

AES-256 密码算法的相关差分分析

闫雪萍, 谭 林, 戚文峰

(信息工程大学, 河南 郑州 450001)

摘要:高级加密标准(AES)是目前使用最广泛的分组密码算法,许多密码方案使用减轮 AES 作为其核心部件。AES-256 通过 256 比特密钥提供强大的安全强度,是公认能够有效抵御未来量子计算攻击的 AES 版本。相关差分分析由 AES 的设计者提出,将只使用一个差分特征的传统差分分析扩展成使用一对输入和输出都具有特定关联性的差分特征,已被用于生成 7 轮 AES-128 的密钥恢复攻击,这是 AES-128 轮数最长的攻击之一。目前没有 AES-256 的相关差分分析结果。本文将相关差分分析技术应用于 AES-256 密码算法,给出了 8 轮 AES-256 的相关差分密钥恢复攻击,数据和存储复杂度为 $2^{110.24}$,时间复杂度为 $2^{235.76}$,这是对 AES-256 算法进行相关差分安全性评估的首个结果,填补了 AES-256 在相关差分分析领域的空白。

关键词:分组密码;减轮 AES;AES-256 算法;相关差分;密钥恢复攻击

中图分类号:TN918.1;TP309.7 **文献标识码:**A **文章编号:**1671-0673(2026)03-0310-06

Related Differentials Cryptanalysis on AES-256

YAN Xueping, TAN Lin, QI Wenfeng

(Information Engineering University, Zhengzhou 450001, China)

Abstract: The advanced encryption standard (AES) is the most widely used block cipher. Round-reduced variants of AES are employed as the core components of many cryptographic schemes. AES-256 is widely recognized as the version of AES capable of effectively resisting future quantum computing attacks because it provides robust security strength via a 256-bit key. Related differentials cryptanalysis is proposed by the designers of AES. The traditional differential cryptanalysis that only uses one differential is extended to use a pair of differentials where both the input and output have specific correlations. This technique has been applied to mount a key recovery attack on 7-round AES-128, which is one of the attacks with the longest number of rounds for AES-128. Currently, there are no results about the related differentials cryptanalysis on AES-256. Related differentials cryptanalysis is applied to AES-256 to develop a related differentials key recovery attack for 8-round AES-256 with the data and memory complexities of $2^{110.24}$ and the time complexity of $2^{235.76}$ in this paper. This attack is the first result about the security evaluation of AES-256 against related differentials cryptanalysis, filling the gap in the field of related differentials cryptanalysis on AES-256.

Key words: block cipher; round-reduced AES; AES-256; related differentials; key recovery attack

高级加密标准(Advanced Encryption Standard, AES)^[1]是目前使用最广泛、研究最多的分组密码算法。AES采用SPN(Substitution-Permutation Network)

结构和宽轨迹策略设计,通过简单的轮变换迭代实现混淆和扩散效果。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,

有些密码算法甚至直接使用减轮 AES 作为算法的关键部件。研究 AES 密码的安全性分析在分组密码研究领域具有重大意义。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^[2-3]、零相关线性^[4-7]、子空间路径^[8]、混合差分^[9]、yoyo^[10-11]、交换攻击^[12]、飞去来器^[13]、中间相遇攻击^[14-21]、不可能差分^[22-23]、相关差分^[24-25]等。

AES 算法的分组长度为 128 比特,密钥长度支持 128、192 和 256 比特,分别用 AES-128、AES-192 和 AES-256 来表示。AES-256 因其 256 比特密钥长度能够提供远超实际需求的安全强度,被公认为能够有效抵御未来量子计算攻击的 AES 版本,也是美国国家安全局批准的用于保护绝密级信息的唯一 AES 版本^[26]。对于 8 轮以上 AES-256,目前在单密钥模式下的密钥恢复攻击有中间相遇攻击、不可能差分攻击和积分攻击。下面分别介绍 AES-256 在这 3 类分析方法下的研究进展。

中间相遇攻击把密钥猜测过程从加密方向和解密方向分别推进到某个中间状态,并通过匹配中间值来筛选候选密钥。文献[14-19,21]给出了在单密钥模式下 8~10 轮 AES-256 的中间相遇攻击。不可能差分分析技术利用概率为 0 的差分特征攻击密码算法。Lu 等^[22]利用 4 轮不可能差分区分器给出了 8 轮 AES-256 的密钥恢复攻击。积分分析利用明文分组经过多轮加密后某些比特位的线性组合的性质来攻击算法。Fouque 等^[2]利用 4 轮积分区分器给出了 8 轮 AES-256 的密钥恢复攻击。

相关差分的概念由 AES 的设计者^[24]提出,是多维差分^[27]的一种特殊形式。文献[25]给出 7 轮 AES-128 的相关差分攻击,这是目前 AES-128 轮数最长的密钥恢复攻击之一。之前的研究尚未对 AES-256 进行相关差分分析。本文将相关差分分析技术应用于 AES-256 密码算法,通过把该 7 轮攻击扩展 1 轮,给出 8 轮 AES-256 的相关差分密钥恢复攻击,数据、时间和存储复杂度分别为 $2^{110.24}$ 、 $2^{235.76}$ 、 $2^{110.24}$ 。本文算法是对 AES-256 算法进行相关差分安全性评估的首个结果,填补了 AES-256 在相关差分分析领域的空白。

表 1 给出目前在单密钥模式下 8 轮以上 AES-256 密钥恢复攻击的主要结果,其中:数据复杂度表示选择的明文量;时间复杂度中 MA 表示内存访

问,其他是对应轮数的 AES 加密。

表 1 单密钥模式下 8 轮以上 AES-256 的密钥恢复攻击

轮数	攻击方法	数据复杂度	时间复杂度	存储复杂度	参考文献
8	中间相遇	$2^{34.2}$	$2^{205.8}$	$2^{205.8}$	文献[14]
		2^{80}	2^{241}	2^{123}	文献[15]
		2^{113}	2^{196}	2^{129}	文献[16]
		2^{113}	2^{196}	2^{82}	文献[17]
		2^{107}	2^{196}	2^{96}	文献[17]
		$2^{102.83}$	2^{156}	$2^{140.17}$	文献[18]
		2^{113}	2^{156}	2^{130}	文献[18]
	不可能差分	$2^{89.1}$	$2^{229.7}(\text{MA})$	2^{97}	文献[22]
	积分	$2^{127.997}$	2^{204}	2^{128}	文献[2]
	相关差分	$2^{110.24}$	$2^{235.76}$	$2^{110.24}$	本文
9	中间相遇	2^{120}	2^{203}	2^{203}	文献[17]
		2^{121}	$2^{203.5}$	$2^{169.9}$	文献[19]
		2^{127}	$2^{197.5}$	$2^{162.9}$	文献[21]
10	中间相遇	2^{111}	2^{253}	$2^{211.2}$	文献[20]

1 AES 算法和相关差分分析

1.1 AES 算法和符号说明

AES 算法中,128 比特状态通常用有限域 $\mathbb{F}_{2^8}$ 上 4×4 的矩阵来描述,矩阵中元素顺序如图 1 所示。

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

图 1 AES 状态矩阵元素顺序

有限域 $\mathbb{F}_{2^8}$ 中的元素对应次数小于 8 的多项式,本文用其系数的 16 进制来表示。AES 的轮变换包括以下 4 个操作。1) 字节替换(SB):状态矩阵的每个字节查询同一个 8 比特 S 盒。2) 行移位(SR):将状态矩阵的第 i 行循环左移 i 个字节,其中 $i = 0, 1, 2, 3$ 。3) 列混合(MC):用 $\mathbb{F}_{2^8}$ 上的 MDS 矩阵(Maximum Distance Separable Matrix)乘以状态矩阵的每一列。4) 轮密钥加(AK):将状态与轮密钥逐比特异或。

AES 的一个轮变换为 $R = AK \circ MC \circ SR \circ SB$ 。加密时,明文先进行一个轮密钥加,再进行相应数量的轮变换,最后一轮没有 MC 操作。AES-128、AES-192 和 AES-256 的迭代轮数分别为 10、12 和 14。

本文记“+”表示异或操作。记“ AK_r ”表示与第 r 轮的轮密钥 K_r 进行异或, $r \geq 0$ 。当交换 MC 和 AK 的顺序时,记“ AK_r ”表示与等效轮密钥 $K'_r = MC^{-1}(K_r)$

进行异或,其中 MC^{-1} 表示列混合MC的逆运算。记 R^n 表示 n 轮完整的AES,最后一轮有MC。对于一个向量 $\mathbf{x}$,记 x_i 表示 $\mathbf{x}$ 的第 i 个分量。记 $K'_{i,i}$ 表示等效轮密钥 K'_i 的第 i 个字节, $0 \leq i \leq 15$ 。记 $\alpha \parallel \beta$ 表示 α 与 β 的级联值。对于两个集合 I, J ,满足 $J \subseteq I$,记 $I \setminus J$ 表示所有的元素 i ,满足 $i \in I$ 且 $i \notin J$ 。

1.2 相关差分分析

定义1(相关差分^[24]) 两个差分 $\Delta\mathbf{x}=(\Delta x_0, \Delta x_1, \dots, \Delta x_{n-1})$, $\Delta\mathbf{x}'=(\Delta x'_0, \Delta x'_1, \dots, \Delta x'_{n-1}) \in \mathbb{F}_q^n$ 是相关差分,当且仅当对于 $i=0, 1, \dots, n-1$, $\Delta x_i \Delta x'_i (\Delta x_i + \Delta x'_i) = 0$ 。式中, q 为素数方幂。

任何差分 $\Delta\mathbf{x}$ 都与自身构成相关差分,全零差分与任何差分 $\Delta\mathbf{x}'$ 构成相关差分,本文排除这两种情况。对于任意状态 $\alpha \in \mathbb{F}_q^n$ 及任意相关差分 $\Delta\mathbf{x}, \Delta\mathbf{x}' \in \mathbb{F}_q^n$,可以得到四元组 $(\alpha, \alpha + \Delta\mathbf{x}, \alpha + \Delta\mathbf{x}', \alpha + \Delta\mathbf{x} + \Delta\mathbf{x}')$ 。对于每个 $i=0, 1, \dots, n-1$,集合 $\{\alpha_i, \alpha_i + \Delta x_i, \alpha_i + \Delta x'_i, \alpha_i + \Delta x_i + \Delta x'_i\}$ 由两对相等的值组成。因此,在SPN型密码结构中,相关差分通过双射S盒层的概率为1。在相关差分分析中,只需要考虑相关差分在线性层的传播。

定义2(相关差分特征^[24]) 设 $\Delta\mathbf{x}, \Delta\mathbf{x}'$ 为相关差分,对于线性映射 M ,设 $\Delta\mathbf{y}=M(\Delta\mathbf{x}), \Delta\mathbf{y}'=M(\Delta\mathbf{x}')$ 。如果 $\Delta\mathbf{y}, \Delta\mathbf{y}'$ 是相关差分,则称 $\Delta\mathbf{x} \rightarrow \Delta\mathbf{y}, \Delta\mathbf{x}' \rightarrow \Delta\mathbf{y}'$ 是 M 的相关差分特征。

对于AES算法,当状态被看作是由4条对角线构成的 $\mathbb{F}_{2^8}^4$ 中的向量,且 $\Delta\mathbf{x}, \Delta\mathbf{x}' \in \mathbb{F}_{2^8}^4$ 满足定义1时,称 $\Delta\mathbf{x}, \Delta\mathbf{x}'$ 为对角线相关差分。

文献[25]证明由对角线相关差分构成的四元组满足4轮AES的零差分性质,如定理1所示。

定理1^[25] 设 $\Delta\mathbf{x}, \Delta\mathbf{x}' \in \mathbb{F}_{2^8}^{4 \times 4}$ 为对角线相关差分,对任意状态 $\alpha \in \mathbb{F}_{2^8}^{4 \times 4}$,记 $(X_0, X_1, X_2, X_3) = (\alpha, \alpha + \Delta\mathbf{x}, \alpha + \Delta\mathbf{x}', \alpha + \Delta\mathbf{x} + \Delta\mathbf{x}')$,则 $R^2(X_0) + R^2(X_1) + R^2(X_2) + R^2(X_3) = 0$,且经过4轮AES加密后, $MC^{-1}(R^4(X_0) + R^4(X_1))$ 的第 i 条反对角线为零,当且仅当 $MC^{-1}(R^4(X_2) + R^4(X_3))$ 的第 i 条反对角线为零, $i=0, 1, 2, 3$ 。

如果AES算法的输入差分 $\Delta\mathbf{x}, \Delta\mathbf{x}'$ 与输出差分 $\Delta\mathbf{y}, \Delta\mathbf{y}'$ 均为对角线相关差分,则称 $\Delta\mathbf{x} \rightarrow \Delta\mathbf{y}, \Delta\mathbf{x}' \rightarrow \Delta\mathbf{y}'$ 为对角线相关差分特征。对于AES的4个完整轮 R^4 ,文献[25]给出了8个对角线相关差分特征,每个相关差分特征的概率为 2^{-192} 。令 $\Delta\mathbf{x}, \Delta\mathbf{x}'$ 是 R^4 的输入相关差分, $\Delta\mathbf{y}, \Delta\mathbf{y}'$ 是输出相关差分,其中一个对角线相关差分特征如式(1)~(3)所示:

$$\Delta\mathbf{x} = \begin{bmatrix} \Delta x_0 & \Delta x_4 & \Delta x_8 & \Delta x_{12} \\ \Delta x_1 & \Delta x_5 & \Delta x_9 & \Delta x_{13} \\ \Delta x_2 & \Delta x_6 & \Delta x_{10} & \Delta x_{14} \\ \Delta x_3 & \Delta x_7 & \Delta x_{11} & \Delta x_{15} \end{bmatrix} \rightarrow \Delta\mathbf{y} = \begin{bmatrix} E\gamma_0 & 9\gamma_1 & D\gamma_2 & B\gamma_3 \\ 9\gamma_0 & D\gamma_1 & B\gamma_2 & E\gamma_3 \\ D\gamma_0 & B\gamma_1 & E\gamma_2 & 9\gamma_3 \\ B\gamma_0 & E\gamma_1 & 9\gamma_2 & D\gamma_3 \end{bmatrix} \quad (1)$$

$$\Delta\mathbf{x}' = \begin{bmatrix} \Delta x_0 & 0 & \Delta x_8 & 0 \\ 0 & \Delta x_5 & 0 & \Delta x_{13} \\ \Delta x_2 & 0 & \Delta x_{10} & 0 \\ 0 & \Delta x_7 & 0 & \Delta x_{15} \end{bmatrix} \rightarrow \Delta\mathbf{y}' = \begin{bmatrix} E\gamma_0 & 0 & D\gamma_2 & 0 \\ 0 & D\gamma_1 & 0 & E\gamma_3 \\ D\gamma_0 & 0 & E\gamma_2 & 0 \\ 0 & E\gamma_1 & 0 & D\gamma_3 \end{bmatrix} \quad (2)$$

$$\Delta\mathbf{x} + \Delta\mathbf{x}' = \begin{bmatrix} 0 & \Delta x_4 & 0 & \Delta x_{12} \\ \Delta x_1 & 0 & \Delta x_9 & 0 \\ 0 & \Delta x_6 & 0 & \Delta x_{14} \\ \Delta x_3 & 0 & \Delta x_{11} & 0 \end{bmatrix} \rightarrow \Delta\mathbf{y} + \Delta\mathbf{y}' = \begin{bmatrix} 0 & 9\gamma_1 & 0 & B\gamma_3 \\ 9\gamma_0 & 0 & B\gamma_2 & 0 \\ 0 & B\gamma_1 & 0 & 9\gamma_3 \\ B\gamma_0 & 0 & 9\gamma_2 & 0 \end{bmatrix} \quad (3)$$

式中: $\Delta\mathbf{x}$ 在所有对角线上均取非零值, $\gamma_i \in \mathbb{F}_{2^8}$ 不全为零, $i=0, 1, 2, 3$ 。其他7个对角线相关差分特征的输入相关差分与 $\Delta\mathbf{x}, \Delta\mathbf{x}'$ 相同,输出相关差分可以通过将 $\Delta\mathbf{y}, \Delta\mathbf{y}'$ 的所有列进行相同的循环移位,和/或交换 $\Delta\mathbf{y}'$ 与 $(\Delta\mathbf{y} + \Delta\mathbf{y}')$ 的值得到。

文献[25]将这8个对角线相关差分特征后面加上3轮,给出7轮AES-128的密钥恢复攻击。设 $\Delta\mathbf{x}, \Delta\mathbf{x}' \in \mathbb{F}_{2^8}^{4 \times 4}$ 是式(1)~式(3)中的输入对角线相关差分。任意选择明文 $P_0 \in \mathbb{F}_{2^8}^{4 \times 4}$,构造明文四元组 $(P_0, P_1, P_2, P_3) = (P_0, P_0 + \Delta\mathbf{x}, P_0 + \Delta\mathbf{x}', P_0 + \Delta\mathbf{x} + \Delta\mathbf{x}')$,使得平均存在一个明文四元组在前4轮AES上满足这8个对角线相关差分特征中任意一个。由定理1可知,经过6轮AES加密后,该明文四元组满足:

$$R^6(P_0) + R^6(P_1) + R^6(P_2) + R^6(P_3) = 0 \quad (4)$$

对于密文四元组 (C_0, C_1, C_2, C_3) ,逐字节猜测 K_7 的可能值,将密文部分解密,利用式(4)对猜测的密钥值进行筛选,并将剩余的密钥候选值进行加密验证。更多攻击的细节参照文献[25]。

2 AES-256的8轮相关差分攻击

2.1 攻击策略

在8轮AES中,分别交换第6轮、第7轮中MC

和AK的顺序,如图2所示。记4轮加密后的状态为 Y ,第6轮MC后的状态为 Z ,第7轮MC前的状态为 W 。设 $\Delta x, \Delta x' \in \mathbb{F}_2^{4 \times 4}$ 是对角线相关差分,其中 Δx 在所有对角线上取非零值, $\Delta x'$ 在两条不相邻的对角线上取非零值。对任意明文 $P_0 \in \mathbb{F}_2^{4 \times 4}$,令 $(P_0, P_1, P_2, P_3) = (P_0, P_0 + \Delta x, P_0 + \Delta x', P_0 + \Delta x + \Delta x')$ 。对于前4轮AES, (P_0, P_1, P_2, P_3) 满足文献[25]给出的8个对角线相关差分特征中任意一个的概率为 $8 \times 2^{-192} = 2^{-189}$ 。也就是说,经过4轮AES后,输出差分 $(Y_0 + Y_1), (Y_0 + Y_2)$ 仍然是对角线相关差分,其中 $(Y_0 + Y_1)$ 在所有对角线上取非零值, $(Y_0 + Y_2)$ 只在

两条不相邻的对角线上取非零值的概率为 2^{-189} 。此时 $(R(Y_0) + R(Y_2))$ 只在两列上取非零值。为了减少猜测密钥后需要部分解密的四元组数,采用与文献[25]相同的做法,限制 $(R(Y_0) + R(Y_2))$ 在两条对角线上取值为零。对于只在两列上取非零值的 $(R(Y_0) + R(Y_2))$ 来说,该限制条件的概率为 $6 \times 2^{-32} \approx 2^{-29.42}$ 。如果一个明文四元组 (P_0, P_1, P_2, P_3) 满足前4轮的对角线相关差分特征和 $(R(Y_0) + R(Y_2))$ 的限制条件,则称该四元组为正确四元组。任意一个明文四元组是正确四元组的概率为 $2^{-189} \times 2^{-29.42} = 2^{-218.42}$ 。

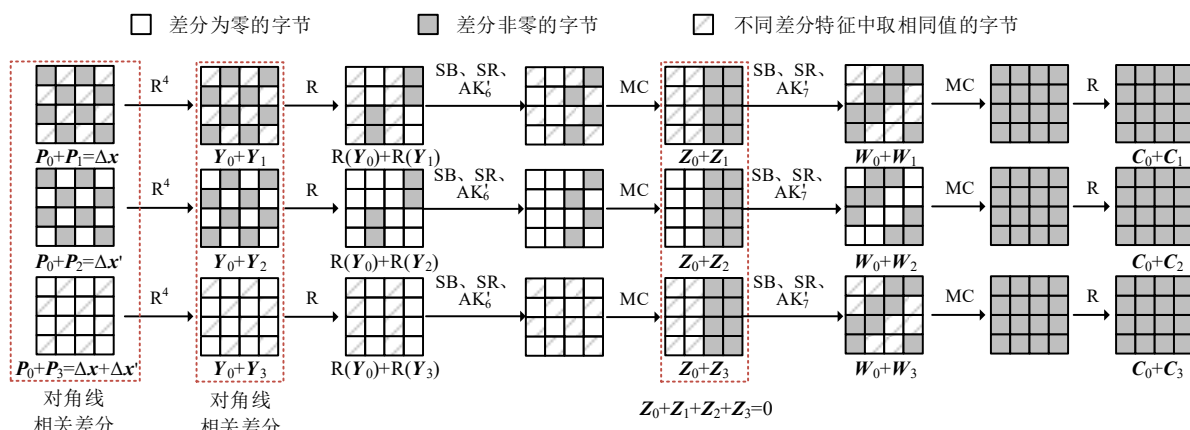


图2 8轮AES-256的相关差分密钥恢复攻击

对于正确四元组 (P_0, P_1, P_2, P_3) ,有 $(Y_0 + Y_2)$ 在两条不相邻的对角线上取值为零, $(Y_0 + Y_3)$ 在另外两条对角线上取值为零,则 $MC^{-1}(Z_0 + Z_2)$ 在两条不相邻的反对角线上取值为零, $MC^{-1}(Z_0 + Z_3)$ 在另外两条反对角线上取值为零。因为 $(Y_0 + Y_1), (Y_0 + Y_2)$ 是对角线相关差分,由定理1可知:

$$Z_0 + Z_1 + Z_2 + Z_3 = 0 \quad (5)$$

由于 $(R(Y_0) + R(Y_2))$ 在两条对角线上取值为零,所以 $(Z_0 + Z_2)$ 在两列上取值为零。由式(5)可得, $(Z_1 + Z_3)$ 在相同的两列上取值为零。因此,在状态 W 处的四元组 (W_0, W_1, W_2, W_3) 满足 $(W_0 + W_2)$ 和 $(W_1 + W_3)$ 各自在相同的两条反对角线上取值为零。对于密文四元组 (C_0, C_1, C_2, C_3) ,猜测 K_8 的全部字节和 K'_7 的部分字节,将密文部分解密到状态 W, Z 处,利用上述差分性质对猜测的密钥值进行筛选。

为了能够成功恢复密钥,需要构造的明文四元组包含一个正确四元组,即需要构造 $2^{218.42}$ 个明文四元组 $(P_0, P_1, P_2, P_3) = (P_0, P_0 + \Delta x, P_0 + \Delta x', P_0 + \Delta x + \Delta x')$,其中: P_0 是任意选择的明文; $\Delta x, \Delta x'$ 是对角线相关差分; Δx 在所有对角线上取非零值;

$\Delta x'$ 在两条不相邻的对角线上取非零值,使得平均存在一个正确四元组。选择规模为 s 的4个集合 $A_i \subseteq \mathbb{F}_2^4 (i = 0, 1, 2, 3)$ 来构成 s^4 个明文,其中第 i 条对角线取集合 A_i 的所有可能值。这些明文能构成 $\frac{1}{2} s^4 (s-1)^4$ 对 (P_0, P_1) 。对每对 (P_0, P_1) ,存在唯一一对 (P_2, P_3) 与其构成明文四元组。考虑到 (P_0, P_1) 和 (P_2, P_3) 在四元组中的先后顺序,构造出的明文四元组数为 $\frac{1}{4} s^4 (s-1)^4$ 。取 $s = 2^{27.56}$,有 $\frac{1}{4} s^4 (s-1)^4 \approx 2^{218.48}$ 。此时攻击的数据复杂度为 $s^4 = 2^{110.24}$ 。

2.2 攻击流程及复杂度分析

在预计算阶段,对任意 $\alpha_i \in \mathbb{F}_2^s, i = 0, 1, 2, 3$,遍历 $k \in \mathbb{F}_2^s$,计算出满足 $\sum_{i=0}^3 SB^{-1}(\alpha_i + k) = 0$ 的 k 的值,并将该值以 $\alpha_0 \| \alpha_1 \| \alpha_2 \| \alpha_3$ 为索引存储到预计算表 T 中。在线阶段的流程如下。

步骤1:选择规模为 $s = 2^{27.56}$ 的4个集合 $A_0, A_1, A_2, A_3 \subseteq \mathbb{F}_2^4$,构造 $2^{110.24}$ 个明文,其中第 i 条对角线取集合 A_i 的所有可能值, $i = 0, 1, 2, 3$ 。询问加密机获得对应的密文,以明文为索引将密文存储到密

文表中。

步骤2:对于 K_8 的每一个可能值,执行如下操作。

1)对集合 A_1, A_3 的每个元素,构造第1、3条反对角线取该对应元素,第0、2条反对角线取 A_0, A_2 所有可能值的 $s^2 = 2^{55.12}$ 个明文 P ,查询密文表得到密文 C 。利用猜测的 K_8 将 C 部分解密得到状态 W ,将 $P \parallel W$ 以 W 的第 m 、 n 条反对角线的值为索引存储到6个Hash表 $H_{m,n}$ 中, $0 \leq m < n \leq 3$ 。对 $2^{55.12}$ 个明文操作完成之后,对于 $H_{m,n}$ 的每个索引,提取出所有对 (W, W') ,并将 P, P' 在第0条和第2条反对角线的级联值作为索引,把 (W, W') 存储到表格 $L_{m,n}$ 中, $0 \leq m < n \leq 3$ 。清空6个Hash表 $H_{m,n}$ 后,对 A_1, A_3 的下一个元素进行相同操作。

2)对于每个表格 $L_{m,n}$, $0 \leq m < n \leq 3$,利用两种方式构造状态四元组。

方式1:对于 $L_{m,n}$ 中任意一对 (W, W') ,取同索引下的另一对 $(\bar{W}, \bar{W}')$,可构成状态四元组 $(W, \bar{W}, W', \bar{W}')$,因其对应的明文 (P, P') 和 $(\bar{P}, \bar{P}')$ 可以构成需要的明文四元组 $(P, \bar{P}, P', \bar{P}') = (P_0, P_0 + \Delta x, P_0 + \Delta x', P_0 + \Delta x + \Delta x')$ 。

方式2:对于 $L_{m,n}$ 索引 $a \parallel b$ 下的任意一对 (W, W') ,其中 a, b 分别代表索引的前半部分和后半部分,取索引 $b \parallel a$ 下的任意一对 $(\bar{W}, \bar{W}')$,它们可以构成状态四元组 $(W, \bar{W}, W', \bar{W}')$,因为对应的明文可构成需要的明文四元组 $(P, \bar{P}, P', \bar{P}') = (P_0, P_0 + \Delta x, P_0 + \Delta x', P_0 + \Delta x + \Delta x')$ 。

3)对于步骤2)中构造的每个四元组,对每个在反对角线 $\{0,1,2,3\} \setminus \{m,n\}$ 上的索引 j ,以 $W_j \parallel W'_j \parallel \bar{W}_j \parallel \bar{W}'_j$ 的值检索预计算表 T ,得到 K'_j 的候选值。对所有的 j 操作完成后,执行如下操作。

对方式1中构造出的四元组 $(W, \bar{W}, W', \bar{W}')$,利用恢复出的 K'_j 候选值将其部分解密,得到 $MC^{-1}(Z + Z'), MC^{-1}(Z + \bar{Z})$ 在列 $\{0,1,2,3\} \setminus \{m,n\}$ 上的值。检查 $MC^{-1}(Z + Z')$ 是否在两条不相邻的反对角线为零、 $MC^{-1}(Z + \bar{Z})$ 是否在另外两条反对角线为零。如果成立,穷举 K'_j 在第 m 条和第 n 条反对角线的可能值,并将对应的密钥进行加密验证。

对方式2中构造出的四元组 $(W, \bar{W}, W', \bar{W}')$,利用恢复出的 K'_j 候选值将其部分解密,得到 $MC^{-1}(Z + Z'), MC^{-1}(Z + \bar{Z})$ 在列 $\{0,1,2,3\} \setminus \{m,n\}$ 上的值。检查 $MC^{-1}(Z + Z')$ 是否在两条不相邻的反对角线为零、

$MC^{-1}(Z + \bar{Z})$ 是否在另外两条反对角线为零。如果成立,穷举 K'_j 在第 m 条和第 n 条反对角线的可能值,并将对应的密钥进行加密验证。

攻击的数据复杂度为 $2^{110.24}$,下面分析攻击的时间复杂度。预计算阶段需要 $2^{32} \times 2^8 \times 4 = 2^{42}$ 次内存访问(MA)。预计算表 T 中,在每个索引下平均存在一个 k 的值。在线阶段,步骤1需要 $2^{110.24}$ 次8轮AES加密加上 $2^{110.24}$ 次MA。在步骤2-1)中,构造6个表格 $H_{m,n}$ 的时间复杂度为 $2^{128} \times 2^{110.24} \times (1 + 16 + 6) \approx 2^{242.76}$ MA。对于 K_8 的每个可能值和每个 m, n ,提取出的 (W, W') 平均有 $2^{55.12} \times \binom{2^{55.12}}{2} \times 2^{-64} \approx 2^{100.36}$ 对。构造6个表格 $L_{m,n}$ 的时间复杂度为 $2^{128} \times 6 \times 2^{100.36} \approx 2^{230.94}$ MA。每个表格 $L_{m,n}$ 的索引有 $2^{110.24}$ 个。步骤2-2)中,对于任意一对 (W, W') ,平均有 $(2^{100.36} - 1) \times 2^{-110.24} \times 2 \approx 2^{-8.88}$ 个对应的 $(\bar{W}, \bar{W}')$ 与之构成四元组。因此,在步骤2-2)中构造出的四元组数一共有 $2^{128} \times 6 \times (2^{100.36} \times 2^{-8.88} / 2) \approx 2^{221.06}$ 。在步骤2-3)中,对每个四元组平均能恢复出一个 K'_j 在反对角线 $\{0,1,2,3\} \setminus \{m,n\}$ 上的候选值,所以部分解密的复杂度为 $2^{221.06} \times (8 + 8 \times 2) \approx 2^{225.64}$ MA,加密验证的复杂度为 $2^{221.06} \times 2^{-63} \times 2^{64} = 2^{222.06}$ 次8轮加密。因此,整个攻击的时间复杂度取决于步骤2-1)中构造6个表格 $H_{m,n}$ 的复杂度,为 $2^{242.76}$ MA,等价于 $2^{242.76} / (16 \times 8) = 2^{235.76}$ 次8轮加密。

下面分析攻击的存储复杂度。预计算表 T 的规模为 2^{32} 。步骤1中密文表的规模为 $2^{110.24}$ 。步骤2-1)中对集合 A_1, A_3 的每个元素,6个Hash表 $H_{m,n}$ 的空间可以复用,所以这6个Hash表的规模一共为 $6 \times 2^{55.12} \approx 2^{57.71}$ 。6个表格 $L_{m,n}$ 的规模一共为 $6 \times 2^{100.36} \times 2 \approx 2^{103.94}$ 。因此,攻击的存储复杂度取决于密文表的规模 $2^{110.24}$ 。

3 结束语

目前,在单密钥模式下对8轮以上AES-256的密钥恢复攻击有中间相遇攻击、不可能差分攻击和积分攻击。本文将相关差分分析技术应用于AES-256密码算法,通过在7轮AES-128的攻击后面增加1轮给出8轮AES-256的相关差分密钥恢复攻击,数据、时间和存储复杂度分别为 $2^{110.24}$ 、 $2^{235.76}$ 和 $2^{110.24}$ 。该攻击算法是对AES-256算法进行相关差分安全性评估的首个结果。如何结合中间相遇、状态检测等技术进一步降低该攻击的复杂度是下一步研究的问题。

参考文献:

- [1] DAEMEN J, RIJMEN V. The design of rijndael: the advanced encryption standard(AES)[M]. Berlin, Germany: Springer, 2002.
- [2] FOUQUE P A, KARPMAN P, KIRCHNER P, et al. Efficient and provable white-box primitives[C]// Advances in cryptology-ASIACRYPT 2016. Berlin, Germany: Springer, 2016:159-188.
- [3] DUNKELMAN O, GHOSH S, KELLER N, et al. Partial sums meet FFT: improved attack on 6-round AES[C]// Advances in Cryptology-EUROCRYPT 2024. Cham, Switzerland: Springer, 2024:128-157.
- [4] 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.
- [5] SUN B, LIU M C, GUO J, et al. Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis [C] // Advances in Cryptology-EUROCRYPT 2016. Berlin, Germany: Springer, 2016:196-213.
- [6] SUN B, LIU M C, GUO J, et al. New insights on AES-like SPN ciphers[C]// Advances in Cryptology-CRYPTO 2016. Berlin, Germany: Springer, 2016:605-624.
- [7] HU K, CUI T T, GAO C, et al. Towards key-dependent integral and impossible differential distinguishers on 5-round AES [C] // Proceedings of the 25th International Conference on Selected Areas in Cryptography. Cham, Switzerland: Springer, 2019:139-162.
- [8] 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.
- [9] 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.
- [10] RØNJOM S, BARDEH N G, HELLESETH T. Yoyo tricks with AES[C]// Advances in Cryptology-ASIACRYPT 2017. Cham, Switzerland: Springer, 2017:217-243.
- [11] MONDAL S K, RAHMAN M, SARKAR S, et al. Revisiting yoyo tricks on AES[J]. IACR Transactions on Symmetric Cryptology, 2023, 2023(4):28-57.
- [12] BARDEH N G, RØNJOM S. The exchange attack: how to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts [C]// Advances in Cryptology-ASIACRYPT 2019. Cham, Switzerland: Springer, 2019:347-370.
- [13] DUNKELMAN O, KELLER N, RONEN E, et al. The re-tracing boomerang attack [C] //Advances in Cryptology-EUROCRYPT 2020. Cham, Switzerland: Springer, 2020: 280-309.
- [14] DEMIRCI H, SELÇUK A A. A meet-in-the-middle attack on 8-round AES [C]// Fast Software Encryption. Berlin, Germany: Springer, 2008:116-126.
- [15] DEMIRCI H, TAŞKIN İ, ÇOBAN M, et al. Improved meet-in-the-middle attacks on AES [C] // Proceedings of the 10th International Conference on Cryptology in India. Berlin, Germany: Springer, 2009:144-156.
- [16] DUNKELMAN O, KELLER N, SHAMIR A. Improved single-key attacks on 8-round AES-192 and AES-256 [C]// Advances in Cryptology: ASIACRYPT 2010. Berlin, Germany: Springer, 2010:158-176.
- [17] DERBEZ P, FOUQUE P A, JEAN J. Improved key recovery attacks on reduced-round AES in the single-key setting [C]// Advances in cryptology-EUROCRYPT 2013. Berlin, Germany: Springer, 2013:371-387.
- [18] DERBEZ P, FOUQUE P A. Exhausting demirci-selçuk meet-in-the-middle attacks against reduced-round AES [C]// Fast Software Encryption. Berlin, Germany: Springer, 2014:541-560.
- [19] LI L B, JIA K T, WANG X Y. Improved single-key attacks on 9-round AES-192/256[C]// Fast Software Encryption. Berlin, Germany: Springer, 2015:127-146.
- [20] LI R J, JIN C H. Meet-in-the-middle attacks on 10-round AES-256[J]. Designs, Codes and Cryptography, 2016, 80(3):459-471.
- [21] DONG X L, LIU J, WEI Y Z, et al. Meet-in-the-middle attacks on AES with value constraints[J]. Designs, Codes and Cryptography, 2024, 92(9):2423-2449.
- [22] LU J Q, DUNKELMAN O, KELLER N, et al. New impossible differential attacks on AES [C]// Proceedings of the 9th International Conference on Cryptology in India. Berlin, Germany: Springer, 2008:279-293.
- [23] LEURENT G, PERNOT C. New representations of the AES key schedule[J]. Journal of Cryptology, 2024, 38(1):No.2.
- [24] DAEMEN J, RIJMEN V. New criteria for linear maps in AES-like ciphers[J]. Cryptography and Communications, 2009, 1(1):47-69.
- [25] GHAEDI BARDEH N, RIJMEN V. New key-recovery attack on reduced-round AES [J]. IACR Transactions on Symmetric Cryptology, 2022, 2022(2):43-62.
- [26] National Security Agency, Cybersecurity Directorate. Announcing the commercial national security algorithm suite 2.0[EB/OL]. (2025-05-30)[2026-06-23]. http://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF.
- [27] TIESSEN T. Polytopic cryptanalysis[C]// Advances in Cryptology-EUROCRYPT 2016. Berlin, Germany: Springer, 2016:214-239.

(编辑: 邵 华)