第八届（2023）全国高校密码数学挑战赛

赛题二

一、赛题名称：对称密码算法的量子电路构造

二、赛题描述

2.1 基础知识

1）**二元域：** $\boldsymbol{F}_2$ 为含有两个元素0,1的有限域。元素0,1满足如下加法与乘法性质，$0+0=0, 0+1=1, 1+1=0, 0\times 0=0, 0\times 1=0, 1\times 1=1$。

2）**布尔多项式：**环 $\boldsymbol{F}_2[x_1, x_2, \dots, x_n]/\langle x_1^2+x_1, x_2^2+x_2, \dots, x_n^2+x_n\rangle$ 中的元素被称为变量为 $x_1, x_2, \dots, x_n$ 的布尔多项式。直观上来说，布尔多项式的系数为 $\boldsymbol{F}_2$ 中的元素，并且该多项式的每个单项式中的 x_i 的次数小于等于 1 次。例如: $x_1x_2+x_2x_3+x_1x_2x_3+x_3+1$ 为一个含有 3 个变量的布尔多项式。布尔多项式的最简形式，我们称为它的**代数标准型**(ANF, algebraic normal form)。

3）**布尔多项式的乘法：**计算两个布尔多项式乘法结果的代数标准型时，可以先按照一般的多项式乘法进行运算，再将每个 x_i 的高次项替换为 1 次项后消去相同的单项式。

例如：$(x_1+x_2x_3)(x_1x_2+x_2)=x_1^2x_2+x_1x_2^2x_3+x_1x_2+x_2^2x_3$

$$=x_1x_2+x_1x_2x_3+x_1x_2+x_2x_3=x_1x_2x_3+x_2x_3$$

4）**向量布尔函数：**一个 n 个变量的 m 维向量布尔函数是指由 m 个 n 个变量的布尔多项式 $f_1, f_2, \dots, f_m$ 构成的向量 $(f_1, f_2, \dots, f_m)$。

5）**NCT 门集**：NCT 门集包括 3 种可逆门：NOT 门、CNOT 门、Toffoli 门。其中，

- NOT 门可以看成一个关于布尔函数的可逆映射，它将输入 x 映射为输出 $x+1$；
- CNOT 门可以看成一个关于二维布尔函数的可逆映射，它将输入 (x_1, x_2) 映射为输出 (x_1, x_1+x_2);
- Toffoli 门可以看成一个关于三维布尔函数的可逆映射，它将输入(x_1, x_2, x_3) 映射为输出 $(x_1, x_2, x_3+x_1x_2)$

可以看出 NCT 门的逆变换均为它们本身。

6）**布尔函数的 NCT 门实现**：给定一个n个变量的 n 维向量布尔函数 $(f_1, f_2, \ldots, f_n)$，很多时候我们可以通过 NCT 门集将n个变量所构成的向量布尔函数 $(x_1, x_2, \ldots, x_n)$ 映射为这个给定的向量布尔函数 $(f_1, f_2, \ldots, f_n)$。

例 1　对于一个 n 维的布尔函数，我们用 NOT_i 表示 NOT 门作用于向量布尔函数的第 i 位上，用 $\mathrm{CNOT}_{i,j}$ 表示 CNOT 门是将第 i 位的多项式加到第 j 位，用 $\mathrm{Toffoli}_{i,j,k}$ 表示 Toffoli 门是将第 i 位与第 j 位的多项式相乘后加到第 k 位。

基于上述符号，我们可以通过如下的步骤生成向量布尔函数 $(x_1+x_2, x_1x_3+x_2x_3+x_1, x_3+1)$:

$\mathrm{CNOT}_{2,1}$:　$(x_1, x_2, x_3) \to (x_1+x_2, x_2, x_3)$;

NOT_3: $(x_1 + x_2, x_2, x_3) \rightarrow (x_1 + x_2, x_2, x_3 + 1)$;

$\mathrm{Toffoli}_{1,3,2}$: $(x_1 + x_2, x_2, x_3 + 1) \rightarrow (x_1 + x_2, x_1x_3 + x_2x_3 + x_1, x_3 + 1)$

7）**基于辅助位的 NCT 实现**：对于有些布尔函数$(f_1, f_2, \ldots, f_n)$，我们无法直接利用 NCT 门集将 $(x_1, x_2, \ldots, x_n)$转化为 $(f_1, f_2, \ldots, f_n)$。但是，我们可以利用 NCT 门集将$(x_1, x_2, \ldots, x_n, 0,0, \ldots,0)$ 转化为 $(f_1, f_2, \ldots, f_n, 0,0, \ldots,0)$, 其中这些 0 所对应的位我们称为**辅助位**（或者辅助比特）。

例 2 对于向量布尔函数 $(x_1, x_2, x_3, x_4 + x_1x_2x_3)$，我们可以通过下述步骤利用 1 个辅助位将其生成：

$\mathrm{Toffoli}_{1,2,5}$: $(x_1, x_2, x_3, x_4, 0) \rightarrow (x_1, x_2, x_3, x_4, x_1x_2)$

$\mathrm{Toffoli}_{3,5,4}$: $(x_1, x_2, x_3, x_4, x_1x_2) \rightarrow (x_1, x_2, x_3, x_4 + x_1x_2x_3, x_1x_2)$

$\mathrm{Toffoli}_{1,2,5}$: $(x_1, x_2, x_3, x_4 + x_1x_2x_3, x_1x_2) \rightarrow (x_1, x_2, x_3, x_4 + x_1x_2x_3, 0)$

上述基于 NCT 门集生成向量布尔函数的过程对应了一个实现该函数的可逆（量子）电路，或称为可逆（量子）线路，即 Reversible (Quantum) Circuit。可以看出，上述问题的布尔函数的维数和变量的个数相同，并且电路最终得到的函数每一位都在最初输入变量的位置上，我们一般称上述实现为该函数的一个**原位(in-place)**实现，并称这个电路为一个原位电路。

这个电路的**宽度**（Width, 即需要的逻辑量子比特数）为整个过

程的位数（包括值为 0 的位）。例如，例 1 中的电路的宽度为 3，例 2 中电路的宽度为 5。

对于例 1，可以看出， $\mathrm{CNOT}_{2,1}$ 与 NOT_3 两个门可以在第一步同时进行操作，互相并不影响。因此，我们可以通过下面两步生成 $(x_1 + x_2, x_1x_3 + x_2x_3 + x_1, x_3 + 1)$：

Step 1：$\{\mathrm{CNOT}_{2,1}, \mathrm{NOT}_3\}$；

Step 2：$\{\mathrm{Toffoli}_{1,3,2}\}$；

上述两步的实现称为一个**总深度**(full depth)为 2 的实现，对应一个总深度为 2 的电路。

除了总深度，基于 NCT 门集的电路实现还有 **Toffoli 深度**（Toffoli-depth）的概念，即实现中含有 Toffoli 门的步数。显然，为了降低电路的 Toffoli 深度，我们需要将更多的 Toffoli 门在同一步执行，而这样的策略可能会增加整个实现的总深度。

例 3　下面是一个深度为 2 的 NCT 电路:

Step 1：　$\{\mathrm{Toffoli}_{1,2,3}$，$\mathrm{CNOT}_{5,6}\}$；

Step 2：　$\{\mathrm{CNOT}_{3,1}, \mathrm{Toffoli}_{4,5,6}\}$;

可以看出，该电路的 Toffoli 深度也为 2。我们为了降低电路实现的 Toffoli 深度，可以将上述电路改写成:

Step 1：$\{\mathrm{CNOT}_{5,6}\}$；

Step 2：$\{\mathrm{Toffoli}_{1,2,3}$，$\mathrm{Toffoli}_{4,5,6}\}$;

Step 3：$\{\mathrm{CNOT}_{3,1}\}$

这样，我们就得到了一个 Toffoli 深度为 1，总深度为 3 的电路。

8）**换位操作**：对于布尔函数 $G_1 = (f_1, f_2, \dots, f_n)$，若我们利用 NCT 门实现了布尔函数 $G_2 = (f_{i_1}, f_{i_2}, \dots, f_{i_n})$，其中 $i_1, i_2, \dots, i_n$ 是 $1,2, \dots, n$ 的一个置换，则 G_1 可以从 G_2 进行换位操作得到，在本题中我们将这种**换位操作看作是无消耗**的，因此若我们给出了一个G_2 的 NCT 电路实现，则我们认为这个电路也实现了G_1。

2.2 问题描述

设 $X_1 = \{x_1, x_2, \dots, x_{32}\}$, $X_2 = \{x_{33}, \dots, x_{64}\}, X_3 = \{x_{65}, \dots, x_{96}\}$, $X_4 = \{x_{97}, \dots, x_{128}\}$ 为 4 个布尔变量集合。$X = \{X_1, X_2, X_3, X_4\}$ 为 128 个变量的集合。F为一个 128 个变量 128 维的向量布尔函数：

$$F(X_1, X_2, X_3, X_4) = (X_2, X_3, X_4, X_1 + L \circ \tau(X_2 \oplus X_3 \oplus X_4))$$

其中

- $X_2 \oplus X_3 \oplus X_4 = \{x_{33} + x_{65} + x_{97}, x_{34} + x_{66} + x_{98}, \dots, x_{64} + x_{96} + x_{128}\}$ 表示对位相加。
- τ 为一个 32 个变量 32 维的非线性向量布尔函数。若将 τ 的 32 位输入$\{y_1, y_2, \dots, y_{32}\}$按每 8 位分成 4 组$Y_1 = \{y_1, y_2, \dots, y_8\}, Y_2 = \{y_9, y_{10}, \dots, y_{16}\}, Y_3 = \{y_{17}, y_{18}, \dots, y_{24}\}, Y_4 = \{y_{25}, y_{26}, \dots, y_{32}\}$，则我们有 $\tau(y_1, y_2, \dots, y_{32}) = (S(Y_1), S(Y_2), S(Y_3), S(Y_4))$。其中$S$为一个 8 个变量 8 维的向量布尔函数，其代数标准型见附件 S_ANF.txt。
- L 为一个 32 个变量 32 维的线性布尔函数，其对应的代数标准型

见附件 L_ANF.txt。

问题：对于上述F，基于 NCT 门集给出一个优化的原位电路实现（即该量子电路可以将$(X,0)$映射为$(F(X),0)$）。

2.3 成绩评判标准

以两个指标作为评分依据

指标 1：T-DW-cost，即电路的宽度（本题中=128+辅助位数）× 电路的 Toffoli 深度

指标 2：DW-cost, 即电路的宽度 × 电路的总深度

- **指标 1 得分：**各参赛队伍的结果中，指标 1 数值最低的队伍在该项指标上得到满分 100 分。设指标 1 满分队伍 A 队的指标 1 数值为X，若另一个参赛队伍 B 队的指标 1 数值为Y，则 B 队在指标 1 的得分为$100 \times \sqrt{X/Y}$；
  - 指标 1 参考值：7000，该值为一个较优电路实现大概对应的数值，供参赛队伍预估自己结果的优劣。
- **指标 2 得分：**各参赛队伍的结果中，指标 2 数值最低的队伍在该项指标上得到满分 100 分。设指标 2 满分队伍 A 队的指标 2 数值为X，若另一个参赛队伍 B 队的指标 2 数值为Y，则 B 队在指标 2 的得分为$100 \times \sqrt{X/Y}$；
  - 指标 2 参考值：90000，该值为一个较优电路实现大概对应的数值，供参赛队伍预估自己结果的优劣。

- **总得分 = 指标1得分× 60% + 指标2得分× 40%；**各队伍按照总得分的高低排序。
- **答案格式：**提交电路设计方法描述的文档以及电路的具体实现方案，为了验证电路的 Toffoli 深度与总深度，电路具体实现方案需要用文件 circuit_standard.txt 中的格式给出。

  注：在附件中，文件夹 SM4_ANF 中的文件分别给出了 32 维布尔函数 $X_1 + L \circ \tau(X_2 \oplus X_3 \oplus X_4)$ 的每个分量的代数标准型。此外，文件 SM4_ANF_Generation.sage 是一个生成这些代数标准型的 SageMath 脚本。上述文件用于帮助参赛团队验证自己的结果是否正确。

三、密码学背景及相关问题的研究进展

近年来，随着量子计算机的快速发展，研究量子计算对于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，可以更精确的评估算法抵抗量子攻击的安全强度。

为了得到加密过程的量子电路，一个常用的技术路线是，首先实现加密过程的 NCT 电路，之后再将 Toffoli 门分解为更基本的容错量子门（Clifford 门+T 门）。对于一个容错量子电路来说，它的逻辑量

子比特数是衡量其规模的一个重要指标。另一个重要指标则是电路的 T 深度，电路运行时间主要由 T 深度的大小所决定。对于加密过程的量子电路实现问题，由于 T 门来自于 Toffoli 门的分解，因此其 NCT 实现中的 Toffoli 深度同样也会决定最终得到的容错量子电路的运行时间。

本赛题来源于我国商用密码算法 SM4 的轮函数的 NCT 电路构造问题。问题需要实现的布尔函数 F 对应了修改后的 SM4 轮函数。F 中的 L 函数与 SM4 算法的线性层稍有不同。F 中的 τ 函数可以看成 4 个并行执行的 S 函数，在密码学中我们一般称该 S 函数为 S 盒。在 SM4 的官方文档中，这个 S 盒是基于真值表给出的，而在本赛题中，我们直接给出了该 S 盒的代数标准型。此外，SM4 的 S 盒还可以看成下述对于有限域 $\boldsymbol{F}_{2^8}$ 上元素的操作，其中 Inv 表示对 $\boldsymbol{F}_{2^8}$ 中元素求乘法逆：

$$S(b) = M_2 \cdot Inv(M_1 \cdot b \oplus C_1) \oplus C_2, b \in \boldsymbol{F}_2^8$$

$$M_1 = \begin{bmatrix} 1&1&0&1&0&0&1&1 \\ 1&1&1&0&1&0&0&1 \\ 1&1&1&1&0&1&0&0 \\ 0&1&1&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1 \\ 1&0&0&1&1&1&1&0 \\ 0&1&0&0&1&1&1&1 \\ 1&0&1&0&0&1&1&1 \end{bmatrix}, C_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}, M_2 = \begin{bmatrix} 1&1&0&1&0&0&1&1 \\ 1&1&1&0&1&0&0&1 \\ 1&1&1&1&0&1&0&0 \\ 0&1&1&1&1&0&1&0 \\ 0&0&1&1&1&1&0&1 \\ 1&0&0&1&1&1&1&0 \\ 0&1&0&0&1&1&1&1 \\ 1&0&1&0&0&1&1&1 \end{bmatrix}, C_2 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

近年来，密码学界围绕对称密码算法尤其是 AES 的加密过程的量子电路优化问题展开了一系列研究。其中很多技术可以应用于本题的解答中。

首先，我们介绍一种最直接的布尔函数 NCT 电路原位实现方法。设 $f(x)$ 为我们需要原位实现的布尔函数，即我们希望用 NCT 电路实现变换 $(x,0)\to(f(x),0)$。我们可以从 f 的经典实现入手，即基于 XOR 门（加法）和 AND 门（乘法）的经典实现，将 XOR 门替换为 CNOT 门并将 AND 门替换为 Toffoli 门，从而构造出 f 的表达式。很容易看出，由于 Toffoli 门和 CNOT 门的输出位都会保留部分输入，当我们计算出最终输出 $f(x)$ 时，往往输出位会保留输入 x，并且会产生一些冗余的输出 $g(x)$。即我们得到的变换是：

Step 1: $(x,0,0)\to(x,g(x),f(x))$

为了清除掉这些冗余输出，一个常用的方法是通过（多个）CNOT 门，将 $f(x)$ 的每一位复制到新的辅助位上，即实现：

Step 2: $(x,g(x),f(x),0)\to\big(x,g(x),f(x),f(x)\big)$

之后，将 Step 1 中的门全部按逆序重新操作，等于进行了 Step 1 的逆变换，则实现了：

Step 3：$\big(x,g(x),f(x),f(x)\big)\to(x,0,0,f(x))$

我们一般称 Step 3 的过程为逆计算（Uncomputation）。组合 Step 1、2、3，我们就能实现:

$$(x,0,0,0)\to(x,0,0,f(x))$$

如果我们忽略为 0 的辅助位，则该变换可以看成 $(x,0)\to(x,f(x))$。由于在该实现中$f(x)$ 并没有存储在初始的输入位上，我们一般称这类实现为 $f(x)$的异位(out-of-place)实现。在上述例 2 中，若我们将 x_4

设为 0，则其变成了实现 $x_1x_2x_3$ 的一个异位实现。在著作[1]的 3.2.5 节中，对该方法以及经典可逆计算进行了更详细的介绍。

但是，从题目的描述中，本赛题需要构造的是原位实现：$(x,0)\to(f(x),0)$。对于如何利用异位实现构造原位实现的问题，论文[2]给出了比较系统的解答，相关方法可以运用到本题的解决中。

对于 SM4 的量子电路实现问题，论文[3]给出了最新的公开结果。该文给出的 SM4 S 盒的实现是基于有限域 $\boldsymbol{F}_{2^8}$ 元素求逆运算的 Tower Field 结构，参赛团队可以更细致的分析基于 Tower Field 结构的电路实现，从而优化[3]中的电路。此外，论文[2]中还介绍了一种降低 *T* 深度的技术，该技术主要是基于低 AND 深度的经典电路构造低 Toffoli 深度的量子电路，进而得到低 *T* 深度的量子电路。因此，[2]中提到的降低 Toffoli 深度的技术以及相关低深度 AES S 盒的构造结果（因为，AES S 盒与 SM4 S 盒的核心非线性部分相同，均为 F_{2^8} 中元素的乘法逆）也可以运用到本题的 Toffoli 深度优化中。

四、参考文献

[1] Michael A. Nielsen & Isaac L. Chuang, Quantum Computation and Quantum Information *10th Anniversary Edition*, Cambridge University Press.

[2] Zhenyu Huang and Siwei Sun, Synthesizing quantum circuits of AES with less qubits and lower *T*-depth. ASIACRYPT 2022.

[3] Jian Zou, Liji Li, Zihao Wei, Yiyuan Luo, Qian Liu, Wenling Wu,

New quantum circuit implementations of SM4 and SM3. Quantum Information Processing (2022) 21:181