密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2022, 9(4): 755–766

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

AES 和 PRINCE 的 6 轮混合差分攻击*

谭 林, 闫雪萍, 戚文峰

战略支援部队信息工程大学, 郑州 450001
通信作者: 谭林, E-mail: tanlin100@163.com

摘 要: AES 是目前使用最广泛的分组密码, PRINCE 是一个具有 AES 相似结构的低时延轻量级密码算法. 混合差分分析是 Grassi 提出的针对 AES 的一种新型密码分析技术. 目前, AES 最好的 5 轮、6 轮区分攻击和 5 轮密钥恢复攻击都与混合差分技术有很大关系. 在 2018 年美密会和 2020 年 Journal of Cryptology 上, Bar-On 等给出了具有实际数据和存储复杂度的 6 轮 AES-128 的混合差分密钥恢复攻击, 时间复杂度为 2^{73}. 本文通过对密文差分增设条件限制来提高混合差分攻击中 Good Pair 出现的概率, 以适当提升数据和存储复杂度为代价, 改进了 6 轮 AES-128 混合差分攻击的时间复杂度, 使得总复杂度为 $2^{62.62}$. 此外, 本文将改进的 6 轮混合差分攻击应用于 PRINCE 和 $\text{PRINCE}_{\text{core}}$, 给出了总复杂度分别为 $2^{30.66}$ 和 2^{22} 的密钥恢复攻击, 其中 6 轮 $\text{PRINCE}_{\text{core}}$ 的攻击结果优于积分攻击和差分攻击.

关键词: AES; PRINCE; 混合结构; 混合差分分析

中图分类号: TN918.1 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000547

中文引用格式: 谭林, 闫雪萍, 戚文峰. AES 和 PRINCE 的 6 轮混合差分攻击[J]. 密码学报, 2022, 9(4): 755–766. [DOI: 10.13868/j.cnki.jcr.000547]

英文引用格式: TAN L, YAN X P, QI W F. Mixture differential attacks on 6 rounds of AES and PRINCE[J]. Journal of Cryptologic Research, 2022, 9(4): 755–766. [DOI: 10.13868/j.cnki.jcr.000547]

Mixture Differential Attacks on 6 Rounds of AES and PRINCE

TAN Lin, YAN Xue-Ping, QI Wen-Feng

Strategic Support Force Information Engineering University, Zhengzhou 450001, China
Corresponding Author: YAN Xue-Ping, E-mail: tanlin100@163.com

Abstract: AES is the most widely used block cipher currently, and PRINCE is a low-latency and lightweight cipher with AES-like structure. Mixture differential cryptanalysis proposed by Grassi is a new cryptanalysis technology for AES. At present, the best distinguishers on 5 and 6 rounds of AES as well as the best key recovery attacks on 5 rounds of AES are all closely related to mixture differential cryptanalysis. At CRYPTO 2018 and in Journal of Cryptology 2020, Bar-On et al. proposed mixture differential attacks on 6 rounds of AES-128 with time complexity of 2^{73} and practical data and memory complexities. This paper adds restrictions to ciphertext differentials to increase the probability of Good Pair in mixture differential attacks. At the expense of increasing data and memory complexities reasonably, the time complexity of mixture differential attack on 6 rounds of AES is improved, leading to the overall complexity of $2^{62.62}$. In addition, this paper applies the improved mixture differential

* 基金项目: 国家密码发展基金 (MMJJ20180204, MMJJ20170103)
Foundation: National Cryptography Development Fund of China (MMJJ20180204, MMJJ20170103)
收稿日期: 2021-10-12 定稿日期: 2022-05-13

attack on 6 rounds of PRINCE and $\text{PRINCE}_{\text{core}}$, and presents the key recovery attacks with overall complexities of $2^{30.66}$ and 2^{22} respectively. The mixture differential attack on 6 rounds of $\text{PRINCE}_{\text{core}}$ is better than the integral attack and the differential attack.

Key words: AES; PRINCE; mixture; mixture differential cryptanalysis

1 引言

高级加密标准 AES [1] 是目前使用最多、研究最多的分组密码算法. 许多密码算法、Hash 函数和伪随机数发生器采用类似 AES 的结构来设计, 甚至直接采用减轮 AES 作为核心部件. 从 AES 提出至今二十多年来, 学者们进行了大量密码分析研究. 虽然未对 AES 产生实际的威胁, 但学术界持续的研究促进了人们对 AES 密码结构性质的认识和 AES 型密码分析技术的发展. 对 AES 主要的密码分析技术有: 积分 [1,2]、不可能差分 [3–6]、零相关线性 [7–10]、子空间路径 [11]、混合差分 [12–16]、yoyo [17]、交换攻击 [18]、飞镖 [19]、中间相遇攻击 [20] 等. 2016 年以前, 针对 AES 的区分攻击最多只到 4 轮, 包括经典的积分、不可能差分和零相关线性等. 利用 AES 列混合矩阵的特点, 文献 [9,10,21] 给出了密钥相关的 5 轮区分器. 在 2017 年欧密会上, Grassi 等人 [16] 发现了 5 轮 AES 具有 “8 的倍数” 结构性差分特征, 首次给出了 5 轮 AES 与密钥独立的区分器. 文献 [22] 给出了 “8 的倍数” 结构性差分特征的一般化证明. 该特征揭示了 5 轮 AES 具有结构性的不随机性, 基于此, 文献 [12] 提出了针对 AES 的混合差分分析. 在 2017 年亚密会上, Rønjom 等人 [17] 将 yoyo 技术应用于 SPN 型密码分析, 给出了首个与密钥独立的 6 轮 AES 区分器. Yoyo 技术与混合差分具有很强的关联性, 文献 [23] 指出了 AES 的 4 轮 yoyo 区分器等价于广义混合差分区分器. 文献 [14,15] 利用混合差分技术给出了减轮 AES 的具有实际数据和存储复杂度的攻击方案. 其中, 5 轮 AES-128 的混合差分攻击的复杂度为 2^{24}, 这是目前选择明文模式下 5 轮 AES 密钥恢复攻击的最好结果. 在 2019 年亚密会上, Bardeh 等人 [18] 将混合差分、yoyo 等技术与概率分析方法相结合, 给出了首个选择明文模式下的 6 轮 AES 区分器, 这是目前为止对 AES 区分分析的最好结果. 在 2020 年欧密会上, Dunkelman 等人 [19] 基于混合差分技术提出 “折回镖” 攻击, 给出了适应性选择明密文模式下 5 轮 AES 密钥恢复攻击的最好结果. 本文在文献 [14,15] 的基础上, 适当地提升数据和存储复杂度, 改进了 6 轮 AES 混合差分攻击的时间复杂度, 使得总复杂度为 $2^{62.62}$. 在本文中, 总复杂度是指数据复杂度、时间复杂度和存储复杂度的最大值. 表 1 给出了目前 5 轮以上 AES-128 密钥恢复攻击的主要结果, 数据复杂度中 ACC 表示适应性选择明密文, 其余是选择明文.

表 **1** 5 轮以上 AES-128 密钥恢复攻击主要结果

Table 1 Key recovery attacks on 5 and more rounds of AES-128

轮数	攻击技术	数据复杂度	时间复杂度	存储复杂度	参考文献
5	混合差分	2^{24}	2^{24}	$2^{21.5}$	[14]
	折回镖	2^{15} ACC	$2^{16.5}$	2^{9}	[19]
6	积分	$2^{34.6}$	2^{44}	2^{32}	[2]
	不可能差分	$2^{114.5}$	2^{46}	2^{45}	[4]
		$2^{75.5}$	2^{104}	2^{45}	[4]
	混合差分	$2^{72.8}$	2^{105}	2^{33}	[13]
		$2^{27.5}$	2^{81}	$2^{27.5}$	[14]
		$2^{30.5}$	2^{73}	$2^{30.5}$	[14]
		2^{26}	2^{80}	2^{35}	[15]
		$2^{44.42}$	$2^{62.62}$	$2^{44.42}$	本文第 3.2 节
7	中间相遇	2^{97}	2^{99}	2^{98}	[20]
	不可能差分	$2^{104.9}$	$2^{110.9}$	$2^{71.9}$	[6]

PRINCE [24] 是 Borghoff 等在 2012 年亚密会上提出的一种 AES-like 低时延轻量级分组算法, 适用于物联网环境下的加密. 它基于 FX 结构设计, 采用 α 反射技术, 加解密具有对称性, 在硬件实现上具有优势. 2014 年 PRINCE 的设计者发起了针对该算法实际攻击的公开挑战, 使其成为研究的热点. 对 PRINCE 主要的密码分析技术有: 积分 [25–27]、差分 [28,29]、截断差分 [26,30]、多重差分 [23,31]、高阶差分 [25]、中间相遇 [28,32] 等. 目前, PRINCE 的密钥恢复攻击最长的是 10 轮多重差分攻击 [31] 和 10 轮中间相遇攻击 [28,32]. 由于 PRINCE 具有 AES-like 结构, 针对 AES 的许多分析技术可以直接应用于 PRINCE 和 PRINCE$_{\rm core}$ 的分析. 文献 [23] 将混合差分攻击技术应用于 PRINCE, 给出了 5 轮 PRINCE$_{\rm core}$ 的混合差分密钥恢复攻击. 本文将改进的 6 轮 AES 混合差分攻击应用到 6 轮的 PRINCE 和 PRINCE$_{\rm core}$, 给出了总复杂度分别为 $2^{30.66}$ 和 2^{22} 的密钥恢复攻击, 其中 6 轮 PRINCE$_{\rm core}$ 的攻击结果优于积分攻击和差分攻击. 表 2 给出了目前 6 轮以上 PRINCE 和 PRINCE$_{\rm core}$ 的密钥恢复攻击的主要结果.

表 **2** 6 轮以上 PRINCE 和 PRINCE$_{\rm core}$ 密钥恢复攻击主要结果

Table 2 Key recovery attacks on 6 and more rounds of PRINCE and PRINCE$_{\rm core}$

算法	轮数	攻击技术	数据复杂度	时间复杂度	存储复杂度	参考文献
PRINCE	6	积分	2^{13}	$2^{24.6}$	2^{13}	[25]
		积分	$2^{18.58}$	2^{41}	2^{16}	[26]
		中间相遇	2^{16}	$2^{33.7}$	$2^{31.9}$	[28]
		差分	$2^{14.9}$	$2^{25.1}$	$2^{14.9}$	[28]
		混合差分	2^{23}	$2^{30.66}$	2^{23}	本文第 4.2 节
	7	高阶差分	2^{33}	$2^{44.3}$	2^{33}	[25]
		中间相遇	2^{53}	2^{60}	2^{30}	[32]
	8	中间相遇	2^{16}	$2^{66.25}$	$2^{49.9}$	[28]
		多重差分	$2^{61.89}$	$2^{19.68}$	$2^{15.21}$	[23]
	9	多重差分	$2^{46.9}$	$2^{51.2}$	$2^{52.2}$	[31]
	10	多重差分	$2^{57.9}$	$2^{60.6}$	$2^{61.5}$	[31]
		中间相遇	2^{57}	2^{68}	2^{41}	[28]
PRINCE$_{\rm core}$	6	积分	2^{16}	2^{30}	2^{16}	[27]
		差分	2^{48}	$2^{56.26}$	2^{48}	[29]
		混合差分	2^{16}	2^{22}	2^{16}	本文第 4.3 节
	8	中间相遇	2^{53}	2^{53}	2^{28}	[32]

2 准备工作

在 AES 和 PRINCE 算法中, 通常将明文、密文、轮密钥以及中间状态用 4×4 的矩阵来描述, 元素顺序如图 1 所示. 记 $\mathrm{col}(i)$ 表示矩阵的第 i 列, $\mathrm{SR}(\mathrm{col}(i))$ 表示矩阵的第 i 条反对角线, $\mathrm{SR}^{-1}(\mathrm{col}(i))$ 表示矩阵的第 i 条对角线, $i=0,1,2,3$. 对矩阵 X, 记 $X_{\{i_1,i_2,\cdots,i_n\}}$ 表示 X 的第 $i_1,i_2,\cdots,i_n$ 个元素, $X_{\mathrm{col}(i_1,i_2,\cdots,i_n)}$ 表示 X 的第 $i_1,i_2,\cdots,i_n$ 列. X 的对角线和反对角线采用相似的方式表示.

文献 [12] 提出了明文混合结构的概念并应用于减轮 AES 的混合差分分析, 文献 [15] 给出了混合结构和混合四元组更一般的定义.

定义 1 [15] 设 X_1,X_2,X_3,X_4 是四个 4×4 的矩阵, 它们仅在第 j 列的值不同, $0\le j\le 3$.

0	4	8	12
1	5	9	13
2	6	10	14
3	7	11	15

图 1 状态矩阵元素顺序
Figure 1 Order of elements in state matrix

如果对于每个 $i \in \{0,1,2,3\}$, 四元组 $(X_{1,4j+i}, X_{2,4j+i}, X_{3,4j+i}, X_{4,4j+i})$ 由两个相同的对组成, 则称 (X_1, X_2, X_3, X_4) 是一个混合四元组, 称 (X_3, X_4) 是 (X_1, X_2) 的一个混合结构.

例如,

$$X_1 = \begin{bmatrix} x_1^1 & y^1 & z^1 & w^1 \\ x_1^2 & y^2 & z^2 & w^2 \\ x_1^3 & y^3 & z^3 & w^3 \\ x_1^4 & y^4 & z^4 & w^4 \end{bmatrix}, X_2 = \begin{bmatrix} x_2^1 & y^1 & z^1 & w^1 \\ x_2^2 & y^2 & z^2 & w^2 \\ x_2^3 & y^3 & z^3 & w^3 \\ x_2^4 & y^4 & z^4 & w^4 \end{bmatrix},$$

和

$$X_3 = \begin{bmatrix} x_2^1 & y^1 & z^1 & w^1 \\ x_1^2 & y^2 & z^2 & w^2 \\ x_1^3 & y^3 & z^3 & w^3 \\ x_1^4 & y^4 & z^4 & w^4 \end{bmatrix}, X_4 = \begin{bmatrix} x_1^1 & y^1 & z^1 & w^1 \\ x_2^2 & y^2 & z^2 & w^2 \\ x_2^3 & y^3 & z^3 & w^3 \\ x_2^4 & y^4 & z^4 & w^4 \end{bmatrix},$$

构成混合四元组, 其中 $x_1^i \neq x_2^i$, $i = 1,2,3,4$.

引理 1 设 $\mathbb{F}_2^s$ 是 s 比特的向量空间, X_1, X_2 是元素取自 $\mathbb{F}_2^s$ 的 4×4 矩阵, 它们仅在第 j 列的值不同, $0 \leq j \leq 3$, 则 (X_1, X_2) 的混合结构 (X_3, X_4) 的个数形如 $8n-1$, 这里 n 为正整数.

证明: 如果对所有 $i \in \{0,1,2,3\}$, $X_{1,4j+i} \neq X_{2,4j+i}$, 则 (X_3, X_4) 只能通过交换 (X_1, X_2) 第 j 列的 1 个或者 2 个元素构造, 故有 $\binom{4}{1} + \binom{4}{2}/2 = 7$ 个. 如果只有一个 $i \in \{0,1,2,3\}$ 使得 $X_{1,4j+i} = X_{2,4j+i}$, 则 (X_3, X_4) 可以通过以下两种方式构造: (1) 交换 (X_1, X_2) 第 j 列三个不同元素中的任意一个, 且令 $X_{3,4j+i} = X_{4,4j+i}$ 取 $\mathbb{F}_2^s$ 中任意值; (2) 令 $X_{3,4j+i} = X_{4,4j+i}$ 取 $\mathbb{F}_2^s$ 中除 $X_{1,4j+i}$ 之外的任意值, 在其余位置上 (X_3, X_4) 与 (X_1, X_2) 相同. 这样的 (X_3, X_4) 共有 $(2^s - 1) + \binom{3}{1} \times 2^s = 2^{s+2} - 1$ 个. 相似地, 如果 (X_1, X_2) 第 j 列有两个元素相同, 则 (X_3, X_4) 共有 $(2^{2s} - 1) + 2^{2s} = 2^{2s+1} - 1$ 个. 如果 (X_1, X_2) 第 j 列有三个元素相同, 则 (X_3, X_4) 有 $2^{3s} - 1$ 个. 由于 $s \geq 1$, 所以 (X_1, X_2) 的混合结构 (X_3, X_4) 的个数形如 $8n-1$, 其中 n 为正整数. □

3 AES 的 6 轮混合差分攻击

3.1 AES 简介与 4 轮混合差分区分器

AES 算法的分组长度为 128 比特, 密钥长度支持 128、192 和 256 比特, 相应的迭代轮数分别为 10、12 和 14, 分别用 AES-128、AES-192 和 AES-256 来表示. 轮变换包括以下 4 个操作:

- 字节替换 (SB): 状态矩阵的每个字节查询同一个 8 比特的 S 盒.
- 行移位 (SR): 将状态矩阵的第 i 行循环左移 i 个字节, 其中 $i = 0,1,2,3$.
- 列混合 (MC): 用 $\mathbb{F}_{2^8}$ 上一个 MDS 矩阵乘以状态矩阵的每一列.
- 轮密钥加 (AK): 将状态与轮密钥逐比特异或.

AES 算法中明文先与主密钥异或, 再进行相应的轮变换, 最后一轮没有 MC. 关于 AES 详细的介绍参见文献 [1]. 记 K_r 表示第 r 轮轮密钥, 它由主密钥 K_0 通过密钥扩展算法产生. 记 $R = \mathrm{AK} \circ \mathrm{MC} \circ \mathrm{SR} \circ \mathrm{SB}$

表示 AES 的轮函数, 和绝大多数文献一样, 用 R^n 表示 n 轮 AES, 最后一轮没有 MC. 本文的研究对象是 6 轮 AES-128.

在文献 [12] 中, Grassi 发现了明文混合结构经过 4 轮 AES 后保持差分的某种关联性, 由此构造了 4 轮混合差分区分器.

定理 1 [12] 设 (X_1, X_2, X_3, X_4) 是 AES 算法中一个混合四元组, 则 $(R^4(X_1)+R^4(X_2))_{\mathrm{SR}(\mathrm{col}(i))} = 0$ 当且仅当 $(R^4(X_3) + R^4(X_4))_{\mathrm{SR}(\mathrm{col}(i))} = 0$, $i \in \{0, 1, 2, 3\}$.

在 4 轮 AES 混合差分区分器的基础上往前增加一轮, 文献 [16] 给出了首个与密钥独立的 5 轮 AES 区分器 "8 的倍数". 选择第 0 条对角线遍历、其余 12 字节取任意固定值的 2^{32} 个明文, 经过 1 轮后状态仅在第一列活跃. 对任意的状态对 (X_1, X_2), 存在 $8n-1$ 个对 (X_3, X_4) 与其构成混合四元组, 所以密文差分在任意反对角线为 0 的密文对个数是 8 的倍数. 文献 [12] 基于 4 轮 AES 的混合差分区分器给出了 5 轮密钥恢复攻击, 其猜测 K_0 的某条对角线, 在第一轮 MC 后构造混合四元组, 利用定理 1 来判断猜测密钥的正确性, 恢复全部密钥的复杂度为 2^{34}. Bar-On 等人 [14,15] 利用更少的混合结构和预处理表等技术进一步改进了 5 轮 AES 的混合差分攻击, 总复杂度为 2^{24}. 在 5 轮混合差分攻击的基础上往后增加一轮, Bar-On 等也给出了具有实际数据和存储复杂度的 6 轮混合差分攻击, 数据、存储复杂度均为 $2^{30.5}$, 时间复杂度为 2^{73}. 本节在文献 [14,15] 的基础上, 适当地提升数据和存储复杂度, 改进了 6 轮 AES 混合差分攻击的时间复杂度, 使得总复杂度为 $2^{62.62}$.

3.2 改进 6 轮 AES 混合差分攻击的时间复杂度

交换第 5 轮的 AK 和 MC, 用等效的轮密钥加 AK′ 来表示, 6 轮 AES 加密过程如图 2 所示. 记第 1 轮 MC 后的状态为 X, 第 5 轮 MC 后的状态为 W, $Z = \mathrm{MC}^{-1}(W)$. 我们选择第 0 条对角线遍历、其余 12 字节取任意固定值的明文结构, 每个结构约有 2^{63} 个明文对. 猜测 K_0 的第 0 条对角线 $K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}$, 在状态 X 处构造混合四元组 (X_1, X_2, X_3, X_4). 由于 AK 操作不改变混合结构关系, 由定理 1, 如果存在某个 $i \in \{0, 1, 2, 3\}$ 使得 $(Z_1 + Z_2)_{\mathrm{SR}(\mathrm{col}(i))} = 0$, 则 $(Z_3 + Z_4)_{\mathrm{SR}(\mathrm{col}(i))} = 0$. 猜测第 6 轮部分轮密钥, 解密至状态 Z, 利用 4 轮区分器对猜测密钥进行筛选. 文献 [15] 称满足存在 $i \in \{0, 1, 2, 3\}$ 使得 $(Z_1 + Z_2)_{\mathrm{SR}(\mathrm{col}(i))} = 0$ 的明文对 (P_1, P_2) 为 Good Pair. 筛选密钥需要至少有一对 Good Pair, 平均意义下找到一个 Good Pair 的概率为 $4 \times 2^{-32} = 2^{-30}$, 所以每次密钥猜测需要对至少 2^{30} 个明文对进行部分加密和解密. 我们对密文对施加限制条件来提高找到 Good Pair 的概率. 选择密文差分有两条反对角线为 0 的密文对 (C_1, C_2), 例如 $(C_1 + C_2)_{\mathrm{SR}(\mathrm{col}(2,3))} = 0$, 则 $(Z_1 + Z_2)_{\mathrm{col}(2,3)} = 0$, 从而 Good Pair 存在的概率为 $2^{-16} \times 4 = 2^{-14}$. 这样, 对每次密钥猜测所要进行操作的数据对从 2^{30} 降低到 2^{14}, 改进了筛选密钥的计算复杂度, 付出的代价是为了找到满足密文差分条件的密文对需要增加数据复杂度. 为获得满足条件的 2^{14} 个数据对, 需要 2^{15} 个明文结构. 下面详细介绍我们 6 轮 AES 混合差分攻击的流程.

(1) 选择 2^{15} 个不同的明文结构, 每个明文结构在第 0 条对角线遍历、其余 12 字节取固定值, 得到 $2^{15}\times 2^{63} = 2^{78}$ 个只在第 0 条对角线有差分的明文对. 筛选满足密文差分条件 $(C_1 + C_2)_{\mathrm{SR}(\mathrm{col}(2,3))} = 0$ 的 $2^{78}\times 2^{-64} = 2^{14}$ 个明文对存入表 L 中.

(2) 对表 L 中每个明文对 (P_1, P_2), 执行如下操作:

(a) 猜测 $K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}$, $K_{6,\mathrm{SR}(\mathrm{col}(0))}$. 对密文 C_1, C_2 进行部分解密计算 $(Z_1 + Z_2)_{\mathrm{col}(0)}$, 如果存在某个 $i \in \{0, 1, 2, 3\}$ 使得第 i 字节差分 $(Z_1 + Z_2)_i = 0$, 则对 P_1, P_2 部分加密至 (X_1, X_2), 由 $X_{1,\mathrm{col}(0)}$ 和 $X_{2,\mathrm{col}(0)}$ 构造 (X_1, X_2) 的 7 个混合结构 (X_3^j, X_4^j), $1 \le j \le 7$. 利用猜测的 $K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}$ 对 X_3^j, X_4^j 进行 1 轮部分解密得到其明文 P_3^j, P_4^j, 查询获得相应的密文 C_3^j, C_4^j, $1 \le j \le 7$. 利用猜测的 $K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 对 C_3^j, C_4^j 进行部分解密, 验证 $(Z_3^j + Z_4^j)_i = 0, 1 \le j \le 7$ 是否都成立. 如果都成立, 则将 $K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}, K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 的猜测值和指标 i 保留. 如果 (P_1, P_2) 是 Good Pair, 则正确的密钥值一定会被保留. 无论 (P_1, P_2) 是否是 Good Pair, 错误密钥被保留的概率为 $2^{-6}\times(2^{-8})^7 = 2^{-62}$, 约有 $2^{64}\times 2^{-62} = 4$ 个 $K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}, K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 的猜测值被保留.

(b) 对保留下来密钥中的 $K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}$ 和指标 i, 猜测 $K_{6,\mathrm{SR}(\mathrm{col}(1))}$, 部分解密 C_1, C_2 和 C_3^j, C_4^j, $1 \le j \le 7$. 验证 $(Z_1 + Z_2)_t = (Z_3^j + Z_4^j)_t = 0$, $1 \le j \le 7$ 是否都成立来筛选 $K_{6,\mathrm{SR}(\mathrm{col}(1))}$, 这里脚标 $t \in \mathrm{col}(1) \cap \mathrm{SR}(\mathrm{col}(i))$. 这一步猜测的密钥量为 $4 \times 2^{32} = 2^{34}$, 筛选概率为

$(2^{-8})^8 = 2^{-64}$, 期望留下的密钥个数为 2^{-30}. 也就是说, 错误密钥基本不可能留下, 正确的 $K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}, K_{6,\mathrm{SR}(\mathrm{col}(0,1))}$ 将被留下. 如果有密钥留下则判断该明文对 (P_1, P_2) 是 Good Pair, 且满足 $(Z_1 + Z_2)_{\mathrm{SR}(\mathrm{col}(i))} = 0$.

(3) 利用找到的 Good Pair (P_1, P_2) 及密钥 $K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}$ 在 X 处构造混合结构获得相应的密文 C_3^j, C_4^j, $1 \le j \le 7$. 猜测 $K_{6,\mathrm{SR}(\mathrm{col}(2))}$, 部分解密验证是否 $(Z_3^j + Z_4^j)_t = 0$, $1 \le j \le 7$ 都成立, 这里脚标 $t \in \mathrm{col}(2) \cap \mathrm{SR}(\mathrm{col}(i))$. 猜测 $K_{6,\mathrm{SR}(\mathrm{col}(3))}$, 部分解密验证是否 $(Z_3^j + Z_4^j)_t = 0$, $1 \le j \le 7$ 都成立, 这里脚标 $t \in \mathrm{col}(3) \cap \mathrm{SR}(\mathrm{col}(i))$. 错误的 $K_{6,\mathrm{SR}(\mathrm{col}(2))}$ 和 $K_{6,\mathrm{SR}(\mathrm{col}(3))}$ 通过验证的概率均为 $(2^{-8})^7 = 2^{-56}$, 足以排除错误猜测, 只保留正确的 $K_{6,\mathrm{SR}(\mathrm{col}(2))}$ 和 $K_{6,\mathrm{SR}(\mathrm{col}(3))}$.

(4) 对得到的候选密钥 K_6 进行加密验证.

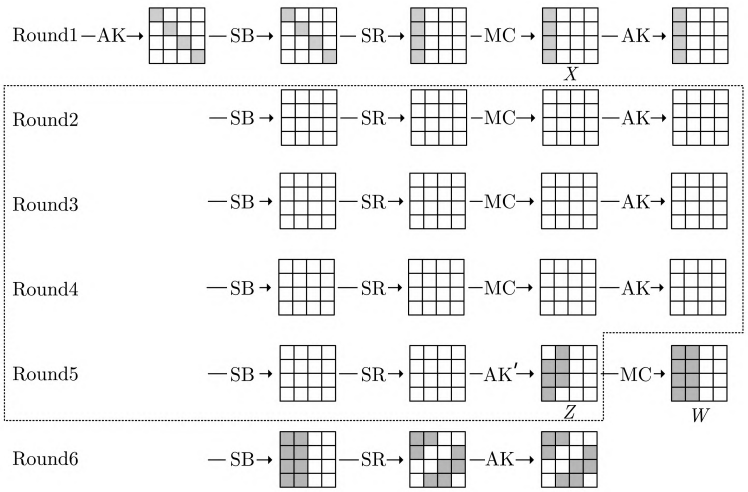

图 2 6 轮 AES 算法

Figure 2 6 rounds of AES

该攻击步骤中计算复杂度最大的部分是 (2)(a), 需对 L 中每个明文对做 2^{64} 次密钥猜测, 相当于 $(2^{14} \times 2^{64} \times 8 \times 2 \times 4)/(20 \times 6) \approx 2^{77.09}$ 次 6 轮 AES 加密. 我们采用与文献 [14] 相同的中间相遇技术来减少对 $K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 的猜测次数. 筛选 $K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 的条件是 (C_1, C_2) 和 (C_3^j, C_4^j), $1 \le j \le 7$ 八对数据在状态 Z 的第 i 字节差分同时为 0. 因为 $Z = \mathrm{MC}^{-1}(W)$, 所以

$$\Delta Z_i = a_{i,0} \times \Delta W_0 + a_{i,1} \times \Delta W_1 + a_{i,2} \times \Delta W_2 + a_{i,3} \times \Delta W_3,$$

其中 $a_{i,j}$ 是 MC^{-1} 矩阵第 i 行、第 j 列的元素, $i, j \in \{0, 1, 2, 3\}$. 如果 $\Delta Z_i = 0$, 则有

$$a_{i,0} \times \Delta W_0 + a_{i,1} \times \Delta W_1 = a_{i,2} \times \Delta W_2 + a_{i,3} \times \Delta W_3. \tag{1}$$

将 $K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 分成 $K_{6,\{0,13\}}$ 和 $K_{6,\{7,10\}}$ 两部分. 猜测 $K_{6,\{0,13\}}$, 对 (C_1, C_2) 和 (C_3^j, C_4^j), $1 \le j \le 2$ 三组密文部分解密计算 ΔZ_i 关于 $\Delta W_{\{0,1\}}$ 的部分和, 即等式 (1) 的左边. 将三个字节部分和级联存入表 $L_{1,i}$ 中, 以猜测的 $K_{6,\{0,13\}}$ 为索引, $i \in \{0, 1, 2, 3\}$. 猜测 $K_{6,\{7,10\}}$, 同样对这三组密文部分解密计算 ΔZ_i 关于 $\Delta W_{\{2,3\}}$ 的部分和, 即等式 (1) 的右边. 将三字节的部分和依相同次序级联存入表 $L_{2,i}$ 中, 以猜测的 $K_{6,\{7,10\}}$ 为索引, $i \in \{0, 1, 2, 3\}$. 在表 $L_{1,i}$ 和 $L_{2,i}$ 中进行三字节的匹配, $i \in \{0, 1, 2, 3\}$, 根据匹配在两个表中的索引确定 $K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 的候选值. 平均有 $2^{32} \times 2^{-24} \times 4 = 2^{10}$ 个匹配发生, 相应确定 2^{10} 个 $K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 的候选值. 对每个候选值, 将剩余的五对密文 (C_3^j, C_4^j), $3 \le j \le 7$ 部分解密, 验证 $(Z_3^j + Z_4^j)_i = 0$, $3 \le j \le 7$ 是否都成立. 错误的 $K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 通过筛选被留下的个数期望为 $2^{10} \times 2^{-8 \times 5} = 2^{-30}$, 所以几乎只有正确的 $K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 被留下.

对 L 中每个明文对和 $K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}$ 的每次猜测, 构造表 $L_{1,i}$ 和 $L_{2,i}$ 的复杂度为 $2\times 2^{16}\times 6\times 2\approx 2^{20.58}$ 次 S 盒计算, 表匹配找碰撞的复杂度为 $2\times 2^{16}\times 4=2^{19}$ 次查表, 相当于 2^{19} 次一轮加密, 验证碰撞确定的 $K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 的计算复杂度为 $2^{10}\times 10\times 4\approx 2^{15.32}$ 次 S 盒计算. 所以使用中间相遇技术改进后步骤 (2)(a) 的总复杂度为 $(2^{14}\times 2^{32}\times(2^{20.58}/20+2^{19}+2^{15.32}/20))/6\approx 2^{62.62}$ 次 6 轮 AES 加密. 步骤 (2)(b) 的计算复杂度为 $(2^{14}\times 4\times 2^{32}\times 16\times 4)/(20\times 6)\approx 2^{47.09}$, 步骤 (3) 和步骤 (4) 的计算量相比之下可以忽略. 改进的 6 轮 AES 混合差分攻击算法 1 的数据复杂度为 $2^{15}\times 2^{32}=2^{47}$, 时间复杂度为 $2^{62.62}$. 筛选满足密文差分条件的明文对时构建 Hash 表的大小为 2^{32}, 表 $L_{1,i}$ 和 $L_{2,i}$ 的大小均为 2^{16}, 表 T 的大小约为 2^8, 所以算法的主要存储复杂度为明密文数据存储. 算法成功的概率等于 L 中 2^{14} 个明文对存在 Good Pair 的概率 $1-(1-2^{-14})^{2^{14}}\approx 1-e^{-1}\approx 63\%$. 如果将密文筛选条件 $(C_1+C_2)_{\mathrm{SR}(\mathrm{col}(2,3))}=0$ 改为任意两条反对角线差分为 0, 算法 1 仍然有效. 我们仍在 2^{14} 个对中寻找 Good Pair, 数据和存储复杂度可降为 $2^{47}/6\approx 2^{44.42}$, 时间复杂度和成功率不变.

算法 1 AES 的 6 轮混合差分攻击

选择 2^{15} 个明文结构, 每个明文结构第 0 条对角线遍历、其余字节取随机固定值. 询问加密机获取它们的密文.
对每个明文结构, 以密文的第 2、3 条反对角线的值构建 Hash 表, 将满足密文差分 $(C_1+C_2)_{\mathrm{SR}(\mathrm{col}(2,3))}=0$ 的明文对 (P_1,P_2) 存入表 L 中.
for L 中每个明文对(P_1,P_2) **do**
  for 猜测$K_{0,\mathrm{SR}^{-1}(\mathrm{col}(0))}$ **do**
    部分加密 1 轮到 (X_1,X_2), 由 $X_{1,\mathrm{col}(0)}$ 和 $X_{2,\mathrm{col}(0)}$ 构造 7 个混合结构 (X_3^j,X_4^j), $1\le j\le 7$.
    对 X_3^j,X_4^j 部分解密 1 轮得到其明文 P_3^j,P_4^j, 查询获得相应的密文 C_3^j,C_4^j, $1\le j\le 7$.
    for 猜测$K_{6,\{0,13\}}$ **do**
      分别对 (C_1,C_2), (C_3^1,C_4^1), (C_3^2,C_4^2) 部分解密计算 ΔZ_i 关于 $\Delta W_{\{0,1\}}$ 的部分和, 并将它们级联以 $K_{6,\{0,13\}}$ 为索引存入表 $L_{1,i}$ 中, $i=0,1,2,3$;
    end
    for 猜测$K_{6,\{7,10\}}$ **do**
      分别对 (C_1,C_2), (C_3^1,C_4^1), (C_3^2,C_4^2) 部分解密计算 ΔZ_i 关于 $\Delta W_{\{2,3\}}$ 的部分和, 并将它们级联以 $K_{6,\{7,10\}}$ 为索引存入表 $L_{2,i}$ 中, $i=0,1,2,3$;
    end
    for $0\le i\le 3$ **do**
      对表 $L_{1,i}$ 和 $L_{2,i}$ 进行匹配找碰撞, 将碰撞对应的索引 $K_{6,\{0,7,10,13\}}$ 存储到表 T 中;
      for T 中$K_{6,\mathrm{SR}(\mathrm{col}(0))}$ 的每个候选值 **do**
        部分解密 (C_3^j,C_4^j), 如果存在 $(Z_3^j+Z_4^j)_i\ne 0$, $3\le j\le 7$, 则将该候选值从表 T 中删除;
      end
      if T 不是空集 **then**
        利用 $(Z_1+Z_2)_{\mathrm{SR}(\mathrm{col}(i))}=(Z_3^j+Z_4^j)_{\mathrm{SR}(\mathrm{col}(i))}=0$, $1\le j\le 7$ 分别筛选 K_6 的另外三条反对角线.
      end
    end
  end
end
对候选的 K_6 进行加密验证.

4 PRINCE 和 PRINCE$_{\mathrm{core}}$ 的 6 轮混合差分攻击

4.1 PRINCE 算法简介

PRINCE 算法的分组长度为 64 比特, 密钥长度为 128 比特, 迭代轮数为 12 轮, 算法结构如图 3 所示. 64 比特状态用 4×4 的矩阵来描述时, 矩阵中每个元素是一个 4 比特块. 128 比特的密钥被分为 2 个 64 比特的子密钥 k_0 和 k_1, 其中 k_1 应用于算法的核心部件 PRINCE$_{\mathrm{core}}$, k_0 和 k_0' 用于算法输入、输出两端的白化, 这里 $k_0'=(k_0\ggg 1)+(k_0\gg 63)$. PRINCE$_{\mathrm{core}}$ 采用对称结构, 中间 2 轮是对合的, 前后 5 轮除轮常数不同外互为逆变换. 轮常数满足 $\mathrm{RC}_i+\mathrm{RC}_{11-i}=\alpha$, $0\le i\le 11$, 这里 α 是固定常数. PRINCE 算法的解密可以通过加密操作来实现, 即 $D_{(k_0\|k_0'\|k_1)}(\cdot)=E_{(k_0'\|k_0\|k_1+\alpha)}(\cdot)$. 本文使用 R^n 表示 n 轮的 PRINCE 变换, 轮变换包括以下 5 个操作:

- S 层: 状态矩阵的 16 个块同时查询一个 4 比特的 S 盒.

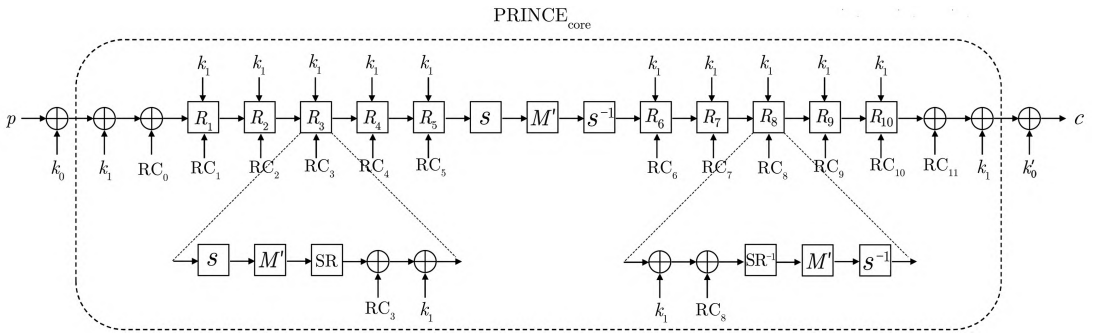

图 3 PRINCE 算法
Figure 3 PRINCE cipher

- 扩散层 (M'): 使用 $\mathbb{F}_2$ 上的一个 64×64 的矩阵乘以 64 比特状态, $M'^{-1}=M'$.
- 行移位 (SR): 将状态矩阵的第 i 行循环左移 i 个块, 其中 $i=0,1,2,3$.
- 轮常数加 (ARC): 将状态与一个 64 比特轮常数 RC_i 异或, $0\le i\le 11$.
- 密钥加 (AK): 将状态比特异或 64 比特密钥 k_1.

4.2 6 轮 PRINCE 的混合差分攻击

由于 PRINCE 与 AES 具有相似的结构, 所以我们能够得到如下 4 轮 PRINCE 的混合差分性质.

定理 2 设 (X_1,X_2,X_3,X_4) 是 PRINCE 的一个混合四元组, 则 $(R^4\circ\mathrm{SR}(X_1)+R^4\circ\mathrm{SR}(X_2))_{\mathrm{col}(i)}=0$ 当且仅当 $(R^4\circ\mathrm{SR}(X_3)+R^4\circ\mathrm{SR}(X_4))_{\mathrm{col}(i)}=0$, $i\in\{0,1,2,3\}$.

证明: 忽略不影响差分的 AK 和 ARC,

$$R^4\circ\mathrm{SR}=(S^{-1}\circ M'\circ\mathrm{SR}^{-1})\circ(S^{-1}\circ M'\circ S)\circ(\mathrm{SR}\circ M'\circ S)\circ\mathrm{SR}.$$

交换 SR 与 S 的顺序,

$$R^4\circ\mathrm{SR}=(S^{-1})\circ(M'\circ\mathrm{SR}^{-1}\circ S^{-1})\circ(M'\circ\mathrm{SR}\circ S)\circ(M'\circ\mathrm{SR}\circ S).$$

与 4 轮 AES 相比最后少一个 SR. 4 轮混合差分性质与 S 盒和列混合矩阵的细节无关, 故结论成立. □

6 轮 PRINCE 算法如图4所示. 记 $K_0=k_0+k_1$, $K_0'=k_0'+k_1$. 记第 1 轮 M' 后的状态为 X, 第 5 轮 AK 后的状态为 Y, $Z=\mathrm{SR}^{-1}(Y)$, $W=M'(Z)$. 设 (X_1,X_2,X_3,X_4) 是在状态 X 处的混合四元组, 由定理2, $(Y_1+Y_2)_{\mathrm{col}(i)}=0$ 当且仅当 $(Y_3+Y_4)_{\mathrm{col}(i)}=0$, 进而有 $(Z_1+Z_2)_{\mathrm{SR}^{-1}(\mathrm{col}(i))}=0$ 当且仅当 $(Z_3+Z_4)_{\mathrm{SR}^{-1}(\mathrm{col}(i))}=0$, $i\in\{0,1,2,3\}$. 利用混合差分的性质, 我们可对 6 轮 PRINCE 执行与 6 轮 AES 相似的混合差分攻击. 不同的是, 我们选择第 0 列遍历、其他字节取固定值的明文结构, 筛选密文满足差分条件 $(C_1+C_2)_{\mathrm{col}(2,3)}=0$ 的明文对. 一个明文对满足密文筛选条件的概率为 2^{-32}, 在该条件下是 Good Pair 的概率是 $2^{-8}\times 4=2^{-6}$, 因此需要 2^7 个不同明文结构平均有 $2^7\times 2^{31}\times 2^{-32-6}=1$ 个 Good Pair. 执行类似算法1的过程后, 我们可恢复密钥 $K_{0,\mathrm{col}(0)}$、K_0'. 为了恢复 PRINCE 的主密钥, 我们需进一步恢复 K_0 的另外三列. 选择在第 1 列遍历、其他字节取固定值的 2^{16} 个明文, 平均构成 2^{31} 个明文对. 任选其中的 2^{14} 个明文对, 利用已恢复的 K_0' 将密文部分解密至状态 Z, 平均能找到一对满足存在某个 $i\in\{0,1,2,3\}$ 使得 $(Z_1+Z_2)_{\mathrm{SR}^{-1}(\mathrm{col}(i))}=0$ 的明文对 (P_1,P_2). 猜测 $K_{0,\mathrm{col}(1)}$, 将 (P_1,P_2) 部分加密得到 (X_1,X_2). 构造 (X_1,X_2) 的混合结构 (X_3,X_4), 部分解密得到明文 (P_3,P_4), 查询获得相应的密文 (C_3,C_4). 利用已恢复的 K_0' 将 (C_3,C_4) 部分解密, 验证 $(Z_3+Z_4)_{\mathrm{SR}^{-1}(\mathrm{col}(i))}=0$ 是否成立. 对于错误的 $K_{0,\mathrm{col}(1)}$, 验证通过的概率为 2^{-16}, 平均只有 1 个 $K_{0,\mathrm{col}(1)}$ 留下. 采用相似的过程继续恢复 $K_{0,\mathrm{col}(2)}$ 和 $K_{0,\mathrm{col}(3)}$, 最终我们能够得到完整的 K_0 和 K_0', 并利用它们恢复出主密钥 k_0,k_1. 6 轮 PRINCE 混合差分

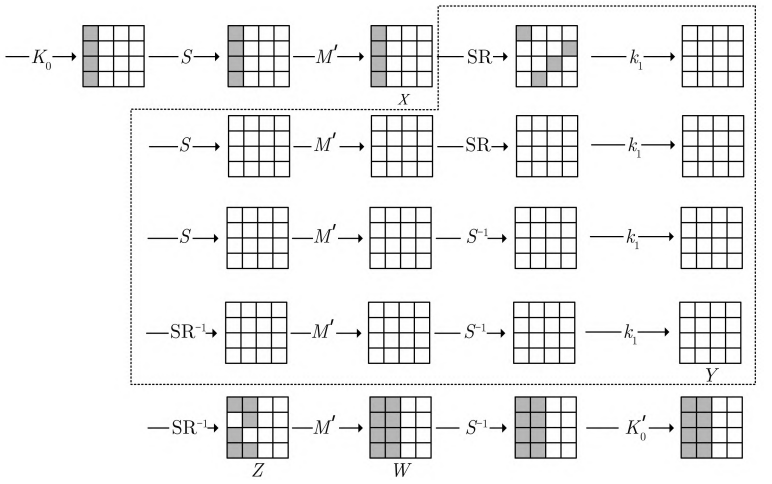

图 4 6 轮 PRINCE 算法

Figure 4 6 rounds of PRINCE

攻击的数据复杂度为 $2^7\times 2^{16}+2^{16}\times 3\approx 2^{23}$, 存储复杂度为 2^{23}. 时间复杂度最高的步骤是恢复 $K_{0,\mathrm{col}(0)}$、K_0', 大约为 $(2^6\times 2^{16}\times 2^9\times 6\times 2)/(16\times 6)+(2^6\times 2^{16}\times 2^8\times 2\times 4)/6\approx 2^{30.66}$ 次 6 轮 PRINCE 加密.

4.3 6 轮 PRINCE$_{\mathrm{core}}$ 的混合差分攻击

6 轮 PRINCE$_{\mathrm{core}}$ 如图5所示. 对 6 轮 PRINCE$_{\mathrm{core}}$ 的混合差分攻击与 PRINCE 相似, 选取的明文结构和混合差分区分器均相同. 不同之处在于 PRINCE$_{\mathrm{core}}$ 没有白化密钥, 轮密钥都是 k_1, 我们只猜测 k_1 的某一列即可进行明文的部分加密和密文的部分解密, 故计算复杂度与 PRINCE 相比有较大减少. 下面介绍 6 轮 PRINCE$_{\mathrm{core}}$ 的混合差分攻击流程.

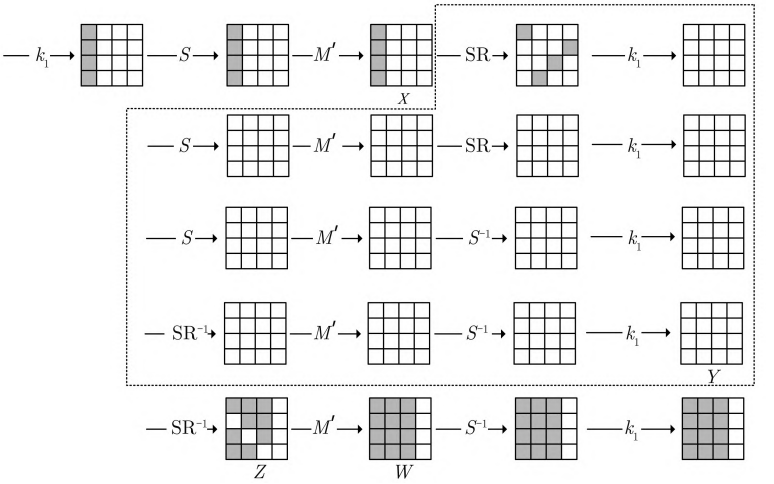

图 5 6 轮 PRINCE$_{\mathrm{core}}$ 算法

Figure 5 6 rounds of PRINCE$_{\mathrm{core}}$

(1) 选择第 0 列遍历、其余字节取任意固定值的 2^{16} 个明文, 筛选出密文差分满足 $(C_1+C_2)_{\mathrm{col}(3)}=0$ 的 $2^{31}\times 2^{-16}=2^{15}$ 个明文对, 从中随机选择 2^{10} 个存入表 L 中, 平均有 $2^{10}\times 2^{-12}\times 4=1$ 个对是 Good Pair.

(2) 对表 L 中的每个明文对 (P_1,P_2), 执行如下操作:

(a) 利用中间相遇技术猜测 $k_{1,\mathrm{col}(0)}$, 部分解密 (C_1,C_2) 并验证是否存在 $i\in\{0,1,2,3\}$ 使得

$(Z_1+Z_2)_i=0$. 如果这样的 i 存在, 我们就将该 $k_{1,\mathrm{col}(0)}$ 和指标 i 存到表格 T 中, 否则直接将该值删去. 这样将 $k_{1,\mathrm{col}(0)}$ 的候选值由 2^{16} 降到 $2^{16}\times 2^{-4}\times 4=2^{14}$.

(b) 对于 T 中的每一个 $k_{1,\mathrm{col}(0)}$ 和对应的 i, 将 (P_1,P_2) 进行一轮部分加密得到 (X_1,X_2). 构造 (X_1,X_2) 的混合结构 (X_3^1,X_4^1), 部分解密得到 (P_3^1,P_4^1), 查询得到 (C_3^1,C_4^1) 并部分解密, 验证 $(Z_3^1+Z_4^1)_i=0$ 是否成立. 如果成立再构造 (X_3^2,X_4^2) 并验证 $(Z_3^2+Z_4^2)_i=0$, 否则将 $k_{1,\mathrm{col}(0)}$ 的值从表 T 中删去. 对剩余的 5 个混合结构使用相同的方法依次进行验证. 错误密钥被保留的概率为 $(2^{-4})^7=2^{-28}$, 平均有 $2^{14}\times 2^{-28}=2^{-14}$ 个 $k_{1,\mathrm{col}(0)}$ 被保留. 因此, 如果 T 不为空, 可以认为 T 中的 $k_{1,\mathrm{col}(0)}$ 是正确的, 其对应的 (P_1,P_2) 是 Good Pair, 且满足 $(Z_1+Z_2)_{\mathrm{SR}^{-1}(\mathrm{col}(-i \bmod 4))}=0$.

(3) 利用找到的 Good Pair(P_1,P_2) 及密钥 $k_{1,\mathrm{col}(0)}$ 在 X 处构造混合结构并获得相应的密文 C_3^j,C_4^j, $1\le j\le 7$. 猜测 $k_{1,\mathrm{col}(1)}$, 部分解密验证是否 $(Z_1+Z_2)_t=(Z_3^j+Z_4^j)_t=0$, $1\le j\le 7$ 都成立, 这里脚标 $t\in \mathrm{col}(1)\cap \mathrm{SR}^{-1}(\mathrm{col}(-i \bmod 4))$. 猜测 $k_{1,\mathrm{col}(2)}$, 部分解密验证是否 $(Z_1+Z_2)_t=(Z_3^j+Z_4^j)_t=0, 1\le j\le 7$ 都成立, 这里脚标 $t\in \mathrm{col}(2)\cap \mathrm{SR}^{-1}(\mathrm{col}(-i \bmod 4))$. 猜测 $k_{1,\mathrm{col}(3)}$, 部分解密验证是否 $(Z_3^j+Z_4^j)_t=0, 1\le j\le 7$ 都成立, 这里脚标 $t\in \mathrm{col}(3)\cap \mathrm{SR}^{-1}(\mathrm{col}(-i \bmod 4))$. 错误的 $k_{1,\mathrm{col}(1)}$ 和 $k_{1,\mathrm{col}(2)}$ 通过验证的概率均为 $(2^{-4})^8=2^{-32}$, 错误的 $k_{1,\mathrm{col}(3)}$ 通过验证的概率为 $(2^{-4})^7=2^{-28}$, 足以排除错误猜测, 只保留正确的 $k_{1,\mathrm{col}(1,2,3)}$.

(4) 对得到的候选密钥 k_1 进行加密验证.

算法 2 给出了 6 轮 $\mathrm{PRINCE}_{\mathrm{core}}$ 的混合差分攻击. 算法的数据和存储复杂度均为 2^{16}. 算法的时间复杂度主要取决于步骤 (2)(a). 在 (2)(a) 中, 计算 (X_1,X_2) 需要 $(2^{10}\times 2^{14}\times 4\times 2)/(16\times 6)\approx 2^{20.42}$ 次 6 轮加密, 构造 (X_3^1,X_4^1) 并计算 $(Z_3^1+Z_4^1)_i$ 的时间复杂度是 $(2^{10}\times 2^{14}\times 4\times 2+2^{10}\times 2^{14}\times 8)/(16\times 6)\approx 2^{21.42}$. 验证完毕平均剩下 $2^{14}\times 2^{-4}=2^{10}$ 个 $k_{1,\mathrm{col}(0)}$ 的值, 因此构造 (X_3^2,X_4^2) 并计算 $(Z_3^2+Z_4^2)_i$ 的时间复杂度为 $(2^{10}\times 2^{10}\times 4\times 2\times 2)/(16\times 6)\approx 2^{17.42}$. (X_3^j,X_4^j), $2\le j\le 7$ 的构造和验证的时间复杂度相比之下可以忽略不计. 算法最终的时间复杂度为 $2^{20.42}+2^{21.42}\approx 2^{22}$. 算法成功的概率是 $1-(1-2^{-10})^{2^{10}}\approx 63\%$.

算法 2 $\mathrm{PRINCE}_{\mathrm{core}}$ **的 6 轮混合差分攻击**

选择一个明文结构, 在第 0 列取所有可能值, 其他字节取任意固定值. 询问加密机获取它们的密文.
将 2^{16} 个密文按照第 3 列的值构建 Hash 表, 构造满足 $(C_1+C_2)_{\mathrm{col}(3)}=0$ 的明文对 (P_1,P_2), 任选其中 2^{10} 个对存储到表格 L 中.
for L 中每个明文对(P_1,P_2) **do**
  for 猜测$k_{1,\{0,1\}}$ **do**
    对 (C_1,C_2) 部分解密计算 ΔZ_i 关于 $\Delta W_{\{0,1\}}$ 的部分和, 以 $k_{1,\{0,1\}}$ 为索引存入表 $L_{1,i}$ 中, $i=0,1,2,3$;
  end
  for 猜测$k_{1,\{2,3\}}$ **do**
    对 (C_1,C_2) 部分解密计算 ΔZ_i 关于 $\Delta W_{\{2,3\}}$ 的部分和, 以 $k_{1,\{2,3\}}$ 为索引存储到 $L_{2,i}$ 中, $i=0,1,2,3$;
  end
  for $0\le i\le 3$ **do**
    对表 $L_{1,i}$ 和 $L_{2,i}$ 进行匹配找碰撞, 将碰撞对应的索引 $k_{1,\mathrm{col}(0)}$ 存储到表 T 中;
    for T 中$k_{1,\mathrm{col}(0)}$ 的每个候选值 **do**
      对 (P_1,P_2) 进行一轮部分加密得到 $(X_{1,\mathrm{col}(0)},X_{2,\mathrm{col}(0)})$;
      for $1\le j\le 7$ **do**
        由 $X_{1,\mathrm{col}(0)}$ 和 $X_{2,\mathrm{col}(0)}$ 构造 (X_3^j,X_4^j);
        对 (X_3^j,X_4^j) 部分解密一轮得到明文 (P_3^j,P_4^j), 查询获得密文 (C_3^j,C_4^j);
        部分解密 (C_3^j,C_4^j), 如果 $\Delta Z_i\ne 0$, 将该候选值从 T 中删除;
      end
    end
    if T 不是空集 **then**
      利用 $(Z_1+Z_2)_{\mathrm{SR}^{-1}(\mathrm{col}(-i \bmod 4))}=(Z_3^j+Z_4^j)_{\mathrm{SR}^{-1}(\mathrm{col}(-i \bmod 4))}=0$, $1\le j\le 7$ 分别筛选 K_0 的另外三列.
    end
  end
end
对候选的 k_1 进行加密验证.

5 结论

文献 [14] 和 [15] 表明混合差分攻击可以将数据和存储复杂度限制到较小的程度, 而不追求时间复杂度的最优. 本文在文献 [14, 15] 中的 6 轮 AES-128 混合差分攻击的基础上, 通过对密文差分增设条件限制来提高 Good Pair 出现的概率, 减少了每次密钥猜测需要验证的数据对数, 将 6 轮 AES-128 混合差分攻击的时间复杂度由 2^{73} 改进到 $2^{62.62}$, 数据和存储复杂度提高到 $2^{44.42}$. 在所有 6 轮 AES-128 的密钥恢复攻击中, 本文攻击方案的总复杂度优于除了积分攻击以外的其他所有攻击. 将改进的 6 轮混合差分攻击应用于 PRINCE 和 $\text{PRINCE}_{\text{core}}$, 我们给出了总复杂度分别为 $2^{30.66}$ 和 2^{22} 的密钥恢复攻击, 其中 6 轮 $\text{PRINCE}_{\text{core}}$ 的攻击结果优于积分攻击和差分攻击. 如何以追求时间复杂度、总复杂度最优为目标改进 AES 和 PRINCE 的混合差分攻击是值得后续深入研究的问题.

参考文献

[1] DAEMEN J, RIJMEN V. The Design of Rijndael: AES—The Advanced Encryption Standard[M]. In: Information Security and Cryptography, Springer Berlin Heidelberg, 2002: 1–160. [DOI: 10.1007/978-3-662-04722-4]

[2] FERGUSON N, KELSEY J, LUCKS S, et al. Improved cryptanalysis of Rijndael[C]. In: Fast Software Encryption—FSE 2000. Springer Berlin Heidelberg, 2001: 213–230. [DOI: 10.1007/3-540-44706-7_15]

[3] BIHAM E, KELLER N. Cryptanalysis of reduced variants of Rijndael[EB/OL]. 2000. http://madchat.fr/crypto/codebreakers/35-ebiham.pdf

[4] ZHANG W T, WU W L, FENG D G. New results on impossible differential cryptanalysis of reduced AES[C]. In: Information Security and Cryptology—ICISC 2007. Springer Berlin Heidelberg, 2007: 239–250. [DOI: 10.1007/978-3-540-76788-6_19]

[5] BOURA C, LALLEMAND V, NAYA-PLASENCIA M, et al. Making the impossible possible[J]. Journal of Cryptology, 2018, 31(1): 101–133. [DOI: 10.1007/s00145-016-9251-7]

[6] LEURENT G, PERNOT C. New representations of the AES key schedule[C]. In: Advances in Cryptology—EUROCRYPT 2021, Part I. Springer Cham, 2021: 54–84. [DOI: 10.1007/978-3-030-77870-5_3]

[7] BOGDANOV A, RIJMEN V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers[J]. Designs, Codes and Cryptography, 2014, 70(3): 369–383. [DOI: 10.1007/s10623-012-9697-z]

[8] SUN B, LIU M C, GUO J, et al. Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis[C]. In: Advances in Cryptology—EUROCRYPT 2016, Part I. Springer Berlin Heidelberg, 2016: 196–213. [DOI: 10.1007/978-3-662-49890-3_8]

[9] SUN B, LIU M C, GUO J, et al. New insights on AES-like SPN ciphers[C]. In: Advances in Cryptology—CRYPTO 2016, Part I. Springer Berlin Heidelberg, 2016: 605–624. [DOI: 10.1007/978-3-662-53018-4_22]

[10] HU K, CUI T T, GAO C, et al. Towards key-dependent integral and impossible differential distinguishers on 5-round AES[C]. In: Selected Areas in Cryptography—SAC 2018. Springer Cham, 2019: 139–162. [DOI: 10.1007/978-3-030-10970-7_7]

[11] GRASSI L, RECHBERGER C, RØNJOM S. Subspace trail cryptanalysis and its applications to AES[J]. IACR Transactions on Symmetric Cryptology, 2016, 2016(2): 192–225. [DOI: 10.13154/tosc.v2016.i2.192-225]

[12] GRASSI L. Mixture differential cryptanalysis: A new approach to distinguishers and attacks on round-reduced AES[J]. IACR Transactions on Symmetric Cryptology, 2018, 2018(2): 133–160. [DOI: 10.13154/tosc.v2018.i2.133-160]

[13] GRASSI L. Probabilistic mixture differential cryptanalysis on round-reduced AES[C]. In: Selected Areas in Cryptography—SAC 2019. Springer Cham, 2020: 53–84. [DOI: 10.1007/978-3-030-38471-5_3]

[14] BAR-ON A, DUNKELMAN O, KELLER N, et al. Improved key recovery attacks on reduced-round AES with practical data and memory complexities[C]. In: Advances in Cryptology—CRYPTO 2018, Part II. Springer Cham, 2018: 185–212. [DOI: 10.1007/978-3-319-96881-0_7]

[15] BAR-ON A, DUNKELMAN O, KELLER N, et al. Improved key recovery attacks on reduced-round AES with practical data and memory complexities[J]. Journal of Cryptology, 2020, 33(3): 1003–1043. [DOI: 10.1007/s00145-019-09336-w]

[16] GRASSI L, RECHBERGER C, RØNJOM S. A new structural-differential property of 5-round AES[C]. In: Advances in Cryptology—EUROCRYPT 2017, Part II. Springer Cham, 2017: 289–317. [DOI: 10.1007/978-3-319-56614-6_10]

[17] RØNJOM S, BARDEH N G, HELLESETH T. Yoyo tricks with AES[C]. In: Advances in Cryptology—ASIACRYPT 2017, Part I. Springer Cham, 2017: 217–243. [DOI: 10.1007/978-3-319-70694-8_8]

[18] BARDEH N G, RØNJOM S. The exchange attack: How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts[C]. In: Advances in Cryptology—ASIACRYPT 2019, Part III. Springer Cham, 2019: 347–370. [DOI: 10.1007/978-3-030-34618-8_12]

[19] DUNKELMAN O, KELLER N, RONEN E, et al. The retracing boomerang attack[C]. In: Advances in Cryptology—EUROCRYPT 2020, Part I. Springer Cham, 2020: 280–309. [DOI: 10.1007/978-3-030-45721-1_11]

[20] DERBEZ P, FOUQUE P A, JEAN J. Improved key recovery attacks on reduced-round AES in the single-key setting[C]. In: Advances in Cryptology—EUROCRYPT 2013. Springer Berlin Heidelberg, 2013: 371–387. [DOI: 10.1007/978-3-642-38348-9_23]

[21] GRASSI L. MixColumns properties and attacks on (round-reduced) AES with a single secret S-box[C]. In: Topics in Cryptology—CT-RSA 2018. Springer Cham, 2018: 243–263. [DOI: 10.1007/978-3-319-76953-0_13]

[22] BOURA C, CANTEAUT A, COGGIA D. A general proof framework for recent AES distinguishers[J]. IACR Transactions on Symmetric Cryptology, 2019, 2019(1): 170–191. [DOI: 10.13154/tosc.v2019.i1.170-191]

[23] DUAN C H. Cryptanalysis of Round-reduced AES and Round-reduced PRINCE[D]. Zhengzhou: Strategic Support Force Information Engineering University. 2020.
段春晖. 减轮 AES 和减轮 PRINCE 的密码分析 [D]. 郑州: 战略支援部队信息工程大学, 2020.

[24] BORGHOFF J, CANTEAUT A, GÜNEYSU T, et al. PRINCE—A low-latency block cipher for pervasive computing applications[C]. In: Advances in Cryptology—ASIACRYPT 2012. Springer Berlin Heidelberg, 2012: 208–225. [DOI: 10.1007/978-3-642-34961-4_14]

[25] RASOOLZADEH S, RADDUM H. Faster key recovery attack on round-reduced PRINCE[C]. In: Lightweight Cryptography for Security and Privacy—LightSec 2016. Springer Cham, 2017: 3–17. [DOI: 10.1007/978-3-319-55714-4_1]

[26] MORAWIECKI P. Practical attacks on the round-reduced PRINCE[J]. IET Information Security, 2017, 11(3): 146–151. [DOI: 10.1049/iet-ifs.2015.0432]

[27] JEAN J, NIKOLIĆ I, PEYRIN T, et al. Security analysis of PRINCE[C]. In: Fast Software Encryption—FSE 2013. Springer Berlin Heidelberg, 2014: 92–111. [DOI: 10.1007/978-3-662-43933-3_6]

[28] DERBEZ P, PERRIN L. Meet-in-the-middle attacks and structural analysis of round-reduced PRINCE[J]. Journal of Cryptology, 2020, 33(3): 1184–1215. [DOI: 10.1007/s00145-020-09345-0]

[29] ABED F, LIST E, LUCKS S. On the security of the core of PRINCE against biclique and differential cryptanalysis[J/OL]. IACR Cryptology ePrint Archive, 2012: 2012/712. https://eprint.iacr.org/2012/712.pdf

[30] ZHAO G Y, SUN B, LI C, et al. Truncated differential cryptanalysis of PRINCE[J]. Security and Communication Networks, 2015, 8: 2875–2887. [DOI: 10.1002/sec.1213]

[31] CANTEAUT A, FUHR T, GILBERT H, et al. Multiple differential cryptanalysis of round-reduced PRINCE[C]. In: Fast Software Encryption—FSE 2014. Springer Berlin Heidelberg, 2015: 591–610. [DOI: 10.1007/978-3-662-46706-0_30]

[32] LI L B, JIA K T, WANG X Y. Improved meet-in-the-middle attacks on AES-192 and PRINCE[J/OL]. IACR Cryptology ePrint Archive, 2013: 2013/573. https://eprint.iacr.org/2013/573.pdf

作者信息

闫雪萍 (1997–), 河南焦作人, 研究生在读. 主要研究领域为分组密码的安全性分析.
yanxueping163@163.com

谭林 (1983–), 湖北天门人, 副教授. 主要研究领域为对称密码的设计与分析.
tanlin100@163.com

戚文峰 (1963–), 浙江宁波人, 博士生导师, 教授. 主要研究领域为对称密码的设计与分析.
wenfeng.qi@263.net