

3D密码的7轮子空间迹区分器

杨 阳 刘文豪* 曾 光

(信息工程大学密码工程学院 郑州 450000)

摘 要: 子空间迹攻击是一种新型分组密码分析方法, 该文对使用了类AES密码新结构的3D密码子空间性质进行研究。首先利用3D密码的3轮明确子空间迹, 结合子空间的交集性质, 首次构造出3D密码的7轮子空间迹不可能差分区分器, 数据复杂度为 $2^{193.1}$ 个选择明文, 时间复杂度为 $2^{202.3}$ 次查表操作, 成功率为60.6%; “ n 倍”性质指子空间的全部明文对经过一轮加密, 差分属于同一子空间的密文对个数为 n 的倍数。利用该性质, 构造了3D密码的7轮结构区分器, 数据复杂度为 2^{128} 个选择明文, 时间复杂度为 $2^{129.6}$ 次查表操作, 存储复杂度为 2^{128} Byte, 成功率大于99.99%。

关键词: 子空间迹; 不可能差分; 结构区分器; 3D密码

中图分类号: TN918.1

文献标识码: A

文章编号: 1009-5896(2023)02-0617-09

DOI: 10.11999/JEIT211438

7-round Subspace Trail Distinguisher of 3D Cipher

YANG Yang LIU Wenhao ZENG Guang

(School of Cryptography Engineering, Information Engineering University, Zhengzhou 450000, China)

Abstract: Subspace trail attack is a new analysis method for block ciphers. The properties of subspaces of 3D cipher which uses a new structure of AES-like ciphers is studied. First of all, a 3-round definite subspace trail of 3D cipher is constructed in this paper, combined with the intersection property of subspaces, and the 7-round subspace trail impossible differential distinguisher of 3D cipher is obtained for the first time. Its data complexity is $2^{193.1}$ chosen plaintexts, time complexity is $2^{202.3}$ look-up operations, and the success rate is 60.6%. The multiple-of- n property means that all plaintext pairs in the subspace undergo a round of encryption, and the number of ciphertext pairs whose differences belong to a certain subspace is a multiple of n . Using this property, a 7-round structural distinguisher of 3D cipher is constructed. The data complexity is 2^{128} chosen plaintexts, the time complexity is $2^{129.6}$ look-up operations, the storage complexity is 2^{128} Byte, and the success rate is greater than 99.99%.

Key words: Subspace trail; Impossible difference; Structural distinguisher; 3D cipher

1 引言

2008年, Nakahara^[1]在CANS2008上提出3D密码。3D密码可视为3维的AES算法, 将 4×4 的字节矩阵扩展为 $4 \times 4 \times 4$, 分组长度和密钥规模均为512 bit, 共22轮。

3D密码设计理念新颖, 对它的安全性分析自提出起持续至今。2010年王美一等人^[2]提出了9轮

3D密码的Square攻击, 唐学海等人^[3]给出了9轮不可能差分攻击, 之后Nakahara^[4]将不可能差分攻击提升到10轮。2012年, 苏崇茂等人^[5]构造出3D密码的5轮中间相遇区分器, 给出了10轮中间相遇攻击, Koyama等人^[6]于同年给出11轮3D密码的截断差分分析, 成功率约为24%。2014年, 谢作敏等人^[7]给出了11轮3D密码的不可能差分攻击。2015年, 任炯炯等人^[8]给出了11轮3D密码的中间相遇攻击。2021年, Hou等人^[9]利用3D密码的6轮yoyo区分器, 给出了实际可行的7轮3D密码算法的密钥恢复攻击。

在关注对3D密码的攻击的同时, 可以发现上述攻击使用的区分器轮数均小于7轮。Square攻击使用了5.25轮、6.25轮区分器, 11轮3D密码的不可能差分和中间相遇攻击均构造出6轮区分器, 且区

收稿日期: 2021-12-06; 改回日期: 2022-06-13; 网络出版: 2022-06-30

*通信作者: 刘文豪 13605538396@163.com

基金项目: 数学工程与先进计算国家重点实验室开放基金课题 (2020A08)

Foundation Item: The Open Fund Project of the State Key Laboratory of Mathematical Engineering and Advanced Computing (2020A08)

分优势均为 2^{-504} , 区分3D密码与随机函数所需数据量不低于 $2^{252.5}$ 。7轮3D密码的yoyo攻击使用了6轮yoyo区分器。为突破现有的区分器轮数, 本文研究子空间迹分析方法在3D密码上的应用。

2016年, Grassi等人^[10]提出了子空间迹的概念。子空间迹不强调子空间结构在轮函数下的不变性, 而是表现了子空间结构在轮函数下变化的规律, 进而利用具有一定规律的子空间迹建立区分器。自提出以来, 子空间迹主要用于对AES, Midori等SPN密码算法的分析^[11], 利用该方法在构造区分器或进行密钥恢复时, 不需要S盒的具体信息。

下面描述基于子空间迹的区分器——结构区分器。

2017年文献^[12]利用子空间迹, 找到了AES的新性质——穷举子空间 D_i 的全部明文对, 经过5轮加密, 将有固定倍数个密文对的差分属于子空间 M_J (子空间 D_i 和 M_J 将在第3节中定义)。将这样的“ n 倍”性质与明确子空间迹结合, 构造出5轮AES子空间迹结构区分器。同年, Grassi^[13]给出了基于AES结构区分器的混合差分攻击。2019年Boura等人^[14]给出了结构区分器的构造条

件。2020年, Grassi等人^[15]利用子空间迹给出9轮AES-128的选择密钥区分器。2021年, Grassi等人^[16]对P-SPN结构及Hades结构进行子空间迹分析并给出判断线性层是否易受攻击的工具。

子空间迹分析方法在构造区分器上有独特的优势, 往往可以找到轮数更长的区分器。本文将基于子空间的性质, 寻找3D密码的7轮区分器。

第2节介绍3D密码算法, 定义其子空间并研究子空间传播规律; 第3节证明了3D密码两个子空间交集为0, 由此给出在选择明文条件下, 区分优势最大的6轮3D密码差分区分器, 进一步给出首个7轮3D密码的子空间迹不可能差分区分器; 第4节介绍兼容、信息集、等价关系的定义及相关定理, 说明了3D密码特定子空间与S层的可兼容性, 据此给出3D密码的7轮结构区分器; 第5节总结成果并提出开放性问题。

2 初步准备

2.1 3D密码算法

3D密码算法的分组规模和密钥规模都是512 bit, 迭代轮数为22轮。分组状态表示为64 Byte的形式, 可视为4个子块的联结

$$\left(\begin{array}{cc|cc|cc|cc} s_0 & s_4 & s_8 & s_{12} & s_{16} & s_{20} & s_{24} & s_{28} & s_{32} & s_{36} & s_{40} & s_{44} & s_{48} & s_{52} & s_{56} & s_{60} \\ s_1 & s_5 & s_9 & s_{13} & s_{17} & s_{21} & s_{25} & s_{29} & s_{33} & s_{37} & s_{41} & s_{45} & s_{49} & s_{53} & s_{57} & s_{61} \\ s_2 & s_6 & s_{10} & s_{14} & s_{18} & s_{22} & s_{26} & s_{30} & s_{34} & s_{38} & s_{42} & s_{46} & s_{50} & s_{54} & s_{58} & s_{62} \\ s_3 & s_7 & s_{11} & s_{15} & s_{19} & s_{23} & s_{27} & s_{31} & s_{35} & s_{39} & s_{43} & s_{47} & s_{51} & s_{55} & s_{59} & s_{63} \end{array} \right) \quad (1)$$

3D算法采用SPN结构, 轮函数依次由非线性变换、行移位、列混合变换、密钥异或这4个变换组成。具体介绍如下。

非线性变换 γ 。使用AES的8 bit S盒。

行移位 θ_1, θ_2 。 θ_1 是对3D密码的4个子块做AES的行移位变换, θ_2 是将字节块视为一个整体进行行移位。 θ_1 将式(1)中的状态矩阵变为

$$\left(\begin{array}{cc|cc|cc|cc} s_0 & s_4 & s_8 & s_{12} & s_{16} & s_{20} & s_{24} & s_{28} & s_{32} & s_{36} & s_{40} & s_{44} & s_{48} & s_{52} & s_{56} & s_{60} \\ s_5 & s_9 & s_{13} & s_1 & s_{21} & s_{25} & s_{29} & s_{17} & s_{37} & s_{41} & s_{45} & s_{33} & s_{53} & s_{57} & s_{61} & s_{49} \\ s_{10} & s_{14} & s_2 & s_6 & s_{26} & s_{30} & s_{18} & s_{22} & s_{42} & s_{46} & s_{34} & s_{38} & s_{58} & s_{62} & s_{50} & s_{54} \\ s_{15} & s_3 & s_7 & s_{11} & s_{31} & s_{19} & s_{23} & s_{27} & s_{47} & s_{35} & s_{39} & s_{43} & s_{63} & s_{51} & s_{55} & s_{59} \end{array} \right)$$

θ_2 将式(1)中的状态矩阵变为

$$\left(\begin{array}{cc|cc|cc|cc} s_0 & s_4 & s_8 & s_{12} & s_{16} & s_{20} & s_{24} & s_{28} & s_{32} & s_{36} & s_{40} & s_{44} & s_{48} & s_{52} & s_{56} & s_{60} \\ s_{17} & s_{21} & s_{25} & s_{29} & s_{33} & s_{37} & s_{41} & s_{45} & s_{49} & s_{53} & s_{57} & s_{61} & s_1 & s_5 & s_9 & s_{13} \\ s_{34} & s_{38} & s_{42} & s_{46} & s_{50} & s_{54} & s_{58} & s_{62} & s_2 & s_6 & s_{10} & s_{14} & s_{18} & s_{22} & s_{26} & s_{30} \\ s_{51} & s_{55} & s_{59} & s_{63} & s_3 & s_7 & s_{11} & s_{15} & s_{19} & s_{23} & s_{27} & s_{31} & s_{35} & s_{39} & s_{43} & s_{47} \end{array} \right)$$

θ_1 应用于奇数轮, θ_2 应用于偶数轮。

列混合变换 π 。使用 $F_{2^8}^{4 \times 4}$ 上对合矩阵 M 对状态中每一列进行有限域上乘法, 即 $M \cdot (s_i, s_{i+1}, s_{i+2}, s_{i+3})' \rightarrow (s_i, s_{i+1}, s_{i+2}, s_{i+3})'$, 其中 $i = 0, 4, \dots, 60$, M 及其逆矩阵 M^{-1} 为

$$M = \begin{pmatrix} 01x & 02x & 04x & 06x \\ 02x & 01x & 06x & 04x \\ 04x & 06x & 01x & 02x \\ 06x & 04x & 02x & 01x \end{pmatrix},$$

$$M^{-1} = \begin{pmatrix} 01x & 02x & 04x & 06x \\ 02x & 01x & 06x & 04x \\ 04x & 06x & 01x & 02x \\ 06x & 04x & 02x & 01x \end{pmatrix}.$$

密钥异或KeyAdd。将状态矩阵与轮子密钥对应字节进行模2加运算。

密钥扩展算法与子空间迹分析无关, 在此不做介绍。记 E_k 和 E_k' 分别表示奇数轮和偶数轮加密函数, 旨在突出两种行移位变换, 不区分圈子密钥。使用 F_k^m 表示 m 轮3D密码加密函数。 a 加密一轮的结果为 $F_k(a) = \pi \cdot \theta \cdot \gamma \cdot \text{KeyAdd}(a)$ 。为保证3D密码算法加脱密相似性, 算法在最后一轮省略列混合变换。

2.2 3D密码的子空间与传播规律

首先介绍子空间迹的定义。

定义1^[10] 设 $F_K(\cdot) = F(\cdot) \oplus K$ 为某分组密码的轮函数, $(V_1, V_2, \dots, V_{r+1})$ 为满足 $\dim(V_i) \leq \dim(V_j)$, $1 \leq i < j \leq r+1$ 的 $r+1$ 个子空间且他们包含于 F_2^n 。若任意 a_i 属于 $V_i^\perp$, 存在 a_{i+1} 属于 $V_{i+1}^\perp$, 使得 $F_K(V_i \oplus a_i)$ 包含于 $V_{i+1} \oplus a_{i+1}$, 则称 $(V_1, V_2, \dots, V_{r+1})$ 为 F_K 的长度为 r 的子空间迹, 记为 $V_1 \rightarrow V_2 \rightarrow \dots \rightarrow V_{r+1}$ 。称 V_i 为 V_{i+1} 的前驱, V_{i+1} 为 V_i 的后继。若 $U \xrightarrow{F_K} V$, 且有 $V \xrightarrow{F_K} U$, 将这样加、脱密都以概率1成立的子空间迹称为明确子空间迹, 记为 $U \rightleftharpoons V$ 。

3D密码可以视作3维的AES密码算法, 因此, 可利用文献[10]中的AES子空间刻画3D密码的子空间, 并研究子空间传播规律。下面若不特别说明, 下标 i, j, h 为正整数, 取值范围均为 $[0, 3]$ 。

对于向量空间 V 和 $F_{2^8}^{4 \times 4}$ 上的函数 F , 令 $F(V) = \{F(v) | v \in V\}$ 。本文所有的子空间都定义为域

$$\left(\begin{array}{cccc|cccc} x_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & x_3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_4 & 0 & 0 & 0 & 0 \end{array} \right).$$

根据 $D_I \rightleftharpoons C_I$, 容易得到3D密码的一条明确子空间迹 $(D_i, D_i, D_i, D_i) \xrightarrow{E_k} (C_i, C_i, C_i, C_i)$ 。

引理1 $(C_i, C_i, C_i, C_i) \xrightarrow{E_k'} (C_i, C_i, C_i, C_i)$ 。

证明 S盒保持子空间 (C_i, C_i, C_i, C_i) 的形式。由于 (C_i, C_i, C_i, C_i) 的变量均在4个子块的第 i 列, 且 θ_2 是对字节块整体进行行移位, 并不改变各个变量在子块中的位置, 故经过 θ_2 变换后仍然为 (C_i, C_i, C_i, C_i) 。列空间是列混合函数的不变子空间, 故有

F_{2^8} 上空间 $F_{2^8}^{4 \times 4}$ 的子空间。另外, 记 $E = \{e_{0,0,0}, e_{0,0,1}, \dots, e_{3,3,3}\} = \{e_0, e_1, \dots, e_{63}\}$ 为 $F_{2^8}^{4 \times 4 \times 4}$ 的单位基空间, 其中, $e_{i,j,h}$ 是第 i 子块的第 j 行第 h 列字节为1, 其他63个字节全为0的状态矩阵。下面定义3D密码子块的子空间。

列空间: $C_i = \langle e_{4i}, e_{4i+1}, e_{4i+2}, e_{4i+3} \rangle$; 对角空间: $D_i = \theta_1^{-1}(C_i)$; 逆对角空间: $ID_i = \theta_1(C_i)$; 混合空间 $M_i = M(ID_i)$ 。

举例说明, 若 $\forall x_1, x_2, x_3, x_4 \in F_2^8$, 则

$$C_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ x_2 & 0 & 0 & 0 \\ x_3 & 0 & 0 & 0 \\ x_4 & 0 & 0 & 0 \end{bmatrix} \right\},$$

$$D_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{bmatrix} \right\},$$

$$ID_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & x_2 \\ 0 & 0 & x_3 & 0 \\ 0 & x_4 & 0 & 0 \end{bmatrix} \right\},$$

$$M_0 = \left\{ \begin{bmatrix} x_1 & 02x \cdot x_4 & 04x \cdot x_3 & 06x \cdot x_2 \\ 02x \cdot x_1 & x_4 & 06x \cdot x_3 & 04x \cdot x_2 \\ 04x \cdot x_1 & 06x \cdot x_4 & x_3 & 02x \cdot x_2 \\ 06x \cdot x_1 & 04x \cdot x_4 & 02x \cdot x_3 & x_2 \end{bmatrix} \right\}.$$

定义2 给定 $I \subseteq \{0, 1, 2, 3\}$, 其中 $0 < |I| \leq 3$, 定义

$$C_I = \bigoplus_{i \in I} C_i, D_I = \bigoplus_{i \in I} D_i, ID_I = \bigoplus_{i \in I} ID_i, M_I = \bigoplus_{i \in I} M_i.$$

文献[10]证明了 $D_I \rightleftharpoons C_I$, $C_I \rightleftharpoons M_I$, 这是两条明确子空间迹, 即加、脱密概率均为1。下面给出3D密码算法的子空间传播规律及子空间迹。

3D密码的状态矩阵可以视为4个 4×4 矩阵的联结, 故可用以上4种 $F_{2^8}^{4 \times 4}$ 上的子空间来表示3D密码的子空间。例如, 用 $(D_0, 0, 0, 0)$ 表示子空间

$$\left(\begin{array}{cccc|cccc} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right).$$

$(C_i, C_i, C_i, C_i) \xrightarrow{E_k'} (C_i, C_i, C_i, C_i)$ 。脱密的过程与加密类似, 有 $(C_i, C_i, C_i, C_i) \xrightarrow{E_k'^{-1}} (C_i, C_i, C_i, C_i)$, 即 $(C_i, C_i, C_i, C_i) \xrightarrow{E_k'} (C_i, C_i, C_i, C_i)$ 。证毕

结合上面两个结论与 $C_I \rightleftharpoons M_I$ 得到引理2。

引理2 3D密码有3轮明确子空间迹。

$$(D_i, D_i, D_i, D_i) \xrightarrow{E_k} (C_i, C_i, C_i, C_i) \xrightarrow{E_k'} (C_i, C_i, C_i, C_i) \xrightarrow{E_k} (M_i, M_i, M_i, M_i)$$

3 3D密码的子空间迹不可能差分区器

本节研究3D密码子空间的交集性质,寻找交集为 $\{0\}$ 的两个子空间,构造出区分优势最大的6轮3D密码不可能差分区器。文献[10]介绍了一种将密钥恢复攻击转化成区分器的技术,能把基于子空间迹区分器的攻击变为新区分器,从而延长区分器轮数。将这种技术应用于3D密码,首次构造出3D密码的7轮子空间迹不可能差分区器。

3.1 3D密码子空间的交集性质及6轮子空间迹不可能差分区器

研究子空间的交集性质对子空间迹分析有重要意义,根据迹端点的交集属性,可以得到较长迹的可预测子空间属性,原因是两个子空间的交集经过密码函数时,交集属性被保持。而交集能够降低子空间的维数,故精确地刻画一个子空间是哪些子空间的交集,并以交集的形式进行传播,能有效降低子空间经过密码函数时增长的维数,从而寻找到更长的子空间迹。先定义两个新的子空间。

定义3(行空间) 行空间 R_i 定义为 $R_i = \theta_2(M_i) = \langle e_i, e_{i+4}, e_{i+8}, e_{i+12} \rangle$ 。

例如,行空间 R_0 为矩阵

$$R_0 = \left\{ \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \mid \forall x_1, x_2, x_3, x_4 \in F_{2^8} \right\}。$$

行空间由混合空间经过 θ_2 得到,例如: $(M_0, 0, 0, 0) \xrightarrow{\theta_2} (R_0, R_3, R_2, R_1)$ 。

定义4(窗口空间) 窗口空间 W_i 定义为 $W_i = \pi(R_i)$ 。

例如,窗口空间 W_0 为矩阵

$$W_0 = \left\{ \begin{bmatrix} x_1 & x_2 & x_3 & x_4 \\ 02x \cdot x_1 & 02x \cdot x_2 & 02x \cdot x_3 & 02x \cdot x_4 \\ 04x \cdot x_1 & 04x \cdot x_2 & 04x \cdot x_3 & 04x \cdot x_4 \\ 06x \cdot x_1 & 06x \cdot x_2 & 06x \cdot x_3 & 06x \cdot x_4 \end{bmatrix} \mid \forall x_1, x_2, x_3, x_4 \in F_{2^8} \right\}。$$

下面给出一个与3D密码不可能差分相关的重要引理。

引理3 $D_i \cap W_j = \{0\}$ 对所有 $i, j=0, 1, 2, 3$ 成立。

证明 W_j 的一个基为

$$W_j = \langle \pi(e_j), \pi(e_{j+4}), \pi(e_{j+8}), \pi(e_{j+12}) \rangle,$$

$D_i = \langle e_{4i}, e_{4i+5}, e_{4i+10}, e_{4i+15} \rangle$, 其中所有下标均模16。

注意到 $\{e_0, e_1, \dots, e_{15}\} = \{e_{0,0}, e_{0,1}, \dots, e_{3,3}\}$, 可将上面两个子空间的基改写为

$$W_j = \langle \pi(e_{j,0}), \pi(e_{j,1}), \pi(e_{j,2}), \pi(e_{j,3}) \rangle,$$

$$D_i = \langle e_{0,i}, e_{1,i+1}, e_{2,i+2}, e_{3,i+3} \rangle。$$

假设 $D_i \cap W_j \neq \{0\}$, 这表明存在 x_k, y_k , 对于 $k=0, 1, 2, 3$, 使得

$$\begin{aligned} & \bigoplus_{k=0}^3 x_k \cdot e_{k,i+k} \oplus \bigoplus_{k=0}^3 y_k \cdot \pi(e_{j,k}) \\ &= \bigoplus_{k=0}^3 [x_{k-i} \cdot e_{k-i,k} \oplus y_k \cdot \pi(e_{j,k})] = 0 \end{aligned}$$

存在非平凡解, 且唯一解为

$$x_{k-i} \cdot e_{k-i,k} \oplus y_k \cdot \pi(e_{j,k}) = 0。$$

对每个 k 都成立, 而这显然不可能, 因为 $e_{k-i,k}$ 与 $\pi(e_{j,k})$ 线性无关。故 $D_i \cap W_j = \{0\}$ 。 证毕

当 $|I| + |J| \leq 4$ 时, D_I 和 W_J 的交集只有 $\{0\}$ 。实际上, 考虑引理4.2.1证明中的等式, 当 $|I| + |J| \leq 4$ 时, 每个 k (即每列)至多有4项, 其中至少有一项来自 $\{e_{0,0}, e_{0,1}, \dots, e_{3,3}\}$ 的第 k 列, 至少一项来自 $\{\pi(e_{0,0}), \pi(e_{0,1}), \dots, \pi(e_{3,3})\}$ 的第 k 列, 因此等式只有平凡解。当 $|I| + |J| > 5$ 时, 每个等式中至少有5项, 而方程组一共只有4行, 等式必有非零解。故可得出引理4的结论。

引理4 当 $|I| + |J| \leq 4$ 时, $D_I \cap W_J = \{0\}$ 。

设3D密码第2轮的起始子空间为 $(D_{1,2,3} \cap C_0, 0, 0, 0)$, 根据2.2节的子空间传播规律有

$$\begin{aligned} (D_{1,2,3} \cap C_0, 0, 0, 0) & \xrightarrow{E'_k} (0, C_0, C_0, C_0) \\ & \xrightarrow{E_k} (0, M_0, M_0, M_0) \end{aligned}$$

引理5 对 $\forall h, i, j \in \{0, 1, 2, 3\}$, 且 $a \in (0, M_0, M_0, M_0)^\perp$, 存在 $b \in (W_{1,2,3}, W_{0,1,2}, W_{0,1,3}, W_{0,2,3})^\perp$, 使得

$$\begin{aligned} & E'_k [(0, M_h, M_i, M_j) \oplus a] \\ &= (W_{1,2,3}, W_{0,1,2}, W_{0,1,3}, W_{0,2,3}) \oplus b。 \end{aligned}$$

证明 将全空间记为 F , 则有 $\gamma[(0, M_h, M_i, M_j) \oplus a] = (0, F, F, F) \oplus a'$, 此时 $a'_t = S(a_t)$, $t=0, 1, \dots, 63$ 。行移位 θ_2 将0子块的4行分散到4个子块, 即有 $\theta_2[(0, F, F, F) \oplus a'] = (R_{1,2,3}, R_{0,1,2}, R_{0,1,3}, R_{0,2,3}) \oplus a''$, 其中 $a'' = \theta_2(a')$ 。因为列混合变换是线性变换, 所以 $\pi[(R_{1,2,3}, R_{0,1,2}, R_{0,1,3}, R_{0,2,3}) \oplus a''] = (W_{1,2,3}, W_{0,1,2}, W_{0,1,3}, W_{0,2,3}) \oplus b$, 其中 $b = \pi(a'')$ 。 证毕

结合引理5与上面结论, 有

$$\begin{aligned} (D_{1,2,3} \cap C_0, 0, 0, 0) & \xrightarrow{E'_k} (0, C_0, C_0, C_0) \\ & \xrightarrow{E_k} (0, M_0, M_0, M_0) \\ & \xrightarrow{E'_k} (W_{1,2,3}, W_{0,1,2}, W_{0,1,3}, W_{0,2,3}) \end{aligned}$$

结合引理2, 得到3D密码的一条6轮子空间迹不可能差分

$$\begin{aligned} (D_{1,2,3} \cap C_0, 0, 0, 0) &\xrightarrow{E'_k \circ E_k \circ E'_k} \\ (W_{1,2,3}, W_{0,1,2}, W_{0,1,3}, W_{0,2,3}) &\stackrel{\text{impossible}}{=} \\ (D_0, D_0, D_0, D_0) &\stackrel{F_k^3}{\rightleftharpoons} (M_0, M_0, M_0, M_0). \end{aligned}$$

截断不可能差分区器从终点差分矩阵脱密到中间差分矩阵, 再与起始差分加密得到的中间状态产生矛盾。为延长区分器, 一般终点差分矩阵只有一个变量, 例如3D密码的6轮截断不可能差分区器^[7], 其区分优势为 $2^8/2^{512} \approx 2^{-504}$, 与3D密码的6轮中间相遇区分器^[8]区分优势相同。

而子空间迹不可能差分区器在中间矛盾处, 利用的是两个子空间交集为 $\{0\}$ 的性质, 且后几轮为明确子空间迹, 维数保持不变, 故终点子空间的差分变量更多。上面给出的3D密码的6轮子空间迹不可能差分区器的区分优势为 $2^{4 \times 4 \times 8}/2^{512} \approx 2^{-384}$, 这是目前选择明文条件下区分优势最大的6轮3D密码区分器。

注意到, 上面的子空间迹不可能差分区器与密码规模、S盒和密钥的具体信息无关, 即对带一个秘密S盒的3D密码同样有效。

3.2 3D密码的7轮子空间迹不可能差分区器

下面在6轮子空间迹不可能差分的基础上给出7轮3D密码的子空间迹不可能差分区器。

给定明文 $P^0, P^1 \in F_{2^8}^{4 \times 4}$, 在第0 Byte、第5 Byte差分非零, 即 $P^0 \oplus P^1 \in D_0 \cap C_{0,1}$, 第0 Byte、第5 Byte上的变量分别记为 $\{p_0^0, p_5^0\}, \{p_0^1, p_5^1\}$, 其余14 Byte对应相等。记轮子密钥第0 Byte、第5 Byte为 k_0, k_5 , 经过一轮加密后, 密文对在第0 Byte的差分为

$$\begin{aligned} S(p_0^0 \oplus k_0) \oplus 02x \cdot S(p_5^0 \oplus k_5) \oplus S(p_0^1 \oplus k_0) \\ \oplus 02x \cdot S(p_5^1 \oplus k_5). \end{aligned}$$

存在明文对与对应密钥使上式为0, 则有子空间迹 $D_0 \cap C_{0,1} \rightarrow D_{1,2,3} \cap C_0$, 对应3D密码的子空间迹

$$\begin{aligned} (D_0 \cap C_{0,1}, 0, 0, 0) &\xrightarrow{E_k} (D_{1,2,3} \cap C_0, 0, 0, 0) \\ &\xrightarrow{E'_k} (0, C_0, C_0, C_0) \\ &\xrightarrow{E_k} (0, M_0, M_0, M_0). \end{aligned}$$

建立表格 T , 存储 $S(x) \oplus 02x \cdot S(y) \oplus S(z) \oplus 02x \cdot S(w) = 0$ 的全部解, 当明文与密钥异或后等于表 T 中值时, 子空间迹成立。

根据2.2节给出的3D密码子空间传播规律及引理5得到一条3D密码的子空间迹

$$\begin{aligned} (D_0 \cap C_{0,1}, 0, 0, 0) &\xrightarrow{E_k} (D_{1,2,3} \cap C_0, 0, 0, 0) \\ &\xrightarrow{E'_k} (0, C_0, C_0, C_0) \xrightarrow{E_k} (0, M_0, M_0, M_0) \\ &\xrightarrow{E'_k} (W_{1,2,3}, W_{0,1,2}, W_{0,1,3}, W_{0,2,3}). \end{aligned}$$

根据引理4, 有 $(W_{1,2,3}, W_{0,1,2}, W_{0,1,3}, W_{0,2,3}) \cap (D_0, D_0, D_0, D_0) = \{0\}$, 再由引理2, 得到一条3D密码的7轮子空间迹不可能差分

$$\begin{aligned} (D_0 \cap C_{0,1}, 0, 0, 0) &\xrightarrow{F_k^4} (W_{1,2,3}, W_{0,1,2}, W_{0,1,3}, W_{0,2,3}) \\ &\stackrel{\text{impossible}}{=} (D_0, D_0, D_0, D_0) \\ &\stackrel{F_k^3}{\rightleftharpoons} (M_0, M_0, M_0, M_0). \end{aligned}$$

为计算区分器的数据复杂度, 首先介绍“生日悖论”, 寻找所需输入明文的最小数目, 以保证在随机情形中以高概率产生碰撞。

给定 d 值和 n 个变量, 其中至少两个变量具有相同值的概率可以计算为

$$p = 1 - \frac{n!}{(n-d)! \cdot n^d} = 1 - \frac{(d)!}{n^d} C_n^d \cong 1 - e^{-\frac{d(d-1)}{2n}}.$$

最终检测的子空间为 (M_j, M_j, M_j, M_j) , j 的取值有4种, 故密文对差分落入 (M_j, M_j, M_j, M_j) 的概率为 $4 \times 2^{-512+32 \cdot 4} = 2^{-382}$ 。当有 $2^{192.3}$ 个明文, 即明文对数 $n=2^{383.6}$ 时, 有94%的概率得到碰撞; 当有 $2^{193.1}$ 个明文, 即明文对数 $n=2^{385.2}$, 则碰撞概率 p 大于99.98% ($0.9998^{256} = 0.95$, 即得到256次碰撞的概率为95%)。

下面计算该区分器所需数据量及时间复杂度。

实验数据表明, 256次碰撞中有63.8%的概率得到正确密钥对应的明文对。当函数为3D密码时, 修改该明文对第0 Byte、第5 Byte以外的值并加密, 不会得到碰撞。512次碰撞对应概率为87.8%。

以256次碰撞为区分界限, 使用 $2^{193.1}$ 个选择明文, 将以95%的概率得到256次碰撞, 有63.8%的概率将7轮3D密码与随机函数区分开。故该3D密码的7轮子空间迹不可能差分区器的数据复杂度为 $2^{193.1}$ 个选择明文, 成功率为 $95\% \times 63.8\% = 60.6\%$ 。

敌手需要构造 $(D_0 \cap C_{0,1}, 0, 0, 0)$ 中的消息对, 计算落入 (M_j, M_j, M_j, M_j) ($j = 0, 1, 2, 3$) 同一陪集中的密文对对数, 最好的减少计算复杂度的方法是对集合中的全部元素“re-order”^[10], 算法描述在文献^[10]中, 仅计算排过序的消息的碰撞数。此时共有 $2^{193.1}$ 个元素, “re-order”算法需要 $3 \times 2^{193.1} \times (\log 2^{193.1} + 1) \approx 2^{202.3}$ 次查找表操作, 即此区分器的时间复杂度为 $2^{202.3}$ 。

最后给出3D密码的7轮子空间迹不可能差分区器的具体算法:

给定 $2^{193.1}$ 个选择明密对 (p^i, c^i) , $i = 0, 1, \dots, [2^{193.1} - 1]$, 每个 p^i 都属于 $(D_0 \cap C_{0,1}, 0, 0, 0)$ 的同一陪集。

离线阶段。 建立表格 T , 存储 $S(x) \oplus 02x \cdot S(y) \oplus S(z) \oplus 02x \cdot S(w) = 0$ 全部解。

步骤1 随机选择明密对, 检测经逆列混合变换后的密文对差分是否属于子空间 (ID_i, ID_i, ID_i, ID_i) , 其中 $i = 0, 1, 2, 3$ 。若无碰撞且已经使用 $2^{193.1}$ 个明密对, 输出1, 否则返回步骤1; 若产生碰撞, 进入步骤2;

步骤2 排除明文对与表格 T 中的解异或后的密钥值。若全部密钥被排除, 输出0; 否则, 返回步骤1。

4 3D密码的结构区分器

第3节研究了3D密码子空间交集性质, 给出了3D密码的7轮子空间迹不可能差分区器, 下面给出兼容、信息集、等价概念的定義及相关定理, 利用3D密码子空间与S层的可兼容性, 得到“ n 倍”性质并给出3D密码的7轮区分器。现有密

$$\begin{pmatrix} * & \cdots & * \\ \cdots & \lambda_{0,l,i} & \cdots \\ * & \cdots & * \\ & & * & \cdots & * \\ & & \cdots & \lambda_{k,l,i} & \cdots \\ & & * & \cdots & * \\ & & & & * & \cdots & * \\ & & & & \cdots & \lambda_{h-1,l,i} & \cdots \\ & & & & * & \cdots & * \end{pmatrix} \begin{matrix} \leftarrow j_0 + l \\ \leftarrow j_k + l \\ \leftarrow j_{h-1} + l \end{matrix}$$

$$\begin{matrix} \uparrow & \uparrow & \uparrow \\ g_{0,i} & g_{k,i} & g_{h-1,i} \\ i < i_0 & i < i_k & i < i_{h-1} \end{matrix} \quad (2)$$

式(2)为兼容基在 $\{f_0, f_1, \dots, f_{N-1}\}$ 上的矩阵表示, h 表示(对角矩阵)块的个数, 第 k 块 $(0 \leq k < h)$ 的基向量数量表示为 i_k , 有 $\sum_{k=0}^{h-1} i_k = \dim V$ 。 V 的基表示为 $(g_{k,i})_{k < h, i < i_k} \in (\mathbb{Q}^N)^{\dim V}$, 即 $V = \text{vect}_K(g_{k,i} | k < h, i < i_k)$ 。这里 k 代表块数, i 表示向量在第 k 块中的位置。存在 $h+1$ 个整数 $\{j_0, j_1, \dots, j_h\}$, 其中 $j_0 = 0, j_h \leq N$, 使得对第 k 块的全部向量, 除 $\{j_0, j_1, \dots, j_{k+1} - 1\}$ 以外的数值均为0。

这样, 每个基向量可以写成 $g_{k,i} = \sum_{l=0}^{j_{k+1}-j_k-1} \lambda_{k,l,i} f_{j_k+l}$, 其中 $\lambda_{k,l,i} \in \mathbb{Q}$, $(0 \leq k < h), 0 \leq i < i_k$ 。

固定 $a \in \mathbb{Q}^N$, 有与S层兼容的子空间 V , 兼容基为 g 。下面定义信息集、等价关系及相关定理。

定义6(信息集)^[14] 令 $\{p^0, p^1\}$ 为 $V \oplus a$ 中的一组无顺序消息对, 写作

码的结构区分器长度均不超过5轮, 这是目前轮数最长的结构区分器。

4.1 兼容、信息集与等价关系

令 d 为S盒操作在二元域 F_2 上的扩张系数, $\mathbb{Q} = F_2^d$, 对于3D密码, $d = 8$ 。设SPN密码作用于 N 个字, 每个字的规模等于S盒的规模, 则状态矩阵和圈密钥可表示为 $\mathbb{Q}^N$ 上的向量, SPN密码的圈函数为 $R = K \circ L \circ S$ 。

S 是字节代替层, 对状态矩阵中的比特块做非线性变换, $\{f_0, f_1, \dots, f_{N-1}\}$ 为 $\mathbb{Q}^N$ 一组基。

L 是 $\mathbb{Q}^N$ 上的一个 F_2 -线性双射。 $\mathbb{Q} \rightarrow \mathbb{Q}$ 。

K 是轮密钥加操作, 将内部状态与轮密钥异或。

定义5(兼容)^[14] 设 V 是 $\mathbb{Q}^N$ 的子空间, 如果 V 存在一组基在 $\{f_0, f_1, \dots, f_{N-1}\}$ 上表示为块对角矩阵时, 则 V 与 S 兼容, 并且称这类基为 V 的兼容基。

根据兼容的定义, 文献[14]给出了信息集、等价关系的定义, 并证明当存在与S层兼容的子空间时, 密码算法有“ n 倍”性质, 可以构造结构区分器, 进一步给出结构区分器的构造条件。

$$p^0 = \sum_{k=0}^{h-1} \sum_{i=0}^{i_k-1} p_{i,k}^0 g_{i,k} + a, \quad p^1 = \sum_{k=0}^{h-1} \sum_{i=0}^{i_k-1} p_{i,k}^1 g_{i,k} + a$$

$$p_{i,k}^0, p_{i,k}^1 \in \mathbb{Q}. \{p^0, p^1\} \text{ 的信息集 } \Lambda \text{ 定义为}$$

$$\Lambda = \{k \in \{0, 1, \dots, 15\} \mid p_k^0 \neq p_k^1\}.$$

定义7(等价)^[14] 设 $P = \{p^0, p^1\}$ 和 $Q = \{q^0, q^1\}$, $p^0, p^1, q^0, q^1 \in V \oplus a$ 。 P 与 Q 等价, 记 $P \sim Q$, 当:

(1) $\{p^0, p^1\}$ 与 $\{q^0, q^1\}$ 有相同的信息集 Λ 。

(2) $\forall k \in \Lambda, \exists b \in \{0, 1\}: \exists i < i_k, q_{i,k}^0 \neq p_{i,k}^b, q_{i,k}^1 \neq p_{i,k}^{1-b}$ 。

显然, $\sim$ 是一种等价关系。举个例子, 下面两个消息对 $\{p^0, p^1\}$ 与 $\{q^0, q^1\}$ 是等价的。

$$\{\mathbf{p}^0, \mathbf{p}^1\} = \left\{ \begin{pmatrix} 0 & x_2 & z_3 & z_4 \\ x_1 & x_2 & 0 & z_4 \\ x_1 & x_2 & z_3 & 0 \\ x_1 & 0 & z_3 & z_4 \end{pmatrix}, \begin{pmatrix} 0 & y_2 & z_3 & z_4 \\ y_1 & y_2 & 0 & z_4 \\ y_1 & y_2 & z_3 & 0 \\ y_1 & 0 & z_3 & z_4 \end{pmatrix} \right\},$$

$$\{\mathbf{q}^0, \mathbf{q}^1\} = \left\{ \begin{pmatrix} 0 & y_2 & z_3 & z_4 \\ x_1 & y_2 & 0 & z_4 \\ x_1 & y_2 & z_3 & 0 \\ x_1 & 0 & z_3 & z_4 \end{pmatrix}, \begin{pmatrix} 0 & x_2 & z_3 & z_4 \\ y_1 & x_2 & 0 & z_4 \\ y_1 & x_2 & z_3 & 0 \\ y_1 & 0 & z_3 & z_4 \end{pmatrix} \right\}.$$

它们的信息集 $|A| = 2$ 。

定理1^[14] 对任意 $a \in \mathbb{Q}^N$, 函数 Δ 作用在 $V \oplus a$ 的无顺序消息对上, 定义为

$$\Delta: \{p^0, p^1\} \mapsto R(p^0) + R(p^1),$$

Δ 在 $\sim$ 的等价集上是定值。

推论1^[14] 令 $\mathbb{C}$ 为信息集的等价集, $\mathbb{C}$ 的势为

$$|\mathbb{C}| = 2^{|\Lambda|-1+d} \sum_{k \notin \Lambda} i_k$$

它总是 2^{h-1} 的倍数。

$$A = \begin{pmatrix} 01x & 02x & 04x & 06x & 01x & 02x & 04x & 06x \\ 02x & 04x & 06x & 01x & 04x & 06x & 01x & 02x \\ 04x & 06x & 01x & 02x & 06x & 01x & 02x & 04x \\ 06x & 01x & 02x & 04x & 01x & 02x & 04x & 06x \\ 01x & 02x & 04x & 06x & 02x & 04x & 06x & 01x \\ 02x & 04x & 06x & 01x & 06x & 01x & 02x & 04x \\ 04x & 06x & 01x & 02x & 01x & 02x & 04x & 06x \\ 06x & 01x & 02x & 04x & 02x & 04x & 06x & 01x \end{pmatrix}$$

$\mathbf{B}$ 为 64×16 矩阵, 即子空间 $(\mathbf{M}_0, \mathbf{M}_0, \mathbf{M}_0, \mathbf{M}_0)$ 的维数为16。由于矩阵 $\mathbf{B}$ 为准对角矩阵, 因此子空间 $(\mathbf{M}_0, \mathbf{M}_0, \mathbf{M}_0, \mathbf{M}_0)$ 与 S 层兼容。容易发现, 对任意 $i, j, s, t \in \{0, 1, 2, 3\}$, 子空间 $(\mathbf{M}_i, \mathbf{M}_j, \mathbf{M}_s, \mathbf{M}_t)$ 与 S 层兼容。故3D密码中存在“ n 倍”性质。下面根据定义6给出3D密码的信息集。

定义8 $\{p^0, p^1\}$ 为 $(M_i, M_j, M_s, M_t) + a$ 中的一对消息, 记 $M_B = (a_{l,k})_{0 \leq l \leq 63, 0 \leq k \leq 16}$, 则

$$\begin{aligned} \mathbf{p}^0 &= \sum_{k=0}^{16} p_k^0 \sum_{l=0}^{63} a_{l,k} \mathbf{e}_l + a = \sum_{k,l} (p_k^0 a_{l,k} + a_l) \mathbf{e}_l, \\ \mathbf{p}^1 &= \sum_{k=0}^{15} p_k^1 \sum_{l=0}^{63} a_{l,k} \mathbf{e}_l + a = \sum_{k,l} (p_k^1 a_{l,k} + a_l) \mathbf{e}_l. \end{aligned}$$

对变量 $p_k^0, p_k^1 \in \mathbb{Q}$, $0 \leq k \leq 15$ 。 $\{\mathbf{p}^0, \mathbf{p}^1\}$ 的信息集 A 定义为 $A = \{k \in \{0, 1, \dots, 15\} \mid p_k^0 \neq p_k^1\}$ 。

引理 6 令 $a \in F_{2^8}^{64}$, $i \in \{0, 1, 2, 3\}$, $J \subseteq \{0, 1, 2, 3\}$ 。令

$$n = \# \{ (\mathbf{p}^0, \mathbf{p}^1) \mid p^0, p^1 \in (M_i, M_j, M_s, M_t) \\ + a [E_k' (p^0) + E_k' (p^0)] \in (D_I, D_J, D_S, D_T) \},$$

则有 $n \equiv 0 \pmod{2^{15}}$ 。

根据子空间 (M_i, M_j, M_s, M_t) 与 S 层的可兼容性, 结合定理1, 容易得到引理6。证明思路是交换碰撞对的某几列, 得到等价消息对, 结合定理1, 等价消息对加密一轮差分相等, 即仍然碰撞。

命题1(n 倍性质)^[14] 设 H 为 $\mathbb{Q}^N$ 的子集, 令

$$|A| = 2, \Delta, \mathbb{C}, 2^{h-1}, n = \# \{ \{ \mathbf{p}^0, \mathbf{p}^1 \} \mid \mathbf{p}^0, \mathbf{p}^1 \in V \oplus a \mid R(\mathbf{p}^0) + R(\mathbf{p}^1) \in H \},$$

则有 $n \equiv 0 \pmod{2^{h-1}}$ 。

命题1说明当子空间 $\mathbf{V}$ 与 S 层兼容时, 穷举 $\mathbf{V}$ 一个陪集中全部明文对并加密, 差分属于同一子空间的密文对个数总是 2^{h-1} 的倍数, 这种规律被称为密码算法的“ n 倍性质”。

4.2 3D密码的7轮结构区分器

为构造3D密码的结构区分器，首先需要找到与S层兼容的子空间。研究3D密码的混合空间，以 (M_0, M_0, M_0, M_0) 为例，它的一组基在单位基空

间 E 上可以写成准对角矩阵 $B = \begin{pmatrix} A & & \\ & A & \\ & & A \\ & & & A \end{pmatrix}$,

其中

$$\begin{pmatrix} 01x & 02x & 04x & 06x \\ & 01x & 02x & 04x & 06x \end{pmatrix}^T.$$

根据定义8和推论1, 矩阵 M_B 的列数为 $h=16$, 故碰撞数一定为 $2^{16-1} = 2^{15}$ 的倍数。

结合引理2与引理6得到定理2。

定理2 令 $a \in F_{2^4}^{16}$, $i \in \{0, 1, 2, 3\}$, $J \subseteq \{0, 1, 2, 3\}$ 。令

$$n = \# \{ (\mathbf{p}^0, \mathbf{p}^1) \text{ with } \mathbf{p}^0, \mathbf{p}^1 \in (D_i, D_i, D_i, D_i) \\ + a | F_k^7(\mathbf{p}^0) + F_k^7(\mathbf{p}^1) \in (M_J, M_J, M_J, M_J) \},$$

则 $n \equiv 0 \pmod{2^{15}_o}$.

最终检测子空间为 (M_J, M_J, M_J, M_J) , 取 $|J| = 3$, 则密文对差分落入 (M_J, M_J, M_J, M_J) 的概率为 $2^{-512+32 \cdot |J| \cdot 4} = 2^{-128}$. 穷举 $(D_i, D_i, D_i, D_i) + a$ 中全部明文对, 平均有

$$\binom{2^{128}}{2} \cdot 2^{-128} = 2^{127} \cdot (2^{128} - 1) \cdot 2^{-128} \simeq 2^{127}$$

个不同密文对属于 (M_J, M_J, M_J, M_J) 同一陪集。此即3D密码的7轮结构区分器，其子空间迹表示为

$$\begin{aligned} (D_i, D_i, D_i, D_i) &\stackrel{E_k}{\rightleftharpoons} (C_i, C_i, C_i, C_i) \stackrel{E'_k}{\rightleftharpoons} (C_i, C_i, C_i, C_i) \\ &\stackrel{E_k}{\rightleftharpoons} (M_i, M_i, M_i, M_i) \stackrel{E'_k}{\rightleftharpoons} (D_J, D_J, D_J, D_J) \\ &\stackrel{E_k}{\rightleftharpoons} (C_J, C_J, C_J, C_J) \stackrel{E'_k}{\rightleftharpoons} (C_J, C_J, C_J, C_J) \\ &\stackrel{E_k}{\rightleftharpoons} (M_J, M_J, M_J, M_J) \end{aligned}$$

以碰撞数模 2^{15} 的数值作为区分依据, 定理2说明穷举 $(D_i, D_i, D_i, D_i) + a$ 全部明文对, 7轮

3D密码得到的碰撞数模 2^{15} 为0, 而随机函数的碰撞数模 2^{15} 为0的概率为 2^{-15} 。区分成功的概率为 $1 - 2^{-15}$, 大于99.99%, 且利用的性质与密钥无关。需要 $3 \cdot 2^{128} \approx 2^{129.6}$ 次查表操作, 存储复杂度为 2^{128} Byte。

5 结束语

本文对3D密码进行子空间迹分析, 研究子空间传播规律, 首先利用找到的3轮明确子空间迹, 结合子空间的交集性质, 构造了7轮3D密码的子空间迹不可能差分区分离器。然后利用与S层兼容的子空间, 给出了3D密码的7轮结构区分器, 为基于子空间迹的攻击提供了基础。本文寻找子空间迹不可能差分区分离器与结构区分器的方法, 适用于任何SPN密码。

在利用子空间迹分析3D密码的过程中, 发现其在寻找区分器上拥有优势。首先, 截断不可能差分相比与子空间迹不可能差分, 前者利用的中间相遇思想是从维数较小的终点差分矩阵脱密, 在中间产生矛盾, 因此区分优势较小, 而后者利用的矛盾是两个子空间交集为 $\{0\}$, 脱密过程是一条明确子空间迹, 维数保持不变, 区分优势往往更大。结构区分器的原理是当输入子空间与S层兼容时, 等价消息对经过一轮加密函数, 差分为常数, 这是SPN结构密码的新性质, 但对明确子空间迹依赖很强, 例如AES只有5轮结构区分器, 而3D密码存在3轮明确子空间迹, 故可以构造7轮结构区分器。

因此能否得到子空间迹区分器与明确子空间迹的关系, 给出基于子空间迹攻击的轮数的下界是有待解决的问题。

参 考 文 献

- [1] NAKAHARA Jr J. 3D: A three-dimensional block cipher[C]. The 7th International Conference on Cryptology and Network Security, Hong Kong, China, 2008: 252–267. doi: [10.1007/978-3-540-89641-8_18](https://doi.org/10.1007/978-3-540-89641-8_18).
- [2] 王美一, 唐学海, 李超, 等. 3D密码的Square攻击[J]. 电子与信息学报, 2010, 32(1): 157–161. doi: [10.3724/SP.J.1146.2008.01846](https://doi.org/10.3724/SP.J.1146.2008.01846).
WANG Meiyi, TANG Xuehai, LI Chao, et al. Square attacks on 3D cipher[J]. *Journal of Electronics & Information Technology*, 2010, 32(1): 157–161. doi: [10.3724/SP.J.1146.2008.01846](https://doi.org/10.3724/SP.J.1146.2008.01846).
- [3] 唐学海, 李超, 王美一, 等. 3D密码的不可能差分攻击[J]. 电子与信息学报, 2010, 32(10): 2516–2520. doi: [10.3724/SP.J.1146.2009.01375](https://doi.org/10.3724/SP.J.1146.2009.01375).
TANG Xuehai, LI Chao, WANG Meiyi, et al. Impossible differential attack on 3D cipher[J]. *Journal of Electronics & Information Technology*, 2010, 32(10): 2516–2520. doi: [10.3724/SP.J.1146.2009.01375](https://doi.org/10.3724/SP.J.1146.2009.01375).
- [4] NAKAHARA Jr J. New impossible differential and known-key distinguishers for the 3D cipher[C]. The 7th International Conference on Information Security Practice and Experience, Guangzhou, China, 2011: 208–221. doi: [10.1007/978-3-642-21031-0_16](https://doi.org/10.1007/978-3-642-21031-0_16).
- [5] 苏崇茂, 韦永壮, 马春波. 10轮3D分组密码算法的中间相遇攻击[J]. 电子与信息学报, 2012, 34(3): 694–697. doi: [10.3724/SP.J.1146.2011.00888](https://doi.org/10.3724/SP.J.1146.2011.00888).
SU Chongmao, WEI Yongzhuang, and MA Chunbo. Meet-in-the-middle attack on 10-round reduced 3D block cipher[J]. *Journal of Electronics & Information Technology*, 2012, 34(3): 694–697. doi: [10.3724/SP.J.1146.2011.00888](https://doi.org/10.3724/SP.J.1146.2011.00888).
- [6] KOYAMA T, WANG Lei, and SASAKI Y. New truncated differential cryptanalysis on 3D block cipher[C]. The 8th International Conference on Information Security Practice and Experience, Hangzhou, China, 2012: 109–125. doi: [10.1007/978-3-642-29101-2_8](https://doi.org/10.1007/978-3-642-29101-2_8).
- [7] 谢作敏, 陈少真, 鲁林真. 11轮3D密码的不可能差分攻击[J]. 电子与信息学报, 2014, 36(5): 1215–1220. doi: [10.3724/SP.J.1146.2013.00948](https://doi.org/10.3724/SP.J.1146.2013.00948).
XIE Zuomin, CHEN Shaozhen, and LU Linzhen. Impossible differential cryptanalysis of 11-round 3D cipher[J]. *Journal of Electronics & Information Technology*, 2014, 36(5): 1215–1220. doi: [10.3724/SP.J.1146.2013.00948](https://doi.org/10.3724/SP.J.1146.2013.00948).
- [8] 任炯炯, 陈少真. 11轮3D密码算法的中间相遇攻击[J]. 通信学报, 2015, 36(8): 182–191. doi: [10.11959/j.issn.1000-436x.2015131](https://doi.org/10.11959/j.issn.1000-436x.2015131).
REN Jiongiong and CHEN Shaozhen. Meet-in-the-middle attack on 11-round 3D cipher[J]. *Journal on Communications*, 2015, 36(8): 182–191. doi: [10.11959/j.issn.1000-436x.2015131](https://doi.org/10.11959/j.issn.1000-436x.2015131).
- [9] HOU Tao, CUI Ting, and ZHANG Jiyan. Practical attacks on reduced-round 3D and saturnin[J/OL]. *The Computer Journal*. doi: [10.1093/comjnl/bxab174](https://doi.org/10.1093/comjnl/bxab174).
- [10] GRASSI L, RECHBERGER C, and RÖNJOM S. Subspace Trail Cryptanalysis and its Applications to AES[C]. The 24th International Conference on Fast Software Encryption, Tokyo, Japan, 2016: 192–225.
- [11] GRASSI L, RECHBERGER C, and RÖNJOM S. A new structural-differential property of 5-round AES[C]. The 36th Annual International Conference on Advances in Cryptology, Paris, France, 2017: 289–317. doi: [10.1007/978-3-319-56614-6_10](https://doi.org/10.1007/978-3-319-56614-6_10).

- [12] LIU Wenhao and YANG Yang. The 7-round subspace trail-based impossible differential distinguisher of midori-64[J]. *Security and Communication Networks*, 2021, 2021: 6269604. doi: [10.1155/2021/6269604](https://doi.org/10.1155/2021/6269604).
- [13] 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: [10.46586/tosc.v2018.i2.133-160](https://doi.org/10.46586/tosc.v2018.i2.133-160).
- [14] BOURA C, CANTEAUT A, and 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](https://doi.org/10.13154/tosc.v2019.i1.170-191).
- [15] GRASSI L, LEANDER G, RECHBERGER C, *et al.* Weak-key distinguishers for AES[C]. The 27th International Conference on Selected Areas in Cryptography, Halifax, Canada, 2020: 141–170. doi: [10.1007/978-3-030-81652-0_6](https://doi.org/10.1007/978-3-030-81652-0_6).
- [16] GRASSI L, RECHBERGER C, and SCHOFNEGGER M. Proving resistance against infinitely long subspace trails: How to choose the linear layer[J]. *IACR Transactions on Symmetric Cryptology*, 2021, 2021(2): 314–352. doi: [10.46586/tosc.v2021.i2.314-352](https://doi.org/10.46586/tosc.v2021.i2.314-352).
- 杨 阳: 女, 副教授, 研究方向为密码设计与分析.
刘文豪: 男, 硕士生, 研究方向为密码设计与分析.
曾 光: 男, 副教授, 研究方向为密码设计与分析.
- 责任编辑: 马秀强