计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2021.20210549
58(10): 2213-2221, 2021

基于交换等价的缩减轮 AES-128 的密钥恢复攻击

张 丽 吴文玲 张 蕾 郑雅菲
(中国科学院软件研究所 北京 100190)
(中国科学院大学 北京 100049)
(zhangli2021@iscas.ac.cn)

Key-Recovery Attack on Reduced-Round AES-128 Using the Exchange-Equivalence

Zhang Li, Wu Wenling, Zhang Lei, and Zheng Yafei
(*Institute of Software, Chinese Academy of Science, Beijing* 100190)
(*University of Chinese Academy of Sciences, Beijing* 100049)

Abstract The advanced encryption standard (AES) is a kind of high-security secret key cryptosystem. It has been widely recognized and used in real life. Since its birth, the research on its security has been the most interesting to cryptographers. At present, it is very difficult to break the full round AES, and the existing analysis methods are difficult to break through the exhaustive search method. So in recent years, researchers have focused on the attacks which can break reduced-round versions of AES, and there are a lot of excellent analysis methods that have emerged, among them, exchange-equivalence attacks, a new cryptanalytic attack technique suitable for SPN-like block cipher designs is widely concerned. Using this technology, researchers have obtained better the secret-key chosen plaintext distinguisher and adaptive chosen ciphertext distinguisher. In this paper, we run through this new technology, based on 5-round adaptive chosen ciphertexts distinguisher on AES, and at the same time, we use a basic property of the Mixcolumns coefficient matrix and a zero difference property to present a new key-recovery attack on 6-round reduced-round AES-128 with a single secret S-Box that requires only $2^{51.5}$ chosen plaintexts and $2^{57.42}$ adaptively chosen ciphertexts data complexity and 2^{72} time complexity. In addition, we practically verified our key-recovery attack on a small-scale variant of the AES. The block size of the small-scale AES is 64 bits, and each word is a 4-bit nibble in the state matrix. The experimental result supports our theory. Finally, the results of the current key-recovery attack on 6-round Reduced-Round AES-128 are better than the previously known attack on Reduced-Round AES-128.

Key words advanced encryption standard (AES); distinguisher; exchange-equivalence attack; key-independent; key-recovery attack

摘 要 高级加密标准(advanced encryption standard, AES)是一种高安全性的密钥加密系统,在实际生活中受到了多方面认可及使用,自它诞生以来对于它的安全性问题的研究一直是密码学者最感兴趣的.目前对全轮的 AES 的攻击难度非常大,现有分析方法难以突破穷举搜索方法.朝着突破全轮 AES 的方向努力,近些年来研究人员十分关注对于缩减轮版本的 AES 攻击,并且已经涌现了许多优秀的分析方法,其中交换等价攻击——一种新的适合于类 SPN 分组密码设计的密码分析攻击技术广受关注.研究

收稿日期:2021-06-07;**修回日期**:2021-07-28
基金项目:国家自然科学基金项目(62072445)
This work was supported by the National Natural Science Foundation of China (62072445).

人员利用该技术得到了比以往更好的秘密密钥选择明文区分器和自适应选择密文区分器.使用了这一新技术,基于 AES 的 5 轮自适应选择密文区分器,在恢复密钥时利用了 AES 加密算法列混合变换系数矩阵的基本性质和 0 差分性质,提出了一种带有秘密 S 盒的 6 轮缩减轮 AES-128 的密钥恢复攻击,该攻击只要求 $2^{51.5}$ 选择明文和 $2^{57.42}$ 自适应选择密文的数据复杂度以及 2^{72} 时间复杂度.此外,一个小版本 AES 上的实验验证了提出的密钥恢复攻击.该版本 AES 块大小为 64b,在状态中的每一个字是 4b 半字节,该实验结果也支持了该研究的理论.最后,当前的对 6 轮缩减轮 AES-128 密钥恢复攻击结果比已有的对缩减轮 AES-128 的密钥恢复攻击结果更优.

关键词 高级加密标准;区分器;交换等价攻击;密钥独立;密钥恢复攻击

中图法分类号 TP309

分组密码在对称密码学中起着非常重要的作用,为加密提供了基础的工具,因此,它们是最受信任的加密算法,经常被用作构造其他加密算法的基础工具,这些算法的安全性证明是在假设底层分组密码是理想的情况下进行的.因此对分组密码安全性研究是具有非常重要的现实意义.2001 年美国通过 3 年的征集和评选,新的高级加密标准(advanced encryption standard, AES)[1]得以诞生,成为了至今为止最广为人知和使用最广泛的分组密码.AES 的安全性研究也一直是密码学中最重要的热点之一.AES 已经被证明能够抵抗差分和线性密码分析.在过去 20 年的大量研究中只有 biclique 攻击[2]能比穷举搜索更快地突破全轮的 AES,所以突破全轮的 AES 一直是密码研究人员努力的目标.

近些年,为了研究出更新更好的方法去实现对全轮 AES 的攻击,研究人员更加关注对于缩减轮的 AES 攻击上.对缩减轮 AES 的攻击之所以重要,有 3 个原因:1)它们使我们能够评估 AES 的安全冗余,即可以成功攻击的轮数与全轮 AES 的轮数之比.2)它们使我们能够开发新的攻击技术,随着进一步的改进,这些技术可能会变得更加有效.3)有许多建议使用缩减轮 AES 作为它们的组件,比如 LED[3],WEM[4],ElmD[5]等.

当试图评估密码的安全性时,密码的非随机特性可用来区分密码与随机置换.其中密码分析最重要的工具之一无疑是差分密码分析.差分密码分析方法经过多年的发展,已经有了许多的变体,知名的变体方法有截断差分,不可能差分,高阶差分,飞来去器攻击和差分线性攻击.此外,近些年多面体密码分析[6]、子空间密码分析、yoyo game、混合密码分析[7]、交换等价攻击等方法的使用产生了许多好的分析结果.这些结果使得对 AES 进行越来越多的全新的、更有效的攻击成为可能.

对 AES 算法的安全性分析工作近些年已有许多优秀的成果.在 FSE 2015 Tiessen 等人[8]提出了第 1 个基于积分分析的 6 轮 AES-128 密钥恢复,作者研究了在保持其他信息不变的情况下,用一个秘密的 8 b S 盒去代替 AES 的 S 盒.随机选取的 S 盒有可能高度抵抗差分和线性攻击.结果表明对 6 轮 AES 密钥恢复的复杂度已经远小于穷举搜索.在 Crypto 2016 上,Sun 等人[9]提出了第 1 个 AES 密钥独立 5 轮区分器.密钥独立意味着攻击不关心特定的轮密钥,与相关密钥攻击形成对比.他们利用 AES 列混合矩阵的特性,将 4 轮积分性质扩展到 5 轮.虽然他们的区分器需要整个密码本,但它为 AES 产生了一系列新的基础结果.后来,通过将 4 轮不可能差分性质扩展到 5 轮,它被改进为 $2^{98.2}$ 选择明文和 2^{107} 次计算代价.在 FSE 2017,Grassi 等人[10]提出了子空间密码分析方法,给出了 5 轮子空间迹和 5 轮不可能差分密钥恢复.在 2017 年的欧密会 Eurocrypt 上,Grassi 等人[11]提出了第 1 个 5 轮选择明文区分器,它仅需要 2^{32} 选择明文,计算成本为 $2^{35.6}$,存储内存大小为 2^{36}B.

随后,在 2017 年 Grassi 等人证明,通过加密明文空间的某些子空间的陪集,密文对的差分在状态空间的特定子空间中的次数总是 8 的倍数.亚密会 Asiacrypt 上,Rønjom 等人介绍了 Rijndael 型分组密码设计的新基本特性,给出了基于 Yoyo game[12]的新型 3~6 轮 AES 密钥区分器,打破了所有以前的记录.作者介绍了 AES 的新的确定性 4 轮属性,即通过对角线的任意子集交换而等价的明文对集合在 4 轮后加密到一组密文对集合,在最终的线性层之前的完全相同列中它们的差分都为 0.该结果在混合密码分析中得到了进一步的探讨.在 Asiacrypt 2019 上,Bardeh 和 Rønjom 提出了一种适用于类 SPN 分组密码的新技术——交换等价攻击[13].交换

等价攻击属于差分密码分析,是一种选择明文攻击方法,它通过研究特定明文差分的交换性质以及对应密文的 0 差分模型,将分组密码与随机置换区分开,并在此基础上进行密钥恢复攻击.该文中给出了交换等价的定义,以及如何利用对明文状态进行交换等价及 AES 的性质来得到在最终的线性层之前的完全相同列中它们的差分都为 0.结果表明,当明文从一个特定的集合(交换等价集)中选择时,AES 的 5 轮和 6 轮选择明文区分器可以区别于随机置换.随后 Bardeh 基于交换等价的基础知识提出了 5 轮和 6 轮 AES 自适应选择密文区分器[14],它是从密文出发做交换等价,去寻找解密后明文状态是否具有相同列差分为 0,6 轮自适应密文区分器需要有 2^{83} 数据和时间复杂度,因此交换等价攻击方法的提出可以看作是 AES 密码分析的一个巨大飞跃.在 Africacrypt 2019 中,Bardeh 基于子空间的知识提出了对 5 轮 AES 的有效攻击[15].到目前为止,最好的密钥恢复攻击可以达到 7 轮 AES.

本文的主要贡献有 3 个方面:

1) 基于由交换等价攻击提出的 5 轮自适应选择密文区分器上向前扩展一轮,提出了一个新的 6 轮 AES-128 密钥恢复攻击;

2) 攻击主要利用了 AES 列混合矩阵系数的基本性质.列混合矩阵的每一行或每一列都有 3 个和为 0 的元素,使得在选取明文时满足这一性质,另外使得一轮后的状态满足 0 差分指定状态;

3) 用分组长度为 64 b 的小版本 AES 实验验证了我们的理论结果,并且该实验结果支持我们的理论.

本文对 6 轮 AES 密钥恢复攻击的结果和已有的 6 轮 AES 密钥恢复的结果进行了比较,如表 1 所示,其中文献[14]中的结果是区分器的结果,其余均表示密钥恢复攻击结果.在数据复杂度、时间复杂度和存储复杂度 3 方面分别进行了对比,结果表明本文的数据复杂度、时间复杂度的结果是最优的.数据复杂度以选择明文(chosen plaintext, CP)数量/自适应选择密文(adaptive chosen ciphertext, ACC)数量表示,时间复杂度以加密(encryption, E)等价形式来表示,空间复杂度以 128 b 块大小为单位表示.我们假定一轮加密约等于 20 次查表[8].因其他文献中复杂度单位不一致,为了方便对比,在这里我们统一换算单位.

Table 1　Key-recovery Attacks on Round-reduced AES-128

表 1　6 轮 AES-128 密钥恢复攻击

攻击方法	数据复杂度	时间复杂度	存储复杂度
交换攻击(本文)	$2^{57.42}$ ACC	2^{72} E	2^{58}
积分攻击[8]	2^{64} CP	$2^{91.68}$ E	2^{69}
交换攻击[13]	2^{83} CP+2^{83} ACC	2^{83} E	
不可能差分[16]	$2^{91.5}$ CP	2^{122} E	2^{89}
概率混合差分[17]	$2^{72.77}$ CP	$2^{104.93}$ E	2^{33}

1　AES 加密算法介绍

AES 分组密码算法是美国于 2001 年颁布的高级加密标准,分组长度为 128 b,128 b 明文将内部状态初始化为一个 4×4 字节矩阵,即所有的运算均在有限域 F_{2^8} 上进行.密钥长度分别为 128 b,192 b 和 256 b,根据 AES 密钥长度的不同,迭代轮数和密钥长度关系为:AES-128 的轮数为 10 轮;AES-192 的轮数为 12 轮;AES-256 的轮数为 14 轮.AES 加密算法的轮函数由 4 种不同变换组成:

1) 字节代替变换(Subbytes, SB).S 盒的变换就是字节代替变换的本质,它是一个作用于状态字节的非线性变换,在状态中,其每一个字节都会经过同一个 8×8 的 S 盒变换为另一个字节,简记为 SB.

2) 行移位变换(Shiftrows, SR).AES 加密算法中线性运算包括行移位变换,而且它的移位方案仅仅与状态有关,对一个状态的每一行循环左移不同的位移量,第 0 行不移位保持不变,第 1 行循环左移 1 B,第 2 行循环左移 2 B,第 3 行循环左移 3 B,简记为 SR.

3) 列混合变换(Mixcolumns, MC).列混合用 $F_{2^8}^{4\times4}$ 中的矩阵左乘状态矩阵的每列,元素之间的乘法运算定义在有限域 F_{2^8} 上.其目的是将状态矩阵的每一列的元素进行混合,简记为 MC,列混合系数:

$$\boldsymbol{M}\equiv\begin{pmatrix}02 & 03 & 01 & 01\\ 01 & 02 & 03 & 01\\ 01 & 01 & 02 & 03\\ 03 & 01 & 01 & 02\end{pmatrix},$$

$$\boldsymbol{M}^{-1}\equiv\begin{pmatrix}0e & 0b & 0d & 09\\ 09 & 0e & 0b & 0d\\ 0d & 09 & 0e & 0b\\ 0b & 0d & 09 & 0e\end{pmatrix}.$$

列混合变换有 2 个基本性质:

性质 1. 列混合系数矩阵的每一行或每一列都有 2 个和为 0 的元素.

性质 2. 列混合系数矩阵的每一行或每一列都有 3 个和为 0 的元素.

4) 子密钥加变换(Addroundkey, *ARK*).轮子密钥长度是 128 b,一个字为 32 b.将一个轮子密钥按位异或到一个状态上.轮子密钥按顺序取自扩展密钥,简记为 *ARK*.

此外,AES 在第 1 轮加密之前,有一个白化密钥层,且最后一轮没有列混合变换.

我们用 $R(*)=MC\circ SR\circ SB\circ ARK(*)$ 表示一轮加密 AES.在本文中,为了方便描述,我们考虑保留最后一轮的 *MC* 作为全轮 AES.此外,S 盒被一个秘密的 S 盒取代,其他结构和组件与原 AES 加密算法相同.

2 交换等价攻击方法

本节我们主要介绍交换等价的概念和相关的定理.以及在自适应选择下 5 轮自适应密文区分器的原理.我们先给出一些基本的定义及定理.

2.1 基本定义及定理

定义 1. 列交换差分[13].给定一对状态 $\boldsymbol{\alpha},\boldsymbol{\beta}\in F_{2^8}^{4\times 4}$ 和一个向量 $\boldsymbol{v}\in F_2^4$,定义列交换差分 $\Delta_{\boldsymbol{v}}^{\boldsymbol{\alpha},\boldsymbol{\beta}}\in F_{2^8}^{4\times 4}$,状态的第 i 列差分定义为 $(\Delta_{\boldsymbol{v}}^{\boldsymbol{\alpha},\boldsymbol{\beta}})_i=(\boldsymbol{\alpha}_i\oplus\boldsymbol{\beta}_i)\boldsymbol{v}_i$,其中 $\boldsymbol{\alpha}_i$ 和 $\boldsymbol{\beta}_i$ 表示状态 $\boldsymbol{\alpha}$ 和 $\boldsymbol{\beta}$ 的第 i 列.

一对状态定义了一个有 $2^{wt_c(\boldsymbol{\alpha}\oplus\boldsymbol{\beta})}$ 可能的列交换差分的集合,其中 $wt_c(x)$ 表示 x 的非零列的数量.现在可以定义 3 个相关的运算符,在一对 AES 状态之间交换对角、列和混合值.

定义 2. 列交换[13](column exchange).给定一对状态 $\boldsymbol{\alpha},\boldsymbol{\beta}\in F_{2^8}^{4\times 4}$ 和一个变量 $\boldsymbol{v}\in F_2^4$,定义列交换为

$$\rho_c^{\boldsymbol{v}}(\boldsymbol{\alpha},\boldsymbol{\beta})=\boldsymbol{\alpha}\oplus\Delta_{\boldsymbol{v}}^{\boldsymbol{\alpha},\boldsymbol{\beta}}.$$

很容易看出 $(\rho_c^{\boldsymbol{v}}(\boldsymbol{\alpha},\boldsymbol{\beta}),\rho_c^{\boldsymbol{v}}(\boldsymbol{\beta},\boldsymbol{\alpha}))=(\boldsymbol{\alpha}\oplus\Delta_{\boldsymbol{v}}^{\boldsymbol{\alpha},\boldsymbol{\beta}},\boldsymbol{\beta}\oplus\Delta_{\boldsymbol{v}}^{\boldsymbol{\alpha},\boldsymbol{\beta}})$ 是通过在 $\boldsymbol{\alpha}$ 和 $\boldsymbol{\beta}$ 之间交换独立的列得到的.因此,对于任意 $\boldsymbol{v}$ 很容易得到 $\boldsymbol{\alpha}\oplus\boldsymbol{\beta}=\rho_c^{\boldsymbol{v}}(\boldsymbol{\alpha},\boldsymbol{\beta})\oplus\rho_c^{\boldsymbol{v}}(\boldsymbol{\beta},\boldsymbol{\alpha})$.

定义 3. 对角交换[13](diagonal exchange).给定一对状态 $\boldsymbol{\alpha},\boldsymbol{\beta}\in F_{2^8}^{4\times 4}$ 和一个变量 $\boldsymbol{v}\in F_2^4$,定义对角交换为

$$\rho_d^{\boldsymbol{v}}(\boldsymbol{\alpha},\boldsymbol{\beta})=\boldsymbol{\alpha}\oplus SR^{-1}(\Delta_{\boldsymbol{v}}^{SR(\boldsymbol{\alpha}),SR(\boldsymbol{\beta})}).$$

对角交换与列交换之间的关系是直接的,即 $R(\rho_d^{\boldsymbol{v}}(\boldsymbol{\alpha},\boldsymbol{\beta}))=\rho_c^{\boldsymbol{v}}(R(\boldsymbol{\alpha}),R(\boldsymbol{\beta}))$,$R$ 表示一轮加密操作.

定义 4. 混合交换[10](mixed exchange).给定一对状态 $\boldsymbol{\alpha},\boldsymbol{\beta}\in F_{2^8}^{4\times 4}$ 和一个变量 $\boldsymbol{v}\in F_2^4$,定义混合交换为

$$\rho_m^{\boldsymbol{v}}(\boldsymbol{\alpha},\boldsymbol{\beta})=\boldsymbol{\alpha}\oplus L(\Delta_{\boldsymbol{v}}^{L^{-1}(\boldsymbol{\alpha}),L^{-1}(\boldsymbol{\beta})}),$$

其中 $L=MC\circ SR$.

因此可以得到混合交换和列交换之间的关系:$R(\rho_c^{\boldsymbol{v}}(\boldsymbol{\alpha},\boldsymbol{\beta}))=\rho_m^{\boldsymbol{v}}(R(\boldsymbol{\alpha}),R(\boldsymbol{\beta}))$,进而可以推出对角交换和混合交换之间的关系:

$$R^2(\rho_d^{\boldsymbol{v}}(\boldsymbol{\alpha},\boldsymbol{\beta}))=\rho_m^{\boldsymbol{v}}(R^2(\boldsymbol{\alpha}),R^2(\boldsymbol{\beta})).$$

定义 5. 0 差分模式[12](the zero difference pattern).令状态为 $\boldsymbol{x}\in F_{2^8}^{4\times 4}$,定义 0 差分模式 $\boldsymbol{v}(\boldsymbol{x})=(z_0,z_1,z_2,z_3)$,其中 $z_i\in F_2^4$,$\boldsymbol{v}(\boldsymbol{x})$ 表示二进制向量,如果状态 $\boldsymbol{x}\in F_{2^8}^{4\times 4}$ 的第 i 列活跃则 $z_i=0$,否则为 1.

对于在第 1 个线性层后或最后一个线性层前的状态为 0 的列,定义为:$\boldsymbol{v}_m(\boldsymbol{x})=\boldsymbol{v}(L^{-1}(\boldsymbol{x}))$ 和 $\boldsymbol{v}_d(\boldsymbol{x})=\boldsymbol{v}(SR(\boldsymbol{x}))$.对于子集 $I\subset\{0,1,2,3\}$,记 $\boldsymbol{v}^I\in F_2^4$ 表示二进制向量,如果 $i\in I$,则 $\boldsymbol{v}_i^I=1$,否则为 0.使用这种表示法来简化结果,避免使用更复杂的状态空间.

定理 1[13]. 令 $I,J,K\subset\{0,1,2,3\}$ 分别表示列集合,对角集合和 0 差分列集合,$\boldsymbol{\alpha},\boldsymbol{\beta}\in F_{2^8}^{4\times 4}$ 表示 2 个随机状态.当状态差分 $\boldsymbol{\alpha}\oplus\boldsymbol{\beta}$ 在 K 列为 0 时,对角集合 J 被交换等价于列集合被交换,即:

$$(\rho_d^{\boldsymbol{v}^J}(\boldsymbol{\alpha},\boldsymbol{\beta}),\rho_d^{\boldsymbol{v}^J}(\boldsymbol{\beta},\boldsymbol{\alpha}))=(\rho_c^{\boldsymbol{v}^I}(\boldsymbol{\alpha},\boldsymbol{\beta}),\rho_c^{\boldsymbol{v}^I}(\boldsymbol{\beta},\boldsymbol{\alpha}))$$

概率为

$$P(|I|,|J|,|K|)=(2^{-8})^{4(|I|+|J|)-|K||J|-2|I||J|}.$$

定理 2[13]. 明文状态 $\boldsymbol{\alpha},\boldsymbol{\beta}\in F_{2^8}^{4\times 4}$ 在 $|K|$ 个对角相等 $K\subset\{0,1,2,3\}$,假设 $0<wt(\nu(R^5(\boldsymbol{\alpha})\oplus R^5(\boldsymbol{\beta})))<4$,则对于 $I\subset\{0,1,2,3\}\backslash K$ 的关系

$$\boldsymbol{v}_m(R^5(\boldsymbol{\alpha})\oplus R^5(\boldsymbol{\beta}))=$$

$$\boldsymbol{v}_m(R^5(\rho_d^{\boldsymbol{v}^I}(\boldsymbol{\alpha},\boldsymbol{\beta}))\oplus R^5(\rho_d^{\boldsymbol{v}^I}(\boldsymbol{\beta},\boldsymbol{\alpha})))$$

成立的概率为

$$P_5(|I|,|K|)=\sum_{d=1}^{3}\binom{4}{d}P(|I|,d,|K|).$$

我们注意到定理 2 的结果在解密方向上同样适用,通过应用适当的交换操作来考虑相应的线性层.

2.2 5 轮自适应选择密文区分器

本节我们介绍基于交换等价的 5 轮自适应选择密文区分器.

定理 3[14]. 令明文状态 $\boldsymbol{\alpha},\boldsymbol{\beta}\in F_{2^8}^{4\times 4}$ 表示 2 个明文状态,$\boldsymbol{\alpha}',\boldsymbol{\beta}'\in F_{2^8}^{4\times 4}$ 表示经过 5 轮加密后的密文状态.假设 $0<wt(\boldsymbol{v}_d(\boldsymbol{\alpha}\oplus\boldsymbol{\beta}))<4$,则对于 $I\subset\{0,1,2,3\}$ 的关系

$$\boldsymbol{v}_d(\boldsymbol{\alpha}\oplus\boldsymbol{\beta})=\boldsymbol{v}_d(R^{-5}(\rho_m^{v^I}(\boldsymbol{\alpha}',\boldsymbol{\beta}'))\oplus R^{-5}(\rho_m^{v^I}(\boldsymbol{\beta}',\boldsymbol{\alpha}'))$$

成立的概率为

$$P_5(|I|,0)=\sum_{d=1}^{3}\binom{4}{d}P(|I|,d,0).$$

由于密文是随机的,在定理 3 中只考虑 $|K|=0$ 的情况.Bardeh 根据定理 3 的结果建立一个 5 轮的区分器.其主要思想是自适应地生成一个新的明文对为

$$\boldsymbol{v}_d(\boldsymbol{\alpha}\oplus\boldsymbol{\beta})=\boldsymbol{v}_d(R^{-5}(\rho_m^{v^I}(\boldsymbol{\alpha}',\boldsymbol{\beta}'))\oplus R^{-5}(\rho_m^{v^I}(\boldsymbol{\beta}',\boldsymbol{\alpha}'))=\boldsymbol{v}_d(\boldsymbol{\alpha}''\oplus\boldsymbol{\beta}''),$$

其中 $\boldsymbol{\alpha}''\oplus\boldsymbol{\beta}''$ 表示 $\boldsymbol{\alpha}'\oplus\boldsymbol{\beta}'$ 经过 5 轮解密得到的新的明文状态对.Bardeh 在文章中给出了一个例子,例如选取明文状态仅在第 1,2 对角活跃,另外 2 个对角取常数值,即 $d=2$.且在混合操作时仅交换一列,即 $|I|=1$.则根据定理 3 可得:该 5 轮自适应选择密文区分器概率为 $p_5(|I|,0)=2^{-46}$,而随机置换的概率为 $p_{rand}=2^{-32\times(4-d)}=2^{-64}$.

如图 1 所示,上层图表示 5 轮自然加密状态,下层图表示应用了定理 3 得到的新的加密状态.其中灰色格表示差分活跃的字节,白格表示差分为 0 的字节,斜条格表示应用了混合交换操作后被交换的字节.

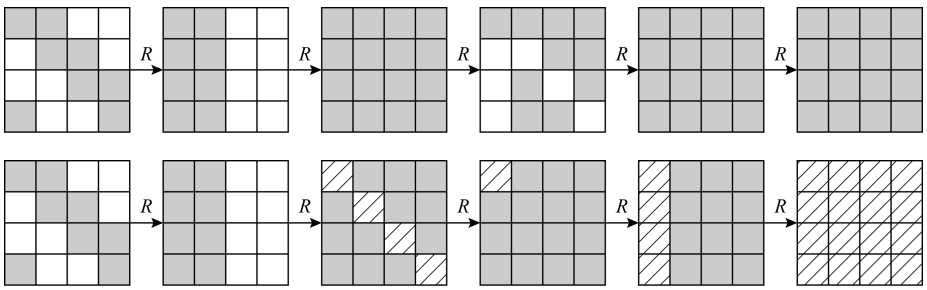

Fig. 1　5-round exchange trail

图 1　5 轮交换迹示意图

3　对 6 轮 AES-128 的密钥恢复攻击

本节介绍是本文的主要内容,基于 5 轮自适应选择密文区分器,我们可以向前扩展一轮得到一个新的 6 轮 AES-128 密钥恢复攻击.

3.1　选择合适的明文集合

首先,我们期望所选择的明文经过一轮加密后满足 5 轮自适应选择密文区分器的输入状态,即 $R(\boldsymbol{p}^0)\oplus R(\boldsymbol{p}^1)$ 在 2 个对角保持活跃状态,剩余对角差分为 0. 4 个对角状态表示如图 2 所示:

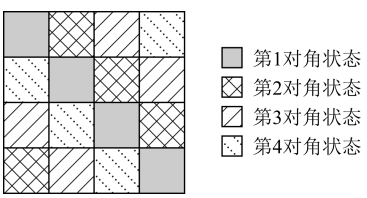

Fig. 2　Diagonal state

图 2　对角状态示意图

基于 AES 列混合变换的基本性质 2:列混合系数矩阵的每一行或每一列都有 3 个和为 0 的元素.如果在列混合变换的 4 个输入字节中有 3 个字节非 0 且有相同的值,剩余一个字节值为 0,那么 4 个输出字节中将有 2 个 0 字节,该事件发生的概率为 1.不失一般性,我们假设输入差分状态为 $[a,a,a,0]^{\mathrm{T}}$,其中 $a\in F_{2^8}$ 且非 0.那么可以得到输出差分状态中的前 2 个字节为 0.

$$\begin{pmatrix}02&03&01&01\\01&02&03&01\\01&01&02&03\\03&01&01&02\end{pmatrix}\times\begin{pmatrix}a\\a\\a\\0\end{pmatrix}=\begin{pmatrix}0\\0\\2a\\3a\end{pmatrix}.\tag{1}$$

为了得到 $[a,a,a,0]^{\mathrm{T}}$ 的输入差分状态,我们定义明文集合 $A_{\alpha,\delta}$ 的形式,

$$A_{\alpha,\delta_0,\delta_1}\equiv\left\{c\oplus\begin{pmatrix}\alpha&0&0&0\\0&\alpha\oplus\delta_0&0&0\\0&0&\alpha\oplus\delta_1&0\\0&0&0&0\end{pmatrix}\right\},\tag{2}$$

其中,$\alpha,\delta_0,\delta_1\in F_{2^8}$,$\alpha$ 是非 0 随机数,c 是常数,那么对于每一个 δ_0,δ_1,每一个明文集合包含 2^{16} 明文对.

3.2　寻找候选值 $\boldsymbol{\delta_0},\boldsymbol{\delta_1}$

从该集合中选取 2 个不同的明文状态 $\boldsymbol{p}^0\in A_{\alpha,\delta_0,\delta_1}$,$\boldsymbol{p}^1\in A_{\alpha,\delta_0,\delta_1}$,满足仅第 1 对角有活跃状态,其余对角均取常数值.明文状态为

$$\boldsymbol{p}^0=\begin{pmatrix}\alpha & 0 & 0 & 0\\ 0 & \alpha\oplus\delta_0 & 0 & 0\\ 0 & 0 & \alpha\oplus\delta_1 & 0\\ 0 & 0 & 0 & 0\end{pmatrix},$$

$$\boldsymbol{p}^1=\begin{pmatrix}0 & 0 & 0 & 0\\ 0 & \delta_0 & 0 & 0\\ 0 & 0 & \delta_1 & 0\\ 0 & 0 & 0 & 0\end{pmatrix}. \tag{3}$$

然后我们定义异或明文状态的密钥为 k,且分为 4 个对角密钥为 $k=(k_0,k_1,k_2,k_3)$.第 1 对角的密钥为 $k_0=(k_{0,0},k_{1,1},k_{2,2},k_{3,3})$,2 个明文状态经过 1 轮加密后得到中间状态 $\boldsymbol{x}^0$,$\boldsymbol{x}^1$ 及差分 $\boldsymbol{x}^0\oplus\boldsymbol{x}^1$,中间状态差分 $\boldsymbol{x}^0\oplus\boldsymbol{x}^1$ 形式为

$$\boldsymbol{x}^0\oplus\boldsymbol{x}^1=R(\boldsymbol{p}^0)\oplus R(\boldsymbol{p}^1)=\begin{pmatrix}z_0 & 0 & 0 & 0\\ z_1 & 0 & 0 & 0\\ z_2 & 0 & 0 & 0\\ z_3 & 0 & 0 & 0\end{pmatrix}. \tag{4}$$

我们期望 1 轮加密后的中间状态差分 $\boldsymbol{x}^0\oplus\boldsymbol{x}^1$ 符合 5 轮自适应选择密文区分器的输入形式,即有 2 个对角保持差分活跃状态.此时如 3.1 节所述,如果中间状态差分 $\boldsymbol{x}^0\oplus\boldsymbol{x}^1$ 的第 1 列中有 2 B 为 0,那么就满足区分器输入状态,即式(1).

令 $f=SR\circ SB\circ ARK$ 表示 MC 之前的操作,则 $f(\boldsymbol{p}^0)$和 $f(\boldsymbol{p}^1)$的第 1 列差分记为

$$f(\boldsymbol{p}^0)_{C_1}\oplus f(\boldsymbol{p}^1)_{C_1}=\begin{pmatrix}S(k_{0,0}\oplus\alpha)\oplus S(k_{0,0})\\ S(k_{1,1}\oplus\alpha\oplus\delta_0)\oplus S(k_{1,1}\oplus\delta_0)\\ S(k_{2,2}\oplus\alpha\oplus\delta_1)\oplus S(k_{2,2}\oplus\delta_1)\\ 0\end{pmatrix}. \tag{5}$$

其中 S 为 SB 的简记,我们令式(5)的前 3 个字节简记为

$$\beta_0=S(k_{0,0}\oplus\alpha)\oplus S(k_{0,0}),$$
$$\beta_1=S(k_{1,1}\oplus\alpha\oplus\delta_0)\oplus S(k_{1,1}\oplus\delta_0),$$
$$\beta_2=S(k_{2,2}\oplus\alpha\oplus\delta_1)\oplus S(k_{2,2}\oplus\delta_1).$$

为了满足式(1),需要满足 $\beta_0=\beta_1=\beta_2$,即 $\beta_0=\beta_1=\beta_2$ 时,中间状态第 1 列为 0,0,z_2,z_3,这样就可以满足 5 轮区分器的输入要求,即在第 2,3 对角差分活跃.如图 3 所示:

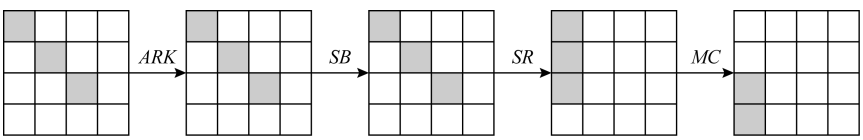

Fig. 3 One round of encryption operation

图 3 1 轮加密操作

如果我们令 δ_0,δ_1 遍历有限域 $F_{2^8}\times F_{2^8}$ 所有值可以得到至少 4 个值能够保证 $z_0=z_1=0$,即,

$$(\delta_0,\delta_1)=(k_{0,0}\oplus k_{1,1},k_{0,0}\oplus k_{2,2}),$$
$$(\delta_0,\delta_1)=(k_{0,0}\oplus k_{1,1},\alpha\oplus k_{0,0}\oplus k_{2,2}),$$
$$(\delta_0,\delta_1)=(\alpha\oplus k_{0,0}\oplus k_{1,1},k_{0,0}\oplus k_{2,2}),$$
$$(\delta_0,\delta_1)=(\alpha\oplus k_{0,0}\oplus k_{1,1},\alpha\oplus k_{0,0}\oplus k_{2,2}).$$

这样我们就可以找到候选值 δ_0,δ_1,即找到正确密钥信息 $k_{0,0}\oplus k_{1,1}$ 和 $k_{0,0}\oplus k_{2,2}$.

3.3 猜测正确密钥

对于每一个 δ_0,δ_1 值,都可以生成一对属于明文集合 $A_{\alpha,\delta_0,\delta_1}$ 中的明文状态$(\boldsymbol{p}^0,\boldsymbol{p}^1)$,并且令明文 $\boldsymbol{p}^0$ 的第 1 对角为 $\boldsymbol{p}_0^0=(\alpha,\alpha\oplus\delta_0,\alpha\oplus\delta_1,0)$,令明文 $\boldsymbol{p}^1$ 的第 1 对角为 $\boldsymbol{p}_0^1=(0,\delta_0,\delta_1,0)$.然后对明文进行 6 轮加密得到密文$(\boldsymbol{c}^0,\boldsymbol{c}^1)$.再根据定义 4 对密文进行混合交换,因为设定在混合操作时仅交换一列,即$|I|=1$.假设我们令 $I=\{0\}$,可以生成和原密文状态 $\boldsymbol{c}^0$,$\boldsymbol{c}^1$ 具有相同的性质的 7 对新的密文对 $\tilde{\boldsymbol{c}}^0$,$\tilde{\boldsymbol{c}}^1=(\rho^v(\boldsymbol{c}^0,\boldsymbol{c}^1),\rho^v(\boldsymbol{c}^1,\boldsymbol{c}^0))$.

再对新的密文对$(\tilde{\boldsymbol{c}}^0,\tilde{\boldsymbol{c}}^1)$进行 6 轮解密得到对应的新明文,记作$(\boldsymbol{p}'^0,\boldsymbol{p}'^1)$,如果新明文对满足一轮加密后的状态差分在第 2,3 对角活跃,即

$$\boldsymbol{v}_d(R(\boldsymbol{p}'^0\oplus k)\oplus R(\boldsymbol{p}'^0\oplus k))=\boldsymbol{v}_d(0,1,1,0). \tag{6}$$

那么就可以筛选出正确密钥,通过对 7 个新的明文对测试每个对角剩余的 2^{16} 个候选密钥来检测式(6)是否成立,如果成立,那么就可能过滤所有错误密钥.为了减少复杂度,我们对明文的 4 个对角状态独立进行检测,即对于每一个新的明文对,首先猜测新明文对$(\boldsymbol{p}'^0,\boldsymbol{p}'^1)$第 1 对角剩余的 2^{16} 密钥,经过一轮加密后,满足式(6)的密钥筛选概率为 2^{-16};然后再依次猜测第 2,3 和 4 对角密钥,经过一轮加密后,分别满足式(6)的密钥筛选概率均为 2^{-16};最后就可以和随机置换区分开.

3.4 算法的主要攻击过程

主要攻击过程由 6 个步骤构成:

1) 选择满足式(3)的明文状态$(\boldsymbol{p}^0,\boldsymbol{p}^1)$;

2) 对所选的明文状态进行 6 轮加密操作得到对应的密文对$(\boldsymbol{c}^0,\boldsymbol{c}^1)$;

3) 对密文对$(\boldsymbol{c}^0,\boldsymbol{c}^1)$进行定义 4 的混合交换操作,得到新的密文对 $\tilde{\boldsymbol{c}}^0,\tilde{\boldsymbol{c}}^1=(\rho^v(\boldsymbol{c}^0,\boldsymbol{c}^1),\rho^v(\boldsymbol{c}^1,\boldsymbol{c}^0))$,共有 7 种不同的交换组合;

4) 取其中 5 对新的密文对进行 6 轮解密操作得到对应的新的明文对$(\boldsymbol{p}'^0,\boldsymbol{p}'^1)$;

5) 检查新的明文对$(\boldsymbol{p}'^0,\boldsymbol{p}'^1)$经过一轮加密后的状态差分是否满足式(6);

6) 满足式(6)的密钥则为正确密钥,不满足的则为错误密钥.

攻击过程如算法 1 所示:

算法 1. 6 轮 AES 密钥恢复攻击算法.

输入:$2^{51.5}$个不同的明文;

输出:密钥 k_0

① for δ_0 from 0 to 2^8-1 do
② for δ_1 from 0 to 2^8-1 do
③ 选择明文的第 1 对角为 $\boldsymbol{p}_0^0=(1,1\oplus\delta_0,1\oplus\delta_1,0)$, $\boldsymbol{p}_0^1=(0,\delta_0,\delta_1,0)$;且令 $\boldsymbol{p}_l^0=\boldsymbol{p}_l^1,l=1,2,3$ 取随机常数值;
④ $\boldsymbol{c}^0\leftarrow enc_k(\boldsymbol{p}^0,6),\boldsymbol{c}^1\leftarrow enc_k(\boldsymbol{p}^1,6)$;/* 明文加密 6 轮得到密文 */
⑤ for m from 0 to 5 do
/* 取 5 对新密文对 */
⑥ $\tilde{\boldsymbol{c}}^0\leftarrow\rho_m^{vI}(\boldsymbol{c}^0,\boldsymbol{c}^1),\tilde{\boldsymbol{c}}^1\leftarrow\rho_m^{vI}(\boldsymbol{c}^1,\boldsymbol{c}^0)$, $|I|=1$;
⑦ $\boldsymbol{p}'^0\leftarrow dec_k(\tilde{\boldsymbol{c}}^0,6),\boldsymbol{p}'^1\leftarrow dec_k(\tilde{\boldsymbol{c}}^1,6)$;
/* 新密文对解密 6 轮得到新明文对 */
⑧ $P\leftarrow P\cup\{(\boldsymbol{p}'^0,\boldsymbol{p}'^1)\}$
⑨ for all $(\boldsymbol{p}'^0,\boldsymbol{p}'^1)\in P$ do
⑩ if $wt(\boldsymbol{v}_d(enc_k(\boldsymbol{p}'^0\oplus k,1)\oplus enc_k(\boldsymbol{p}'^1\oplus k,1)))\neq 2$ then
/* 检查是否满足判定条件(6) */
⑪ break and jump to next key
⑫ end if
⑬ end for
⑭ return k_0
⑮ end for
⑯ end for
⑰ end for

3.5 复杂度计算

1) 数据复杂度

首先,该 5 轮自适应选择密文区分器的概率为 2^{-46},可以构造 $2^{23.5}$ 选择明文和 2^{47} 自适应密文.文献[14]为了减少数据复杂度,对区分器进行了优化,令 3 轮加密后的第 2 个对角差分为 0,则密文状态仅有 3 列活跃,最终构造了 $2^{35.5}$ 选择明文和 2^{39} 自适应密文.

因此,对于 2^{39} 自适应密文,我们可以生成 $2^{39}\times 7$ 对新的新密文对$(\tilde{\boldsymbol{c}}^0,\tilde{\boldsymbol{c}}^1)$,以及对应的 $2^{39}\times 7$ 新明文$(\boldsymbol{p}'^0,\boldsymbol{p}'^1)$.此时猜测每一个对角的 2^{16} 剩余密钥时,错误密钥满足式(6)的概率为 $2^{-16\times 7}=2^{-112}$,因此错误密钥通过的个数为 $2^{39}\times 7\times 2^{16}\times 2^{-112}\approx 2^{-54.19}\ll 1$.实际上,我们仅考虑 5 对新的密文对,去检查是否符合式(6)也是足够的.对于错误密钥,这 5 对新的密文对满足式(6)的概率为 $2^{-16\times 5}=2^{-80}$,因此错误密钥通过的个数为 $2^{39}\times 5\times 2^{16}\times 2^{-80}\approx 2^{-22.68}\ll 1$.所以用5 对就可以过滤掉错误密钥,而不需要 7 对.在实验中,当前 5 对测试成功时,攻击者总是可以通过生成更多的对来消除不确定性,并且不会影响每次攻击的总数据复杂度.因此,要找到正确密钥 $k_{0,0},k_{1,1},k_{2,2},k_{3,3}$,我们需要 $2^{35.5}\times 2^{16}=2^{51.5}$ 选择明文和 $2^{39}\times 2^{16}\times 5\approx 2^{57.42}$ 自适应选择密文.

2) 时间复杂度

对于每一个对角,猜测密钥的集合应该是 2^{16} 而不是 2×2^{16}.因为 δ_0,δ_1 将遍历所有 2^{16} 个可能的值.足以测试 $k_{1,1}=k_{0,0}\oplus\delta_0,k_{2,2}=k_{0,0}\oplus\delta_1$,并没有必要测试 $k_{1,1}=k_{0,0}\oplus\delta_0\oplus\alpha$ 和 $k_{2,2}=k_{0,0}\oplus\delta_1\oplus\alpha$.并且当我们知道 $k_{1,1}\oplus k_{0,0}$ 和 $k_{2,2}\oplus k_{0,0}$ 的值时,我们就可以得到第 3 个密钥信息 $k_{2,2}\oplus k_{1,1}$.

步骤 5 中复杂度的计算:对于每一个新明文对$(\boldsymbol{p}'^0,\boldsymbol{p}'^1)$的每一个对角的密钥我们要检查是否满足式(6),那么每一次需要 2×4 次 S 盒查表,共需要 2^{16}次和 $5\times 2^{39}\times 2^{16}$新的明文,所以这一步所需的时间复杂度为

$$2\times 4\times(5\times 2^{39}\times 2^{16})\times 2^{16}\approx 2^{76.32}.$$

另外,在对新明文检查时,我们对新明文的 4 个对角状态同时且独立得去检查,过滤掉不满足式(6)的密钥,该步所需时间复杂度为 $2^{76.32}\times 4\approx 2^{78.32}$.

所以总时间复杂度为 $2^{78.32}$,一轮加密约等于 20 次查表或 16 次 S 盒查表[9],所以总时间复杂度约为 2^{72}次 6 轮加密.

3) 空间复杂度

我们需要存储 $2^{39}\times 5\times 2^{16}$新明文,因此需要一个顺序表大小为 $2^{57.42}$.另外去检查满足条件的状态对时,需要把明文经过一轮后的状态分别放到大小为 2^{32}的存储表中去寻找碰撞.所以最终需要空间复杂度为 $2^{57.42}+2^{32}\times 4\approx 2^{58}$个 AES-128 块.

4 小版本 AES 实验验证

小版本[18] AES(small-scale AES)分组长度为64 b,64 b 明文将内部状态初始化为一个 4×4 半字节矩阵,在矩阵中每一个字是 4 b.密钥长度为 64 b.轮函数和 AES 一致,其中字节代替变换使用的是 4 b S 盒.行移位变换和列混合变换保持不变.

采用和第 3 节相同的攻击方法,我们可以得到复杂度分析:

数据复杂度.区分器在小版本 AES 的规模下成立的概率应为 2^{-23},因为 AES 的字节是属于有限域 F_{2^8},小版本 AES 的半字节属于有限域 F_{2^4},所以经过优化后最后区分器概率为 2^{-35},我们构造了 2^{18} 选择明文和 2^{20} 对自适应密文.我们考虑了 5 对新的密文对,去检查是否符合式(6).因为这 5 对新的密文对满足式(4)的概率为 $2^{-8\times5}=2^{-40}$,因此错误密钥通过的概率为 $2^{20}\times5\times2^8\times2^{-40}\approx2^{-11.68}\ll1$.所以用 5 对就可以过滤掉错误密钥.因此,要找到 2 个半字节的密钥,我们需要 $2^{18}\times2^8=2^{26}$ 选择明文和 $2^{20}\times2^8\times5\approx2^{30.32}$ 自适应选择密文.

时间复杂度.对于总计算复杂度,测试猜测密钥的集合应该是 2^8.考虑 δ_0,δ_1 将遍历所有 2^8 个可能的值.因此,步骤 5:对于 5 对中的每一对新明文对 $(\boldsymbol{p}'^0,\boldsymbol{p}'^1)$ 的每一个密钥我们要检查是否满足式(6),那么每一次需要 2×4 次 S 盒查表,共需要 2^8 次和 $5\times2^{20}\times2^8$ 新的明文,所以这一步所需的时间复杂度为

$$2\times4\times(5\times2^{20}\times2^8)\times2^8\approx2^{41.32}.$$

另外,在对新明文检查时,我们可以对新明文的 4 个对角状态同时且独立得去检查,过滤掉不满足式(6)的密钥,该步所需时间复杂度为 $2^{41.32}\times4\approx2^{43.32}$.

所以总时间复杂度为 $2^{43.32}$,一轮加密约等于 20 次查表或 16 次 S 盒查表,所以总时间复杂度约为 2^{36} 次 6 轮加密.

空间复杂度.我们需要存储 $5\times2^{20}\times2^8$ 新明文,因此需要一个顺序表大小为 $2^{30.32}$.另外去检查满足条件的状态对时,需要把新明文一轮加密后的状态分别放到大小为 2^{16} 的存储表中去寻找碰撞.所以最终需要空间复杂度为 $2^{30.32}+2^{16}\times4\approx2^{30.32}$ 个 AES-64 块.

通过在 C/C++语言中实现了小版本 AES,如算法 1 所示,总共进行了 10 次测试.所使用的计算机参数为 lntel® Core™ i7-9700 CPU @ 3.00 GHz,内存为 16 GB.实验验证了所提出的密钥恢复攻击的有效性,所以实验结果支持理论结果.

5 总 结

在本文中,我们提出了一种对于 6 轮 AES 新的密钥恢复攻击结果.该攻击过程利用了基于交换等价提出的 5 轮自适应选择密文的区分器和 AES 列混合操作系数矩阵的基本性质,通过在 5 轮自适应选择密文区分器前扩展一轮,利用列混合操作系数矩阵的基本性质和 0 差分性质恢复第 1 轮所需的密钥.结果表明,本文提出的密钥恢复攻击结果在秘密 S 盒下是最优的结果.另外,我们用一个小版本的 AES 去测试来支撑理论结果的正确性.

参 考 文 献

[1] Daemen J, Rijmen V. The design of rijndael: AES—The advanced encryption standard [C] //Proc of Information Security and Cryptography, 2nd eds. Berlin: Springer, 2002: 1-8

[2] Bogdanov A, Khovratovich D, Rechberger C. Biclique cryptanalysis of the full AES [C] //Proc of the 17th Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2011: 344-371

[3] Guo Jian, Peyrin T, Poschmann A, et al. The LED block cipher [G] //LNCS 6917: CHES 2011. Berlin: Springer, 2011: 326-341

[4] Cho J, Choi K Y, Dinur I, et al. WEM: A new family of white-box block ciphers based on the even-mansour construction [G] //LNCS 10159: CT-RSA 2017. Berlin: Springer, 2017: 293-308

[5] Bossuet L, Datta N, Mancillas-López C, et al. ElmD: A pipelineable authenticated encryption and its hardware implementation [C] //Proc of IEEE Transactions Computers65. Berlin: Springer, 2016: 3318-3331

[6] Tiessen T. Polytopic cryptanalysis [G] //LNCS 9665: EUROCRYPT 2016. Berlin: Springer, 2016: 214-239

[7] Grassi L. Mixture differential cryptanalysis: A new approach to distinguishers and attacks on round-reduced AES [C] // IACR Transactions Symmetric Cryptology ISSN 2519-173X. Berlin: Springer, 2018: 133-160

[8] Tiessen T, Knudsen L, Kölbl S, et al. Security of the AES with a secret s-box [G] //LNCS 9054: FSE 2015. Berlin: Springer, 2015: 175-189

[9] Sun Bing, Liu M, Guo Jian, et al. New insights on aes-like SPN ciphers [G] //LNCS 9814: CRYPTO 2016. Berlin: Springer, 2016: 605-624

[10] Grassi L, Rechberger C, Rønjom S. Subspace trail cryptanalysis and its applications to AES [C] //Proc of IACR Transactions Symmetric Cryptol. Berlin: Springer, 2016: 192-225

[11] Grassi L, Rechberger C, Rønjom S. A new structural-differential property of 5-round AES [G] //LNCS 10211: EUROCRYPT 2017. Berlin: Springer, 2017: 289-317

[12] Rønjom S, Bardeh N, Helleseth T. Yoyo tricks with AES [G] //LNCS 10624: ASIACRYPT 2017. Berlin: Springer, 2017: 217-243

[13] Bardeh N, Rønjom S. The exchange attack: How to distinguish six rounds of AES with $2^{88.2}$ chosen plaintexts [G] //LNCS 11923: ASIACRYPT 2019. Berlin: Springer, 2019: 347-370

[14] Bardeh N. A key-independent distinguisher for 6-round aes in an adaptive setting [EB/OL]. IACR Cryptol. ePrint Arch. 2019 [2021-04-23]. https://eprint.iacr.org/2019/945.pdf

[15] Bardeh N, Rønjom S. Practical attacks on reduced-round AES [G] //LNCS 11627: AFRICACRYPT 2019. Berlin: Springer, 2019: 770-783

[16] Cheon J, Kim M, Kim K, et al. Improved impossible differential cryptanalysis of rijndael and crypton [G] //LNCS 2288: ICISC 2001. Berlin: Springer, 2001: 39-49

[17] Grassi L. Probabilistic mixture differential cryptanalysis on round-reduced AES [G] //LNCS11959: SAC 2019. Berlin: Springer, 2019: 53-84

[18] Cid C, Murphy S, Robshaw M. Small scale variants of the AES [G] //LNCS 3557: FSE 2005. Berlin: Springer, 2005: 145-162

Zhang Li, born in 1994. PhD. Her main research interests include cryptanalysis of block ciphers.

张　丽,1994 年生.博士.主要研究方向为分组密码的密码分析.

Wu Wenling, born in 1966. PhD, professor, and PhD supervisor in the Chinese Academy of Sciences. Senior member of CCF. Her main research interests include design and cryptanalysis of block ciphers and Hash functions, and cryptography.

吴文玲,1966 年生.博士,教授,中国科学院博士生导师,CCF 高级会员.主要研究方向为分组密码和 Hash 函数的设计与密码分析以及密码学.

Zhang Lei, born in 1981. PhD, associate professor. Her main research interests include design and cryptanalysis of block ciphers and Hash functions, and cryptography.

张　蕾,1981 年生.博士,副教授.主要研究方向为分组密码和 Hash 函数的设计与密码分析以及密码学.

Zhang Yafei, born in 1981. PhD. Her main research interests include design and cryptanalysis of block ciphers.

郑雅菲,1988 年生.博士.主要研究方向为分组密码的设计与密码分析.