第二届（2017）全国高校密码数学挑战赛

赛题三

一、赛题名称：密码算法布尔函数代数次数问题

二、赛题描述：

1.1 基本概念

循环左移操作（⋘）：设$x = (\mathrm{x}_0, \mathrm{x}_1, \cdots, \mathrm{x}_{\mathrm{n}-1})$为n比特串，则$x \lll 8 = (\mathrm{x}_8, \cdots, \mathrm{x}_{\mathrm{n}-1}, \mathrm{x}_0 \cdots, \mathrm{x}_7)$。

按位与运算（&）：设$x = (\mathrm{x}_0, \mathrm{x}_1, \cdots, \mathrm{x}_{\mathrm{n}-1}), y = (\mathrm{y}_0, \mathrm{y}_1, \cdots, \mathrm{y}_{\mathrm{n}-1})$为n比特串，则$x\& \, y = (\mathrm{x}_0 \& \mathrm{y}_0, \mathrm{x}_1 \& \mathrm{y}_1, \cdots \mathrm{x}_{\mathrm{n}-1} \& \mathrm{y}_{\mathrm{n}-1}) = (\mathrm{x}_0\mathrm{y}_0, \mathrm{x}_1\mathrm{y}_1, \cdots \mathrm{x}_{\mathrm{n}-1}\mathrm{y}_{\mathrm{n}-1})$。

异或运算（⊕）：设$x = (\mathrm{x}_0, \mathrm{x}_1, \cdots, \mathrm{x}_{\mathrm{n}-1}), y = (\mathrm{y}_0, \mathrm{y}_1, \cdots, \mathrm{y}_{\mathrm{n}-1})$为n比特串，则$x \oplus \, y = (\mathrm{x}_0 \oplus \mathrm{y}_0, \mathrm{x}_1 \oplus \mathrm{y}_1, \cdots \mathrm{x}_{\mathrm{n}-1} \oplus \mathrm{y}_{\mathrm{n}-1})$。

明文（ Plaintext ）：被隐蔽的消息称作明文。

密文（ Ciphertext ）：将明文隐蔽后的结果称作密文。

加密（ Encryption ）：将明文变换成密文的过程称作加密。

解密（ Decryption ）：合法用户由密文恢复出明文的过程称作解密。

密钥（ Key ） ：控制或参与密码变换的可变参数。

分组密码（ Block Cipher ）：将明文消息编码表示后的数字（简称明文数字）序列，划分成长度为 n 的组，每组分别在密钥的控制下变换成等长的输出数字序列。

迭代型分组密码：目前流行的分组密码均是迭代型密码，依赖同一个轮函数（或变换）的迭代来实现明文的变换。

1.2 问题描述

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。布尔函数可形式化的表示为：

$$\mathrm{f}: \mathbb{F}_2^{\mathrm{n}} \to \mathbb{F}_2$$

$$(\mathrm{x}_0, \mathrm{x}_1, \cdots, \mathrm{x}_{\mathrm{n}-1}) \mapsto \mathrm{y}$$

其中x_i和y均为取值在{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写做只关于与运算（&）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。

在分组密码算法中，轮函数可以表示为关于该轮输入的布尔函数，当我们不断将轮函数进行迭代时，每一轮的输出比特理论上可以表示为关于明文输入比特的布尔函数。通过研究这些迭代的布尔函数的性质，我们可以发掘一些可以有助于密码分析的新方法。目前，在对称密码的分析中，所使用的最多的布尔函数的性质为代数次数，也已经出现了许多或直接、或间接的利用布尔函数及其代数次数的攻击方法，如：代数攻击[1]、高阶差分攻击[1]、Cube 攻击[1]、积分攻击[1]等。所以对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。

SIMON[2]是 NSA 在 2013 年提出的轻量级加密算法，其轮函数的构造十分简单，只包含：循环移位（⋘）、与运算（&）和异或运算（⊕）。

这里给出 SIMON 的一个改编版本（称为 SIMON-V），我们改变了原有 SIMON 构造中的循环移位参数。SIMON-V 的具体结构见图 1（为简单起见，我们去掉了异或轮密钥的步骤）。

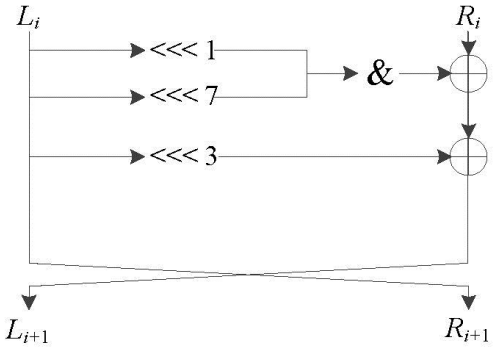

图 1：SIMON-V 的轮函数

请针对分组长度分别为 32 比特、48 比特和 64 比特的 SIMON-V 推导尽可能长轮数的布尔函数代数次数，或给出尽可能长轮数的布尔函数代数次数的上界。

1.3 简单示例

为帮助解题者理解题意，我们这里给出一个简单的例子。下面我们考虑一个

分组长度为 8 比特的 SIMON 的缩减版本（称为 SIMON-S），轮函数的具体构造见图 2。

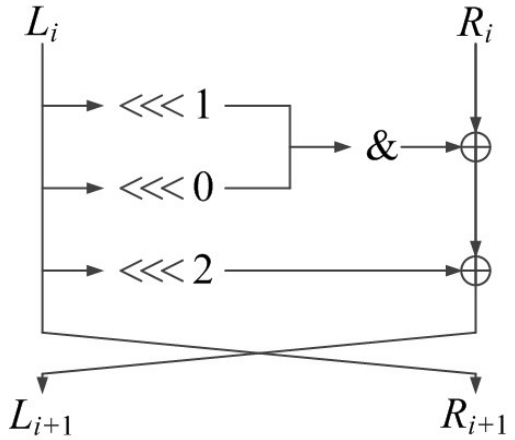

图 2：8 比特算法 SIMON-S 的轮函数

设$L_0 = (p_0, p_1, p_2, p_3)$，$R_0 = (p_4, p_5, p_6, p_7)$，$L_1 = (y_0, y_1, y_2, y_3)$，$R_0 = (y_4, y_5, y_6, y_7)$。按照轮函数的运算规则，我们有（具体推导过程请参考图 3）:

$$y_0 = p_1 p_0 \oplus p_2 \oplus p_4$$

$$y_1 = p_2 p_1 \oplus p_3 \oplus p_5$$

$$y_2 = p_3 p_2 \oplus p_0 \oplus p_6$$

$$y_3 = p_0 p_3 \oplus p_1 \oplus p_7$$

$$y_4 = p_0$$

$$y_5 = p_1$$

$$y_6 = p_2$$

$$y_7 = p_3$$

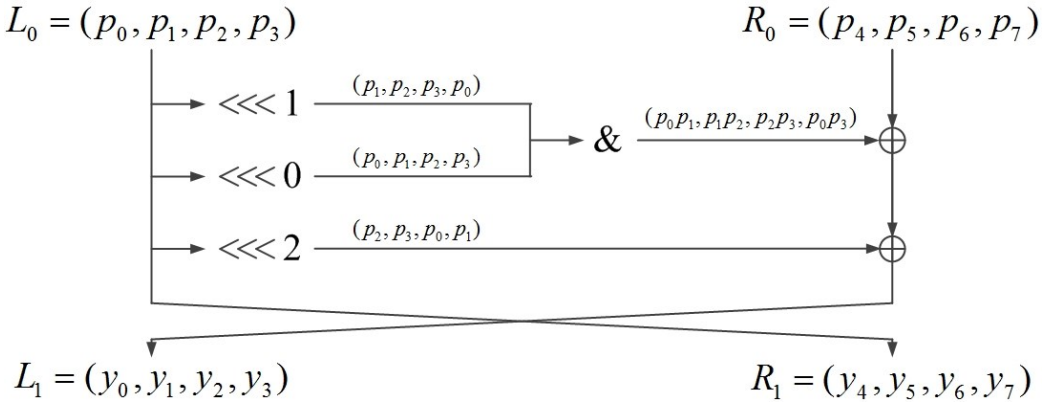

图 3：一轮 SIMON-S 布尔函数推导示意图

将第一轮的输出结果作为第二轮的输入进行迭代，我们可以类似的给出第二轮输出用p_i（$0 \le i \le 7$）表示的布尔函数。

注意到随着轮数的增长，布尔函数复杂程度也随之增大，特别是当分组长度较长、轮函数较复杂时，给出密码算法确切的布尔函数表达式并不是件平凡的事。

1.3 成绩评判

(1) 必要时，可以使用相关软件进行辅助推导，如：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，推导轮数越长，给分越多。

(4) 在轮数相同的前提下，给出的代数次数上界越紧，分数越多。

(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

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、空间、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（当分组长度较长、轮函数较复杂时，即便短轮数的布尔函数推导也并不容易）。

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建立区分器，进而恢复密钥。已有的许多攻击方法都或直接、或间接的利用了布尔函数的代数表达式，如：代数攻击、高阶差分攻击、Cube 攻击、积分攻击等。在这些攻击方法中，积分攻击是比较特殊的一种。积分区分器的构造并不单纯的由布尔函数的代数次数所决定，布尔函数的具体表达式（或者说布尔函数中的项）也会对积分区分器产生影响。

欧密 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。FSE 2016 上，Todo 和 Morii[4]将分离特性应用于 SIMON，并在理论上证明了 SIMON32 积分区分器的正确性。同时对于分组长度大于 32 的算法，文中也给出了区分器上界的评估。正如 Todo 和 Morii 在文中指出的那样，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。

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] 分组密码的攻击方法与实例分析，李超，孙兵，李瑞林著，科学出版社, 2010.

[2] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2015). The SIMON and SPECK lightweight block ciphers. In Proceedings of the 52nd Annual Design Automation Conference (p. 175). ACM.

[3] Todo, Y. (2015). Structural evaluation by generalized integral property. In Advances in Cryptology--EUROCRYPT 2015 (pp. 287-314). Springer Berlin Heidelberg.

[4] Todo, Y & Morii, M. (2016) Bit-based division property and application to simon family. In Fast Software Encryption (pp. 357-377). Springer Berlin Heidelberg.