软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(Suppl.(1)):8−16

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

轻量级分组密码 MIBS-80 算法的 Biclique 分析*

罗 芳, 欧庆于, 周学广, 陈 云, 李石磊

(海军工程大学 信息安全系,湖北 武汉 430033)

通讯作者: 欧庆于, E-mail: ouqingyv@163.com

摘 要: 提出了针对轻量级分组密码算法 MIBS-80 的 Biclique 分析.利用两条独立的相关密钥差分路径,构造了 4 轮维度为 4 的 Biclique 结构,在此基础上对密钥空间进行了划分,结合预计算技术,对每一个密钥子空间进行筛选以降低中间相遇攻击所需的计算复杂度,实施了对 12 轮 MIBS-80 的密钥恢复攻击.攻击的数据复杂度为 2^{52} 个选择明文,计算复杂度约为 $2^{77.13}$ 次 12 轮 MIBS-80 加密,存储复杂度约为 $2^{8.17}$,成功实施攻击的概率为 1.与已有攻击方法相比,在存储复杂度及成功率方面具有优势.

关键词: 轻量级分组密码;MIBS-80 算法; Biclique 分析;复杂度

中文引用格式: 罗芳,欧庆于,周学广,陈云,李石磊.轻量级分组密码 MIBS-80 算法的 Biclique 分析.软件学报,2015,26(Suppl.(1)):8−16. http://www.jos.org.cn/1000-9825/15002.htm

英文引用格式: Luo F, Ou QY, Zhou XG, Chen Y, Li SL. A biclique cryptanalysis on lightweight block cipher MIBS-80. Ruan Jian Xue Bao/Journal of Software, 2015,26(Suppl.(1)):8−16 (in Chinese). http://www.jos.org.cn/1000-9825/15002.htm

A Biclique Cryptanalysis on Lightweight Block Cipher MIBS-80

LUO Fang, OU Qing-Yu, ZHOU Xue-Guang, CHEN Yun, LI Shi-Lei

(Department of Information Security, Naval University of Engineering, Wuhan 430033, China)

Abstract: A Biclique cryptanalysis on lightweight block cipher MIBS-80 is presented in this paper. Exploiting two independent related-key difference trails, 4-round Biclique of dimension 4 is constructed and the key space is partitioned. To reduce the computational complexity, the precomputation and meet-in-the-middle technique is applied to sieve out the correct key for 12-round MIBS-80. The data complexity of this cryptanalysis is 2^{52} chosen plaintexts, the computational complexity is about $2^{77.13}$ 12-round MIBS-80 encryptions, the storage complexity is about $2^{8.17}$, and the success probability is 1. Compared with the previous known cryptanalysis, the new method has advantages in the storage complexity and success probability.

Key words: lightweight block cipher; MIBS-80; Biclique cryptanalysis; complexity

随着无线传感器网络 WSN(wireless sensor network)和射频识别标签 RFID(radio frequency identification)的广泛应用,物联网等无线网络传输领域日益突出的信息安全问题正引起人们的极大关注.与传统计算平台不同,物联网等系统中的应用组件多是计算、存储能力有限的微型处理设备,导致传统分组密码算法,如 AES 等已无法较好地解决其中的数据安全问题.为更好地适应资源受限环境的密码应用需求,许多轻量级分组密码算法被设计出来,如 LBlock[1]、LED[2]、Piccolo[3]、KLEIN[4]、MIBS[5]等.

其中,MIBS 是由 Izadi 等人在 CANS 2009 上提出的轻量级分组密码,算法分组长度为 64 比特,支持长度为 64 比特和 80 比特的密钥,分别对应于 MIBS-64 和 MIBS-80.与其他轻量级分组密码相比,该算法硬件实现效率高,计算资源消耗少,广泛应用于 WSN 及 RFID 中.目前,对 MIBS 的安全性分析仅限于差分分析、不可能差分分

* 基金项目: 国家自然科学基金(11202239, 61202338); 中国博士后基金(2014M562555); 国家社会科学基金(14GJ003-152); 海军工程大学自然科学基金(HGDQNEQJJ15016)

收稿时间: 2015-04-15; 定稿时间: 2015-07-20

析、线性分析及积分攻击,其中,文献[6]对 MIBS-80 进行了 18 轮线性分析,这是目前已公开文献中对 MIBS-80 轮数最多的分析结果.同时,文献[6]还对该算法进行了 14 轮差分分析以及 12 轮不可能差分分析.文献[7]指出了文献[6]中不可能差分分析的错误,对 12 轮 MIBS-80 进行了密钥恢复攻击.文献[8]给出了 MIBS-80 的 5 轮积分区分器,在此基础上对算法进行了 9 轮积分攻击.

由于轻量级分组密码在设计时就已充分考虑了差分分析、线性分析等传统分析方法带来的威胁,导致这些传统方法在轻量级分组密码分析领域存在一定局限性.2011 年,Bogdanov[9]等人在亚洲密码年会上基于中间相遇攻击 MITM (Meet-In-The-Middle Attack)技术,首次提出了 Biclique 分析方法.研究表明,轻量级分组密码 HIGHT[10]、Piccolo[11]、LBlock[12]、PRSENT[13]在 Biclique 攻击下无法达到理想安全性,主要原因在于为了降低实现代价,算法往往采用简单的循环移位以及与轮常量异或的方式来产生圈子密钥,导致圈子密钥生成算法的扩散性较弱,Biclique 分析方法正是利用这一弱点来构造长轮数、多维度的 Biclique 结构以实施密钥恢复攻击.

本文从 Biclique 分析的角度对 MIBS-80 的安全性进行了分析,通过对圈子密钥生成算法性质的研究,给出了两条独立的相关密钥差分路径,通过构造 4 轮维度为 4 的 Biclique 结构,并结合预计算技术对 12 轮 MIBS-80 实施了 Biclique 分析,解决了需通过穷举整个密钥空间来实施中间相遇攻击的问题,同时也为轻量级分组密码中圈子密钥生成算法的设计与分析提供了新思路.

1 MIBS-80 算法简介

MIBS 算法整体采用 Feistel 结构,加密轮数为 32 轮,算法所有的内部操作都是以 4 bit 为一个单位.第 i 轮的结构如图 1 所示,轮函数 F 包括圈子密钥加变换,非线性变换 S 和线性变换 P.

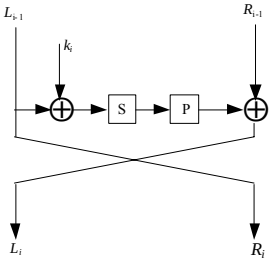

图 1 MIBS 算法第 i 轮结构

1.1 加密过程

设 64 比特明文为 $L_0||R_0$,从左至右为高比特位到低比特位的排列顺序,F 函数为圈函数,具体结构如图 2 所示,加密得密文 $L_{32}||R_{32}$ 过程如下:

对于 $1\leqslant i\leqslant 32$,$L_i=F(L_{i-1},k_i)\oplus R_{i-1}$.

(1) 密钥加变换:$X=L_{i-1}\oplus k_i$;

(2) 非线性 S 盒变换:非线性变换由 8 个相同的 4×4 S 盒并置,令 $X=x_8||x_7||x_6||x_5||x_4||x_3||x_2||x_1$,则 $y_i=S(x_i)(i=1,2,\ldots,8)$;

(3) 线性 P 盒变换见下列公式:

$$y_1'=y_1\oplus y_2\oplus y_4\oplus y_5\oplus y_7\oplus y_8;\quad y_2'=y_2\oplus y_3\oplus y_4\oplus y_5\oplus y_6\oplus y_7;$$
$$y_3'=y_1\oplus y_2\oplus y_3\oplus y_5\oplus y_6\oplus y_8;\quad y_4'=y_2\oplus y_3\oplus y_4\oplus y_7\oplus y_8;$$
$$y_5'=y_1\oplus y_3\oplus y_4\oplus y_5\oplus y_8;\quad y_6'=y_1\oplus y_2\oplus y_4\oplus y_5\oplus y_6;$$
$$y_7'=y_1\oplus y_2\oplus y_3\oplus y_6\oplus y_7;\quad y_8'=y_1\oplus y_3\oplus y_4\oplus y_6\oplus y_7\oplus y_8$$

$F(L_{i-1},k_i)$输出为 $y_8'||y_7'||y_6'||y_5'||y_4'||y_3'||y_2'||y_1'$.

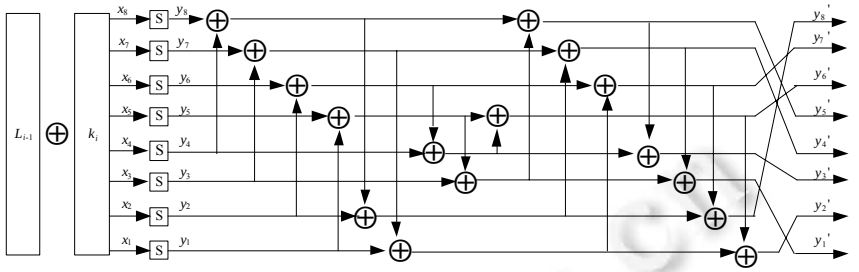

图 2 MIBS 算法 F 函数结构

1.2 MIBS-80圈子密钥生成算法

设 80 比特的密钥为 $K=(K_{79}, K_{78}, \ldots, K_0)$,$[a\sim b]$表示从比特位 i~比特位 j 之间的 $i–j+1$ 比特.由 K 经过行移位、S 盒变换及与轮常量异或得到 32 个长度为 32 比特的圈子密钥 $k_i(1\leqslant i\leqslant 32)$的过程如下:

$state^1\leftarrow K$,对于 $1\leqslant i\leqslant 32$

(1) $state^i \leftarrow state^i >>> 19$;

(2) $state^i \leftarrow S(state^i_{[79\sim 76]}) \| S(state^i_{[75\sim 72]}) \| state^i_{[71\sim 0]}$;

(3) $state^i \leftarrow state^i_{[79\sim 19]} \| state^i_{[18\sim 14]} \oplus Round\_Counter \| state^i_{[13\sim 0]}$;

(4) $k_i \leftarrow state^i_{[79\sim 48]}$,

其中,$>>>19$ 表示循环右移 19 位,圈子密钥生成算法中的 S 盒与加密算法中的 S 盒一致,*Round_Counter* 表示轮数.

由上述过程可知,MIBS-80 的圈子密钥满足如下线性关系:

性质 1. 令第 i 圈的圈子密钥 $k_i=(k_{i,1},k_{i,2},\ldots,k_{i,8})$,则 k_1 和 k_2 有 13 个比特位相同,$k_{1,1}\|k_{1,2}\|k_{1,3}\|k_{1,4}[1]=k_{2,5}[4]\|k_{2,6}\|k_{2,7}\|k_{2,8}$,方括号中的数字代表半字节中的比特位.

性质 2. 由 $K[18\text{-}0]$和 $K[79\text{-}67]$即可确定圈子密钥 k_1,记为 $K[18\text{-}0]\|K[79\text{-}67]\rightarrow k_1$.

2 Biclique 分析方法

中间相遇攻击优势在于低数据复杂度,但与其他攻击方法相比计算复杂度较高.Biclique 分析通过构造 Biclique 结构将密钥空间划分为若干子空间,再利用中间相遇攻击对每一密钥子空间进行测试,以降低中间相遇攻击所需计算复杂度.

2.1 Biclique结构

设分组密码算法 E 的分组长度为 n bit,密钥长度为 k bit,则 $E:\{0,1\}^n\times\{0,1\}^k\rightarrow\{0,1\}^n$,且 E 可以表示为 3 个独立变换的复合,即 $E=E_f\circ E_{\Phi_1}\circ E_{\Phi_2}$.若函数 f 在密钥 $K[i,j]$的作用下,将明文 P_i 映射为中间状态 S_j,且对于 $i,j\in\{0,\ldots,2^{\text{d}}1\}$,$S_j=f_{K[i,j]}(P_i)$均成立,则称三元组$[\{P_i\},\{S_j\},\{K[i,j]\}]$是一个维度为 d 的 Biclique,其中$\{K[i,j]\}$是一个 $2^d\times 2^d$ 的密钥矩阵:

$$\{K[i,j]\}=\begin{Bmatrix} K[0,0] & K[0,1] & \cdots & K[0,2^d-1] \\ \vdots & \vdots & & \vdots \\ K[2^d-1,0] & K[2^d-1,1] & \cdots & K[2^d-1,2^d-1] \end{Bmatrix},$$

函数 f 中所包含的叠代轮数即 Biclique 的长度,如图 3 所示为一个 d 维 Biclique.

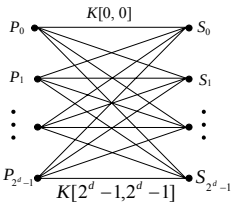

图 3 d 维 Biclique 结构

2.2 Biclique攻击步骤

Step 1. 密钥空间划分.

将密钥空间划分为 2^{k-2d} 个子空间,每个子空间中密钥个数为 2^{2d}.对于任意子空间中的所有密钥,有 k–$2d$ 个固定密钥比特位取值一致,剩余 $2d$ 位则遍历 2^{2d} 个可能值,将这 $2d$ 个比特位取值为全 0 的密钥记为子空间的基础密钥 $K[0,0]$,该子空间中的其他密钥都可通过前向密钥差分路径 Δ_i^K 及后向密钥差分路径 ∇_j^K 相对于 $K[0,0]$ 定义.

$$\Delta_i^K = K[0,0] \oplus K[i,0], i \in \{0,...,2^d-1\}\ \ \nabla_j^K = K[0,0] \oplus K[0,\ j], j \in \{0,...,2^d-1\}.$$

Step 2. Biclique 构造.

对于每一个密钥子空间构造 Biclique,使得明文、中间状态及密钥三者之间建立如图 3 所示关系.

Step 3. 筛选密钥.

对于每一个 Biclique:

1. 通过加密预言机加密明文 P_i 得到对应密文 $C_i, i \in \{0,\ldots,2^d-1\}$;
2. 选择中间状态部分比特作内部匹配变量 v_{ij};
3. 在密钥子空间中检测是否存在 $K[i,j]$满足以下条件:

$$S_j \xrightarrow[\Phi_1]{K[i,j]} \vec{V}_{i,j} = \overleftarrow{V}_{i,j} \xleftarrow[\Phi_2]{K[i,j]} C_i \tag{1}$$

满足该条件的密钥为正确密钥,若不满足,则返回 Step 2,检测下一个密钥子空间,直至找到正确密钥,具体过程如图 4 所示.

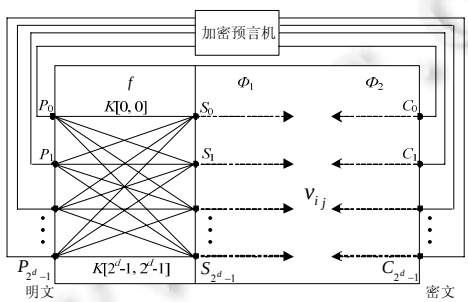

图 4 基于 Biclique 的密钥恢复攻击

3 对 12 轮 MIBS-80 的密钥恢复攻击

为对 12 轮 MIBS-80 进行密钥恢复攻击,本节首先在 1-4 轮构造了维度为 4 的 Biclique 结构,并选取第 8 轮加密输出的第 1、第 5 个半字节字 $X_8^{1,5}$,以及第 9 轮解密输出的第 1、第 5 个半字节字 $Y_9^{1,5}$ 作为中间匹配变量,对算法的 5-12 轮进行中间相遇攻击,具体参数见表 1.

表 1 12 轮 MIBS-80 Biclique 攻击的参数

算法	轮数	Biclique 长度	Biclique 维度	匹配变量 v_{ij}	前向计算轮数	后向计算轮数
MIBS-80	12	4(1~4)	4	$x_8^{1,5}, y_9^{1,5}$	5~8	9~12

3.1 密钥空间划分

Biclique 的维度及长度是 Biclique 分析的关键因素,两者直接决定了攻击的计算复杂度,由于大多数轻量级分组密码在设计时已充分考虑了轮函数的快速扩散性,导致多轮数、高维度的 Biclique 构造一直是 Biclique 分析的难点.针对 AES 的 Biclique 分析,文献[10]首次提出了利用两条独立相关密钥差分路径构造 Biclique 结构的方法.基于该方法,本文找到了 12 轮 MIBS-80 两条独立的相关密钥差分路径,并对密钥空间进行了划分.

定义 1. 若一个状态位的输入差分非 0,称其为活跃状态位,否则,为非活跃状态位.

定义 2. 若一条差分路径中的活跃状态位在另一条差分路径中均为非活跃状态位,称这两条差分路径为独立差分路径.

由于 MIBS 内部操作都是以 4 比特字为单位,相关密钥差分路径仍以 4 比特为单位.由 MIBS-80 的圈子密钥性质 1 和性质 2,将 K[74-71]和 K[56-53]作为 MIBS-80 两条独立相关密钥差分路径的起始位置,则 1~12 轮的相关密钥差分路径可由表 2 得到.基于两条独立的相关密钥差分路径,将 MIBS-80 的密钥空间划分为 2^{72} 个子空间,每个子空间中的密钥个数为 2^8 个.对于一个子空间中的所有密钥,除第 74~71 位及第 56~53 位,剩下的 72 比特位均相同,将每个子空间中第 74~71 位及第 56~53 位取值均为 0 的密钥记为该子空间的基础密钥 K[0,0].

表 2 12 轮 MIBS-80 相关密钥差分路径

轮数	0				1				2				3				4				5				6				7			
1	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67
2	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6
3	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25
4	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44
5	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63
6	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2
7	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21
8	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40
9	10	9	8	7	6	5	4	3	2	1	0	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59
10	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	79	78
11	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
12	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36

□:圈子密钥生成算法中 S 盒作用位置 ▨:由 K[74~71]导致的 12 轮圈子密钥差分 ■:由 K[56~53]导致的 12 轮圈子密钥差分

3.2 维度为4的4轮Bclique构造

在划分密钥空间的基础上,对每一个密钥子空间构造 Biclique 结构,使得三元组$\{\{P_i\},\{S_j\},K[i,j]\}$($0\leqslant i, j\leqslant 2^4-1$)满足如图 3 所示关系.

令$\nabla_j=S_0+S_j$,$\triangle_i=P_0+P_i$,则 Biclique 构造过程如下:

(1) 取 P_0=0,f 为 MIBS-80 的第 1~4 轮映射,在密钥 K[0, 0]的作用下计算:

$$P_0 \xrightarrow[f]{K[0,0]} S_0 \tag{2}$$

为避免重复计算,降低攻击的计算复杂度,可将式(3)作为基础运算存储,后续步骤只需计算与基础运算不同部分.

(2) 利用密钥 K[0, j]($0\leqslant j\leqslant 2^4-1$)加密 P_0 得到中间状态 S_j.

与 $K[0,0]$相比,$K[0,j]$仅在密钥第{74,73,72,71}比特位取值不同,因此该步计算复杂度为 2^4,且满足:

$$0 \xrightarrow[f]{\nabla_j^K} \nabla_j \tag{3}$$

(3) 利用密钥 $K[i,0](0\leqslant i\leqslant 2^4-1)$解密 S_0 得明文 P_i.

与 $K[0,0]$相比,$K[i,0]$仅在密钥第{56,55,54,53}比特位取值不同,因此前向密钥差分 Δ_i^K 决定了该步的计算复杂度为 2^4,且同时满足:

$$\nabla_i \xrightarrow[f]{\nabla_i^K} 0 \tag{4}$$

步骤(2)和步骤(3)的具体计算过程见表 3,在第{74,73,72,71}密钥比特位的作用下,后向差分路径由全零扩散到影响第 4 轮的若干状态位,同时,在第{56, 55, 54, 53}密钥比特位的作用下,前向差分路径经过 4 轮迭代后归零.由于所有前向差分路径和后向差分路径无共同的活跃状态位,由式(3)~式(5),对于每一个密钥子空间,可在算法的 1~4 轮构造维度为 4 的 Biclique 结构,满足如下关系:

$$\nabla_j \oplus P_0 \xrightarrow[f]{\Delta_i^K \oplus \nabla_j^K \oplus K[0,0]} S_0 \oplus \Delta_i \tag{5}$$

表 3 4 轮 MIBS-80 独立相关密钥差分路径

轮数	后向差分路径∇_j		前向差分路径$\triangle_i$	
	后向密钥差分 ∇_j^K	中间值输入差分	前向密钥差分 Δ_i^K	中间值输入差分
		中间值输出差分		中间值输出差分
1	0000 00x0	0000 0000 0000 0000	0000 0000	xxx0 xx00 xxxx xxxx
		0000 0000 0000 0000		0000 x000 xxx0 xx00
2	0000 0000	0000 0000 0000 0000	0000 0000	0000 x000 xxx0 xx00
		0000 00x0 0000 0000		0000 0000 0000 x000
3	0000 0000	0000 00x0 0000 0000	x000 0000	0000 0000 0000 x000
		xx0x 00xx 0000 00x0		0000 0000 0000 0000
4	xx00 0000	xx0x 00xx 0000 00x0	0000 xx00	0000 0000 0000 0000
		xxxx xxxx xx0x 00xx		0000 0000 0000 0000

x:活跃 4 比特字

3.3 MIBS-80的8轮中间相遇攻击

为筛选出密钥子空间中的正确密钥,还需通过验证等式(2)是否成立来对剩下的 8 轮 MIBS-80 实施中间相遇攻击.因此,在验证等式之前,需首先通过 5~8 轮后向计算及 9~12 轮前向计算来得到中间匹配变量 $X_8^{1,5}$ 及 $Y_9^{1,5}$,但若每检测一个密钥都需重新计算中间变量,中间相遇攻击的计算复杂度将会抵销 Biclique 构造所带来的计算上的优势.为了降低攻击的计算复杂度,在前向计算时可预先进行下列基础运算,并存储该过程:

$$S_j \xrightarrow[\Phi_1]{K[0,j]} v_{0j} \tag{6}$$

当计算 $S_j \xrightarrow[\Phi_1]{K[i,j]} v_{ij}$ 时,仅需计算与过程(6)不同的部分,因此该过程的计算复杂度主要取决于 ∇_j^K . ∇_j^K 的起始位置为密钥第 74~71 比特位,由此导致的 5~8 轮圈子密钥差分及各轮的输入、输出差分见表 4.

表 4 5~8 轮后向计算

轮数	密钥差分 ∇_j^K	中间值输入差分	仅 1 次计算 S 盒	活跃 S 盒
		中间值输出差分		
5	0000 xxx0	0000 0000 0000 0000	5	3
		x00x xx0x 0000 0000		
6	0000 0000	x00x xx0x 0000 0000	3	5
		xxxx xxxx x00x xx0x		
7	0000 0000	xxxx xxxx x00x xx0x	0	8
		0xx0 00x0 xxxx xxxx		
8	xx00 0000	0xx0 00x0 xxxx xxxx	0	3
		0000 0000 0x$\underline{x}$0 00$\underline{x}$0		

前向计算需首先通过加密预言机得到 2^4 个已知明-密文对.固定密文 C_i,预先进行并存储下列基础运算:

$$C_i \xrightarrow[\Phi_2]{K[i,0]} v_{i0} \tag{7}$$

当计算 $C_i \xrightarrow[\Phi_2]{K[i,j]} v_{ij}$ 时, 仅需计算与过程(7)不同的部分, ∇_j^K 仅在密钥第 56~53 比特位取值不同,由此导致的 9~12 轮圈子密钥差分及各轮的输入、输出差分见表 5.

表 5 9~12 轮前向计算

轮数	密钥差分 Δ_i^K	中间值输入差分 中间值输出差分	仅 1 次计算 S 盒	活跃 S 盒
9	0000 000x	000x 0000 xxxx xxxx xxxx xxxx 000x 0000	6	2
10	0000 0000	xxxx xxxx 000x 0000 xxx0 xxxx xxxx xxxx	0	8
11	0000 0000	xxx0 xxxx xxxx xxxx 0000 0000 xxx0 xxxx	0	7
12	0xxx x000	0000 0000 xxx0 xxxx 0000 0000 0000 0000	0	4

若 $X_8^{1,5}$ 的输出差分与 $Y_9^{1,5}$ 的输出差分不满足式(1)条件,则将 $\nabla_j^K \oplus \Delta_i^K \oplus K[0,0]$ 从子密钥空间中删除,一旦满足,将其作为可能的正确密钥,并进一步检测该密钥是否满足明-密文关系.

为了判断式(1)是否成立,攻击者仅需计算中间匹配变量的非零部分,由于仅有非线性运算部件 S 盒会对其非零部分产生影响,因此,8 轮中间相遇攻击的计算复杂度由仅需 1 次计算的 S 盒数量,以及需重复计算的活跃 S 盒数量共同决定.由表 4 和表 5,对于后向计算,仅需 1 次计算的 S 盒数量为 8,活跃 S 盒数量为 2^4×19;对于前向计算,仅需 1 次计算的 S 盒数量为 6,活跃 S 盒数量为 2^4×21.

3.4 攻击复杂度分析

攻击所需的数据复杂度由需加密的明文 P_i 的数量决定,在构造 1~4 轮的 Biclique 结构时,将 P_0 固定为 0,由表 3 可知,所有 P_i 的第 8、9、12 个半字节字的取值均相等,因此,数据复杂度不会超出 2^{52} 个选择明文.

对于某一个 Biclique,攻击所需的计算复杂度由构造 Biclique 所需复杂度 $C_{Biclique}$、中间相遇攻击的计算复杂度 C_{match}、Biclique 构造中由密钥差分导致的复杂度 $C_{key\text{-}schedule}$ 以及密钥重复检测的复杂度 $C_{recheck}$ 共同决定,因此,总计算复杂度 C_{full} 由下式可得:

$$C_{full} = 2^{k-2d} \times (C_{Biclique} + C_{match} + C_{key-schedule} + C_{recheck}).$$

构造 Biclique 的基础运算阶段共需计算 4 轮,每轮需计算 8 个 S 盒,共需计算 32 个 S 盒.1-4 轮后向差分路径共涉及 7 个活跃 S 盒,前向差分路径所涉及的活跃 S 盒数量为 9,因此,构造 Biclique 需计算 S 盒的总数为 (7+9)×2^4+32=288.

后向计算阶段需计算的 S 盒总数为 2^4×(8+2^4×19),前向计算阶段需计算的 S 盒总数为 2^4×(6+2^4×21),因此,对于每一个 Biclique 结构,中间相遇攻击所涉及的 S 盒总数为 10 464.

同一 Biclique 中密钥差分的两组起始状态位置导致的活跃 S 盒是相互独立的,通过将表 3 中间值的左半部分输入与密钥差分异或可知,共有 16 个 S 盒需重复计算 2^4 次,剩下 16 个 S 盒仅需计算 1 次,因此,$C_{key\text{-}schedule}$ 涉及的 S 盒总数为 16+2^4×16=112.

中间相遇攻击需通过 8 比特中间匹配变量对密钥子空间中 2^8 个密钥进行测试,导致每个密钥子空间中平均有 2^{8-8}=1 个密钥需重复测试.

由于 32 轮完整加密及圈子密钥生成过程共需计算的 S 盒总数为 32×(8+2)=320,将上述计算复杂度换算为一次加、解密的计算复杂度,C_{full} 可由下式计算得到:

$$C_{full} = 2^{80-2\times4} \times \left(\frac{288 + 10464 + 112}{320} + 1 \right) \approx 2^{77.13}.$$

攻击的存储复杂度为 2^4+2^4+2^8≈$2^{8.17}$,即存储 1 个 Biclique 结构所需空间.

3.5 结果比较

目前,还没有公开文献对完整轮数 MIBS-80 算法进行分析,对约减轮数的 MIBS-80 的安全性分析也仅限于差分分析、不可能差分分析、线性分析以及积分攻击.在单密钥模式下与对约减轮数的 MIBS-80 的其他攻击结果比较见表 6.

表 6 单密钥模式下对 MIBS-80 的攻击结果比较

攻击方法	轮数	计算复杂度	数据复杂度	存储复杂度	成功率(%)	文献
线性攻击	18	$2^{76.13}$	$2^{60.98}$KP	$2^{60.98}$	72.14	[6]
差分攻击	14	2^{40}	2^{40}CP	2^{40}	50.15	[6]
不可能差分攻击	12	2^{63}	2^{59}CP	—	—	[7]
积分攻击	9	$2^{68.4}$	$2^{39.6}$CP	—	—	[8]
相关密钥不可能差分攻击	14	2^{56}	2^{54}CP	—	—	[14]
Biclique 攻击	12	$2^{77.13}$	2^{52}CP	$2^{8.17}$	1	本文

注:CP 为选择明文,KP 为已知明文

在本文分析方法中,由于所有密钥子空间的并集即为整个密钥空间,且对每个密钥子空间中的所有密钥都依次重复上述攻击过程,因此,该攻击的成功率为 1.与其他攻击方法相比,本文攻击方法在成功率方面具有优势,但同时这也导致攻击所需的计算复杂度较高.本文结合预计算技术及中间相遇攻击来降低计算复杂度,使其低于穷举攻击所需计算复杂度,这对于密钥长度已较短的轻量级分组密码分析具有一定实际意义.与文献[6]相比,本文攻击方法所需的存储复杂度仅为 $O(2^{8.17})$,在存储复杂度方面也具有一定优势.但与文献[6,14]相比,本文分析方法在攻击轮数上有待提高.

4 结 论

基于 Biclique 分析方法本文对 MIBS-80 的安全性进行了分析,结合圈子密钥生成算法的性质,给出了两条独立的相关密钥差分路径,通过构造 4 轮维度为 4 的 Biclique 结构对密钥空间进行划分,并利用中间相遇攻击对 12 轮 MIBS-80 进行了密钥恢复攻击.攻击所需数据复杂度为 $O(2^{52})$,计算复杂度为 $O(2^{77.13})$,存储复杂度为 $O(2^{8.17})$.分析表明本文攻击方法在成功率及存储复杂度方面具有优势,适用于对成功率要求较高且存储资源受限的攻击环境.但由于算法总轮数较多,如何构造足够长度或维度的 Biclique 以实施更多轮数的密钥恢复攻击将是下一步研究重点.

References:

[1] Wu WL, Zhang L. LBlock: A lightweight block cipher. In: Lopez J, Tsudik G, eds. Proc. of the ACNS 2011. LNCS 6715, Heidelberg: Springer-Verlag, 2011. 327−344.

[2] Guo J, Peyrin T, Poshman A, Robshaw M. The LED block cipher. In: Preneel B, Takagi T, eds. Proc. of the CHES 2011. LNCS 6917, Heidelberg: Springer-Verlag, 2011. 326−341.

[3] Shibutani K, Isobe T, Hiwatari H, Mitsuda A, Akishita T, Shirai T. Piccolo: An ultra-lightweight blockcipher. In: Preneel B, TakagiT, eds. Proc. of the CHES 2011. LNCS 6917, Heidelberg: Springer-Verlag, 2011. 342−357.

[4] Gong Z, Nikova S, Law YW. KLEIN: A new family of lightweight block cipher. In: Juels A, PaarC, eds. Proc. of the RFIDSec 2011. LNCS 7055, Heidelberg: Springer-Verlag, 2011. 1−18.

[5] Izadi M, Sadeghiyan B, Sadeghian SS, Khanooki HA. MIBS: A new lightweight block cipher. In: Garay JA, MiyajiA, Otsuka A, eds. Proc. of the CANS 2009. LNCS 5888, Heidelberg: Springer-Verlag, 2009. 334−348.

[6] Bay A, Nakahara J, Vaudenay S. Cryptanalysis of reduced-round MIBS block cipher. In: Heng SH, Wright RN, Goi BM, eds. Proc. of the CANS 2010. LNCS 6467, Heidelberg: Springer-Verlag, 2010. 1−19.

[7] Du CH, Chen JZ. Impossible differential cryptanalysis of reduced-round MIBS. Journal of Shandong University (Natural Science), 2012,47(7):55−58. (in Chinese with English abstract).

[8] Wang GL, Wang SH. Integral cryptanalysis of reduced-round MIBS block cipher. Journal of Chinese Computer Systems, 2012, 33(4):773−777 (in Chinese with English abstract).

[9] Bogdanov A, Khovratovich D, Rechberger C. Biclique cryptanalysis of the full AES. In: Lee DH, WangXY, eds. Proc. of the ASIACRYPT 2011. LNCS 7073, Heidelberg: Springer-Verlag, 2011. 344−371.

[10] Hong D, Koo B, Kwon D. Biclique attack on the full HIGHT. In: Kim H, eds. Proc. of the ICISC 2011. LNCS 7259, Heidelberg: Springer-Verlag, 2012. 365−374.

[11] Wang YF, Wu WL, Yu XL. Biclique cryptanalysis of reduced-round Piccolo block cipher. In: Ryan MD, SmythB, Wang GL, eds. Proc. of the ISPEC 2012. LNCS 7232, Heidelberg: Springer-Verlag, 2012. 337−352.

[12] Wang YF, Wu WL, Yu XL, Zhang L. Security on LBlock against Biclique cryptanalysis. In: Lee DH, Yung M, eds. Proc. of the WISA 2012. LNCS 7232, Heidelberg: Springer-Verlag, 2012. 1−14.

[13] Gong Z, Liu SS, Wen YM, Tang SH. Biclique analysis on the reduce-round pRESENT. Chinese Journal of Computers, 2013,36(6):1130−1148 (in Chinese with English abstract).

[14] Chen P, Liao FC, Wei HR. Related-Key impossible differential attack on a lightweight block cipher MIBS. Journal of Communications, 2014,35(2):190−193 (in Chinese with English abstract).

附中文参考文献:

[7] 杜承航,陈佳哲.轻量级分组密码算法 MIBS 不可能差分分析.山东大学学报(理学版),2012,47(7):55−58.

[8] 王高丽,王少辉.对 MIBS 算法的 Integral 攻击.小型微型计算机系统,2012,33(4):773−777.

[13] 龚征,刘树生,温雅敏,唐韶华.约减轮数 PRESENT 算法的 Biclique 分析.计算机学报,2013,36(6):1130−1148.

[14] 陈平,廖福成,卫宏儒.对轻量级密码算法 MIBS 的相关密钥不可能差分攻击.通信学报,2014,35(2):190−193.

罗芳(1983－),女,江西吉安人,讲师,主要研究领域为密码算法设计与分析.

陈云(1978－),男,博士,讲师,主要研究领域为系统工程,信息安全.

欧庆于(1978－),男,副教授,主要研究领域为密码侧信道分析.

李石磊(1980－),男,博士,讲师,主要研究领域为信息安全,系统仿真.

周学广(1966－),男,教授,博士生导师,CCF 高级会员,主要研究领域为信息内容安全,网络安全协议分析.