第三届（2018）全国高校密码数学挑战赛

赛题四

一、赛题名称：密码算法布尔函数代数次数问题

二、赛题描述：

2.1 问题描述

一个n元布尔函数可形式化的表示为：

$$f\colon \mathbb{F}_2^n \to \mathbb{F}_2$$

$$(x_0, x_1, \cdots, x_{n-1}) \mapsto y$$

其中x_i和y均为取值在$\mathbb{F}_2 = \{0,1\}$中的变量。x_i称为输入比特，y称为输出比特。布尔函数可以唯一的表示为仅关于与运算（&）和异或运算（⊕）的表达式，这种表达式称为布尔函数的代数标准型（Algebraic Normal Form, ANF）。布尔函数的代数次数被定义为出现在代数标准型的乘积项中x_i的最高次数。例如：$f(x_0, x_1, x_2) = x_1 \oplus x_2$的代数次数是 1，$f(x_0, x_1, x_2) = x_1 \oplus x_0 \& x_1 \& x_2 = x_1 \oplus x_0 x_1 x_2$的代数次数是 3。由于布尔变量满足$x_i \& x_i = x_i$，因而$n$元布尔函数的代数次数至多为$n$。

ACORN[2]是新加坡学者 H. Wu 在 2014 年设计的轻量级认证加密算法，2018 年入选为凯撒竞赛（CAESAR Competition）最终轮算法之一。这里给出 ACORN 初始化阶段的一个简化版本（称为 ACORN-S），其递归表示如下：

$$s_i^{(0)} = 0,\ 0 \le i \le 292$$

$$v_i = \begin{cases} x_i, & 0 \le i \le 255 \\ 0, & i \ge 256 \end{cases}$$

$$s_{288}^{(t+1)} = s_{289}^{(t)} \oplus s_{235}^{(t)} \oplus s_{230}^{(t)}$$

$$s_{229}^{(t+1)} = s_{230}^{(t)} \oplus s_{196}^{(t)} \oplus s_{193}^{(t)}$$

$$s_{192}^{(t+1)} = s_{193}^{(t)} \oplus s_{160}^{(t)} \oplus s_{154}^{(t)}$$

$$s_{153}^{(t+1)} = s_{154}^{(t)} \oplus s_{111}^{(t)} \oplus s_{107}^{(t)}$$

$$s_{106}^{(t+1)} = s_{107}^{(t)} \oplus s_{66}^{(t)} \oplus s_{61}^{(t)}$$

$$s_{60}^{(t+1)} = s_{61}^{(t)} \oplus s_{23}^{(t)} \oplus s_0^{(t)}$$

$$s_i^{(t+1)} = s_{i+1}^{(t)},\ 0 \le i \le 291 \text{ 且 } i \notin \{60,106,153,192,229,288\}$$

$$\begin{aligned} s_{292}^{(t+1)} = {} & v_t \oplus 1 \oplus s_0^{(t)} \oplus s_{12}^{(t)} \oplus s_{66}^{(t)} \oplus s_{106}^{(t+1)} \oplus s_{153}^{(t+1)} \oplus s_{196}^{(t)} \\ & \oplus s_{23}^{(t)} \& s_{160}^{(t)} \oplus s_{23}^{(t)} \& s_{244}^{(t)} \oplus s_{160}^{(t)} \& s_{244}^{(t)} \oplus s_{66}^{(t)} \& s_{229}^{(t+1)} \\ & \oplus s_{111}^{(t)} \& s_{229}^{(t+1)} \oplus s_{60}^{(t+1)} \& s_{192}^{(t+1)} \oplus s_{60}^{(t+1)} \& s_{235}^{(t)} \oplus s_{192}^{(t+1)} \& s_{235}^{(t)}. \end{aligned}$$

由以上表达式可知，任意$s_i^{(t)}$均可写成关于变元x_i的布尔函数。请推导$s_{292}^{(t)}$的代数次数，或给出其代数次数的上界。

2.2 成绩评判

1) 可以使用相关软件进行辅助推导，如 MAPLE、MATHMATIC、MATLAB、SAGEMATH 等。
2) 解答过程中引用前人方法的必须在报告中明确给出引用，否则报告内容作废。
3) 在保证推导结果正确的前提下，轮数t越大，得分越多。
4) 在轮数t相同的前提下，给出的代数次数上界越紧，得分越多。
5) 解答过程中，提出新方法的，酌情加分。

三、研究背景及主要研究进展

布尔函数描述了输出比特关于输入比特的逻辑运算，它们是研究密码算法和密码技术的重要工具，在对称密码算法的设计中也占据了十分重要的地位。众所周知，任何一个加密算法理论上均可写成关于输入的布尔函数。但通常情况下，由于时间和存储复杂度的限制，得到一个密码算法确切的布尔函数表达式并不是一件容易的事。另一方面，若一个加密算法的布尔函数表达式或其代数次数可知，我们便可利用这一条件进行区分攻击或密钥恢复攻击。目前，在对称密码的分析中，已经出现了许多直接或间接地利用布尔函数及其代数次数的攻击方法，如代数攻击、高阶差分攻击、立方攻击、积分攻击等。可见，布尔函数及其代数次数的研究在密码学中具有非常重要的意义。

在欧密会 2015 上，Todo[3]提出了一种基于分离特性构造积分区分器的方法。在 FSE 2016 上，Todo 和 Morii[4]将分离特性应用于分组密码算法 SIMON，并指出分离特性与布尔函数的推导之间存在着一定的对应关系，所以由分离特性导出的指标集的性质在一定程度上可以反映布尔函数次数的上界。在美密会 2017 上，Todo 等人[5]进一步将分离特性应用于序列密码算法 Trivium、Grain-128a 和 ACORN。在同年美密会上，Liu[6]提出了数值映射的方法，用来估计非线性反馈密码算法的代数次数，并应用于 Trivium 等密码算法。

综上所述，不管是从研究密码算法的布尔函数本身而言，还是从深入理解各种与布尔函数有关的分析方法的角度而言，布尔函数的推导均具有非常重要的意

义。

四、参考文献

[1] 李超, 屈龙江, 周悦. 密码函数的安全性指标分析, 第 1 章. 科学出版社, 2011.

[2] Wu, H. ACORN: A Lightweight Authenticated Cipher (v3). Finalists of the CAESAR Competition. http://competitions.cr.yp.to/round3/acornv3.pdf

[3] Todo, Y. Structural evaluation by generalized integral property. In EUROCRYPT 2015. LNCS, vol. 9056, pp. 287–314. Springer, Heidelberg (2015)

[4] Todo, Y., Morii, M. Bit-based division property and application to Simon family. In FSE 2016. LNCS, vol. 9783, pp. 357–377. Springer, Heidelberg (2016)

[5] Todo, Y., Isobe, T., Hao, Y., Meier, W. Cube attacks on non-blackbox polynomials based on division property. In CRYPTO 2017. LNCS, vol. 10403, pp. 250–279. Springer, Cham (2017)

[6] Liu, M. Degree evaluation of NFSR-based cryptosystems. In CRYPTO 2017. LNCS, vol. 10403, pp. 227–249. Springer, Cham (2017)