对 MIBS 算法的碰撞攻击

段丹青 卫宏儒
(北京科技大学数理学院 北京 100083)

摘 要 MIBS 算法是 Izadi 等于 2009 年提出的一种轻量级分组密码算法。为进一步评估 MIBS 算法的安全性,针对 MIBS 算法抵抗碰撞攻击的能力进行了研究。根据算法的等价结构,构造了 MIBS 算法的一个 6 轮区分器,通过依次在此区分器后面增加 2 轮、在前面增加 2 轮的方法,对 8/9/10 轮的 MIBS 算法进行了碰撞攻击,并给出了相应的攻击过程及复杂度分析。结果表明,8/9/10 轮的 MIBS 算法是不能抵抗碰撞攻击的。

关键词 MIBS 算法,碰撞攻击,密码分析,区分器,复杂度
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.02.038

Collision Attack on MIBS Algorithm

DUAN Dan-qing WEI Hong-ru
(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)

Abstract MIBS algorithm is a lightweight block cipher, which was proposed in 2009. In order to further evaluate its security, the ability of MIBS algorithm against the collision attack was studied. Based on the equivalent structure of MIBS, 6-round distinguisher was constructed. By adding two rounds behind the distinguisher and two rounds in front of it in turn, the collision attack was applied to 8/9/10-round MIBS, and the attacking process and complexity analysis were given. The attacking results show that 8/9/10-round MIBS is not immune to collision attack.

Keywords MIBS algorithm, Collision attack, Cryptanalysis, Distinguisher, Complexity

1 引言

MIBS 算法是 Izadi 等[1]于 2009 年提出的一种轻量级的分组密码算法。自提出以来,其因便于软硬件的实现,适用于电子标签和传感器网络等计算资源严格受限的环境,而受到人们的广泛关注。目前,对 MIBS 算法的分析方法主要有不可能差分分析[2]、中间相遇攻击、深度差分故障分析、Integral 攻击、积分分析等。2010 年,赵新杰等提出了 3 种针对 MIBS 差分故障的分析方法,对 MIBS 算法进行了深度差分故障分析研究[3];王高丽等[4]于 2012 年通过一个 MIBS 算法 Intergral 攻击的一个 4.5 轮区分器,对 MIBS 算法进行了 8 轮和 9 轮的 Integral 攻击;刘超等[5]于 2013 年对 MIBS 算法抵抗中间相遇攻击的能力进行了研究,通过一个中间相遇攻击的区分器,对 8/9/10 轮的 MIBS 算法进行了中间相遇攻击;吴文玲等[6]给出了一个 5 轮的积分区分器,并利用该区分器对 8/9/10 轮的 MIBS 算法进行了积分攻击;潘志舒等[7]于 2014 年针对 MIBS 算法构造出一个 5 轮积分区分器,对 10 轮MIBS-64 和 MIBS-80 进行了积分攻击。

碰撞攻击由 Gilbert 等人首次提出[8],该攻击方法利用生日悖论的原理,通过对算法本身或其等价结构的分析,对加密流程的中间环节进行适当的变形和组合,利用密钥编排算法中轮子密钥之间的关系,得到一个仅与密钥相关的区分性质,通过对该区分性质的碰撞特性进行分析来恢复相关密钥。基于该攻击方法,已经成功分析了 Camellia[9] 和 CLEFIA[10] 等分组密码算法,并取得了较为满意的分析结果。

本文基于 MIBS 算法的一个等价结构,构造了 MIBS 算法的一个 6 轮区分器,基于该区分器对 8/9/10 轮的 MIBS 算法进行了碰撞攻击。碰撞攻击的结果表明,8/9/10 轮的 MIBS 算法对碰撞攻击是不免疫的。

2 MIBS 算法

2.1 MIBS 算法简介

MIBS 算法是一种 Feistel 结构的轻量级分组密码算法。密钥有 64 比特和 80 比特两种规模,加密轮数均为 32 轮,MIBS算法的分组长度为 64 比特;MIBS 以 4 比特为一个单位,也即 MIBS 算法以半字节或半单元为一个单位。本文只研究密钥长度为 64 比特的 MIBS 算法。图 1 给出了 MIBS 算法的加密结构。

到稿日期:2016-12-04 返修日期:2017-03-12 本文受 2016 年国家自然科学基金项目:认证加密算法的设计和分析,2017 年国家自然科学基金项目:面向网络空间的大数据安全与隐私保护研究(U1603116)资助。

段丹青(1993—),女,硕士,主要研究方向为密码学与信息安全,E-mail:1136194825@qq.com;**卫宏儒**(1963—),男,副教授,硕士生导师,主要研究方向为数学、信息安全与密码学、物联网关键技术,E-mail:weihr@ustb.edu.cn(通信作者)。

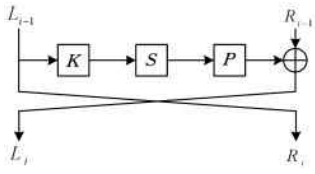


图 1　MIBS 算法的加密结构

Fig. 1　Encryption structure of MIBS algorithm

MIBS 的轮函数 F 是 SP 结构，包括轮子密钥加变换 K，非线性 S 盒变换和线性变换 P 3 个部分。轮函数 F 的结构如图 2 所示。

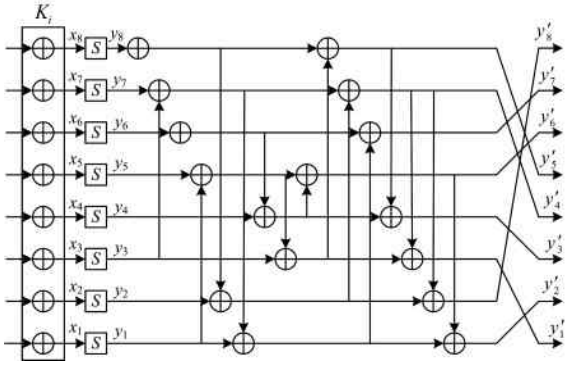


图 2　MIBS 算法的轮函数

Fig. 2　Round function of MIBS

设初始明文输入为 $P_0=(L_0,R_0)$，经过 32 轮加密，输出 64 比特密文 $C_{32}=(L_{32},R_{32})$。记 $K_i(1\leqslant i\leqslant 32)$ 是 32 比特轮密钥，由密钥生成算法获得，且 $K_i=(K_{i,8},K_{i,7},\cdots,K_{i,2},K_{i,1})$，每个 $K_{i,j}$ 是一个 4 比特半字节，则加密轮函数可定义为：

$$\begin{cases}L_i=F(L_{i-1},K_i)\oplus R_{i-1}\\R_i=L_{i-1}\end{cases},1\leqslant i\leqslant 32$$

轮函数由以下 3 个操作构成：

1）轮密钥加变换 K：把每轮密钥与左 32 比特异或相加，即 $X=L_{i-1}\oplus K_i=x_8\parallel x_7\parallel x_6\parallel x_5\parallel x_4\parallel x_3\parallel x_2\parallel x_1$。

2）非线性 S 盒变换：将数据每一半字节进行非线性变换（S 盒）。其中 $S=\{4\ 15\ 3\ 8\ 13\ 10\ 12\ 0\ 11\ 5\ 7\ 14\ 2\ 6\ 1\ 9\}$，$S:F_2^4\rightarrow F_2^4$，$y_i=S(x_i)(1\leqslant i\leqslant 8)$。

3）线性变换 P：

$P:(F_2^4)^8\rightarrow(F_2^4)^8$

$(y_1,y_2,y_3,y_4,y_5,y_6,y_7,y_8)\rightarrow(y_1',y_2',y_3',y_4',y_5',y_6',y_7',y_8')$

线性变换可表示为如下形式：

$$\begin{pmatrix}y_8\\y_7\\\vdots\\y_1\end{pmatrix}\rightarrow\begin{pmatrix}y_8'\\y_7'\\\vdots\\y_1'\end{pmatrix}=P\begin{pmatrix}y_8\\y_7\\\vdots\\y_1\end{pmatrix}$$

其中，$P=\begin{pmatrix}1&1&1&0&1&1&0&1\\0&1&1&0&0&1&1&1\\0&0&1&1&1&0&1&1\\1&0&0&1&1&1&0&1\\1&1&0&0&1&1&1&0\\1&0&1&1&0&1&1&1\\0&1&1&1&1&1&1&0\\1&1&0&1&1&0&1&1\end{pmatrix}$。$P$ 是可逆的，它的逆变换为 P^{-1}，$P^{-1}(y_i')=x_i(1\leqslant i\leqslant 8)$。

2.2　MIBS-64 的密钥扩展算法

设 MIBS-64 的 64 比特主密钥为 $\widetilde{K}=(\widetilde{K}_{63},\widetilde{K}_{62},\cdots,\widetilde{K}_0)$，相应的 MIBS-64 的密钥编排算法如下（$state^i\leftarrow\widetilde{K}$，$i=1,2,\cdots,32$）：

（1）$state^i=state^i\ggg 15$

（2）$state^i=S(state^i_{[63:60]})\parallel state^i_{[59:0]}$

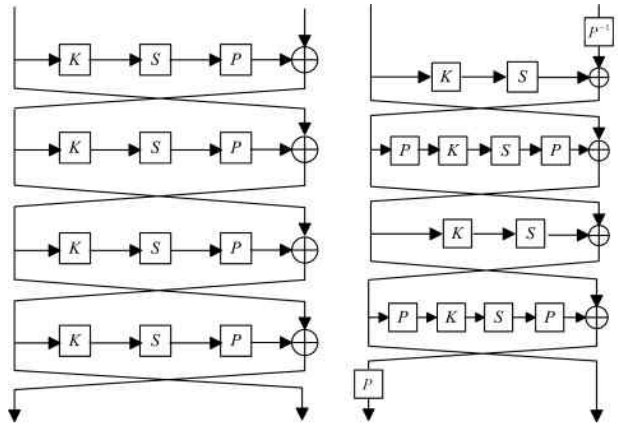
（3）$state^i=(state^i_{[63:16]})\parallel(state^i_{[15:11]})\oplus Round-Counter\parallel state^i_{[10:0]}$

（4）$K_i=state^i_{[63:32]}$

其中，$\ggg 15$ 表示循环右移 15 位，S 即为上述加密算法所示的非线性变换，$Round-Counter$ 即为轮数，方括号中的数字指的是半字节中的比特位。

2.3　MIBS 算法的等价结构

由于在利用 Feistel 结构进行加密时总有一半的数据保持不变，通过对其结构的变形，可以达到既不影响算法的加解密结果又改变中间的加密过程的目的，从而利用不同的结构对算法实施攻击得到不同的效果。文献[11]给出了一类分组密码算法的等价结构构造方法。这类分组密码算法是 Feistel 结构，轮函数的结构是 SP 结构。通过研究文献[11]的方法对 MIBS 算法的结构进行相应变形，可以得到 MIBS 算法的四轮等价结构。MIBS 算法的四轮加密结构及其四轮等价结构如图 3 所示。其中，轮密钥加变换记作 K，非线性 S 盒变换记作 S，线性变换记作 P。



（a）MIBS 算法的四轮加密结构　　（b）MIBS 算法的四轮等价结构

图 3　MIBS 算法的四轮加密结构及其等价结构

Fig. 3　4-round encryption structure and its equivalent structure of MIBS

3　MIBS 算法的六轮区分器

本节将利用上述等价结构，构造 MIBS 算法的 6 轮区分器，即给出 MIBS 算法的 6 轮区分性质。鉴于后文提及的符号较多，在此处提前解释，在不考虑下标的前提下，$a,b,c,d,f,\omega,\varepsilon,\delta$ 是经过相应轮数加密变换之后推导式中所涉及的常数的不同表示，且它们仅与相应轮数的子密钥及上一步中所涉及的常数有关，具体含义在以下构造过程中分别给出；e,g,t 表示以 x 为变量的函数；初始输入中的 c 为任意常数。

构造过程如下。

选择初始输入：

$L_0=(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8)$

$R_0=(c_9,c_{10},c_{11},c_{12},c_{13},c_{14},c_{15},x)$

其中，变量 $x\in F_2^4$ 为活动字节的任意取值，$c_i(1\leqslant i\leqslant 14)$ 均是常数，且不要求取相同的值。

在第 1 轮加密中，初始输入经过第 1 轮轮函数($K\rightarrow S$)的输出全为常数。因此，第 1 轮的加密输出为：

$L_1=(x\oplus a_1,x\oplus a_2,a_3,a_4,x\oplus a_5,x\oplus a_6,x\oplus a_7,a_8)$

$R_1=L_0=(c_1,c_2,\cdots,c_8)$

其中，$a_i(1\leqslant i\leqslant 8)$ 仅与 $c_j(1\leqslant j\leqslant 15)$ 及子密钥 K_1 有关，因此取定密钥时，a_i 均为常数。

在第 2 轮加密中，经过第 2 轮轮函数($P\rightarrow K\rightarrow S\rightarrow P$)变换，令 $y=S(x\oplus b_8\oplus K_{2,8})$，并记为 $y=S(x\oplus a_0)$，则第 2 轮加密的输出为：

$L_2=(y\oplus b_1,b_2,y\oplus b_3,y\oplus b_4,y\oplus b_5,b_6,b_7,y\oplus b_8)$

$R_2=L_1$

其中，$K_{2,8}$ 是指 K_2 的第 8 个半字节，b_i 是由常数 $a_i(1\leqslant i\leqslant 8)$ 及子密钥 K_2 决定的常数。

在第 3 轮加密中，令：

$$\begin{cases}e_1=S(y\oplus f_1)\\ e_3=S(y\oplus f_3)\\ e_4=S(y\oplus f_4)\\ e_5=S(y\oplus f_5)\\ e_8=S(y\oplus f_8)\end{cases},\begin{cases}d_2=S(b_2\oplus k_{3,2})\oplus a_2\\ d_6=S(b_6\oplus k_{3,6})\oplus a_6\\ d_7=S(b_7\oplus k_{3,7})\oplus a_7\end{cases}$$

则第 3 轮加密的输出为：

$L_3=(e_1\oplus x\oplus a_1,x\oplus d_2,e_3\oplus x\oplus a_3,e_4\oplus x\oplus a_4,e_5\oplus x\oplus a_5,x\oplus d_6,x\oplus d_7,e_8\oplus x\oplus a_8)$

$R_3=L_2$

其中，$e_i(i=1,3,4,5,8)$ 由轮密钥 $K_{3,i}$ 和 b_i 决定，$d_i(i=2,6,7)$ 是由 $b_i,K_{3,i},a_i$ 决定的常数。

在第 4 轮加密中，令：

$g_1=S(e_1\oplus e_4\oplus e_5\oplus e_8\oplus\omega_1)$

$g_2=S(e_3\oplus e_4\oplus e_5\oplus\omega_2)$

$g_3=S(e_1\oplus e_3\oplus e_5\oplus e_8\oplus\omega_3)$

$g_4=S(e_3\oplus e_4\oplus e_8\oplus\omega_4)$

$g_5=S(e_1\oplus e_3\oplus e_4\oplus e_5\oplus e_8\oplus\omega_5)$

$g_6=S(e_1\oplus e_4\oplus e_5\oplus\omega_6)$

$g_7=S(e_1\oplus e_3\oplus\omega_7)$

$g_8=S(e_1\oplus e_3\oplus e_4\oplus e_8\oplus x\oplus\omega_8)$

并记：

$t_1=g_1\oplus g_2\oplus g_4\oplus g_5\oplus g_7\oplus g_8$

$t_2=g_2\oplus g_3\oplus g_4\oplus g_5\oplus g_6\oplus g_7$

$t_3=g_1\oplus g_2\oplus g_3\oplus g_5\oplus g_6\oplus g_8$

$t_4=g_2\oplus g_3\oplus g_4\oplus g_7\oplus g_8$

$t_5=g_1\oplus g_3\oplus g_4\oplus g_5\oplus g_8$

$t_6=g_1\oplus g_2\oplus g_4\oplus g_5\oplus g_6$

$t_7=g_1\oplus g_2\oplus g_3\oplus g_6\oplus g_7$

$t_8=g_1\oplus g_3\oplus g_4\oplus g_6\oplus g_7\oplus g_8$

则第 4 轮的加密输出为：

$L_4=(t_1\oplus y\oplus\varepsilon_1,t_2\oplus\varepsilon_2,t_3\oplus y\oplus\varepsilon_3,t_4\oplus y\oplus\varepsilon_4,t_5\oplus y\oplus\varepsilon_5,t_6\oplus\varepsilon_6,t_7\oplus\varepsilon_7,t_8\oplus y\oplus\varepsilon_8)$

$R_4=L_3$

其中，$\omega_i(1\leqslant i\leqslant 8)$ 是由 d_i 和 a_i 决定的常数，$\varepsilon_i(1\leqslant i\leqslant 8)$ 是由轮密钥 K_4 和 ω_i 决定的常数。

第 5 轮加密的输出为：

$L_5=(S(t_1\oplus y\oplus\delta_1)\oplus e_1\oplus x\oplus a_1,S(t_2\oplus\delta_2)\oplus x\oplus d_2,S(t_3\oplus y\oplus\delta_3)\oplus e_1\oplus a_3,S(t_4\oplus y\oplus\delta_4)\oplus e_4\oplus a_4,S(t_5\oplus y\oplus\delta_5)\oplus e_5\oplus x\oplus a_5,S(t_6\oplus\delta_6)\oplus x\oplus d_6,S(t_7\oplus\delta_7)\oplus x\oplus d_7,S(t_8\oplus y\oplus\delta_8)\oplus e_8\oplus a_8)$

$R_5=L_4$

其中，$\delta_i(1\leqslant i\leqslant 8)$ 是由轮密钥 K_5 和 b_i 决定的常数。

从而可以得到第 6 轮的加密输出的右半部分为：

$R_6=L_5=(\Delta,\Delta,\Delta,\Delta,\Delta,\Delta,S(t_7\oplus\delta_7)\oplus x\oplus d_7,\Delta)$

性质 1 设明文输入形如 $(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10},c_{11},c_{12},c_{13},c_{14},c_{15},x)$，其中 c_i 表示任意常值半字节，取值不要求相同。对变量 $x\in F_2^4$ 取相同的值进行遍历。如果保持其他半字节的取值不变，只变换 x 的取值，则将此明文经过 6 轮区分器加密所得到的 $R_{6,7}$ 是一个以 x 为变量的函数，它由 x 和 13 个常值半字节 $a_0,f_1,f_3,f_4,f_5,f_8,\omega_1,\omega_2,\omega_3,\omega_6,\omega_7,d_7,\delta_7$ 完全决定。

证明：由区分器的构造过程可知，$R_{6,7}=S(t_7\oplus\delta_7)\oplus x\oplus d_7$，而 $t_7=g_1\oplus g_2\oplus g_3\oplus g_6\oplus g_7$，$d_7=S(b_7\oplus k_{3,7})\oplus a_7$，又因为

$$\begin{cases}g_1=S(e_1\oplus e_4\oplus e_5\oplus e_8\oplus\omega_1)\\ g_2=S(e_3\oplus e_4\oplus e_5\oplus\omega_2)\\ g_3=S(e_1\oplus e_3\oplus e_5\oplus e_8\oplus\omega_3)\\ g_6=S(e_1\oplus e_4\oplus e_5\oplus\omega_6)\\ g_7=S(e_1\oplus e_3\oplus\omega_7)\end{cases},\text{且}\begin{cases}e_1=S(y\oplus f_1)\\ e_3=S(y\oplus f_3)\\ e_4=S(y\oplus f_4)\\ e_5=S(y\oplus f_5)\\ e_8=S(y\oplus f_8)\end{cases},$$

$y=S(x\oplus b_8\oplus K_{2,8})=S(x\oplus a_0)$，故 $R_{6,7}$ 可由 x 和 $a_0,f_1,f_3,f_4,f_5,f_8,\omega_1,\omega_2,\omega_3,\omega_6,\omega_7,d_7,\delta_7$ 这 13 个常值半字节完全决定，即 $R_{6,7}$ 是一个以 x 为变量的函数，它由 x 和上述 13 个常值半字节完全决定。证毕。

4 对 8/9/10 轮 MIBS 算法的碰撞攻击

利用上一节构造的 6 轮区分器尝试对 8/9/10 轮的 MIBS 算法进行碰撞攻击。经过对攻击途径的反复尝试，最终确定具体的攻击过程是依次在六轮区分器后面增加 2 轮，在前面增加 2 轮。

4.1 对 8 轮 MIBS 算法的碰撞攻击

对 8 轮 MIBS 算法的碰撞攻击是在 6 轮区分器的后面增加 2 轮。攻击过程如图 4 所示。

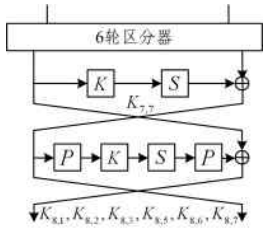


图 4 对 MIBS 算法的 8 轮攻击

Fig. 4 8-round attack of MIBS

Step1 选取 112 个明文 $P^i=(L_0^i,R_0^i)$，使 $P^i=(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8,c_9,c_{10},c_{11},c_{12},c_{13},c_{14},c_{15},x)$，$c_j\in F_2^4(1\leqslant j\leqslant 15)$ 均是任意选择的常数，且不要求取值相同；x 取自 F_2^4 且取相同的值进行遍历，将这组明文加密 8 轮，记相应的密文

为 $C^i=(L_8^i,R_8^i)(1\leqslant i\leqslant 112)$。

Step2　猜测密钥 $K_{7,7},K_{8,1},K_{8,2},K_{8,3},K_{8,5},K_{8,6},K_{8,7}$，对每个候选值进行解密，得到 $R_{8,7}$ 的 112 个值 $R_{8,7}^i(1\leqslant i\leqslant 112)$，检测这些值是否有碰撞，如果有，则将该密钥丢弃；否则则将其输出。

Step3　针对 Step2 输出的 $K_{7,7},K_{8,1},K_{8,2},K_{8,3},K_{8,5},K_{8,6},K_{8,7}$ 的每一个值，根据 Step1 的要求，重新选取若干明文，重复 Step2。

通过对 8 轮 MIBS 算法碰撞攻击过程的分析，及基于现有的碰撞攻击的概率统计模型，可以得到以下结论：部分解密 112 个密文得到相应的 $R_{8,7}^i(1\leqslant i\leqslant 112)$，这个过程产生碰撞的概率大于 $1-\mathrm{e}^{-112\times 111/2^9}$（该值大于或等于 $1-2^{-35}$），所以 Step2 的输出中子密钥通过的概率小于 2^{-35}。因此，正确密钥可以顺利通过碰撞检测，而 $2^{34}-1$ 个错误密钥可以顺利通过的数量不会超过 $(2^{34}-1)\times 2^{-35}\approx 0.5$ 个，故最终仅有约 1.5个候选密钥可以通过碰撞检测，从而第 3 步只需很少的明文。因此，对 8 轮 MIBS 算法的碰撞攻击所需要的选择明文不超过 2^7 个，对 8 轮 MIBS 算法的碰撞攻击的数据复杂度不超过 $2^7\times 2^4=2^{11}$，每进行一次部分解密涉及到 7 个 S 盒，因此攻击的时间复杂度约为 $\frac{112\times 2^4\times 2^{24}\times 7}{8\times 8}\approx 2^{31.62}$。

4.2　对 9 轮 MIBS 算法的碰撞攻击

对 9 轮 MIBS 算法的碰撞攻击是在 8 轮 MIBS 算法碰撞攻击的前面再增加一轮，此时所需猜测的密钥有 $K_{1,8},K_{8,7},K_{9,1},K_{9,2},K_{9,3},K_{9,5},K_{9,6},K_{9,7}$ 这 8 个半字节，具体攻击过程如下。

Step1　对 $K_{1,8}$ 的每个候选值 ω 选取 120 个如下形式的明文：

$$P^i=(c_1,c_2,c_3,c_4,c_5,c_6,c_7,x,S(x\oplus K_{1,8})\oplus\varepsilon_1,\varepsilon_2,S(x\oplus K_{1,8})\oplus\varepsilon_3,S(x\oplus K_{1,8})\oplus\varepsilon_4,S(x\oplus K_{1,8})\oplus\varepsilon_5,\varepsilon_6,\varepsilon_7,S(x\oplus K_{1,8})\oplus\varepsilon_8)$$

其中，$c_j,\varepsilon_k(1\leqslant j\leqslant 7,1\leqslant k\leqslant 8)$ 为常数，取值不要求相同，如果密钥 $K_{1,8}$ 可以猜测正确，则经过第一轮加密之后，其输出肯定为所构造的区分器所需要的初始输入形式。同样地，将这组明文加密 9 轮，输出的密文记为 $C^i=(L_9^i,R_9^i),1\leqslant i\leqslant 120$。

Step2　猜测 $K_{8,7},K_{9,1},K_{9,2},K_{9,3},K_{9,5},K_{9,6},K_{9,7}$，对每个候选值 $(\omega,K_{8,7},K_{9,1},K_{9,2},K_{9,3},K_{9,5},K_{9,6},K_{9,7})$ 进行解密得到 $R_{9,7}$ 对应的 120 个值 $R_{9,7}^i(1\leqslant i\leqslant 120)$，将其中有碰撞的候选值丢弃，将没有碰撞的候选值输出。

Step3　对于 Step2 输出的每一个 $(\omega,K_{8,7},K_{9,1},K_{9,2},K_{9,3},K_{9,5},K_{9,6},K_{9,7})$，如果输出的值不唯一，则利用 Step1 的方法再选取若干明文，继续 Step2。

复杂度分析：部分解密 2^7 个密文，得到相应的 $R_{9,7}^i(1\leqslant i\leqslant 120)$，这个过程产生碰撞的概率大于 $1-\mathrm{e}^{-128\times 127/2^9}$（该值大于或等于 $1-2^{-40}$），所以在 Step2 的输出中，子密钥通过的概率小于 2^{-40}。因此，正确密钥可以顺利通过碰撞检测，而 $2^{39}-1$ 个错误密钥可以顺利通过的数量不会超过 $(2^{39}-1)\times 2^{-40}\approx 0.5$ 个，所以最终通过检测的候选密钥的个数约为 1.5，从而第 3 步只需很少的明文。因此，对 9 轮 MIBS 算法的碰撞攻击所需要的选择明文不超过 2^7 个，对 9 轮 MIBS 算法的碰撞攻击的数据复杂度为 $2^{11.23}$，攻击的时间复杂度约为 $\frac{120\times 2^4\times 2^{28}\times 8}{8\times 8}\approx 2^{35.91}$。

4.3　对 10 轮 MIBS 算法的碰撞攻击

类似于 9 轮碰撞攻击，在算法的前面再增加一轮，即可对 10 轮 MIBS 算法进行碰撞攻击，此时需要猜测 13 个半字节 $K_{1,1},K_{1,3},K_{1,4},K_{1,5},K_{1,8},K_{2,8},K_{8,7},K_{9,1},K_{9,2},K_{9,3},K_{9,5},K_{9,6},K_{9,7}$。攻击过程与 9 轮碰撞攻击相似，不同之处在于此处选择的明文应为如下形式：

$$L_0=(S(x\oplus K_{1,8})\oplus\varepsilon_1,\varepsilon_2,S(x\oplus K_{1,8})\oplus\varepsilon_3,S(x\oplus K_{1,8})\oplus\varepsilon_4,S(x\oplus K_{1,8})\oplus\varepsilon_5,\varepsilon_6,\varepsilon_7 S(x\oplus K_{1,8})\oplus\varepsilon_8)$$

$$R_0=(\mu_1\oplus\mu_4\oplus\mu_5\oplus\mu_8\oplus\tau_1,\mu_3\oplus\mu_4\oplus\mu_5\oplus\tau_2,\mu_1\oplus\mu_3\oplus\mu_5\oplus\mu_8\oplus\tau_3,\mu_3\oplus\mu_4\oplus\mu_8\oplus\tau_4,\mu_1\oplus\mu_3\oplus\mu_4\oplus\mu_5\oplus\mu_8\oplus\tau_5,\mu_1\oplus\mu_4\oplus\mu_5\oplus\tau_6,\mu_1\oplus\mu_3\oplus\tau_7,\mu_1\oplus\mu_3\oplus\mu_4\oplus\mu_8\oplus\tau_8))\oplus(c_1,c_2,\cdots,c_7,x)$$

$\mu_i=(S(S(x\oplus K_{2,8})\oplus\varepsilon_i\oplus K_{1,i}),i=1,3,4,5,8;\varepsilon_i,\tau_i(1\leqslant i\leqslant 8)$ 是随机选择的常数。

如果上述所需猜测的半字节中，前两轮的密钥猜测正确，则所选明文经过前两轮加密后的输出必为区分器的初始输入所需形式。

复杂度分析：对 9 轮 MIBS 算法进行碰撞攻击，上述过程产生碰撞的概率大于 $1-\mathrm{e}^{-128\times 127/2^9}$（该值大于或等于 $1-2^{-46}$），所以 Step2 的输出中子密钥通过的概率小于 2^{-46}。因此，正确密钥可以顺利通过碰撞检测，而 $2^{45}-1$ 个错误密钥可以顺利通过的数量不会超过 $(2^{44}-1)\times 2^{-45}\approx 0.5$ 个，最终通过检测的候选密钥的个数约为 1.5，从而第 3 步只需很少的明文。因此，对 10 轮 MIBS 算法的碰撞攻击所需要的选择明文不超过 2^7 个，对 10 轮 MIBS 算法的碰撞攻击的数据复杂度为 $2^{11.46}$，时间复杂度约为 $2^7\times 2^4\times 2^{40}\times 13/(10\times 8)\approx 2^{48.3}$。

通过不同的攻击方法对 MIBS 算法的不同轮数进行攻击的复杂度对比如表 1 所列。

表 1　对 MIBS 算法不同轮数进行攻击的复杂度比较

Table 1　Comparison of complexity of attacking different rounds of MIBS algorithm

攻击方法	轮数	数据复杂度	时间复杂度	预计算复杂度	文献
Integral 攻击	8	$2^{38.6}$	$2^{24.2}$	—	文献[4]
中间相遇攻击	8	20	$2^{24.9}$	$2^{50.9}$	文献[5]
积分攻击	8	$2^{9.6}$	$2^{35.6}$	—	文献[6]
碰撞攻击	8	$2^{14.3}$	$2^{34.9}$	—	本文
Integral 攻击	9	$2^{39.6}$	$2^{68.4}$	—	文献[4]
中间相遇攻击	9	25	$2^{46.3}$	$2^{51.1}$	文献[5]
积分攻击	9	$2^{37.6}$	2^{40}	—	文献[6]
碰撞攻击	9	$2^{22.8}$	$2^{47.1}$	—	本文
中间相遇攻击	10	$2^{8.7}$	$2^{50.2}$	$2^{51.0}$	文献[5]
积分攻击	10	$2^{61.6}$	2^{40}	—	文献[6]
碰撞攻击	10	$2^{11.5}$	$2^{48.3}$	—	本文

由表 1 可知，与中间相遇攻击相比，碰撞攻击不需要进行预计算，降低了攻击的复杂度；与积分攻击相比，碰撞攻击的数据复杂度较低；与 Integral 攻击相比，碰撞攻击的时间复杂度略优。因此，对 MIBS 算法的碰撞攻击有其可取之处。

结束语　本文利用 MIBS 算法的一个等价结构构造了

（下转第 230 页）

中的应用[J]. 计算机科学,2011,38(5):54-55,73.

[6] YUE S H,WANG J S,TAO G,et al. An unsupervised grid-based approach for clustering analysis[J]. Science China(Information Sciences),2010,53(7):1345-1357.

[7] LI T T. The Research of K-means Clustering Algorithm- Improvement[D]. Hefei:Anhui University,2015. (in Chinese)
李婷婷. 改进 K-means 聚类算法的研究[D]. 合肥:安徽大学,2015.

[8] ZHANG X F,ZHANG G Z,LIU P. Improved K-means algorithm based on clustering criterion function[J]. Computer Engineering and Applications,2011,47(11):123-127. (in Chinese)
张雪凤,张桂珍,刘鹏. 基于聚类准则函数的改进 K-means 算法[J]. 计算机工程与应用,2011,47(11):123-127.

[9] KATSAVOUNIDIS I,JAY KUO C C,ZHANG Z. A new initialization technique for generalized Lloyd iteration[J]. Signal Processing Letters,1994,1(10):144-146.

[10] BOUTSIDIS C,ZOUZIAS A,MAHONEY M W,et al. Randomized Dimensionality Reduction for k-Means Clustering[J]. IEEE Transactions on Information Theory,2011,61(2):1045-1062.

[11] WANG J,KE Q,et al. Fast approximate k-means via cluster closures[C]// IEEE Conference on Computer Vision and Pattern Recognition. IEEE Computer Society,2012:3037-3044.

[12] XIONG K L,PENG J J,YANG X F,et al. K-means Clustering Optimization Based on Kernel Density Estimation[J]. Computer Technology and Development,2017,27(2):1-5. (in Chinese)
熊开玲,彭俊杰,杨晓飞,等. 基于核密度估计的 K-means 聚类优化[J]. 计算机技术与发展,2017,27(2):1-5.

[13] ZHUANG R G,NI Z B,LIU X Y. A Novel Method for Refining the Initial Points for K-means Clustering Based on Quasi-Monte Carlo Method[J]. Journal of University of Jinan(Science and Technology),2017,31(1):35-41. (in Chinese)
庄瑞格,倪泽邦,刘学艺. 基于拟蒙特卡洛的 K 均值聚类中心初始化方法[J]. 济南大学学报(自然科学版),2017,31(1):35-41.

[14] LI M,ZHANG G Z. K-means Algorithm of Optimized Initial Center By Density Peaks[J]. Computer Applications and Software,2017,34(3):212-217. (in Chinese)
李敏,张桂珠. 密度峰值优化初始中心的 K-means 算法[J]. 计算机应用与软件,2017,34(3):212-217.

[15] YUAN T F. Research on Intrusion Detection Based on Data Mining[D]. Chengdu: University of Electronic Science and Technology of China,2014. (in Chinese)
袁腾飞. 基于数据挖掘的入侵检测系统研究[D]. 成都:电子科技大学,2014.

[16] CHENG J. The Research of Fusion Algorithms for Support Vector Machine and K-means Clustering[D]. Dalian: Liaoning Normal University,2008. (in Chinese)
程佳. 支持向量机与 K-均值聚类融合算法研究[J]. 大连:辽宁师范大学,2008.

[17] YU H T,JIA M J,WANG H Q,et al. K-means Clustering Algorithm Based on Artificial Fish Swarm[J]. Computer Science,2012,39(12):60-64. (in Chinese)
于海涛,贾美娟,王慧强,等. 基于人工鱼群的优化 K-means 聚类算法[J]. 计算机科学,2012,39(12):60-64.

[18] XIAO L Z,LIU Y X,CHEN L Q. Research of Accelerating K-Means Algorithm Based on New Particle Swarm Optimization for Intrusion Detection[J]. Journal of System Simulation,2014,26(8):1652-1657. (in Chinese)
肖立中,刘云翔,陈丽琼. 基于改进粒子群的加速 K 均值算法在入侵检测中的研究[J]. 系统仿真学报,2014,26(8):1652-1657.

(上接第 225 页)

MIBS 算法的 6 轮区分器,评估了 MIBS 算法在碰撞攻击下的安全性。分析结果表明,8/9/10 轮的 MIBS 算法对碰撞攻击是不免疫的。

参 考 文 献

[1] IZADI M,SADEGHIYAN B,SADEGHIAN S S,et al. MIBS:a new lightweight block cipher[C]// Proceedings of CANS 2009,Lecture Notes in Computer Science 5888. Berlin:Springer,2009:334-345.

[2] SEBASTIANI F. Machine learning in automated text categorization acmcs[J]. ACM Computing SURCEYS,2002,34(1):1-47.

[3] ZHAO X J,WANG T,WANG S Z,et al. Research on deep differential fault analysis against MIBS[J]. Journal on Communications,2010,31(12):82-88. (in Chinese)
赵新杰,王韬,王素珍,等. MIBS 深度差分故障分析[J]. 通信学报,2010,31(12):82-88.

[4] WANG G L,WANG S H. Integral cryptanalysis of reduced-round MIBS block cipher[J]. Journal of Chinese Computer Systems,2012,33(4):773-777. (in Chinese)
王高丽,王少辉. 对 MIBS 算法的 Integral 攻击[J]. 小型微型计算机系统,2012,33(4):773-777.

[5] LIU C,LIAO F C,WEI H R. Meet-in-the-middle attacks on MIBS[J]. Journal of Inner Mongolia University(Natural Science Edition),2013,44(3):308-313. (in Chinese)
刘超,廖福成,卫宏儒. 对 MIBS 算法的中间相遇攻[J]. 内蒙古大学学报(自然科学版),2013,44(3):308-313.

[6] YU X L,WU W L,LI Y J. Integral cryptanalysis of reduced-round MIBS block cipher[J]. Journal of Computer Research and Development,2013,50(10):2117-2125. (in Chinese)
于晓丽,吴文玲,李俊艳. 低轮 MIBS 分组密码的积分分析[J]. 计算机研究与发展,2013,50(10):2117-2125.

[7] PAN Z S,GUO J S,CAO J K,et al. Integral attack on MIBS block cipher[J]. Journal on Communications,2014,35(7):157-171. (in Chinese)
潘志舒,郭建胜,曹进克,等. MIBS 算法的积分攻击[J]. 通信学报,2014,35(7):157-171.

[8] GILBERT H,MINIER M. A collision attack on 7 rounds of Rijndael[EB/OL]. [2012-10-10]. http://csrc. nist. gov/archive/aes/round2/conf3/papers/11-hgilbert. pdf.

[9] WU W L,FENG D G. Collision attack on reduced-round Camellia[J]. Science in China:Series F,2004,48(1):78-90.

[10] HAN J,ZHANG W J,XU X H. Collision Square Attacks on the Reduced-Round CLEFIA[J]. Acta Electronica Sinica,2009,37(10):2309-2313.

[11] LI C,SUN B,LI R L. Attack method and example analysis of block cipher[M]. Beijing:Science Press,2010:196-199. (in Chinese)
李超,孙兵,李瑞林. 分组密码的攻击方法与实例分析[M]. 北京:科技出版社,2010:196-199.