



Midori64 分组密码算法的积分攻击

王超^{1,2}, 陈怀凤^{1,2}

(1. 中国电子信息产业集团有限公司第六研究所, 北京 102209; 2. 密码科学技术国家重点实验室, 北京 100878)

摘要: 积分攻击是一种重要的密钥恢复攻击方法, 已被广泛应用于多种分组算法分析任务。Midori64 算法是一种轻量级分组密码算法, 为对其进行积分攻击, 构建 3 个 6 轮零相关区分器, 将其分别转化为 6 轮平衡积分区分器并合成为一个性质优良的 6 轮零和积分区分器, 将该零和积分区分器向前扩展 1 轮得到一个 7 轮零和积分区分器。分别采用部分和技术与快速 Walsh-Hadamard 变换技术, 得到 Midori64 算法的 10 轮积分攻击和 11 轮积分攻击。分析结果表明, 10 轮积分攻击的数据复杂度为 2^{40} 个明密文对, 时间复杂度为 $2^{67.85}$ 次 10 轮加密运算, 11 轮积分攻击的数据复杂度为 $2^{40.09}$ 个明密文对, 时间复杂度为 $2^{117.37}$ 次 11 轮加密运算。

关键词: 密码分析; Midori64 算法; 积分攻击; 部分和技术; 快速 Walsh-Hadamard 变换技术

开放科学(资源服务)标志码(OSID):



中文引用格式: 王超, 陈怀凤. Midori64 分组密码算法的积分攻击[J]. 计算机工程, 2021, 47(5): 117-123.

英文引用格式: WANG Chao, CHEN Huaifeng. Integral attacks on Midori64[J]. Computer Engineering, 2021, 47(5): 117-123.

Integral Attacks on Midori64

WANG Chao^{1,2}, CHEN Huaifeng^{1,2}

(1. The 6th Research Institute of China Electronics Corporation, Beijing 102209, China;

2. State Key Laboratory of Cryptology, Beijing 100878, China)

[Abstract] Proven to be an important key recovery method, the technique of integral attacks has been widely used in the analysis of block ciphers. This paper describes an attempt at integral attacks on the lightweight block cipher, Midori64. Three 6-round zero-correlation distinguishers are constructed, transformed into three 6-round balanced integral distinguishers, and then merged into one excellent 6-round zero-sum integral distinguisher, which extends one round forward to obtain a 7-round zero-sum integral distinguisher. On this basis, the partial-sum technique and the fast Walsh-Hadamard transform technique are used for the 10-round and 11-round integral attacks on Midori64. The analysis results show that the data complexity and the time complexity of the 10-round integral attacks are 2^{40} and $2^{67.85}$ respectively, and those of 11-round attacks are $2^{40.09}$ and $2^{117.37}$ respectively.

[Key words] cryptanalysis; Midori64; integral attack; partial-sum technique; fast Walsh-Hadamard transform technique

DOI: 10.19678/j.issn.1000-3428.0057716

0 概述

为了验证 Midori 算法^[1]的安全性, 研究人员对 Midori 算法进行了许多密码分析。文献[2]提出对 Midori64 算法的 14 轮相关密钥不可能差分分析, 共猜测了 84 bit 密钥。文献[3]提出对 Midori64 算法的 12 轮中间相遇攻击, 该攻击的时间复杂度为 $2^{125.5}$ 次 12 轮加密, 数据复杂度为 $2^{55.5}$ 个 64 bit 分组。文献[4]提出对 Midori64 算法的 11 轮不可能差分分

析, 该攻击的时间复杂度为 $2^{121.6}$ 次 11 轮加密, 数据复杂度为 $2^{62.3}$ 个 64 bit 分组。文献[5]对文献[4]的不可能差分分析进行优化, 时间复杂度为 $2^{121.42}$ 次 11 轮加密, 数据复杂度为 $2^{60.82}$ 个 64 bit 分组。文献[6]提出对 Midori64 算法的 10 轮多维零相关线性分析, 其时间复杂度为 $2^{79.35}$ 次 10 轮加密, 数据复杂度为 $2^{62.4}$ 个 64 bit 分组。文献[7]提出对 Midori64 算法的 8 轮积分分析, 其时间复杂度为 2^{65} 次 8 轮加密, 数据复杂度为 $2^{19.80}$ 个 64 bit 分组。文献[8-9]分别提出对

基金项目: 密码科学技术国家重点实验室开放课题“新型轻量级序列密码设计与分析”。

作者简介: 王超 (1982—), 男, 高级工程师、博士, 主研方向为信息安全; 陈怀凤, 高级工程师、博士。

收稿日期: 2020-03-13 修回日期: 2020-04-30 E-mail: wangchao@ncse.com.cn

Midori64算法的不变子空间攻击和非线性不变量攻击,并给出了算法的全轮弱密钥攻击。

文献[10]建立零相关区分器与积分区分器之间的等价关系^[11-12],证明从零相关路线 $a \not\rightarrow b, a = (a_1, 0), b = (b_1, 0), a_1 \neq 0, b_1 \neq 0$ 可以直接推导出一条积分路线,其中,输入掩码部分值 a_1 与输出掩码部分值 b_1 相互独立。利用该性质,可以借助已找到的零相关线性路线构造更优的积分路线。为了消除零相关路线向积分路线转化的条件限制,文献[13]提出一种新方法,无论 a_1 和 b_1 是否独立,都可以将零相关路线 $(a_1, 0) \not\rightarrow (b_1, 0)$ 转为积分路线。分离特性(Division Property)^[14]是一种新型积分路线搜索方法,该方法充分考虑非线性组件的代数次数,对积分性质的刻画更加精细。此后,基于混合整数线性规划MILP技术的分离特性搜索方法也相继被提出,且文献[15]利用该方法构造了7轮积分路线。

本文对Midori64算法的积分攻击问题进行研究,给出算法的6轮零相关区分器,得到相应的6轮积分区分器,向前扩展1轮得到7轮积分区分器,在此基础上,分别研究针对10轮、11轮Midori64算法的积分攻击。

1 预备知识

1.1 符号说明

本文的符号说明如下: \oplus 表示按位异或, \parallel 表示字符串级联, \bullet 表示函数复合, F_2^n 表示 F_2 上的 n 维向量空间, $+$ 表示有限域内的模加运算,LSB表示最低有效位, K_i^j 表示第 j 轮等价轮密钥的第 i 个单元, U 表示单元性质不可知, Z 表示单元具有零和性。

1.2 Midori64算法描述

Midori算法于2015年由BANIK等人在ASIACRYPT会议上提出^[1],其采用SPN(Substitution Permutation Network)结构,具有低功耗的特点,是一种轻量级分组密码算法。Midori算法的密钥长度为128 bit,分组长度为64 bit或128 bit,相应的迭代轮数为16轮或20轮,分别记作Midori64和Midori128。Midori64算法的明文分组长度为64 bit,每个明文分组被分成16个4 bit,矩阵表示如下:

$$S = \begin{bmatrix} S_0 & S_4 & S_8 & S_{12} \\ S_1 & S_5 & S_9 & S_{13} \\ S_2 & S_6 & S_{10} & S_{14} \\ S_3 & S_7 & S_{11} & S_{15} \end{bmatrix} \quad (1)$$

其中, $S_i (i=0, 1, \dots, 15)$ 表示单元(Cell)。式(1)又称状

态矩阵。

Midori64算法轮变换作用在状态矩阵上,由S盒(SubCell,简记为SB)、置换(ShuffleCell,简记为SC)、列混淆(MixColumn,简记为MC)和密钥加(KeyAdd,简记为KA)复合组成。

1.2.1 密钥编排算法

Midori64算法的密钥长度为128 bit,将密钥的高64 bit记为 Key_0 ,低64 bit记为 Key_1 。定义白化密钥 $WK = Key_0 \oplus Key_1$, 轮 密 钥 $RK^i = Key_{i \bmod 2} \oplus q_i (i = 0, 1, \dots, 14)$,其中, q_i 为 4×4 矩阵形式的轮密钥常数,其定义参考文献[1]。将 Key_0 与 Key_1 以 4×4 矩阵形式表示, q_i 按位异或在每个4 bit单元的LSB位。

1.2.2 S盒

Midori64算法使用的非线性S盒取值如表1所示,S盒具有对合性质,即 $SB^{-1} = SB$ 。

表1 Midori64算法的S盒
Table 1 S-box of Midori64

x	SB(x)	x	SB(x)
0	C	8	8
1	A	9	9
2	D	A	1
3	3	B	5
4	E	C	0
5	B	D	2
6	F	E	4
7	7	F	6

1.2.3 置换

重新排列状态矩阵中16个单元的位置称为置换,置换及逆置换分别如式(2)和式(3)所示:

$$\begin{bmatrix} S_0 & S_4 & S_8 & S_{12} \\ S_1 & S_5 & S_9 & S_{13} \\ S_2 & S_6 & S_{10} & S_{14} \\ S_3 & S_7 & S_{11} & S_{15} \end{bmatrix} \xrightarrow{SC} \begin{bmatrix} S_0 & S_{14} & S_9 & S_7 \\ S_{10} & S_4 & S_3 & S_{13} \\ S_5 & S_{11} & S_{12} & S_2 \\ S_{15} & S_1 & S_6 & S_8 \end{bmatrix} \quad (2)$$

$$\begin{bmatrix} S_0 & S_4 & S_8 & S_{12} \\ S_1 & S_5 & S_9 & S_{13} \\ S_2 & S_6 & S_{10} & S_{14} \\ S_3 & S_7 & S_{11} & S_{15} \end{bmatrix} \xrightarrow{SC^{-1}} \begin{bmatrix} S_0 & S_5 & S_{15} & S_{10} \\ S_7 & S_2 & S_8 & S_{13} \\ S_{14} & S_{11} & S_1 & S_4 \\ S_9 & S_{12} & S_6 & S_3 \end{bmatrix} \quad (3)$$

1.2.4 列混淆

以almost MDS^[1]矩阵 M 左乘更新状态矩阵称为列混淆,如式(4)所示,其中,矩阵 M 如式(5)所示,矩阵 M 满足 $M^{-1} = M$ 。

$$\begin{bmatrix} S_0 & S_4 & S_8 & S_{12} \\ S_1 & S_5 & S_9 & S_{13} \\ S_2 & S_6 & S_{10} & S_{14} \\ S_3 & S_7 & S_{11} & S_{15} \end{bmatrix} \xrightarrow{MC} M \bullet \begin{bmatrix} S_0 & S_4 & S_8 & S_{12} \\ S_1 & S_5 & S_9 & S_{13} \\ S_2 & S_6 & S_{10} & S_{14} \\ S_3 & S_7 & S_{11} & S_{15} \end{bmatrix} \quad (4)$$

$$M = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \quad (5)$$

1.2.5 密钥加

Midori64算法在加密过程中使用64 bit白化密钥WK和轮密钥RK_i (i=0,1,...,14)对状态矩阵进行异或更新。

Midori64算法在解密过程中使用64 bit白化密钥WK和SC⁻¹(MC(RK_i)) (i=14,13,...,0)对状态矩阵进行异或更新。

1.2.6 加密流程

Midori64算法的加密流程如图1所示,在第1轮之前添加使用白化密钥的密钥加,第1轮~第15轮使用轮密钥RK_i (i=0,1,...,14)进行密钥加,第16轮使用白化密钥进行密钥加。

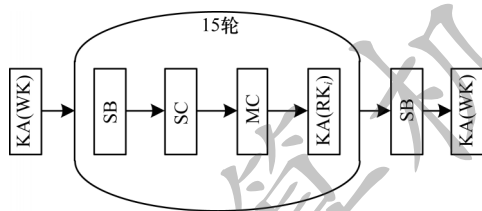


图1 Midori64算法的加密流程

Fig.1 The encryption procedure of Midori64

1.2.7 解密流程

Midori64算法的解密流程如图2所示,在第1轮之前添加使用白化密钥的密钥加,第1轮~第15轮使用SC⁻¹(MC(RK_i)) (i=14,13,...,0)进行密钥加,第16轮使用白化密钥进行密钥加。

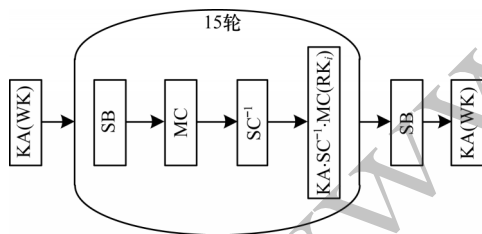


图2 Midori64算法的解密流程

Fig.2 The decryption procedure of Midori64

2 Midori64的6轮零相关区分器

零相关线性分析由BOGDANOV和RIJMEN^[16]于2012年提出,攻击使用分组密码算法中以概率 $\frac{1}{2}$ 成立的线性逼近,即相关度为零的线性逼近,由此区分分组密码算法与随机置换,进而恢复密钥。文献[17]建立了多重零相关分析模型,其克服了经典

零相关线性分析在数据复杂度方面的缺陷。文献[18]建立了卡方多维零相关线性模型,其消除了对零相关数量的限制条件。

函数 $h: F_2^m \rightarrow F_2^n$ 上线性逼近 (α, β) 的相关度定义为:

$$C_h(\alpha, \beta) = \frac{1}{2^n} \sum_{x \in F_2^m} (-1)^{\alpha \cdot x \oplus \beta \cdot h(x)}$$

其中, α 为输入掩码, β 为输出掩码, \cdot 表示向量内积。当 $C_h(\alpha, \beta)=0$ 时,称 (α, β) 为零相关线性逼近^[17]。

命题1(线性映射的相关度)^[17] 对于线性映射 $h(x)=Mx$,若 $\alpha=M^T\beta$,则 $C_h(\alpha, \beta)=1$;否则, $C_h(\alpha, \beta)=0$ 。

零相关区分器是指在输入掩码与输出掩码作用下,目标输入与输出比特的线性相关度为0的一类线性区分器。根据命题1进行自动化搜索,可以得到大量Midori64算法的5轮零相关区分器,按输入掩码权重与输出掩码权重进行分类,零相关区分器的个数统计结果如表2所示。

表2 Midori64算法的5轮零相关区分器个数统计

Table 2 Number statistics of Midori64 5-round zero-correlation discriminator

输入掩码权重	零相关区分器个数						
	输出掩码权重为1	输出掩码权重为2	输出掩码权重为3	输出掩码权重为4	输出掩码权重为5	输出掩码权重为6	输出掩码权重为7
1	256	1 392	3 040	3 280	2 016	672	96
2	1 392	0	0	0	0	0	0
3	3 040	0	0	0	0	0	0
4	3 280	0	0	0	0	0	0
5	2 016	0	0	0	0	0	0
6	672	0	0	0	0	0	0
7	96	0	0	0	0	0	0

取3个输入掩码权重为7且输出掩码权重为1的5轮零相关区分器,然后对输出掩码部分继续扩展1轮,得到6轮零相关区分器。令:

$$\alpha_1 = a_0 \parallel 0 \parallel 0 \parallel a_3 \parallel a_4 \parallel 0 \parallel a_6 \parallel 0 \parallel a_8 \parallel a_9 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0$$

$$\beta_1 = 0 \parallel d_0 \parallel d_0 \parallel d_0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0$$

$$\beta_2 = d_5 \parallel d_5 \parallel 0 \parallel d_5 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0$$

$$\beta_3 = d_{15} \parallel d_{15} \parallel d_{15} \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0 \parallel 0$$

其中, $a_0, a_3, a_4, a_6, a_8, a_9, a_{12}, d_0, d_5, d_{15}$ 均为4 bit向

量, $\mathbf{0}$ 为 4 bit 零向量。($\alpha_1 \xrightarrow{6\text{轮}} \beta_1$)、($\alpha_1 \xrightarrow{6\text{轮}} \beta_2$) 和 ($\alpha_1 \xrightarrow{6\text{轮}} \beta_3$) 都是 Midori64 算法的 6 轮零相关区分

器。第 1 个 6 轮零相关区分器的掩码扩展细节如图 3 所示。

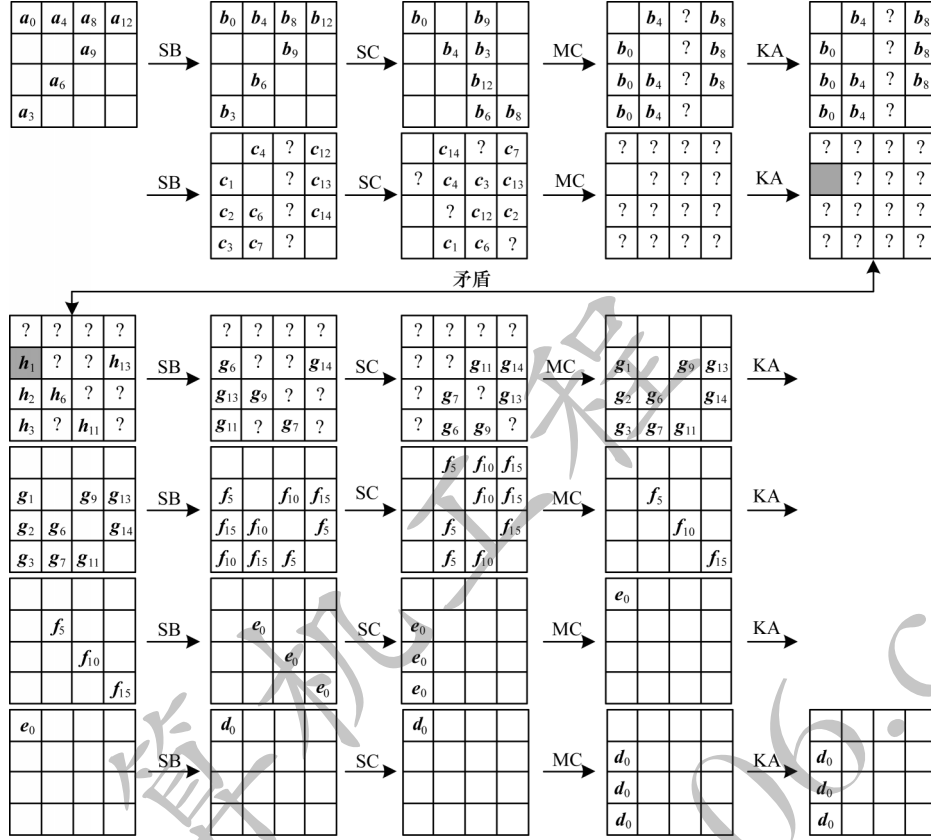


图3 Midori64算法的6轮零相关区分器

Fig.3 6-round zero-correlation discriminator of Midori64

3 Midori64的积分区分器

3.1 积分区分器构造

积分攻击是一种选择明文攻击,最先应用于 Square 分组密码分析,其基本思想是通过分析一系列中间状态的和具有概率为 1 的性质,得出不能通过检测的密钥都是错误密钥,从而利用淘汰法直接恢复出正确密钥。积分攻击的主要环节是寻找积分区分器,积分区分器可以分为如下 2 类:

1) 一系列中间状态的和遍历所有可能取值,且每个可能取值的出现次数相同,该类积分区分器称为平衡积分区分器。

2) 一系列中间状态的异或和为零,该类积分区分器称为零和积分区分器。

当选择特定的输入集合(输入的部分比特固定为常数,其余比特遍历所有可能)时,经过几轮算法加密后,输出的某些比特存在概率为 1 的分布特性,输出目标值异或和为 0 时,为零和积分区分器;输出目标值均匀遍历所有可能时,为平衡积分区分器。实际上,平衡积分区分器与零相关区分器之间

存在一定的等价关系^[10],任意的零相关区分器都可以转化成一个平衡积分区分器,本文利用文献[10]中给出的两区分器等价性进行积分区分器构造。

若所有原像集的势都相同,则函数 $h: F_2^s \rightarrow F_2^t$ 是平衡的^[10],即集合 $h^{-1}(y) = \{x \in F_2^s | h(x) = y\}$ 的大小与 y 无关。

命题 2^[10] 对于函数 $h: F_2^s \times F_2^s \rightarrow F_2^t \times F_2^u, h(x, y) =$

$\begin{pmatrix} h_1(x, y) \\ h_2(x, y) \end{pmatrix}$, 定义 $T_\lambda: F_2^s \rightarrow F_2^t, T_\lambda(y) = h_1(\lambda, y)$ 。若 $\forall a \in$

$F_2^s, b \in F_2^t, b \neq 0$ 且 a 与 b 独立,则函数 h 上线性特征 $(a \parallel 0, b \parallel 0)$ 的相关度为 0 等价于 $\forall \lambda \in F_2^s$, 函数 T_λ 是平衡的。

3.2 Midori64的6轮积分区分器

记集合 $S_{in} = \{x = (c_0, b_1, b_2, c_3, c_4, b_5, c_6, b_7, c_8, c_9, b_{10}, b_{11}, c_{12}, b_{13}, b_{14}, b_{15})\}$, 其中, $c_0 \parallel c_3 \parallel c_4 \parallel c_6 \parallel c_8 \parallel c_9 \parallel c_{12}$ 取常数, $b_1 \parallel b_2 \parallel b_5 \parallel b_7 \parallel b_{10} \parallel b_{11} \parallel b_{13} \parallel b_{14} \parallel b_{15}$ 遍历所有可能取值。 S_{in} 中存在 2^{36} 个元素,存在 2^{28} 个此类集

合。经过6轮加密后,得到对应的输出集合为 $S_{out} = \{y = (y_0, y_1, \dots, y_{15}) | y = E_{Key}^6(x), x \in S_{in}\}$ 。

令 $t_0 = y_1 \oplus y_2 \oplus y_3$ 、 $t_1 = y_0 \oplus y_1 \oplus y_3$ 和 $t_2 = y_0 \oplus y_1 \oplus y_2$, 则加密函数被分割为:

$$E_{Key}^6: F_2^r \times F_2^s \rightarrow F_2^r \times F_2^u, E_{Key}^6(x, y) = \begin{pmatrix} h_1(x, y) \\ h_2(x, y) \end{pmatrix}$$

定理1 当输入为 S_{in} 时,加密6轮后, y_1 是零和的。

证明 加密函数 E_{Key}^6 上线性特征 (a_1, β_1) 、 (a_1, β_2) 和 (a_1, β_3) 的相关度都是0,由命题2可知 $T_\lambda: F_2^s \rightarrow F_2^t, T_\lambda(x_s) = h_1(\lambda, x_s)$ 是平衡的,得到 t_0 、 t_1 和 t_2 每个取值的原像个数相同,于是 $\sum t_0 = 0$, $\sum t_1 = 0$, $\sum t_2 = 0$,从而 $\sum y_1 = \sum t_0 \oplus \sum t_1 \oplus \sum t_2 = 0$,证毕。

6轮零和积分区分器如图4所示。

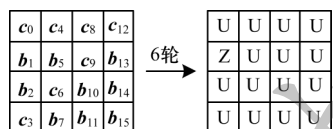


图4 Midori64算法的6轮零和积分区分器

Fig.4 6-round zero-sum integral discriminator of Midori64

3.3 Midori64的7轮积分区分器

在6轮积分区分器的前面解密1轮可以得到7轮积分区分器。对6轮积分区分器的输入 S_{in} 中各单元进行逆向轮密钥异或操作,其中,第0个、第3个、第4个、第6个、第8个、第9个和第12个单元是固定常数,其余单元仍然遍历所有可能取值。因此,在构造7轮积分区分器的过程中,可忽略此逆向密钥加操作。记7轮积分区分器的明文集合为:

$$S_{in}^* = \{y = SB^{-1}(SC^{-1}(MC^{-1}(x))) | x \in S_{in}\}$$

其中,列混淆、置换和S盒都是可逆变换,复合变换 $y = SB^{-1}(SC^{-1}(MC^{-1}(x)))$ 是双射。对由 2^{36} 个明文构成的 S_{in}^* 进行1轮加密,其结果满足6轮零和积分区分器的输入条件,因此,当输入为 S_{in}^* 时,加密7轮后 y_1 是零和的。存在一系列7轮积分路线,令 $\hat{S}_{in} = \{x = (c_0, b_1, b_2, c_3, c_4, b_5, c_6, b_7, b_8, b_9, c_{10}, c_{11}, c_{12}, b_{13}, c_{14}, c_{15})\}$ 。 \hat{S}_{in}^* 的定义与 S_{in}^* 类似,当输入为 \hat{S}_{in}^* 时,加密7轮后 y_{13} 是零和的。

4 Midori64的积分攻击

4.1 Midori64的10轮积分攻击

在7轮积分区分器的后面加密3轮可以得到10轮积分区分器,如图5所示。

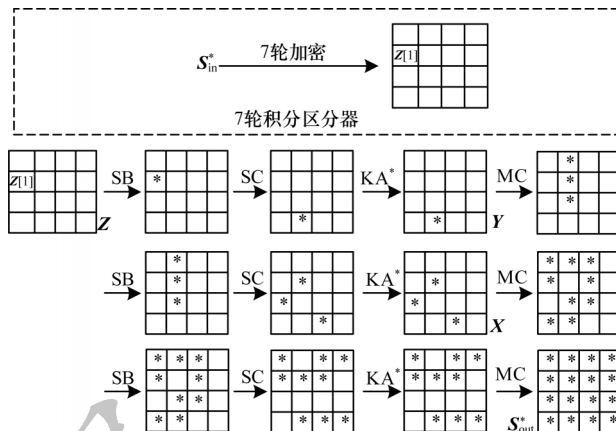


图5 Midori64算法的10轮密钥恢复攻击

Fig.5 10-round key recovery attack of Midori64

为降低密钥的猜测量,本文利用等价密钥技术^[19],该技术结合Midori64算法,将列混淆MC与密钥加KA进行位置交换,其中,线性等价的轮密钥加记为 KA^* ,从而在攻击中减少密钥的猜测量。具体地,将图5中 $S_{out}[1]$ 标注为 $Z[1]$,以*标注每个从 S_{out}^* 计算至 $Z[1]$ 时需要明确值的单元。设轮密钥经过线性变换后的等价轮密钥为 K^i ,即 $K^i = MC(RK^i)$ 。

利用部分和技术^[17],Midori64算法的128 bit 密钥恢复过程具体如下:

步骤1 选择一个明文集合 S_{in}^* ,收集相应的密文得到 S_{out}^* 。

步骤2 猜测第10轮等价轮密钥 $K_0^{10}, K_1^{10}, K_5^{10}, K_7^{10}, K_8^{10}, K_9^{10}, K_{11}^{10}, K_{12}^{10}, K_{15}^{10}$,共计36 bit。对 S_{out}^* 进行解密1轮及列混淆MC逆运算,得到 $X[2]$ 、 $X[5]$ 、 $X[11]$ 对应的值。定义计数器向量 $N_0, X[2] \parallel X[5] \parallel X[11]$ 用于存储 $X[2] \parallel X[5] \parallel X[11]$ 的个数,共有 2^{12} 个计数器。从异或和的角度考虑,仅需考查奇偶性,则计数器只使用1 bit来标识奇偶性即可。

步骤3 猜测第9轮等价轮密钥 K_2^9, K_5^9, K_{11}^9 ,共计12 bit。对 $X[2]$ 、 $X[5]$ 、 $X[11]$ 解密1轮得到 $Y[2]$ 。定义计数器向量 $N_1, Y[2]$ 用于存储 $Y[2]$ 的奇偶性,共有 2^4 个计数器。

步骤4 由 $K_7^8 = MC(MC(K_7^{10}) \oplus q_7 \oplus q_9)$ 可知 K_7^8 不需要猜测,可计算得到 $Z[1]$ 。计算 $\sum Z[1]$,若为0,则相应的猜测密钥作为真实密钥的候选值;否则,淘汰该猜测密钥。

步骤5 针对上述48 bit 密钥,选取 m 组 S_{in}^* ,重复步骤1~步骤4,可平均剩余 2^{128-4m} 个正确候选密钥。

步骤6 重复上述步骤,第9轮猜测12 bit 密钥,第10轮猜测20 bit 密钥,选择 n 组 \hat{S}_{in}^* ,重复步骤1~步骤4,可平均剩余 $2^{128-4m-4n}$ 个正确候选密钥。

步骤7 使用2组明密文对进行剩余正确密钥的穷搜猜测。

4.1.1 数据复杂度分析

为了平衡总时间复杂度与数据复杂度,取 $m=12$, $n=4$ 。10轮积分攻击的数据复杂度为 $2^{36} \times 12 + 2^{36} \times 4 = 2^{40}$ 个64 bit长明密文对。

4.1.2 时间复杂度分析

10轮积分攻击的步骤1复杂度为选择明文的复杂度,计算 S_m^* 时,需要查 SB^{-1} 表共 2^{36} 次,由于10轮算法共查表 16×10 次,因此,在忽略其他运算耗时的假设下,相当于 $2^{36} / (16 \times 10) \approx 2^{28.68}$ 次10轮加密。收集 S_{out}^* 时进行 2^{36} 次10轮加密。步骤2进行 $9 \times 2^{36} \times 2^{36}$ 次查表,相当于 $9 \times 2^{36} \times 2^{36} / (16 \times 10) \approx 2^{67.85}$ 次10轮加密。步骤3进行 $3 \times 2^{36} \times 2^{12} \times 2^{12}$ 次查表,相当于 $3 \times 2^{36} \times 2^{12} \times 2^{12} / (16 \times 10) \approx 2^{54.26}$ 次10轮加密。步骤4进行 $2^{36} \times 2^{12} \times 2^4$ 次查表,相当于 $2^{36} \times 2^{12} \times 2^4 / (16 \times 10) \approx 2^{44.68}$ 次10轮加密。步骤5与步骤6的时间复杂度可以忽略。步骤7进行穷搜验证时,需要 $2^{65} + 3$ 次10轮加密。

综上,10轮积分攻击的总时间复杂度为 $2^{28.68} + 2^{36} + 2^{67.85} + 2^{54.26} + 2^{44.68} + 2^{65} + 3 \approx 2^{67.85}$ 次10轮加密。

4.2 Midori64的11轮积分攻击

利用快速Walsh-Hadamard变换技术^[20-21]对Midori64进行11轮积分攻击,具体步骤如下:

步骤1 选择一个明文集合 S_m^* ,收集相应的密文得到 S_{out}^* 。

步骤2 猜测第10轮等价轮密钥 $K_0^{10}, K_1^{10}, K_5^{10}, K_7^{10}, K_8^{10}, K_9^{10}, K_{11}^{10}, K_{12}^{10}, K_{15}^{10}$ 和第9轮等价轮密钥 K_2^9, K_3^9, K_{11}^9 ,合记为 K_1 ,共计48 bit。根据Midori64密钥编排算法可推导出 $K_7^8 = MC(MC(K_7^{10}) \oplus q_7 \oplus q_9)$, $K_2^{11} = MC(MC(K_2^9) \oplus q_8 \oplus q_{10})$, $K_5^{11} = MC(MC(K_5^9) \oplus q_8 \oplus q_{10})$, $K_{11}^{11} = MC(MC(K_{11}^9) \oplus q_8 \oplus q_{10})$ 。

步骤3 $\sum Z[1]^{(i)} = \sum_{C_1} F_{K_1}^{(i)}(f_{C_1, K_2}(C_2 \oplus K_3))$, 其中, $i=1, 2, 3, 4$, $C_1 = S_{out}^*[2, 5, 11]$, 记 $\overline{C_1} = F_2^{12}$, C_2 为第11轮输出的其余密文,记 $\overline{C_2} = F_2^{52}, K_2 = K_2^{11} \parallel K_5^{11} \parallel K_{11}^{11}, K_3$ 为第11轮使用的其余等价轮密钥, f_{C_1, K_2} 为关于 $\overline{C_2}$ 的第11轮解密函数, $F_{K_1}^{(i)}$ 为获得 $Z[1]^{(i)}$ 的解密函数。遍历 C_1 ,利用快速Walsh-Hadamard变换技术计算 $\sum F_{K_1}^{(i)}(f_{C_1, K_2}(\overline{C_2}))$,然后在 F_2 上关于 C_1 求累加和,若和不为0,则淘汰密钥。

步骤4 选取 m 组 S_m^* ,重复步骤1~步骤3。

步骤5 使用猜测等价轮密钥加密 S_m^* 中的明文,若其与 S_{out}^* 中对应处密文相同,则相应的猜测等价轮密钥作为真实等价轮密钥的候选值;否则,淘汰该猜测等价轮密钥。

步骤6 由上述恢复的等价轮密钥计算密钥。

4.2.1 数据复杂度分析

为了平衡总时间复杂度与数据复杂度,取 $m=17$,11轮积分攻击的数据复杂度为 $2^{36} \times 17 \approx 2^{40.09}$ 个64 bit长明密文对。

4.2.2 时间复杂度分析

11轮积分攻击的步骤1复杂度为选择明文的复杂度,平均重复17次,时间复杂度为 $17 \times (2^{28.54} + 2^{36}) \approx 2^{40.09}$ 次11轮加密。步骤3进行简单运算,相当于 $4 \times 2^{48} \times (2^{12} \times (17 \times 2 \times 52 \times 2^{52} + 52 \times 2^{52}) + 2^{12}) \approx 2^{117.37}$ 次11轮加密。步骤5进行穷搜验证时,需要 $(2^{32} + 1) \times 2^{28} \approx 2^{60}$ 次11轮加密。

综上,11轮积分攻击的时间复杂度为 $2^{40.09} + 2^{117.37} + 2^{60} \approx 2^{117.37}$ 次11轮加密。

4.3 Midori64的积分攻击对比

将本文积分攻击与已有Midori64算法的积分攻击进行性能对比,结果如表3所示,从表3可以看出,本文积分攻击的轮数相比文献[7]积分攻击提高2轮。与文献[15]相比,本文找到的路线输入集合大小为 2^{36} ,而文献[15]中算法分析需要的数据量为 2^{63} ,为整个明文空间的一半。与已有Midori64算法其他攻击相比,在不考虑弱密钥情况下,本文积分攻击的数据复杂度和时间复杂度具有较大优势。

表3 Midori64算法的密钥恢复攻击对比

Table 3 Comparison of key recovery attacks of Midori64

攻击方法	数据复杂度	时间复杂度	攻击轮数
零相关攻击 ^[6]	$2^{62.4}$	$2^{79.35}$	10
积分攻击 ^[7]	$2^{20.90}$	$2^{77.73}$	9
中间相遇攻击 ^[3]	$2^{61.5}$	$2^{99.5}$	10
中间相遇攻击 ^[3]	2^{53}	2^{122}	11
中间相遇攻击 ^[3]	$2^{55.5}$	$2^{125.5}$	12
不可能差分攻击 ^[22]	$2^{62.4}$	$2^{80.81}$	10
不可能差分攻击 ^[4]	$2^{62.3}$	$2^{121.6}$	11
不可能差分攻击 ^[5]	$2^{60.82}$	$2^{121.42}$	11
本文10轮积分攻击	2^{40}	$2^{67.85}$	10
本文11轮积分攻击	$2^{40.09}$	$2^{117.37}$	11

5 结束语

本文构建6轮零相关区分器,利用零相关区分器与平衡积分区分器之间的等价关系,将6轮零相关区分器转换为6轮平衡积分区分器,然后将3个6轮平衡积分区分器合成为一个性能优良的6轮零和积分区分器,向前扩展1轮得到一个7轮零和积分区分器。将该7轮零和积分区分器向后扩展3轮,对10轮Midori64算法实施密钥恢复攻击,攻击的数据复杂度约为 2^{40} 个明密文对,时间复杂度约为 $2^{67.85}$ 次10轮加密运算。将该7轮零和积分区分器向后扩展

4轮,对11轮Midori64算法实施密钥恢复攻击,攻击的数据复杂度约为 $2^{40.09}$ 个明密文对,时间复杂度约为 $2^{117.37}$ 次11轮加密运算。10轮积分攻击中采用部分和技术,11轮积分攻击中采用快速Walsh-Hadamard变换技术。下一步将利用基于MILP技术的分离特性搜索方法攻击Midori64算法。

参考文献

- [1] BANIK S, BOGDANOV A, ISOBE T, et al. Midori: a block cipher for low energy [M]. Berlin, Germany: Springer, 2014.
- [2] REN Yaoyao, ZHANG Wenying. Related-key differential analysis of Midori64 [J]. Application Research of Computers, 2018, 35(6): 1800-1802. (in Chinese)
任瑶瑶, 张文英. Midori64 的相关密钥不可能差分分析[J]. 计算机应用研究, 2018, 35(6): 1800-1802.
- [3] LIN Li, WU Wenling. Meet-in-the-middle attacks on reduced-round Midori64 [EB/OL]. [2020-02-05]. <https://eprint.iacr.org/2015/1165.pdf>.
- [4] YU Zheng, MAO Ming, LI Yanjun. Impossible differential analysis of 11-round Midori64 based on method of step-key-guessing [J]. Application Research of Computers, 2018, 35(9): 2777-2780. (in Chinese)
于政, 毛明, 李艳俊. 基于轮密钥分步猜测方法的Midori64算法11轮不可能差分分析[J]. 计算机应用研究, 2018, 35(9): 2777-2780.
- [5] LI Mingming, GUO Jiansheng, CUI Jingyi, et al. Truncated impossible differential cryptanalysis of Midori-64 [J]. Journal of Software, 2019, 30(8): 2337-2348. (in Chinese)
李明明, 郭建胜, 崔竞一, 等. Midori-64算法的截断不可能差分分析[J]. 软件学报, 2019, 30(8): 2337-2348.
- [6] CHENG Lu, WEI Yuechuan, LI Anhui, et al. Multi-dimensional zero-correlation linear cryptanalysis on Midori [J]. Journal of Shandong University (Natural Science), 2018, 53(2): 88-94. (in Chinese)
程璐, 魏悦川, 李安辉, 等. Midori算法的多维零相关性分析[J]. 山东大学学报(自然科学版), 2018, 53(2): 88-94.
- [7] LIAN Chuang. Integral cryptanalysis of lightweight block ciphers [D]. Xi'an: Xidian University, 2018. (in Chinese)
连闯. 轻量级分组密码的积分分析[D]. 西安: 西安电子科技大学, 2018.
- [8] GUO J, JEAN J, NIKOLIC I, et al. Invariant subspace attack against Midori64 and the resistance criteria for S-box designs [J]. IACR Transactions on Symmetric Cryptology, 2016, 1: 33-56.
- [9] TODO Y, LEANDER G, SASAKI Y. Nonlinear invariant attack: practical attack on full SCREAM, iSCREAM, and Midori64 [J]. Journal of Cryptology, 2019, 32(4): 1383-1422.
- [10] BOGDANOV A, LEANDER G, NYBERG K, et al. Integral and multidimensional linear distinguishers with correlation zero [C]//Proceedings of ASIACRYPT' 12. Berlin, Germany: Springer, 2012: 244-261.
- [11] WEN L, WANG M. Integral zero-correlation distinguisher for ARX block cipher, with application to SHACAL-2 [C]//Proceedings of Australasian Conference on Information Security and Privacy. Berlin, Germany: Springer, 2014: 454-461.
- [12] CHEN Huaifeng. Study on several cryptanalysis models on block ciphers [D]. Jinan: Shandong University, 2017. (in Chinese)
陈怀凤. 分组密码算法几种分析模型的研究[D]. 济南: 山东大学, 2017.
- [13] BING S, LIU Z, RIJMEN V, et al. Links among impossible differential, integral and zero correlation linear cryptanalysis [C]//Proceedings of CRYPTO' 15. Berlin, Germany: Springer, 2015: 95-115.
- [14] TODO Y, MORII M. Bit-based division property and application to simon family [C]//Proceedings of International Conference on Fast Software Encryption. Berlin, Germany: Springer, 2016: 125-136.
- [15] ZHANG W, RIJMEN V. Division cryptanalysis of block ciphers with a binary diffusion layer [J]. IET Information Security, 2018, 13(2): 87-95.
- [16] BOGDANOV A, RIJMEN V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers [J]. Designs Codes & Cryptography, 2014, 70(3): 369-383.
- [17] WANG Meiqin, WEN Long. Research on zero-correlation linear cryptanalysis [J]. Journal of Cryptologic Research, 2014, 1(3): 296-310. (in Chinese)
王美琴, 温隆. 零相关性线性分析研究[J]. 密码学报, 2014, 1(3): 296-310.
- [18] SUN Ling, CHEN Huaifeng, WANG Meiqin. Zero-correlation attacks: statistical models independent of the number of approximations [J]. Designs, Codes and Cryptography, 2018, 86(9): 1923-1945.
- [19] ISOBE T, SHIBUTANI K. Generic key recovery attack on feistel scheme [C]//Proceedings of International Cryptology Conference. Washington D. C., USA: IEEE Press, 2013: 464-485.
- [20] COLLARD B, STANDAERT F, QUISQUATER J. Improving the time complexity of Matsui's linear cryptanalysis [C]//Proceedings of ICISC' 07. Berlin, Germany: Springer, 2007: 77-88.
- [21] TODO Y, AOKI K. FFT key recovery for integral attack [C]//Proceedings of International Conference on Cryptology and Network Security. Berlin, Germany: Springer, 2014: 64-81.
- [22] CHEN Zhan, WANG Xiaoyun. Impossible differential cryptanalysis of Midori [C]//Proceedings of International Conference on Mechatronics and Automation Engineering. Washington D. C., USA: IEEE Press, 2016: 535-543.

编辑 吴云芳