八轮 MISTY1 算法的相关密钥扩大飞来去器攻击*

陈少真,戴艺滨
(信息工程大学 信息工程学院,河南 郑州 450002)

摘 要:密钥扩展算法对分组密码的安全至关重要,目前各种攻击方法越来越关注密钥带来的影响。通过分析非线性函数 FI 和密钥扩展算法,并观察轮子密钥的排列方式,寻找到 MISTY1 算法一个包含 2^{90} 个弱密钥的、可应用于相关密钥扩大飞来去器攻击的弱密钥类。在弱密钥类的基础上,寻找到两条相互独立的相关密钥差分路径,从而构造了一个七轮 MISTY1 算法的相关密钥扩大飞来去器区分器,进而实现了对八轮 MISTY1 算法(不带最后 FL 层)的相关密钥扩大飞来去器攻击。攻击需要 2^{63} 个选择明文,攻击的计算复杂度是 2^{70}。该攻击是第一个对不带最后 FL 层 MISTY1 算法的八轮攻击,且与同类攻击方法相比,攻击算法放宽了所需要的相关密钥的限制条件。

关键词:MISTY1 算法;相关密钥;扩大飞来去器;弱密钥
中图分类号:TP309 **文献标志码**:A **文章编号**:1001-2486(2012)02-0029-05

Related-key amplified boomerang attack on 8-round MISTY1

CHEN Shaozhen, DAI Yibin
(Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China)

Abstract: The key schedule algorithm plays a crucial role in the block cipher, thus many attacks pay more attention to it at present. Through analyzing the non-linear function FI and the key schedule algorithm of MISTY1, and observing the distribution of subkeys as well, a weak-key class of MISTY1 was found, which encompasses 2^{90} weak keys that are vulnerable to related-key amplified boomerang attack. Based on the weak-key class, two related-key differential characteristics were found. Then, the research presented a 7-round related-key amplified boomerang distinguisher of MISTY1, which can accomplish an attack on the 8-round MISTY1 without the last FL lay. The attack requires 2^{63} chosen plaintexts, and the time complexity of the attack is 2^{70}. The attack is the first attack on MISTY1 without the last FL lay. Besides, compared with the similar attacks, the limit of the related-key of our attack is released.

Key words: MISTY1; related-key; amplified boomerang; weak key

MISTY1 算法[1]是由日本学者 M. Matsui 设计的一个分组密码算法,它是第一个基于抵抗差分密码分析和线性密码分析的可证安全性理论而设计的实用分组密码。MISTY1 算法被 NESSIE 选定为过渡型的建议分组密码,同时也是 ISO 分组密码标准之一。

MISTY1 算法自公布以来得到广泛的研究,主要结果有:文献[2]中,Kühn 提出了对四轮 MISTY1 算法的切片攻击;文献[3]中,Kühn 提出了对四轮 MISTY1 算法的碰撞攻击和六轮不带 FL 层 MISTY1 算法的差分攻击;文献[4]中,Knudsen 和 Wagner 给出了四轮和五轮 MISTY1 算法的积分攻击;文献[5-6]中,提出了对 MISTY1 算法的高阶差分攻击,文献[7,8]中提出了六轮 MISTY1 算法的高阶差分攻击,同时,文献[8]中也给出了七轮 MISTY1 算法的高阶差分攻击;文献[9-10]中给出五轮和六轮 MISTY1 算法的不可能差分攻击;利用弱密钥,文献[11]给出了弱密钥下六轮 MISTY1 算法的高阶差分攻击;而加强对密钥的限制,文献[12]中提出了七轮 MISTY1 算法的相关密钥扩大飞来去器攻击。

通过仔细分析,我们找到了一个包含 2^{90} 个相关密钥的弱密钥类,在此基础上,构造了 MISTY1 算法的一个七轮相关密钥扩大飞来去器区分器,进一步实现了对不带最后 FL 层的 MISTY1 算法的八轮攻击。攻击需要 2^{63} 个选择明文,2^{70} 次八轮 MISTY1 算法加密。与文献[12]相比,本文放宽了攻击所需要的相关密钥的限制条件。表1 中给出了对 MISTY1 算法攻击结果的比较。

* **收稿日期**:2011-07-28
基金项目:国家自然科学基金重点资助项目(60833008);全军军事学研究生课题项目(61070178)
作者简介:陈少真(1967—),女,河南郑州人,教授,博士,博士生导师,E-mail: chenshaozhen@vip.sina.com

表 1 MISTY1 算法的主要攻击结果

Tab. 1 Summary of the attack on MISTY1

攻击	FL 层数	轮数	数据复杂度	计算复杂度
高阶差分攻击[11]	4	6	$2^{18.9}$ CP	$2^{80.6}$
高阶差分攻击[7]	4	6	$2^{53.7}$ CP	$2^{64.4}$
高阶差分攻击[8]	4	6	$2^{53.7}$ CP	$2^{53.7}$
不可能差分攻击[9]	4	6	2^{51} CP	$2^{123.4}$
相关密钥扩大飞来去器攻击[12](2^{-55})	3	7	2^{54} CP	$2^{55.3}$
高阶差分攻击[8]	4	7	$2^{54.1}$ KP	$2^{120.7}$
相关密钥扩大飞来去器攻击 (2^{-38})	4	8	2^{63} CP	2^{70}

注：CP——选择明文；KP——已知明文；2^{-55}和2^{-38}表示攻击中相关密钥存在的概率

1 MISTY1 算法和相关密钥扩大飞来去器攻击

1.1 MISTY1 算法

MISTY1 算法[1]是具有 Feistel 结构的分组加密算法，分组长度是 64 – bit，密钥长度是 128 – bit，轮数是 4 的倍数，实际上用的都是八轮 MSITY1 算法。MISTY1 算法轮函数包括一个输入输出为 32 比特的非线性混合函数 *FO* 和一个输入输出为 32 比特的线性混合函数 *FL*。

函数 *FO* 具有三轮 Feistel 结构，其中非线性混合函数是输入输出为 16 比特的函数 *FI*。而函数 *FI* 是由两个非线性的 *S* – 盒 *S*7 和 *S*9 构成的 3 轮 Feistel 结构（*S*7 是 7 进 7 出的置换，*S*9 是 9 进 9 出的置换）。在 MISTY1 算法每一轮中，函数 *FO* 总共用到 112 比特的子密钥——48 比特作用于函数 *FI* 中，64 比特作用于与函数 *FO* 中每一轮的状态异或。

函数 *FL* 是一个输入输出为 32 比特的线性函数，用到两个 16 比特的子密钥字。其中一个子密钥字用 OR 运算影响数据，另一个子密钥字用 AND 运算影响数据。图 1 给出了 MISTY1 算法和函数 *FO*，*FL* 和 *FI* 的框架。

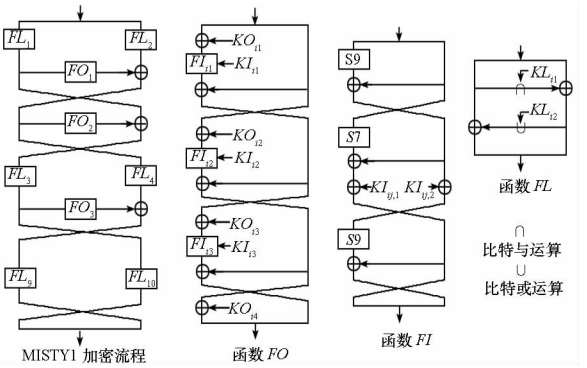

图 1 MISTY1 算法的结构框架

Fig. 1 Outline of MISTY1

MISTY1 算法密钥扩展算法首先将 128 比特种子密钥 K 划分成 8 个 16 比特的字，即 $K = (K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8)$。然后根据 $K'_i = FI_{K_{i+1}}(K_i)$ 生成另一组 8 个 16 比特的字 $K'_1, K'_2, K'_3, K'_4, K'_5, K'_6, K'_7, K'_8$。MISTY1 算法轮子密钥以表 2 的方式由 K_i 和 K'_i 生成。

表 2 MISTY1 的轮密钥生成方式

Tab. 2 The key schedule algorithm of MISTY1

轮密钥	KO_{i1}	KO_{i2}	KO_{i3}	KO_{i4}	KI_{i1}	KI_{i2}	KI_{i3}	$KL_{i1}\|\|KL_{i2}$	
密钥值	K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}	$K_{(i+1)/2}\|\|K'_{(i+1)/2+6}$	i 为奇数
								$K'_{i/2+2}\|\|K_{i/2+4}$	i 为偶数

注：本文中 K_i 的角标 i 均为模 8 的值

1.2 相关密钥扩大飞来去器攻击

相关密钥扩大飞来去器攻击联合使用相关密钥攻击[13-14]和扩大飞来去器攻击[15]，即在不同的、相关的密钥下运用扩大飞来去器攻击。它将分组长度为 n 的密码 E 看成两个子密码的联接 $E = E_1 \circ E_0$。设 $\alpha \to \beta$ 是 E_0 一个概率为 p 的相关密钥差分路径，$\gamma \to \delta$ 是 E_1 一个概率为 q 的相关密钥差分路径。密钥满足 $K_b = K_a \oplus \Delta K_{ab}$，$K_c = K_a \oplus \Delta K_{ac}$，$K_d = K_a \oplus \Delta K_{ab} \oplus \Delta K_{ac}$。由上述路径可构造相关密钥扩大飞来去器区分器（图 2）：

（1）随机选择 n 比特两个明文 P_a 和 P_c，计算另外两个明文 $P_b = P_a \oplus \alpha$ 和 $P_d = P_c \oplus \alpha$；

（2）在相应的密钥下加密得到对应的密文：$Z_a = E(K_a, P_a)$，$Z_b = E(K_b, P_b)$，$Z_c = Z(K_c, P_c)$，$Z_d = E(K_d, P_d)$；

（3）检验是否有 $Z_a \oplus Z_c = Z_b \oplus Z_d = \delta$ 成立。

对明文组（P_a, P_b, P_c, P_d）经过 E_0 加密后的中间值（Y_a, Y_b, Y_c, Y_d），$Y_a \oplus Y_b = Y_c \oplus Y_d = \beta$ 以概率 p^2 成立；由于明文 P_a 和 P_c 是随机选择的，$Y_a \oplus Y_c = \gamma$ 以概率 2^{-n} 成立；当上述两个事件发

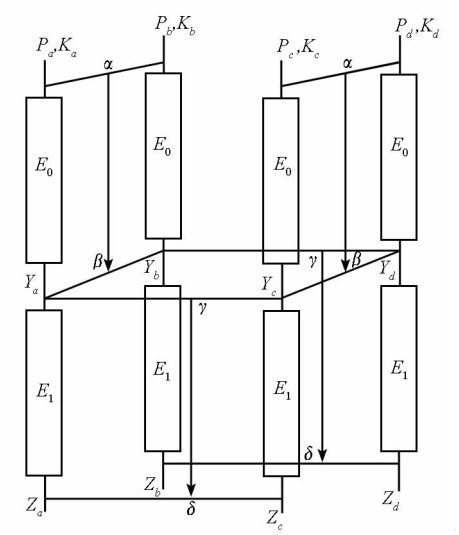

图 2　相关密钥扩大飞去来器攻击

Fig. 2　Related-key amplified boomerang attack

生时，$Y_b \oplus Y_d = \gamma$ 以概率 1 成立；对于中间值 (Y_a, Y_b, Y_c, Y_d) 经过 E_1 后得到密文 (Z_a, Z_b, Z_c, Z_d)，满足 $Z_a \oplus Z_c = Z_b \oplus Z_d = \delta$ 的概率是 q^2。综上，满足第(3)个检验的概率为 $p^2 \cdot q^2 \cdot 2^{-n}$。满足上述检验的四元组 (P_a, P_b, P_c, P_d) 称为正确四元组。

对于一个随机的密码，满足检测条件的概率为 2^{-2n}。若 $p^2 \cdot q^2 > 2^{-n}$ 成立，就可利用上述区分器将密码 E 与随机变换区分开，实现攻击。

2　MISTY1 算法的一类弱密钥

定义符号：$k = a^7 0^9, \beta = a^7 0^2 a^7$，其中 $a^7 = 0010000_2$，$0^t = \overbrace{0,\cdots,0}^{t}{}_2$，$t$ 为正整数；$(K)_j$ 表示 K 左起第 j 比特密钥，如：设 $K = 2000_x$，则 $(K)_3 = 1$。

假设 MISTY1 算法的 4 个 128 比特初始相关密钥 K_a，K_b，K_c，K_d 满足下列关系：

$$K_a = (K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8);$$
$$K_b = (K_1, K_2^*, K_3, K_4, K_5, K_6, K_7, K_8)$$
$$K_c = (K_1, K_2, K_3, K_4, K_5, K_6^*, K_7, K_8);$$
$$K_d = (K_1, K_2^*, K_3, K_4, K_5, K_6^*, K_7, K_8)$$

其中，$K_2 \oplus K_2{}^* = k$，$K_6 \oplus K_6^* = k$。由密钥扩展算法可生成相应的另外 4 个相关密钥：

$$K'_a = (K'_1, K'_2, K'_3, K'_4, K'_5, K'_6, K'_7, K'_8);$$
$$K'_b = (K'_1{}^*, K_2'^*, K'_3, K'_4, K'_5, K'_6, K'_7, K'_8)$$
$$K'_c = (K'_1, K'_2, K'_3, K'_4, K'^*_5, K'^*_6, K'_7, K'_8);$$
$$K'_d = (K'^*_1, K'^*_2, K'_3, K'_4, K'^*_5, K'^*_6, K'_7, K'_8)$$

其中，$K'_1 \oplus K'^*_1 = \beta$，$K'_2 \oplus K'^*_2 = k$，$K_5' \oplus K'^*_5 = \beta$，$K'_6 \oplus K'^*_6 = k$。再假设：

$(K_5)_3 = 1$，$(K_5)_{12} = 0$，$(K'_4)_3 = 0$，$(K_7)_3 = 1$，$(K_7)_{12} = 0$，$(K_8)_3 = 0$

称满足上述条件的相关密钥四元组为 MISTY1 算法的一个弱密钥类。这样的密钥四元组的概率是 2^{-38}（$= 2^{-16} \times 2^{-16} \times 2^{-6}$），这是因为(实验可验证)：

$$Pr[K'_1 \oplus K'^*_1 = \beta \mid K_2 \oplus K_2{}^* = k] = 1;$$
$$Pr[K'_2 \oplus K'^*_2 = k \mid K_2 \oplus K_2^* = k] = 2^{-16}$$
$$Pr[K'_5 \oplus K'^*_5 = \beta \mid K_6 \oplus K_6^* = k] = 1;$$
$$Pr[K'_6 \oplus K'^*_6 = k \mid K_6 \oplus K_6^* = k] = 2^{-16}$$

且 $Pr[(K_5)_3 = 1, (K_5)_{12} = 0, (K'_4)_3 = 0, (K_7)_3 = 1, (K_7)_{12} = 0, (K_8)_3 = 0] = 2^{-6}$。

上述的密钥类共有 2^{90}（$= 2^{128} \times 2^{-38}$）个相关密钥四元组。下面介绍一个实用性质：

性质 1　若 FI 输入差分为 k，密钥差分为 β，则它以概率 2^{-8} 输出为 0^{16}（对 $S9$，输入差分为 $a^7 0^2$，以概率 2^{-8} 输出 $0^2 a^7$，从而可以和密钥差分异或抵消，使函数 FI 输出差分为 0^{16}）。

3　八轮 MISTY1 算法的密钥恢复攻击

3.1　相关密钥差分路径

3.1.1　第一个相关密钥差分路径 E_0

选择密钥 K_a 和 K_b 满足密钥差分为 $\Delta K_{ab} = (0, k, 0, 0, 0, 0, 0, 0)$，$\Delta K'_{ab} = (\beta, k, 0, 0, 0, 0, 0, 0)$，同时假设给定 $(K_5)_3 = 1$，$(K_5)_{12} = 0$ 和 $(K'_4)_3 = 0$，则可构造第一个相关密钥差分路径（图 3）。

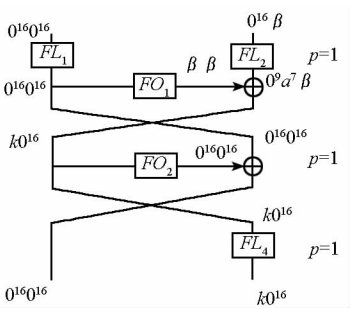

图 3　路径 E_0

Fig. 3　The path E_0

假设第 1 轮的输入差分为 $(0^{16}0^{16}, 0^{16}\beta)$。由 FL_1 的输入差分和子密钥差分为零，则其输出差分为 $0^{16}0^{16}$，即 FO_1 的输入差分为 $0^{16}0^{16}$，又因为除 $\Delta KI_{12} = k$ 外，FO_1 其余子密钥差分为零，FO_1 以概率 1 输出差分 $\beta\beta$；又由 $(KL_{22})_3 = (K_5)_3 = 1$ 且 $(KL_{22})_{12} = (K_5)_{12} = 0$，则当输入差分为 $0^{16}\beta$ 时，FL_2 以概率 1 输出差分 $0^9a^7\beta$，$0^9a^7\beta$ 与 FO_1 的输出差分 $\beta\beta$ 异或得到 FO_2 的输入差分 $k0^{16}$；又因为除 $\Delta KO_{21} = k$ 外，FO_2 其余子密钥差分为

零，FO_2 以概率 1 输出差分 $0^{16}0^{16}$；又 FL_4 的子密钥差分为零且$(KL_{41})_3=(K'_4)_3=0$，则输入差分为 $k\,0^{16}$的 FL_4 以概率为 1 输出差分 $k\,0^{16}$。

因此，可得路径：$(0^{16}0^{16}, 0^{16}\beta)\rightarrow(0^{16}0^{16}, k\,0^{16})$，概率为 $p=1$。

3.1.2 第二个相关密钥差分路径 E_1

选择密钥 K_a 和 K_c 满足密钥差分为 $\Delta K_{ac}=(0,0,0,0,0,k,0,0)$，$\Delta K'_{ac}=(0,0,0,0,\beta,k,0,0)$，同时假设给定$(K_7)_3=1$，$(K_7)_{12}=0$ 和$(K_8)_3=0$，则可构造第二个相关密钥差分路径（图 4）。

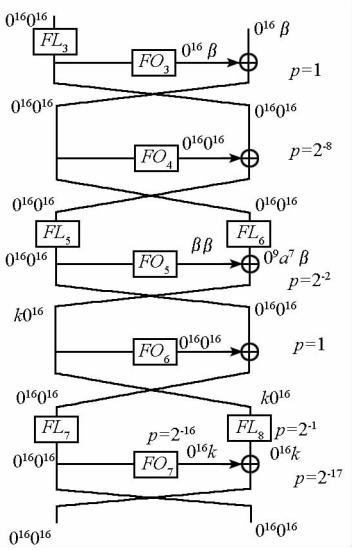

图 4 路径 E_1

Fig. 4 The path E_1

在第 3 轮中，输入差分为$(0^{16}0^{16}, 0^{16}\beta)$。由 FL_3 的输入差分和子密钥差分为零，则其输出差分为 $0^{16}0^{16}$，即 FO_3 的输入差分为 $0^{16}0^{16}$；又因为除 $\Delta KI_{33}=k$ 外，FO_3 其余子密钥差分为零，FO_3 以概率 1 输出差分 $0^{16}\beta$。FO_3 的输出差分 $0^{16}\beta$ 与右半部分输入差分 $0^{16}\beta$ 异或后的差分是 $0^{16}0^{16}$。所以第 3 轮的输出差分为$(0^{16}0^{16}, 0^{16}0^{16})$，即为第 4 轮的输入差分。

在第 4 轮中，FO_4 的输入差分为 $0^{16}0^{16}$，且除 $\Delta KO_{42}=k$ 和 $\Delta KI_{42}=\beta$ 外，FO_4 其余子密钥差分为零，则由性质 1 可知，FO_4 以概率为 2^{-8}使输出差分为 $0^{16}0^{16}$。所以第 4 轮的输出差分为$(0^{16}0^{16}, 0^{16}0^{16})$，即为第 5 轮的输入差分。

在第 5 轮中，FL_5 的输入差分和子密钥差分为零，则 FL_5 的输出差分为 $0^{16}0^{16}$，即为 FO_5 的输入差分；又因为除 $\Delta KI_{52}=k$ 外，FO_5 其余子密钥差分为零，FO_5 以概率 1 输出差分 $\beta\,\beta$。由于 $\Delta KL_{61}=\beta$，则当输入差分为 $0^{16}0^{16}$时，FL_6 以概率 2^{-2}使它的右半部分输出差分为 β，又$(KL_{62})_3=(K_7)_3=1$ 且$(KL_{62})_{12}=(K_7)_{12}=0$，则 FL_6 的左半部分输出差分为 0^9a^7，即 FL_6 以概率 2^{-2}输出差分 $0^9a^7\beta$。FL_6 的输出差分 $0^9a^7\beta$ 与 FO_5 的输出差分 $\beta\,\beta$ 异或后得到和差分为 $k\,0^{16}$。所以第 5 轮的输出差分为$(k\,0^{16}, 0^{16}0^{16})$，即为第 6 轮的输入差分。

在第 6 轮中，FO_6 的输入差分为 $k\,0^{16}$，且除 $\Delta KO_{61}=k$ 外，FO_6 其余子密钥差分为零，当输入差分为 $k\,0^{16}$时，FO_6 以概率 1 输出差分 $0^{16}0^{16}$。所以第 6 轮的输出差分为 $(0^{16}0^{16}, k\,0^{16})$，即为第 7 轮的输入差分。

在第 7 轮中，FL_7 的输入差分和子密钥差分为零，则 FL_7 的输出差分为 $0^{16}0^{16}$，即为 FO_7 的输入差分；又因为除 $\Delta KO_{73}=k$ 外，FO_7 其余子密钥差分为零，由实验可知 FO_7 以概率 2^{-16}输出差分 $0^{16}k$。又$(KL_{82})_3=(K_8)_3=0$ 且 $\Delta KL_{81}=k$，则当输入差分为 $k\,0^{16}$时，FL_8 以概率 2^{-1}输出差分为 $0^{16}k$。FL_8 的输出差分 $0^{16}k$ 与 FO_7 的输出差分 $0^{16}k$ 异或得到的差分为 $0^{16}0^{16}$。所以第 7 轮的输出差分为$(0^{16}0^{16}, 0^{16}0^{16})$。

因此，可得路径：$(0^{16}0^{16}, 0^{16}\beta)\rightarrow(0^{16}0^{16}, 0^{16}0^{16})$，概率为 $q=2^{-1}\times2^{-16}\times2^{-2}\times2^{-8}=2^{-27}$。

3.2 七轮相关密钥扩大飞来去器区分器

我们把七轮 MISTY1 算法看成两个子算法的连接：$E=E_1\circ E_0$（如图 3 和图 4），其中 E_0 是 3.1.1 节中以概率 1 成立的相关密钥差分路径$(0^{16}0^{16}, 0^{16}\beta)\rightarrow(0^{16}0^{16}, k\,0^{16})$，$E_1$ 是 3.1.2 节中以概率 2^{-27}成立的相关密钥差分路径 $(0^{16}0^{16}, 0^{16}\beta)\rightarrow(0^{16}0^{16}, 0^{16}0^{16})$。其中，相关密钥四元组 K_a，$K_b=K_a\oplus\Delta K_{ab}$，$K_c=K_a\oplus\Delta K_{ac}$，$K_d=K_a\oplus\Delta K_{ab}\oplus\Delta K_{ac}$满足：

$$\Delta K_{ab}=\Delta K_{cd}=(0,k,0,0,0,0,0,0)$$
$$\Delta K'_{ab}=\Delta K'_{cd}=(\beta,k,0,0,0,0,0,0)$$
$$\Delta K_{ac}=\Delta K_{bd}=(0,0,0,0,0,k,0,0)$$
$$\Delta K'_{ac}=\Delta K'_{bd}=(0,0,0,0,\beta,k,0,0)$$

且$(K_5)_3=1$，$(K_5)_{12}=0$，$(K'_4)_3=0$，$(K_7)_3=1$，$(K_7)_{12}=0$，$(K_8)_3=0$。

此时，相关密钥扩大飞来去器区分器的概率是 $1\times(2^{-27})^2\times2^{-64}=2^{-118}$，优于随机置换的概率 2^{-128}。攻击中，选取 2^{61}对明文(P_a, P_b)和 2^{61}对明文(P_c, P_d)，得到 2^{122}个四元组，则攻击最终期望得到正确四元组的个数是$(2^{61})^2\times2^{-118}=2^4$。

3.3　八轮 MISTY1 算法的密钥恢复攻击

攻击步骤如下:

(1)选择 2^{61} 个明文对(P_a, $P_b = P_a \oplus 0^{48}\beta$)和 2^{61} 个明文对(P_c, $P_d = P_c \oplus 0^{48}\beta$),分别用 K_a, K_b, K_c 和 K_d 加密得到密文四元组(C_a, C_b, C_c, C_d);

(2)此时有 2^{122} 个四元组。根据相关密钥扩大飞来去器区分器,检测 $C_a^R \oplus C_c^R = 0^{32}$ 和 $C_a^R \oplus C_c^R = 0^{32}$ 是否成立,不成立的去掉,则保留下四元组个数为 $2^{122} \times 2^{-32} \times 2^{-32} = 2^{58}$;

(3)分析剩下的四元组:

(a)由 FI_{81} 的输入差分为 0^{16} 且 $\Delta KI_{81} = \beta$,则可知 FI_{81} 左 7 比特输出差分为 a^7;又由 FI_{82} 的输入差分为 0^{16} 且子密钥差分为零,则可知 FI_{82} 的输出差分为 0^{16};从而可得到 FO_8 的 7 比特输出差分是 a^7,检测是否与 $C_a{}^L \oplus C_c{}^L$ 和 $C_b{}^L \oplus C_d{}^L$ 的相应位符合①,不符合的去掉;

(b)猜测 KO_{81}($KO_{81} = K_8$ 只需猜测 15bits, $(K_8)_3 = 0$)和 $KI_{81,2}$,则可计算 FI_{81} 右 9 比特输出差分;又由 FI_{82} 的输出差分为 0^{16},则可计算 FO_8 的 9 比特输出差分,检测是否与 $C_a^L \oplus C_c^L$ 和 $C_b^L \oplus C_d^L$ 的相应位符合,不符合的去掉;

(c)再猜测 $KI_{81,1}$ 和 KO_{83}($KO_{83} = K_7$ 只需猜测 14bits, $(K_7)_3 = 1$, $(K_7)_{12} = 0$),则可计算 FI_{83} 左 7 比特的输出差分;又由(a)可计算 FO_8 的 7 比特输出差分,检测是否与 $C_a^L \oplus C_c^L$ 和 $C_b^L \oplus C_d^L$ 的相应位符合,不符合的去掉;

(d)再猜测 $KI_{83,2}$,则可计算 FI_{83} 右 9 比特的输出差分;由(b)可计算 FO_8 的 9 比特输出差分,检测是否与 $C_a^L \oplus C_c^L$ 和 $C_b^L \oplus C_d^L$ 的相应位符合,不符合的去掉;若剩下的密文组个数大于等于 10 个,则认为对应的密钥猜是正确的密钥猜测;否则重复(d)。

攻击的成功率可由泊松分布计算。对于错误的密钥猜测,剩余的数据约为 2^{-6},由泊松分布,剩余数据大于 10 的概率小于 2^{-85}, $X \sim Poi(\lambda = 2^{-6})$, $Pr[X \geqslant 10] < 2^{-85}$,因此输出一个错误的密钥猜测概率是非常小的。又由所构造的七轮相关密钥扩大飞来去器区分器可知,对于正确的密钥猜测,大约有 $2^{122} \times 2^{-118} = 2^4$ 个数据剩余,由泊松分布,剩余数据的个数大于 10 的概率是 0.93, $Y \sim Poi(\lambda = 2^4)$, $Pr[Y \geqslant 10] \approx 0.93$。

综上,该攻击需要 $2^{61} \times 4 = 2^{63}$ 个选择明文,计算复杂度是 2^{70},成功概率约是 0.93。

4　总　结

分组密码算法轮函数抵抗差分分析和线性分析是必须具备的安全性质之一,同时,密钥扩展算法也应具有较好的安全性质。本文通过对 MISTY1 算法密钥扩展算法的分析,找到特殊的弱密钥类,从而构造了 MISTY1 的一个七轮相关密钥扩大飞来去器区分器,实现对 MISTY1 算法的八轮攻击。攻击所需要的数据量是 2^{63} 个选择明文,攻击所需要的计算复杂度是 2^{70}。本文攻击也是第一个对不带最后线性函数 *FL* 层的 MISTY1 算法的八轮攻击。

参考文献(References)

[1] Matsui M. New block encryption algorithm MISTY1 [C]// Proc of FSE'97, Berlin: Springer-Verlag, 1997: 64 - 67.

[2] Kühn U. Improved cryptanalysis of MISTY1 [C]// Proc of FSE'02. Berlin: Springer-Verlag, 2002: 61 - 75.

[3] Kühn U. Cryptanalysis of reduced-round MISTY1 [C] // Proc of EUROCRYPT'01, Berlin: Springer-Verlag, 2001: 325 - 339.

[4] Knudsen L R, Wagner D. Integral cryptanalysis [C] // Proc of FSE'02, Berlin: Springer-Verlag, 2002: 112 - 127.

[5] Sugita M. Higher order differential attack of block cipher MISTY1 [R]. IEICE Technical Report, ISEC 98 - 4, 1998.

[6] Babbage S, Frisch L. On MISTY1 higher order differential cryptanalysis [C]// Proc of ICISC'00, Berlin: Springer-Verlag, 2001: 22 - 36.

[7] Tsunoo Y, Saito T, Nakashima H, et al. Higher order differential attack on 6-round MISTY1 [R]. IEICE Transactions 92 - A (1), 2009.

[8] Tsunoo Y, Saito T, Shigeri M, et al. Higher order differential attacks on reduced-round MISTY1 [C] // Proc of ICISC'08, Berlin: Springer-Verlag, 2009: 415 - 431.

[9] Lu J, Kim J, Keller N, et al. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1 [C]// Proc of CT-RSA'08, Berlin: Springer-Verlag, 2008: 370 - 386.

[10] Dunkelman O, Keller N. An improved impossible differential attack on MISTY1 [C] // Proc of ASIACRYPT'08, Berlin: Springer-Verlag, 2008: 441 - 454.

[11] Tanaka H, Hatano Y, Sugio N, et al. Security analysis of MISTY1 [C]// Proc of WISA'07, Berlin: Springer-Verlag, 2008: 215 - 226.

[12] Lee E, Kim J, Hong D, et al. Weak-key classes of 7-round MISTY1 and 2 for related-key amplified boomerang attack [J]. IEICE Transaction 91-A(2), 2008: 642 - 649.

[13] Biham E. New types of cryptanalytic attack using related keys [J]. Journal of Cryptology, 1994, 7(4): 229 - 246.

[14] Knudsen L R. Cryptanalysis of LOKI91 [C] // Proc of Auscrypt'92, Berlin: Springer-Verlag, 1993: 196 - 208.

[15] Kelsey J, Scheneier B, Kohno T. Amplified boomerang attacks against reduced round MARS and Serpent [C]// Proc of FSE'00, Berlin: Springer-Verlag, 2000: 75 - 93.

① 这里是密文差分与区分器输出差分的异或: $C_a^L \oplus C_c^L \oplus 0^{32}$ 和 $C_b^L \oplus C_d^L \oplus 0^{32}$,简记为 $C_a^L \oplus C_c^L$ 和 $C_b^L \oplus C_d^L$.