第七届（2022）全国高校密码数学挑战赛

赛题一

一、赛题名称：分组密码密钥恢复问题

二、赛题描述

2.1 符号说明

令$\mathbb{F}_2 = \{0,1\}$. $\mathbb{F}_2$中元素的“补”按如下定义：

$$\bar{0} = 1，\ \bar{1} = 0；$$

$\mathbb{F}_2$中两个元素的“与”运算按如下定义：

$$0\&0 = 0\&1 = 1\&0 = 0，\ 1\&1 = 1；$$

$\mathbb{F}_2$中两个元素的“异或”运算按如下定义：

$$0 \oplus 0 = 1 \oplus 1 = 0，\ 0 \oplus 1 = 1 \oplus 0 = 1.$$

设$X = (x_{15}, x_{14}, \cdots, x_0)$为$\mathbb{F}_2$上的16维向量，即$x_i \in \mathbb{F}_2$，$i = 0,1,\ldots,15$；

则$\bar{X}$表示按位对X取补，即

$$\overline{(x_{15}, x_{14}, \cdots, x_0)} = (\overline{x_{15}}, \overline{x_{14}}, \cdots, \overline{x_0})；$$

$X \ll a$表示将X左移a位，其中$1 \le a \le 15$：

$$(x_{15}, x_{14}, \cdots, x_0) \ll a = (x_{15-a}, x_{14-a}, \ldots, x_0, \underbrace{0, \ldots, 0}_{a个})；$$

$X \lll a$表示将X循环左移a位，其中$1 \le a \le 15$：

$$(x_{15}, x_{14}, \cdots, x_0) \lll a = (x_{15-a}, x_{14-a}, \ldots, x_0, x_{15}, \ldots, x_{16-a})；$$

$X\&Y$表示X和Y按位与，即

$$(x_{15}, x_{14}, \ldots, x_0)\&(y_{15}, y_{14}, \ldots, y_0) = (x_{15}\&y_{15}, x_{14}\&y_{14}, \ldots, x_0\&y_0)；$$

$X \oplus Y$表示X和Y按位异或，即

$$(x_{15}, x_{14}, \dots, x_0) \oplus (y_{15}, y_{14}, \dots, y_0) = (x_{15} \oplus y_{15}, x_{14} \oplus y_{14}, \dots, x_0 \oplus y_0).$$

2.2 基础知识

所谓分组密码，是指由参数$K \in \mathbb{F}_2^t$（t称为密钥长度）控制的一个从$\mathbb{F}_2^n$到$\mathbb{F}_2^n$（n称为分组长度）的置换E_K. 令$c = E_K(m)$，则称m为明文，c称为明文m在密钥K作用下的密文.

本题所指的密钥恢复攻击，是指在K未知的前提下，攻击者构造具有特殊属性的明文m，并观测相应的密文c，通过这些明文和密文的特殊属性，计算出密钥K的值.

给定一组明密文对(m, c)，通过穷尽搜索密钥K的所有可能值并检验$c = E_K(m)$是否成立，可以得到密钥的正确值，此时攻击复杂度为2^t次检验$c = E_K(m)$是否成立. 该方法具有通用性，但复杂度较高，故有效密钥恢复攻击，通常指比穷尽搜索更好的攻击方法.

2.3 问题描述

本赛题的目标是：在单密钥模型下（即整个攻击过程，所有的密文均在同一密钥下加密得到），攻击者任意选择所需要的明文并得到相应的密文，通过这些明文和密文，恢复出J算法的密钥.

J算法流程如图 1 所示. 算法分组长度n为32比特，密钥K的长度t为64比特. 令明文$m = (L_0, R_0)$，其中L_0和R_0分别为m的左16比特和右16比特，则算法计算流程如下：

$$T_{i,1} = (RK_{i-1} \& L_{i-1}) \oplus R_{i-1} \oplus (\mathrm{i} - 1)$$

$$T_{i,2} = S(T_{i,1}) = \big((T_{i,1} \ll 2) \& (T_{i,1} \ll 1)\big) \oplus T_{i,1}$$

$$T_{i,3} = P(T_{i,2}) = (T_{i,2} \lll 3) \oplus (T_{i,2} \lll 9) \oplus (T_{i,2} \lll 14)$$

$$L_i = R_{i-1} \oplus (RK_{i-1} \& T_{i,3})$$

$R_i = L_{i-1} \oplus T_{i,3}$

其中$i = 1,2,\dots,r$，$RK_{2j+1} = \overline{RK_{2j}}$，$j = 0,1,2,\dots$，i表示$i$的二进制展开（比如当$i = 9$时，$\mathrm{i} = 0000000000001001$）．$r$称为算法的迭代轮数，$RK_i$由密钥$K = k_{63}k_{62}\dots k_0$按如下方式计算得到：

令$\begin{cases} K_3 = (k_{63}, k_{62}, \dots, k_{48}) \\ K_2 = (k_{47}, k_{46}, \dots, k_{32}) \\ K_1 = (k_{31}, k_{30}, \dots, k_{16}) \\ K_0 = (k_{15}, k_{14}, \dots, k_0) \end{cases}$，$K_{i+4} = \overline{K_i} \oplus \mathrm{i}$，其中$i = 0,1,2\dots$，则$RK_{2i} = K_i$，$RK_{2i+1} = \overline{K_i}$.

$c = (R_r, L_r)$定义为明文$m = (L_0, R_0)$在密钥K下的密文.

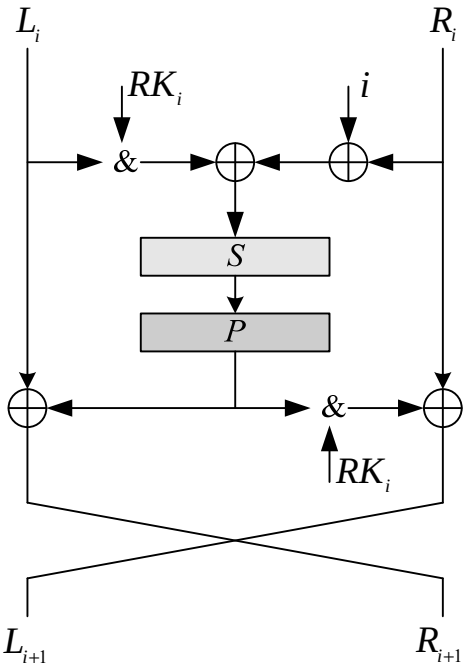

图 1　J算法

针对$r = 1$的情形，下面给出两种恢复密钥的方法实例：

方法一：随机选择明文$m = (m_L, m_R)$，并得到密文$c = (c_L, c_R)$；记P变换的输出为Z，则有$m_L \oplus m_R \oplus c_L \oplus c_R = \overline{RK_0}\&Z$．计算$T = m_L \oplus m_R \oplus c_L \oplus c_R$，若$T$的第$i$位为1，则可断定$RK_0$的第$i$位为0；随机选择$q$个明文并加密，重复上述步骤计算得到$T_1, T_2, \dots, T_q$，若

$T_1, T_2, \ldots, T_q$的第j位均为0，当q较大时，可断定RK_0的第j位为1.

方法二：随机选择明文$m = (m_L, m_R)$，并得到其密文$c = (c_L, c_R)$. 记$e_i = (0, \ldots, 0, \underbrace{1}_{\text{第}i\text{位}}, 0, \ldots, 0)$. 令$m^* = (m_L \oplus e_i, m_R)$，即$m^*$和$m$只在左支的第$i$比特不同，其余比特均相同；记$m^*$对应的密文$c^* = (c_L^*, c_R^*)$，$P$变换的输出分别为$Z$和$Z^*$.

若RK_0的第i比特为0，则$Z = Z^*$，从而

$$c_R \oplus c_R^* = (m_L \oplus Z) \oplus (m_L^* \oplus Z^*) = e_i.$$

若RK_0的第i比特为1，则$Z \neq Z^*$，从而

$$c_R \oplus c_R^* = (m_L \oplus Z) \oplus (m_L^* \oplus Z^*) \neq e_i.$$

根据上述分析，选择明文$m = (m_L, m_R)$和$m^* = ((m_L \oplus e_i), m_R)$，并观测其对应密文的异或值，若$c_R \oplus c_R^* = e_i$，则判断$RK_0$的第$i$比特为0；否则，判断$RK_0$的第$i$比特为1.

2.4 成绩评判标准

要求参赛者在不借助高性能计算平台的前提下，正确恢复出J算法的密钥，恢复的轮数越高，得分越高，具体如下：

（1）给出攻击原理，复杂度分析等；

（2）给出攻击运行的标准 C 代码，要求代码简洁，注释明确；

（3）最终得分为：$Scores = \sum_{j=1}^{r} a_j b_j \times 1.5^j$；

上式中，r表示参赛者能够实际恢复密钥的最高轮数；若参赛者正确给出了第j轮攻击理论分析和实现代码，则$a_j = 1$；若参赛者未给出第j轮攻击，或者给出的攻击错误，则$a_j = 0$. 若参赛者给出的第j轮攻击对所有密钥均成立，则$b_j = 1$，若参赛者给出的攻击只针对某些

特殊类型的密钥（弱密钥）成立，则$b_j = 0.7$.

三、密码学背景及相关问题的研究进展

(1) 差分密码分析是分组密码最重要的分析方法之一，该攻击方法是 Biham 和 Shamir 在 1990 年针对 DES 算法提出的一种攻击手段. 通过观察具有特定输入差分的明文对经过加密后的密文对的差分形式来恢复密钥.

(2) 线性密码分析由 Matsui 在 EUROCRYPT 1993 上提出，该攻击方法通过构造明文比特、密文比特和密钥比特的线性逼近式来恢复算法的密钥.

(3) Knudsen 提出的积分攻击是 Square 攻击的更一般形式. 积分攻击是一种选择明文攻击方法，通过计算特殊形式明文集对应密文集的异或和，从而将密钥恢复出来.

四、参考文献

[1] Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of CRYPTOLOGY, 1991, 4(1): 3-72.

[2] Matsui M. Linear cryptanalysis method for DES cipher[C]. Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1993: 386-397.

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