个T门、4 642个CNOT门、1 612个单比特Clifford门，消耗332个辅助比特。

反计算与资源回收阶段（第5层～第7层），由于QCSA压缩网络消耗了大量辅助量子比特，在得到TT_1和TT_2后，应立即逆序执行计算线路，以将辅助比特复原，供后续轮次复用。由于逆向线路使

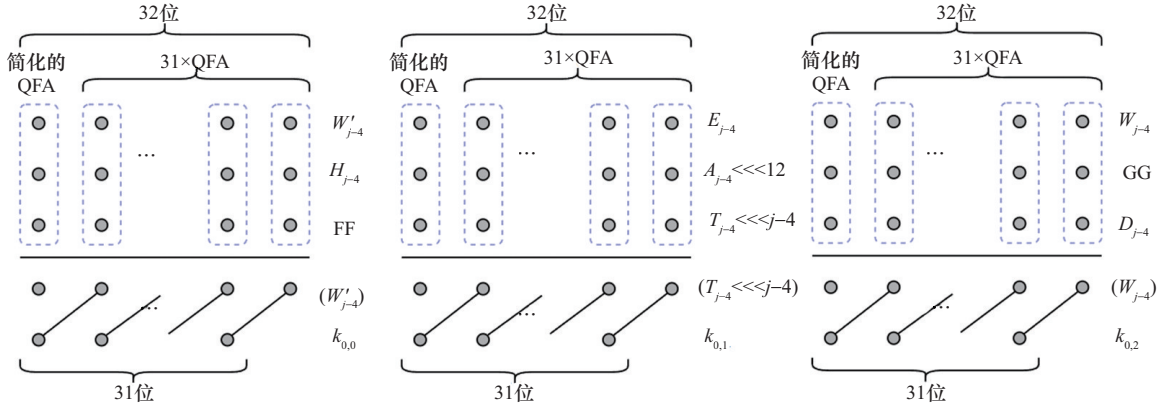


图7 第1层3个多模加分支的比特状态

用的 QAND† 的 T† 门深度为 0，反计算过程极大地优化了深度开销。

第 5 层作为第 3 层的逆，调用 60 个 QFA†、2 个简化 QFA† 及 2 个 QHA†。将 SS_1' 和 SS_2' 还原，并释放 62 个进位辅助比特。第 5 层的 T 深度为 0，消耗 370 个 CNOT 门与 248 个 1qClifford 门。

第 6 层为第 2 层的逆，在第 6 层对 SS_1 执行右移 7 位操作，并调用 31 位模加器的逆线路进行反向拆解，使 SS_1 的相关辅助态彻底复零。第 6 层具有 1 个模加器逆深度（T 深度为 8），消耗 1 024 个 T 门（含 T†）、2 353 个 CNOT 门及 806 个 1qClifford 门。

第 7 层是第 1 层的逆，调用 93 个 QFA† 与 3 个简化 QFA†，将第 1 层生成的所有进位辅助态复原。第 7 层的 T 深度为 0，消耗 567 个 CNOT 门与 372 个 1qClifford 门。

在上述模加与反计算全部执行完毕后，需要执行非线性组件的逆操作（即 FF† 与 GG†），并辅以逻辑移位操作以完成状态更新。因 FF† 与 GG† 仅包含 Clifford 门与测量资源，不产生额外的 T 深度。在 $0 \leqslant j \leqslant 15$ 时，该步骤消耗 192 个 CNOT 门；在 $16 \leqslant j \leqslant 63$ 时，消耗 224 个 CNOT 门。SM3 低 T 深度单轮线路实现如图 8 所示。纵观单轮 SM3 的 7 层架构，当 $0 \leqslant j \leqslant 15$ 时，消耗 T 深度仅为 1+8+1+8+0+8+0=26；当 $16 \leqslant j \leqslant 63$ 时，由于 FF 和 GG 分别对应非线性函数 MAJ 和 CH，T 深度增加 1，每轮总计消耗 T 深度为 27。

在资源消耗上，单轮 QFA 与模加器网络累计消耗 4 716 个 T 门、12 307 个 CNOT 门，以及 4 309 个 1qClifford 门。整个单轮运算峰值消耗 653 个辅助量子比特，其中，64 个比特用于承载 TT_1 和 TT_2 传递至下一轮，其余 589 个辅助比特均通过第 5 层～第 7 层的反计算被复零，可在后续轮次中复用。

4.3　SM3 线路整体资源消耗

本节对 SM3 量子线路在完整 64 轮迭代压缩中的整体资源消耗进行详细的统计与评估。

（1）门资源开销

在本文方案中，T 门的消耗主要集中在非线性布尔函数 MAJ 与 CH，以及多操作数压缩与模加中。在第 16 轮～第 63 轮（共 48 轮）中，FF 与 GG 的非原地计算及其逆线路共需消耗 128×2×48=12 288 个 T 门（含 T† 门）。在核心的 QCSA 压缩与模加器网络中，单轮需消耗 4 716 个 T 门，64 轮共消耗 4 716×64=301 824 个 T 门。整个 SM3 线路的 T 门总数被大幅压缩至 314 112 个。

CNOT 门分布于线路的各个逻辑层。寄存器状态更新与基础异或网络共消耗 32×8×64=16 384 个 CNOT 门。在布尔函数执行环节，FF 与 GG 在前 16 轮的纯异或操作和后 48 轮的非线性操作分别消耗 192×16+672×48=35 328 个 CNOT 门；其反计算线路（FF† 与 GG†）共消耗 192×16+224×48=13 824 个 CNOT 门。此外，置换函数 $P_0(X)$ 与 $P_1(X)$ 的原地计算消耗 68×2×64=8 704 个 CNOT 门。作为线路中占比最大的部分，QFA/QHA 压缩与模加器网络在 64 轮中累计消耗 12 243×64=783 552 个 CNOT 门。综上，CNOT 门总消耗为 857 792 个。

1qClifford 门主要用于底层组件的态制备与相位旋转。其中，FF 与 GG 及其逆线路 FF† 与 GG† 共消耗 (3+4+3+4) ×32×48=21 504 个 1qClifford 门。QFA/QHA 压缩与模加器线路 64 轮累计消耗 4 309×64=275 776 个 1qClifford 门。1qClifford 门总消耗为 297 280 个。

（2）量子比特宽度资源开销

本文在消息扩展阶段，利用轮间比特复用技术，仅需 16×32=512 个逻辑量子比特。对于迭代压缩部分的 A～H 寄存器初始分配 8×32=256 个量子比特。在生成每轮最终的 TT_1 与 TT_2 时，模加器采用了非原地输出设计。因此，每轮均需分配 64 个全新的量子比特用于存放结果，64 轮累计使用 4 096 个比特，而在单轮 QFA/QHA 压缩与合并网络中，峰值需要 589 个可复零辅助比特。这 589 个比特在每轮计算结束后即被复零，可在后续轮次中完全复用。综上，本文方案的总量子比特数为 5 453。

（3）T 深度

本文引入 QCSA 多操作数并行压缩、QAND 门替换策略和非原地状态输出方法，单轮运算的 T 深度维持在较低水平。本文设计的 SM3 量子线路在 64 轮迭代中的整体 T 深度成功下探至 26×16+27×48=1 712。

（4）综合时空代价

如引言所指出，在 FTQC 环境中，杂凑函数的单次 Oracle 受限于量子硬件的 MaxDepth，因此 TD^2-M cost 成为衡量并行 Grover 算法整体物理实现成本的综合时空代价指标。本文方案的综合时空代价为 $1\,712^2 \times 5\,453 = 15\,982\,437\,632 \approx 1.59 \times 10^{10}$。

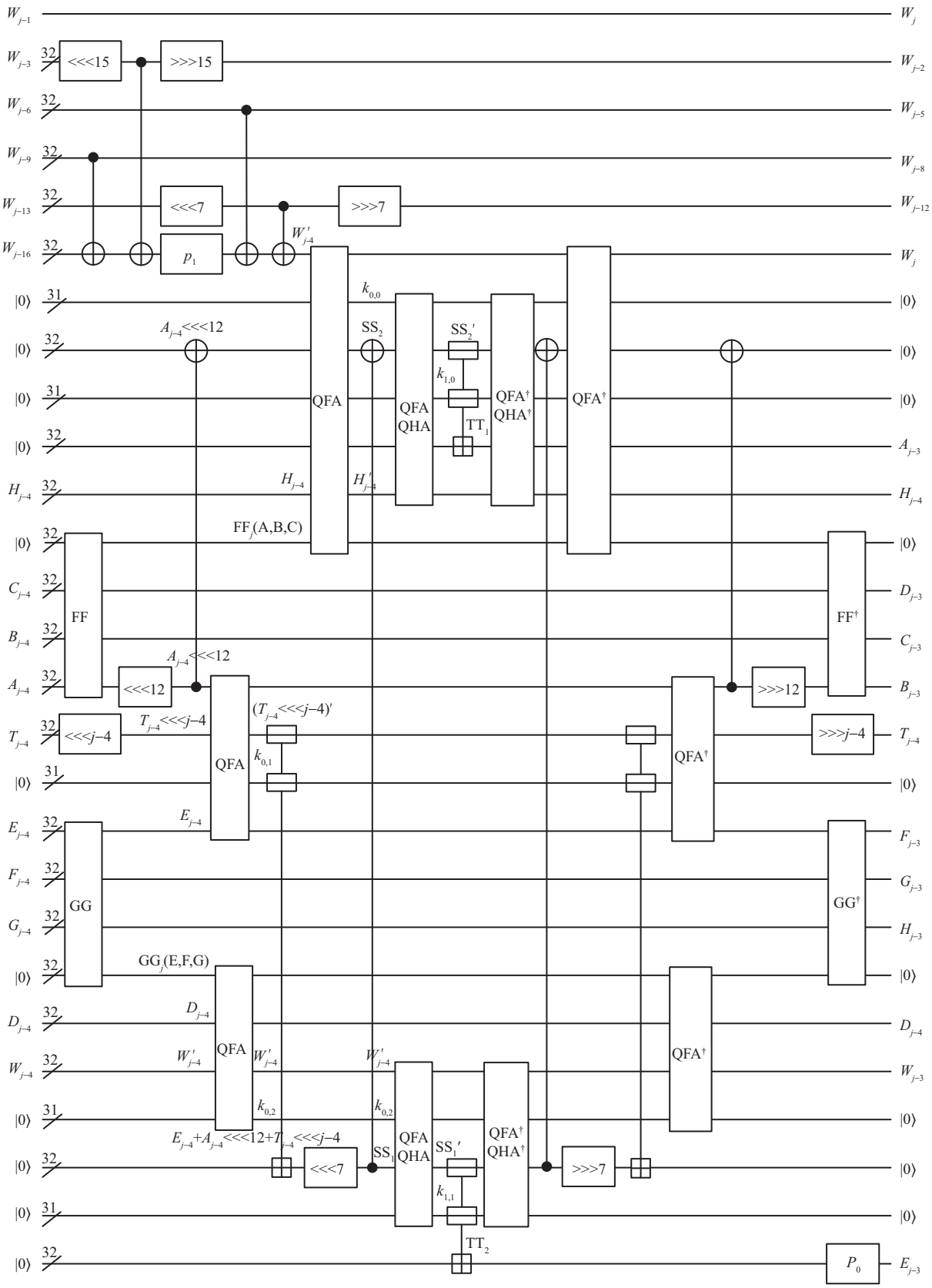


图8　SM3低T深度单轮线路实现

4.4　SM3 量子线路的硬件匹配度分析

在评估量子线路设计的合理性时，所设计量子线路的资源消耗应当与量子硬件的实际发展轨迹相匹配。本文设计的 SM3 量子线路消耗了 5 453 个逻辑量子比特并实现了 1 712 的 T 深度。接下来本文将从量子硬件的比特扩容趋势与量子态退相干限制两方面，对该方案在 FTQC 时代的硬件匹配度进行系统分析。

必须指出的是，当前处于含噪中型量子（noisy intermediate-scale quantum, NISQ）时代的量子处理器通常仅能提供数十至数百个带有噪声的物理量子比特[1]。在 FTQC 环境下，为确保计算的可靠性，需要利用表面码等量子纠错协议将多个物理比特编码为一个无噪声的逻辑量子比特。由于纠错编码的开销比（即为了实现一个逻辑量子比特，需要使用额外物理量子比特进行编码的比率）通常为 10^2～10^3，本文方案所需的 5 453 个逻辑量子比特实际上要求底层硬件具备数百万级别（即 10^6 数量级）的物理量子比特支撑，这远远超出了当前 NISQ 设备的承载极限。然而，主流密码体系面临的实质性量子威胁存在于 FTQC 时代。根据国际领先量子硬件厂商发布的路线图，百万级物理比特并非无法企及的理论数字。以 IBM Quantum 发布的发展路线图为例，其已明确规划在 2033 年后实现十万级物理比特[43]。因此，本文方案在空间维度上的资源开销符合业界对 FTQC 硬件量子比特数的中长期发展预期。

在评估硬件匹配度时，相较于量子比特数量，线路的深度是硬件更为严苛的瓶颈。量子线路的 T 深度越高，运行过程中越容易出现量子退相干现象，导致计算结果出错。正如 Jang 等[31]在评估 NIST 后量子安全强度时所指出的，以往线路设计中一味追求减少量子比特数量的做法，并不适用于真实的 Grover 并行攻击场景。因此，本文主动分配辅助量子比特以减少线路 T 深度的做法顺应了 FTQC 硬件的发展规律。综上所述，本文的线路设计在未来 FTQC 硬件上具有适用性。

5　结束语

本文聚焦于我国商用密码杂凑标准 SM3 的高效量子线路实现。针对多操作数连加与状态更新导致的高 T 深度问题，本文提出了一种低 T 深度和低 T 门数的量子线路架构。首先，通过引入基于 Wallace 树的 QCSA 与 QFA/QHA 压缩方式，成功将多操作数模加的路径压缩至常数级别。其次，本文主动分配额外的量子比特用于存储 SM3 迭代压缩中的所有核心中间状态。实验结果表明，本文方案在消耗 5 453 个量子比特的前提下，将 SM3 整体量子线路的 T 深度大幅压缩至 1 712，同时将 T 门总数锐减至 314 112。更为重要的是，基于 FTQC 中 MaxDepth 的物理约束模型，本文方案在综合评估指标 TD^2-M cost 上也取得了较大的突破，这表明本文以牺牲量子比特数为代价来换取低 T 深度，在面向受到 MaxDepth 约束的时间敏感型场景中，是实现量子硬件资源成本最小化的最优选择。

参考文献：

[1] Huang H L, Xu X Y, Guo C, et al. Near-term quantum computing techniques: variational quantum algorithms, error mitigation, circuit compilation, benchmarking and classical simulation[J]. Science China Physics, Mechanics & Astronomy, 2023, 66(5): 250302.

[2] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring[C]//Proceedings of 35th Annual Symposium on Foundations of Computer Science. Piscataway: IEEE Press, 1994: 124-134.

[3] Milanov E. The RSA algorithm[R]. 2009.

[4] Koblitz N, Menezes A, Vanstone S. The state of elliptic curve cryptography[J]. Designs, Codes and Cryptography, 2000, 19(2/3): 173-193.

[5] Grover L K. A fast quantum mechanical algorithm for database search [C]//Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing. New York: ACM Press, 1996: 212-219.

[6] FIPS PUB197: Advanced encryption standard (AES)[S].

[7] FIPS PUB 180-4: Secure hash standard (SHS)[S].

[8] FIPS PUB202: SHA-3 standard: permutation-based hash and extendable-output functions[S].

[9] Simon D R. On the power of quantum computation[J]. SIAM Journal on Computing, 1997, 26(5): 1474-1483.

[10] National Institute of Standards and Technology. Submission requirements and evaluation criteria for the post-quantum cryptography standardization process[R]. 2016.

[11] Grassl M, Langenberg B, Roetteler M, et al. Applying Grover's algorithm to AES: quantum resource estimates[M]. Berlin: Springer International Publishing, 2016.

[12] Almazrooie M, Samsudin A, Abdullah R, et al. Quantum reversible circuit of AES-128[J]. Quantum Information Processing, 2018, 17 (5): 112.

[13] 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: 2500112.

[14] Zou J, Wei Z H, Sun S W, et al. Quantum circuit implementations of AES with fewer qubits[M] . Berlin: Springer International Publishing, 2020.

[15] Wang Z G, Wei S J, Long G L. A quantum circuit design of AES requiring fewer quantum qubits and gate operations[J]. Frontiers of Physics, 2022, 17(4): 41501.

[16] Li Z Q, Cai B B, Sun H W, et al. Novel quantum circuit implementation of advanced encryption standard with low costs[J]. Science China Physics, Mechanics & Astronomy, 2022, 65(9): 290311.

[17] Lin D, Xiang Z J, Xu R Q, et al. Optimized quantum implementation of AES[J]. Quantum Information Processing, 2023, 22(9): 352.

[18] Huang Z Y, Zhang F X, Lin D D. Constructing quantum implementations with the minimal T-depth or minimal width and their applications [M]. Berlin: Springer International Publishing, 2025.

[19] Jaques S, Naehrig M, Roetteler M, et al. Implementing grover oracles for quantum key search on AES and LowMC[M]. Berlin: Springer International Publishing, 2020.

[20] Li Z Q, Gao F, Qin S J, et al. New record in the number of qubits for a quantum implementation of AES[J]. Frontiers in Physics, 2023, 11: 1171753.

[21] Huang Z Y, Sun S W. Synthesizing quantum circuits of AES with lower T-depth and less qubits[M]. Berlin: Springer International Publishing, 2022.

[22] Liu Q, Preneel B, Zhao Z, et al. Improved quantum circuits for AES: reducing the depth and the number of qubits[M]. Berlin: Springer International Publishing, 2023.

[23] Shi H, Feng X. Quantum circuits of AES with a low-depth linear layer and a new structure[C]//International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer Nature Singapore, 2024: 358-395.

[24] 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[J]. 中国科学: 物理学 力学 天文学, 2023, 53(4): 17-25.
Li Z Q, Gao F, Qin S J, et al. Quantum circuit for implementing Camellia S-box with low costs[J]. Scientia Sinica (Physica, Mechanica & Astronomica), 2023, 53(4): 17-25.

[25] Lin D, Sun B, Xiang Z J, et al. Further insights on constructing quantum circuits for Camellia block cipher[J]. Quantum Information Processing, 2023, 22(12): 455.

[26] 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.

[27] Zou J, Li L J, Wei Z H, et al. New quantum circuit implementations of SM4 and SM3[J]. Quantum Information Processing, 2022, 21(5): 181.

[28] Lin D, Xiang Z J, Xu R Q, et al. Quantum circuit implementations of SM4 block cipher based on different gate sets[J]. Quantum Information Processing, 2023, 22(7): 282.

[29] 孙壮, 黄震宇. ZUC算法的量子电路实现[J]. 信息安全学报, 2025, 10(6): 133-149.
Sun Z, Huang Z Y. Implementing quantum circuit of ZUC algorithm[J]. Journal of Cyber Security, 2025, 10(6): 133-149.

[30] Zou J, Xiang S M, Zou C Z, et al. An efficient quantum circuit implementation of ZUC-128 cipher with low T-depth[J]. Scientia Sinica Physica, Mechanica & Astronomica, 2024, 54(12): 120311.

[31] Jang K, Lim S, Oh Y, et al. Quantum implementation and analysis of SHA-2 and SHA-3[J]. IEEE Transactions on Emerging Topics in Computing, 2025, 13(3): 919-934.

[32] Song G, Jang K, Kim H, et al. Grover on SM3[C]//Proceedings of the 24th International Conference on Information Security and Cryptology. Berlin: Springer, 2021: 421-433.

[33] 杨婷玉, 张莎莎, 向泽军, 等. SM3算法的低T深度与低宽度量子优化实现[J]. 中国科学 (物理学 力学 天文学), 2026, 56(2): 245-260.
Yang T Y, Zhang S S, Xiang Z J, et al. Optimized quantum implementations of SM3 with low T-depth and low width[J]. SCIENTIA SINICA Physica, Mechanica & Astronomica, 2026, 56(2): 245-260.

[34] 邹剑, 郭楠生, 李俊康. SM3和RIPEMD-160杂凑函数的高效量子线路实现[J]. 通信学报, 2025, 46(12): 222-233.
Zou J, Guo N S, Li J K. Efficient quantum circuit implementations of SM3 and RIPEMD-160 hash functions[J]. Journal on Communications, 2025, 46(12): 222-233.

[35] Cuccaro S A, Draper T G, Kutin S A, et al. A new quantum ripple-carry addition circuit[PP]. V1. (2004-10-22) [2026-04-24]. arXiv: arXiv.quant-ph/0410184.

[36] Draper T G, Kutin S A, Rains E M, et al. A logarithmic-depth quantum carry-lookahead adder[J]. Quantum Information and Computation, 2006, 6(4&5): 351-369.

[37] Wang S Y, Mondal A, Chattopadhyay A. Optimal toffoli-depth quantum adder[J]. ACM Transactions on Quantum Computing, 2025, 6(3): 1-16.

[38] Amy M, Maslov D, Mosca M, et al. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2013, 32(6): 818-830.

[39] 王小云, 于红波. SM3密码杂凑算法[J]. 信息安全研究, 2016, 2(11): 983-994.
Wang X Y, Yu H B. SM3 cryptographic hash algorithm[J]. Journal of Information Security Research, 2016, 2(11): 983-994.

[40] Kim H, Lim S, Jang K, et al. Tree-based quantum carry-save adder [R]. 2025.

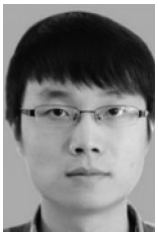
[41] Gossett P. Quantum carry-save arithmetic[PP]. V2. (1998-08-30)[2026-04-24]. arXiv: arXiv.quant-ph/9808061.

[42] Munoz-Coreas E, Thapliyal H. T-count optimized quantum circuit design of multiplier [C]//Proceedings of IEEE Computer Society Annual

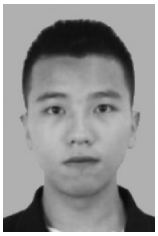
Symposium on VLSI (ISVLSI). Piscataway: IEEE Press, 2017: 290-295.

[43] Yoder T J, Schoute E, Rall P, et al. Tour de gross: a modular quantum computer based on bivariate bicycle codes[PP]. V1. (2025-06-03) [2026-04-24]. arXiv: arXiv.2506.03094, 2025.

[作者简介]



邹剑（1985–），男，博士，福州大学副教授、硕士生导师，主要研究方向为对称密码分析、量子计算。



李俊康（2000–），男，福州大学硕士生，主要研究方向为线路实现、S 盒优化。



郭楠生（2001–），男，回族，福州大学硕士生，主要研究方向为线路实现、S 盒优化。



孙莹（1982–），女，博士，北京电子科技学院副教授，主要研究方向为量子信息技术在现代密码学中的应用。



李子臣（1965–），男，博士，北京印刷学院教授、博士生导师，主要研究方向为信息安全、密码算法与协议。