软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(12):5807−5821 [doi: 10.13328/j.cnki.jos.006761]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

SPN 型密码的通用子空间迹分析*

宋 蝉[1,2], 张 蕾[1,2,3], 吴文玲[1,2]

[1](中国科学院 软件研究所, 北京 100190)

[2](中国科学院大学, 北京 100049)

[3](密码科学技术国家重点实验室, 北京 100878)

通信作者: 宋蝉, E-mail: songchan2020@iscas.ac.cn; 张蕾, E-mail: zhanglei@iscas.ac.cn

摘　要: SPN 结构是目前最广泛使用的一种分组密码整体结构, AES、ARIA 等分组密码算法均采用此结构, 对此类 SPN 型密码的安全性分析是密码分析中的一个研究热点. 将子空间迹密码分析方法应用到典型二维 SPN 型密码和典型三维 SPN 型密码中, 可分别得到其相应的子空间迹和基于子空间迹的通用性质, 该性质与密钥、S 盒以及列混淆矩阵的定义均无关, 可具体描述为: 针对一个状态可形式化为 $n\times m$ 二维数组的典型二维 SPN 型密码, 属于类对角子空间同一陪集的所有明文经过 5 轮加密得到的密文中属于混淆子空间同一陪集的不同密文对数量一定为 2^{n-1} 的倍数; 针对一个状态可形式化为 $l\times n\times m$ 三维数组的典型三维 SPN 型密码, 属于类对角子空间同一陪集的所有明文经过 7 轮加密得到的密文中属于混淆子空间同一陪集的不同密文对数量一定为 2^{nl-1} 的倍数. 此外, 不仅对该性质进行了证明, 还在 PHOTON 算法的内部置换以及小规模版本 Rijndael 算法、3D 算法、Saturnin 算法上进行了实验验证, 结果与该性质完全一致.

关键词: SPN 型密码; 子空间迹; 倍数性质; PHOTON 置换; 3D 算法

中图法分类号: TP309

中文引用格式: 宋蝉, 张蕾, 吴文玲. SPN型密码的通用子空间迹分析. 软件学报, 2023, 34(12): 5807–5821. http://www.jos.org.cn/1000-9825/6761.htm

英文引用格式: Song C, Zhang L, Wu WL. General Subspace Trail Cryptanalysis of SPN Ciphers. Ruan Jian Xue Bao/Journal of Software, 2023, 34(12): 5807–5821 (in Chinese). http://www.jos.org.cn/1000-9825/6761.htm

General Subspace Trail Cryptanalysis of SPN Ciphers

SONG Chan[1,2], ZHANG Lei[1,2,3], WU Wen-Ling[1,2]

[1](Institute of Software, Chinese Academy of Sciences, Beijing 100190, China)

[2](University of Chinese Academy of Sciences, Beijing 100049, China)

[3](State Key Laboratory of Cryptology, Beijing 100878, China)

Abstract: SPN construction is the most widely used overall construction of block ciphers at present, which is adopted by block ciphers such as AES and ARIA. The security analysis of SPN ciphers is a research hotspot in cryptanalysis. The application of the subspace trail cryptanalysis to the typical two-dimensional SPN ciphers and typical three-dimensional SPN ciphers can yield the corresponding subspace trails and general properties based on the subspace trails separately. These properties are independent of the secret key and the detailed definitions of the S-box and MixColumns matrix. They can be specifically described as follows: For a typical two-dimensional SPN cipher whose state can be formalized into a two-dimensional array of $n\times m$, the number of different ciphertext pairs belonging to the same coset of the mixed subspace in the ciphertexts obtained by five rounds of encryption of all plaintexts belonging to the same coset of the quasi-diagonal subspace must be a multiple of 2^{n-1}. For a typical three-dimensional SPN cipher whose state can be formalized into a three-

* 基金项目: 国家自然科学基金 (62072445)
收稿时间: 2022-03-26; 修改时间: 2022-06-28; 采用时间: 2022-07-26; jos 在线出版时间: 2023-04-19
CNKI 网络首发时间: 2023-04-21

dimensional array of $l\times n\times m$, the number of different ciphertext pairs belonging to the same coset of the mixed subspace in the ciphertexts obtained by seven rounds of encryption of all plaintexts belonging to the same coset of the quasi-diagonal subspace must be a multiple of 2^{nl-1}. In addition, this study not only proves these properties but also makes experimental verification on the internal permutations of PHOTON and small-scale variants of Rijndael, 3D, and Saturnin algorithms. The experimental results are completely consistent with these properties.

Key words: SPN cipher; subspace trail; multiple property; PHOTON's permutation; 3D algorithm

随着计算机和通信技术的飞速发展, 用户对信息的安全存储、安全处理和安全传输的需求越来越迫切, 这也使得信息安全成为一个热门的讨论话题, 解决这一问题的有效手段之一是使用现代密码技术. 分组密码是现代密码学中的一个重要分支, 也是最基本的密码算法之一, 它可以用来构造伪随机数生成器、哈希函数、消息认证码、认证加密算法等. 目前流行的分组密码大都采用迭代构造方法, 其中整体结构是迭代型密码算法的一个重要特征, 对算法的安全性和实现效率有很大影响, 在对称密码算法的研究中, 有很多工作都是围绕着算法结构展开的. 分组密码常用的结构有 Feistel 结构、SPN 结构、Lai-Massey 结构等. Feistel 结构是由 Feistel 在设计 Lucifer 分组密码时提出的[1], 又因 DES 的使用而广泛流行. Feistel 结构的优点是"加解密相似性", 可以有效地节省资源, 而相应的缺点是扩散较慢, 为达到一定的安全性通常需要迭代更多的轮数. SPN 结构即替换-置换网络 (substitution-permutation network), 是目前最广泛使用的一种分组密码整体结构, 典型算法有 AES[2], uBlock[3]等. SPN 结构通常包含一个可逆的非线性函数 S 和一个可逆的线性变换 P, 其中 S 变换起混淆作用, P 变换起扩散作用. 直观来看, 混淆层和扩散层的交替使用非常接近 Shannon 所提及的混淆和扩散原则[4]. 当给定 S 和 P 的安全性指标时, 设计者可以估计算法抗差分密码分析和线性密码分析的能力. 相较于 Feistel 结构, SPN 结构的优点是可以得到更快速的扩散, 缺点是加解密通常不一致, 因此实现的时候需要消耗更多的资源. Lai-Massey 结构源于 Lai 等人设计的 IDEA 算法[5], 之后 Vaudenay 将 IDEA 算法中的结构提取出来, 构建了 Lai-Massey 结构[6]. Lai-Massey 结构可以提供与 Feistel 结构相仿的安全性, 且通常也具有加解密一致的优点, 但由于轮函数相对复杂, 算法安全性难于分析, 故没有前两种结构应用广泛.

密码算法的安全性分析和设计密不可分, 从密码分析中获取经验, 才能设计出更好、更安全的密码算法. 现代分组密码大都受到 AES 设计原理的影响, 在一定程度上可以抵抗差分密码分析和线性密码分析等一系列传统攻击方法. 但为了适应具体的应用环境, 很多密码在设计时会采用一些创新手段, 进而导致其可能受到新的攻击. 在 2011 年美密会上 Leander 等人在对 PRINTcipher 的密码分析中首次引入不变子空间攻击这一方法[7]. 在不变子空间攻击提出之后, 研究者们相继提出了针对具体轻量级密码算法的不变子空间攻击, 但仍没有一种通用的方法来搜索密码算法的不变子空间. 为此, Leander 等人在 2015 年又提出了一种通用技术来搜索密码算法的不变子空间, 并将其应用于 iSCREAM、Robin 和 Zorro 算法上[8]. 随着对不变子空间攻击的深入研究, 抗不变子空间攻击的改进方案也相继被提出, 如 Liu 等人在 2017 年提出的抗不变子空间攻击的类 AES 轻量级算法构造方案[9]. 此外, 随着不变子空间攻击的发展, Todo 等人在 2016 年提出了非线性不变攻击 (其本质上是不变子空间攻击的延伸), 并利用该方法在弱密钥设置下对全轮的 (可调) 分组密码算法 SCREAM、iSCREAM 和 Midori64 进行了区分攻击, 但这里的攻击非常依赖于轮常数的选择[10]. 在 2017 年美密会上, Beierle 等人详细分析了线性层的设计和轮常数的特殊选择对不变子空间攻击和非线性不变攻击的适用性的影响[11]. 为了进一步消除轮常数的影响, Wei 等人在非线性不变量的输入中添加了一对常数, 进而提出了一种广义的非线性不变攻击方法[12]. 但不变子空间攻击和非线性不变攻击都是弱密钥条件下的攻击, 当且仅当输入每一轮加密轮函数的密钥都是弱密钥时, 才能构造出概率为 1 的全轮区分器, 进而对算法进行分析. 进而, 在 FSE 2017 上 Grassi 等人提出了一种子空间迹密码分析方法, 并给出 AES 的 2 轮、3 轮和 4 轮子空间迹以及相应的基于子空间迹的低数据复杂度密钥恢复攻击[13]. 这里的子空间迹密码分析也可以看作是不变子空间攻击的推广, 且这种对子空间的分析通常不依赖于轮常数或者轮密钥的特定选择. 随后, 在 2017 年欧密会上, Grassi 等人基于子空间迹的思想又给出了 AES 的一个 5 轮区分器 (后面都简称为"8 倍性质"), 即通过合理地选择输入对差分可以确保密文对中属于一个特定子空间的输出对数量为 8 的倍数[14]. 之后 Boura 等人利用等价类的思想提出了一个新的框架又证明了 Grassi 等人[14]提出的"8 倍性质"和混合差分区

分器[15].

本文以 Grassi 等人[13]提出的 AES 子空间迹性质为出发点, 对 SPN 型密码的子空间迹性质进行了研究, 主要贡献如下.

1) 给出了典型二维 SPN 型密码的一个 5 轮性质: 针对一个状态可形式化为 $n\times m$ 二维数组 (假设 $n\leqslant m$) 的典型二维 SPN 型密码, 属于类对角子空间 D_I 的同一陪集的所有明文经过 5 轮加密得到的密文中属于混淆子空间 M_J 的同一陪集的不同密文对数量一定为 2^{n-1} 的倍数.

2) 给出了典型三维 SPN 型密码的一个 7 轮性质: 针对一个状态可形式化为 $l\times n\times m$ 三维数组 (假设 $n\leqslant m$) 的典型三维 SPN 型密码, 属于类对角子空间 D_I 的同一陪集的所有明文经过 7 轮加密得到的密文中属于混淆子空间 M_J 的同一陪集的不同密文对数量一定为 2^{nl-1} 的倍数.

3) 不同于文献 [14] 的证明中用到了列混淆矩阵具有最大分支数的性质, 本文声明该性质与列混淆矩阵的差分分支数无关.

本文第 1 节主要介绍 AES 的子空间迹和“8 倍性质”. 第 2 节引入本文主要研究的典型二维 SPN 型密码及其子空间迹, 然后基于子空间迹给出典型二维 SPN 型密码的一个 5 轮性质. 第 3 节引入本文主要研究的典型三维 SPN 型密码及其子空间迹, 并基于子空间迹给出典型三维 SPN 型密码的一个 7 轮性质. 第 4 节分别对典型二维 SPN 型密码的“2^{n-1} 倍性质”和典型三维 SPN 型密码的“2^{nl-1} 倍性质”进行了证明. 第 5 节给出了在 PHOTON 的内部置换以及小规模版本 Rijndael 算法、3D 算法、Saturnin 算法上的实验验证. 第 6 节对本文的工作进行总结.

1 预备知识

1.1 AES 的子空间迹

设 F 表示一个迭代分组密码的轮函数, $V\oplus a$ 表示向量空间 V 的一个陪集, 若 $F(V\oplus a)=V\oplus a$ 成立, 则称 $V\oplus a$ 为子空间 V 关于函数 F 的不变陪集. 在 FSE 2017 上, Grassi 等人[13]将这一概念进一步推广为子空间迹, 具体定义如下.

定义 1[13]. 设 $(V_1,V_2,\ldots,V_{r+1})$ 表示 $r+1$ 个满足 $\dim(V_i)\leqslant\dim(V_{i+1})$ 的子空间 (dim 表示子空间的维数), 若对于每个 $i=1,2,\ldots,r$ 和 $a_i\in V_i^{\perp}$(正交补), 都存在 (唯一的) $a_{i+1}\in V_{i+1}^{\perp}$ 使得 $F(V_i\oplus a_i)\subseteq V_{i+1}\oplus a_{i+1}$ 成立, 则称 $(V_1,V_2,\ldots,V_{r+1})$ 为函数 F 的长为 r 的子空间迹. 此外, 如果维数关系 $\dim(V_i)\leqslant\dim(V_{i+1})$ 均满足相等, 则称这个迹为常数维子空间迹.

AES 算法[2]是美国于 2001 年颁布的高级加密标准, 算法采用 SPN 结构, 分组长度为 128 比特, 数据状态可表示为一个 4×4 的字节矩阵, 算法轮函数 (R) 由字节替换 (SB)、行移位 (SR)、列混淆 (MC)、轮密钥加 (ARK) 这 4 个部件构成. 下面简单回顾一下 AES 的几类子空间及其子空间迹, 设 $\{e_{0,0},\ldots,e_{3,3}\}$ 表示 $F_{2^8}^{4\times4}$ 上的单位向量 ($e_{i,j}$ 表示状态的 (i,j) 位置对应的元素为 1).

定义 2[13]. 列子空间 C_i、对角子空间 D_i、反对角子空间 ID_i、混淆子空间 M_i 分别定义为:

$$C_i=\langle e_{0,i},e_{1,i},e_{2,i},e_{3,i}\rangle,\ D_i=SR^{-1}(C_i)=\langle e_{0,i},e_{1,(i+1)\bmod4},e_{2,(i+2)\bmod4},e_{3,(i+3)\bmod4}\rangle,\ ID_i=SR(C_i)$$
$$=\langle e_{0,i},e_{1,(i-1)\bmod4},e_{2,(i-2)\bmod4},e_{3,(i-3)\bmod4}\rangle,\ M_i=MC(ID_i).$$

如 C_0、D_0、ID_0、M_0 的矩阵表示分别为:

$$C_0=\begin{bmatrix}x_1&0&0&0\\x_2&0&0&0\\x_3&0&0&0\\x_4&0&0&0\end{bmatrix},\ D_0=\begin{bmatrix}x_1&0&0&0\\0&x_2&0&0\\0&0&x_3&0\\0&0&0&x_4\end{bmatrix},\ ID_0=\begin{bmatrix}x_1&0&0&0\\0&0&0&x_2\\0&0&x_3&0\\0&x_4&0&0\end{bmatrix},\ M_0=\begin{bmatrix}2x_1&x_4&x_3&3x_2\\x_1&x_4&3x_3&2x_2\\x_1&3x_4&2x_3&x_2\\3x_1&2x_4&x_3&x_2\end{bmatrix}.$$

此外, 给定集合 $I\subseteq\{0,1,2,3\}$, 定义子空间 C_I, D_I, ID_I, M_I 分别为:

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

定理 1[13]. 给定一个集合 $I\subseteq\{0,1,2,3\}$, 对于任意的 $a\in D_I^{\perp}$, 存在唯一一个元素 $b\in M_I^{\perp}$ 可以使得 $R^2(D_I\oplus a)=M_I\oplus b$ 成立, 其中 b 依赖于 a 和密钥的取值, 即:

$$\mathrm{Prob}(R^2(x)\oplus R^2(y)\in M_I | x\oplus y\in D_I)=1.$$

定理 2[13]. 设 $I,J\subseteq\{0,1,2,3\}$, 且 $|I|+|J|\leqslant 4$, 则对于任意的 $x\neq y$ 有:

$$\mathrm{Prob}(R^4(x)\oplus R^4(y)\in M_I | x\oplus y\in D_J)=0.$$

1.2 AES 的“8 倍性质”

基于 AES 的子空间迹, Grassi 等人[14]进一步给出了 5 轮 AES 的一个新性质, 如下所述.

定理 3[14]. 对于固定集合 I 和 J (这里假设 $|I|=1$), 设 D_I 和 M_J 分别表示一个对角子空间和一个混淆子空间. 给定 D_I 的任意一个陪集 $D_I\oplus a$, $a\in D_I^{\perp}$, 考虑属于该陪集的所有 2^{32} 个明文以及相应的经过 5 轮加密后的密文, 记为 (p^i,c^i), $i=0,1,\ldots,2^{32}-1$, 其中 $p^i\in D_I\oplus a$, $c^i=R^5(p^i)$, 则满足 $c^i\oplus c^j\in M_J$ $(i\neq j)$ 的不同密文对 (c^i,c^j) 的数量 n:

$$n:=\left|\left\{(p^i,c^i),(p^j,c^j)\middle|\forall p^i,p^j\in D_I\oplus a,\ p^i<p^j,\ c^i\oplus c^j\in M_J\right\}\right|$$

为 8 的倍数. 其中“<”定义为: 给定两个不同的明文 t^1 和 t^2, $t^1<t^2$ 表示存在 $i,j\in\{0,1,2,3\}$, 使得: (1) 对于所有满足 $k+4\cdot l<i+4\cdot j$ 的 $k,l\in\{0,1,2,3\}$ 有 $t^1_{k,l}=t^2_{k,l}$; (2) $t^1_{i,j}<t^2_{i,j}$.

2 二维 SPN 型密码的通用子空间迹性质

2.1 典型二维 SPN 型密码

分组密码的一般设计原则是 Shannon 提出的混淆和扩散原则[4]. 混淆原则是指密码中密钥和明文以及密文之间的依赖关系应尽可能复杂, 扩散原则是指密码中密钥以及明文的每一比特都应尽可能影响密文的多个比特. 在分组密码的设计中, 通常使用非线性的 S 盒达到混淆, 使用线性变换达到扩散, SPN 型密码的轮函数通常由轮密钥异或、混淆层和扩散层这 3 部分组成. 下面我们给出本文主要研究的典型二维 SPN 型密码的详细描述: 假设密码算法的内部状态可视为 F_{2^s} 上的一个 $n\times m$ 二维数组 (这里假设 $n\leqslant m$), 算法的轮函数由以下 4 个操作组成.

(1) AddRoundKey (ARK): 将一个轮常数或轮密钥与状态进行异或.

(2) SubBytes (SB): 通过对状态的每个元素应用 S 盒 $S:F_{2^s}\to F_{2^s}$ 将其非线性地变换为另一个元素.

(3) ShiftRows (SR): 可定义为一个置换 $\pi=(l_0,l_1,\ldots,l_{n-1})$, $l_i\in\{0,1,\ldots,m-1\}$, 表示对应行元素循环左移 l_i 个位置.

(4) MixColumns (MC): 通过左乘一个 $n\times n$ 的可逆矩阵对状态逐列进行线性变换.

2.2 典型二维 SPN 型密码的子空间迹

下面我们参照文献 [13] 给出典型二维 SPN 型密码的 4 类子空间: 列子空间 C_I、类对角子空间 D_I、类反对角子空间 ID_I、混淆子空间 M_I. 设 $\{e_{0,0},\ldots,e_{n-1,m-1}\}$ 表示 $F_{2^s}^{n\times m}$ 上的单位向量 ($e_{i,j}$ 表示状态的 (i,j) 位置对应的元素为 1).

定义 3. 列子空间 C_i 定义为 $C_i=\langle e_{0,i},e_{1,i},\ldots,e_{n-1,i}\rangle$. 如 C_0 对应的矩阵表示为:

$$C_0=\left\{\begin{bmatrix}x_1&0&\cdots&0\\x_2&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\x_n&0&\cdots&0\end{bmatrix}\middle|\forall x_1,x_2,\ldots,x_n\in F_{2^s}\right\}\equiv\begin{bmatrix}x_1&0&\cdots&0\\x_2&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\x_n&0&\cdots&0\end{bmatrix}.$$

定义 4. 类对角子空间 D_i 和类反对角子空间 ID_i 分别定义为:

$$D_i=SR^{-1}(C_i)=\langle e_{0,(i+l_0)\bmod m},e_{1,(i+l_1)\bmod m},\ldots,e_{n-1,(i+l_{n-1})\bmod m}\rangle,$$

$$ID_i=SR(C_i)=\langle e_{0,(i-l_0)\bmod m},e_{1,(i-l_1)\bmod m},\ldots,e_{n-1,(i-l_{n-1})\bmod m}\rangle.$$

如对于 $(n,m)=(4,6)$ 的典型二维 SPN 型密码, 若行移位操作定义为置换 $(0,1,3,4)$, 则 D_0 和 ID_0 对应的矩阵表示分别为:

$$D_0=\begin{bmatrix}x_1&0&0&0&0&0\\0&x_2&0&0&0&0\\0&0&0&x_3&0&0\\0&0&0&0&x_4&0\end{bmatrix},\ ID_0=\begin{bmatrix}x_1&0&0&0&0&0\\0&0&0&0&0&x_2\\0&0&0&x_3&0&0\\0&0&x_4&0&0&0\end{bmatrix}.$$

定义 5. 混淆子空间 M_i 定义为: $M_i = MC(ID_i)$.

如对于上述 $(n,m)=(4,6)$ 的典型二维 SPN 型密码, 若列混淆操作对应的矩阵定义为 $C=(c_{i,j})_{4\times4}$, 则 M_0 对应的矩阵表示为:

$$M_0=\begin{bmatrix} c_{1,1}\cdot x_1 & 0 & c_{1,4}\cdot x_4 & c_{1,3}\cdot x_3 & 0 & c_{1,2}\cdot x_2 \\ c_{2,1}\cdot x_1 & 0 & c_{2,4}\cdot x_4 & c_{2,3}\cdot x_3 & 0 & c_{2,2}\cdot x_2 \\ c_{3,1}\cdot x_1 & 0 & c_{3,4}\cdot x_4 & c_{3,3}\cdot x_3 & 0 & c_{3,2}\cdot x_2 \\ c_{4,1}\cdot x_1 & 0 & c_{4,4}\cdot x_4 & c_{4,3}\cdot x_3 & 0 & c_{4,2}\cdot x_2 \end{bmatrix}.$$

此外, 给定集合 $I\subseteq\{0,1,\ldots,m-1\}$, 定义子空间 C_I, D_I, ID_I, M_I 分别为:

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

在给出典型二维 SPN 型密码的 4 类子空间定义之后, 我们可以进一步推导典型二维 SPN 型密码的两个子空间迹, 如下述定理所示.

定理 4. 给定一个集合 $I\subseteq\{0,1,\ldots,m-1\}$, 对于任意的 $a\in D_I^{\perp}$, 存在唯一一个元素 $b\in M_I^{\perp}$ 可使得 $R^2(D_I\oplus a)=M_I\oplus b$ 成立, 其中 b 依赖于 a 和密钥的取值, 即:

$$\mathrm{Prob}(R^2(x)\oplus R^2(y)\in M_I | x\oplus y\in D_I)=1.$$

证明: 根据典型二维 SPN 型密码的轮函数定义可知, 给定 D_I 的任意一个陪集 $D_I\oplus a$, $a\in D_I^{\perp}$, 其经过一次轮变换后会映射为 C_I 的一个陪集 $C_I\oplus a'$, $a'\in C_I^{\perp}$; 进而 $C_I\oplus a'$ 再经过一次轮变换后会映射为 M_I 的一个陪集 $M_I\oplus b$, $b\in M_I^{\perp}$, 即证明了定理.

在给出定理 5 之前, 我们先回顾一下分支数的定义.

定义 6 [2]. $GF(2^n)$ 上的一个 $k\times k$ 矩阵 M 的差分分支数指输入向量 v 和输出向量 $u=M\cdot v$ 中非零元素的最小值, 即:

$$B(M)=\min_{v\neq0}(wt(v)+wt(u)),$$

其中, wt 表示汉明重量. 当一个 $k\times k$ 矩阵的差分分支数达到最大值 $k+1$ 时, 称矩阵为 MDS (maximum distance separable) 矩阵.

引理 1. 设 $I,J\subseteq\{0,1,\ldots,m-1\}$, $0<|I|,|J|\leqslant m-1$. 若 $|I|+|J|\leqslant r-1$, 则有 $M_I\cap D_J=\{0\}$, 其中 r 表示列混淆操作对应的 $n\times n$ 矩阵的差分分支数.

证明: 为简单起见, 记 $|I|=a$, $|J|=b$, $a+b\leqslant r-1$. 任取 M_I 的一个非零元素 X, 则 X 的矩阵表示中至少存在一个非零值, 那么由混淆子空间和矩阵的差分分支数定义可知该非零值对应的这一列中至少有 $r-a$ 个元素非零; 而由类对角子空间的定义可知, D_J 的任意一列中至多有 b 个值非零; 又因为 $b<r-a$, 故在 $|I|+|J|\leqslant r-1$ 的条件下, M_I 中的任意非零元素一定不属于 D_J, 即 $M_I\cap D_J=\{0\}$, 即证明了引理.

由引理 1 可以很自然地得到定理 5.

定理 5. 设 $I,J\subseteq\{0,1,\ldots,m-1\}$, 且 $|I|+|J|\leqslant r-1$, 则对于任意的 $x\neq y$ 有:

$$\mathrm{Prob}(R^4(x)\oplus R^4(y)\in M_I | x\oplus y\in D_J)=0.$$

2.3 典型二维 SPN 型密码的“2^{n-1} 倍性质”

考虑属于类对角子空间 D_I 的同一陪集中的所有明文和经过 5 轮加密后的密文, 然后计算属于 M_J 同一陪集的不同密文对数量, 对于典型二维 SPN 型密码该数值以概率 1 为 2^{n-1} 的倍数, 可具体描述为定理 6.

定理 6. 对于固定集合 I 和 J (这里假设 $|I|=1$), 设 D_I 和 M_J 分别表示一个类对角子空间和一个混淆子空间. 给定 D_I 的任意一个陪集 $D_I\oplus a$, $a\in D_I^{\perp}$, 考虑属于该陪集的所有 $2^{n\times s}$ 个明文以及相应的经过 5 轮加密后的密文, 记为 (p^i,c^i), $i=0,1,\ldots,2^{n\times s}-1$, 其中 $p^i\in D_I\oplus a$, $c^i=R^5(p^i)$, 则满足 $c^i\oplus c^j\in M_J(i\neq j)$ 的不同密文对 (c^i,c^j) 的数量 n:

$$n:=\left|\left\{(p^i,c^i),(p^j,c^j)|\forall p^i,p^j\in D_I\oplus a,\ p^i<p^j,\ c^i\oplus c^j\in M_J\right\}\right|$$

为 2^{n-1} 的倍数. 其中“<”定义为: 给定两个不同的明文 t^1 和 t^2, $t^1<t^2$ 表示存在 $i\in\{0,1,\ldots,n-1\}$, $j\in\{0,1,\ldots,m-1\}$, 使得: (1) 对于所有满足 $k+n\cdot l<i+n\cdot j$ 的 $k\in\{0,1,\ldots,n-1\}$, $l\in\{0,1,\ldots,m-1\}$ 有 $t^1_{k,l}=t^2_{k,l}$; (2) $t^1_{i,j}<t^2_{i,j}$.

由定理 4 可知, D_I 的任意一个陪集经过两轮轮变换后会以概率 1 映射为 M_I 的一个陪集, 故定理 6 中的 5 轮性质可以描述为: $D_I\oplus a\xrightarrow[prob.1]{R^2(\cdot)}M_I\oplus b\xrightarrow{R(\cdot)}D_J\oplus c\xrightarrow[prob.1]{R^2(\cdot)}M_J\oplus d$, 则定理 6 的证明核心即转换为中间轮变换 $M_I\to D_J$, 下面我们引入一个引理来形式化描述该中间轮变换.

引理 2. 对于固定集合 I 和 J (这里假设 $|I|=1$), 设 M_I 和 D_J 分别表示一个混淆子空间和一个类对角子空间. 给定 M_I 的任意一个陪集 $M_I\oplus a$, $a\in M_I^{\perp}$, 考虑属于该陪集的所有 $2^{n\times s}$ 个明文以及相应的经过一轮加密后的密文, 记为 $(\hat{p}^i,\hat{c}^i)$, $i=0,1,\ldots,2^{n\times s}-1$, 其中 $\hat{p}^i\in M_I\oplus a$, $\hat{c}^i=R(\hat{p}^i)$, 则满足 $\hat{c}^i\oplus\hat{c}^j\in D_J$ $(i\neq j)$ 的不同密文对 $(\hat{c}^i,\hat{c}^j)$ 的数量 n:

$$n:=\left|\left\{(\hat{p}^i,\hat{c}^i),(\hat{p}^j,\hat{c}^j)\middle|\forall\hat{p}^i,\hat{p}^j\in M_I\oplus a,\ \hat{p}^i<\hat{p}^j,\ \hat{c}^i\oplus\hat{c}^j\in D_J\right\}\right|$$

为 2^{n-1} 的倍数. 其中"<"的定义同定理 6.

3 三维 SPN 型密码的通用子空间迹性质

3.1 典型三维 SPN 型密码

除了二维 SPN 型密码的子空间迹性质, 我们同样对三维 SPN 型密码的子空间迹性质进行了研究, 参考 Cui 等人在文献 [16] 中给出的 3D 密码结构的一般化定义, 下面我们给出本文主要研究的典型三维 SPN 型密码的详细描述: 假设密码算法的内部状态可视为 F_{2^s} 上的一个 $l\times n\times m$ 三维数组 (这里假设 $n\leqslant m$), 记为 $X=\left(x_{k,i,j}\right)_{l\times n\times m}$, $x_{k,i,j}\in F_{2^s}$:

$$X=\begin{pmatrix}x_{0,0,0}&\cdots&x_{0,0,m-1}&\cdots&x_{i,0,0}&\cdots&x_{i,0,m-1}&\cdots&x_{l-1,0,0}&\cdots&x_{l-1,0,m-1}\\ \vdots&\ddots&\vdots&\ddots&\vdots&\ddots&\vdots&\ddots&\vdots&\ddots&\vdots\\ x_{0,n-1,0}&\cdots&x_{0,n-1,m-1}&\cdots&x_{i,n-1,0}&\cdots&x_{i,n-1,m-1}&\cdots&x_{l-1,n-1,0}&\cdots&x_{l-1,n-1,m-1}\end{pmatrix}$$

也称为一个状态立方体. 对于固定的 $0\leqslant k\leqslant l-1$, 称矩阵 $\left(x_{k,i,j}\right)_{n\times m}$ 为状态立方体的一个 slice, 对于固定的 $0\leqslant j\leqslant m-1$, 称矩阵 $\left(x_{k,i,j}\right)_{l\times n}$ 为状态立方体的一个 sheet, 对于固定的 $0\leqslant k\leqslant l-1$, $0\leqslant j\leqslant m-1$, 称 $\left(x_{k,i,j}\right)_{i=0}^{n-1}$ 为状态立方体的一列, 算法的轮函数由以下 4 个操作组成.

(1) 轮密钥加 κ_r: 将轮密钥与状态进行异或, 即 $\kappa_r(X)=X\oplus K_r$.

(2) 字节代换 γ: 对状态的每个字都应用 S 盒变换, 即 $\gamma(X)=(S(x_{0,0,0}),\ldots,S(x_{l-1,n-1,m-1}))$.

(3) 行移位 θ_1,θ_2: 两个不同的行移位变换 θ_1 和 θ_2 在奇数轮和偶数轮交替使用, 其中 θ_1 作用于每个 slice, θ_2 作用于每个 sheet, 即:

$$\theta_1:\left(x_{k,i,j}\right)_{l\times n\times m}\to\left(y_{k,i,j}\right)_{l\times n\times m},\ y_{k,i,j}=x_{k,i,(j+c_i)\bmod m},\ c_i\in\{0,1,\ldots,m-1\},$$

$$\theta_2:\left(x_{k,i,j}\right)_{l\times n\times m}\to\left(z_{k,i,j}\right)_{l\times n\times m},\ z_{k,i,j}=x_{(k+h_i)\bmod l,i,j},\ h_i\in\{0,1,\ldots,l-1\}.$$

(4) 列混淆 π: 对于状态立方体的每一列, 左乘一个定义在 $GF(2^s)$ 上的 $n\times n$ 可逆矩阵.

3.2 典型三维 SPN 型密码的子空间迹

对于典型三维 SPN 型密码我们定义了这样 4 类子空间: sheet 子空间 S_I、类对角子空间 D_I、类反对角子空间 ID_I、混淆子空间 M_I. 设 $\{e_{0,0,0},\ldots,e_{l-1,n-1,m-1}\}$ 表示 $F_{2^s}^{l\times n\times m}$ 上的单位向量 ($e_{k,i,j}$ 表示状态的 (k,i,j) 位置对应的元素为 1).

定义 7. sheet 子空间 S_j 定义为 $S_j=\left\langle e_{k,i,j}\right\rangle_{k\in\{0,\ldots,l-1\},i\in\{0,\ldots,n-1\}}$. 如 S_0 对应的矩阵表示为:

$$S_0=\left\{\left[\begin{array}{cccc|cccc|c|cccc}x_1^1&0&\cdots&0&x_1^2&0&\cdots&0&\cdots&x_1^l&0&\cdots&0\\ x_2^1&0&\cdots&0&x_2^2&0&\cdots&0&&x_2^l&0&\cdots&0\\ \vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\ddots&\vdots&&\vdots&\vdots&\ddots&\vdots\\ x_n^1&0&\cdots&0&x_n^2&0&\cdots&0&&x_n^l&0&\cdots&0\end{array}\right],\ \forall x_1^1,\ldots,x_n^l\in F_{2^s}\right\}$$

$$\equiv\left[\begin{array}{cccc|cccc|c|cccc}x_1^1&0&\cdots&0&x_1^2&0&\cdots&0&\cdots&x_1^l&0&\cdots&0\\ x_2^1&0&\cdots&0&x_2^2&0&\cdots&0&&x_2^l&0&\cdots&0\\ \vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\ddots&\vdots&&\vdots&\vdots&\ddots&\vdots\\ x_n^1&0&\cdots&0&x_n^2&0&\cdots&0&&x_n^l&0&\cdots&0\end{array}\right].$$

定义 8. 类对角子空间 D_j 和类反对角子空间 ID_j 分别定义为:

$$D_j=\theta_1^{-1}(S_j)=\left\langle e_{k,0,(j+c_0) \bmod m},e_{k,1,(j+c_1) \bmod m},\ldots,e_{k,n-1,(j+c_{n-1}) \bmod m}\right\rangle_{k\in\{0,\ldots,l-1\}},$$

$$ID_j=\theta_1(S_j)=\left\langle e_{k,0,(j-c_0) \bmod m},e_{k,1,(j-c_1) \bmod m},\ldots,e_{k,n-1,(j-c_{n-1}) \bmod m}\right\rangle_{k\in\{0,\ldots,l-1\}}.$$

如对于 $(l,n,m)=(4,4,4)$ 的典型三维 SPN 型密码, 若 θ_1 定义为置换 $(0,1,2,3)$, 则 D_0 和 ID_0 对应的矩阵表示分别为:

$$D_0=\left[\begin{array}{cccc|cccc|cccc|cccc}
x_1^1&0&0&0&x_1^2&0&0&0&x_1^3&0&0&0&x_1^4&0&0&0\\
0&x_2^1&0&0&0&x_2^2&0&0&0&x_2^3&0&0&0&x_2^4&0&0\\
0&0&x_3^1&0&0&0&x_3^2&0&0&0&x_3^3&0&0&0&x_3^4&0\\
0&0&0&x_4^1&0&0&0&x_4^2&0&0&0&x_4^3&0&0&0&x_4^4
\end{array}\right],$$

$$ID_0=\left[\begin{array}{cccc|cccc|cccc|cccc}
x_1^1&0&0&0&x_1^2&0&0&0&x_1^3&0&0&0&x_1^4&0&0&0\\
0&0&0&x_2^1&0&0&0&x_2^2&0&0&0&x_2^3&0&0&0&x_2^4\\
0&0&x_3^1&0&0&0&x_3^2&0&0&0&x_3^3&0&0&0&x_3^4&0\\
0&x_4^1&0&0&0&x_4^2&0&0&0&x_4^3&0&0&0&x_4^4&0&0
\end{array}\right].$$

定义 9. 混淆子空间 M_j 定义为: $M_j=\pi(ID_j)$.

此外, 给定集合 $I\subseteq\{0,1,\ldots,m-1\}$, 定义子空间 S_I, D_I, ID_I, M_I 分别为:

$$S_I=\bigoplus_{j\in I}S_j,\ D_I=\bigoplus_{j\in I}D_j,\ ID_I=\bigoplus_{j\in I}ID_j,\ M_I=\bigoplus_{j\in I}M_j.$$

在给出典型三维 SPN 型密码的 4 类子空间定义之后, 我们可以进一步推导典型三维 SPN 型密码的两个子空间迹, 如下述定理所示.

定理 7. 给定一个集合 $I\subseteq\{0,1,\ldots,m-1\}$, 对于任意的 $a\in D_I^{\perp}$, 存在唯一一个元素 $b\in M_I^{\perp}$ 使得 $R^3(D_I\oplus a)=M_I\oplus b$ 成立, 其中 b 依赖于 a 和密钥的取值, 即:

$$\mathrm{Prob}(R^3(x)\oplus R^3(y)\in M_I|x\oplus y\in D_I)=1.$$

证明: 根据典型三维 SPN 型密码的轮函数定义可知, 给定 D_I 的任意一个陪集 $D_I\oplus a$, $a\in D_I^{\perp}$, 其经过一次轮变换后会映射为 S_I 的一个陪集 $S_I\oplus a'$, $a'\in S_I^{\perp}$; $S_I\oplus a'$ 再经过一次轮变换后依然会映射为 S_I 的一个陪集 $S_I\oplus a''$, $a''\in S_I^{\perp}$, 进而 $S_I\oplus a''$ 再经过一次轮变换后会映射为 M_I 的一个陪集 $M_I\oplus b$, $b\in M_I^{\perp}$, 即证明了定理.

定理 8. 设 $I,J\subseteq\{0,1,\ldots,m-1\}$, 且 $|I|+|J|\leqslant r-1$, 则对于任意的 $x\neq y$ 有:

$$\mathrm{Prob}(R^6(x)\oplus R^6(y)\in M_I|x\oplus y\in D_J)=0.$$

证明: 证明与定理 5 类似, 不再详述.

3.3 典型三维 SPN 型密码的“2^{nl-1} 倍性质”

考虑属于类对角子空间 D_I 的同一陪集中的所有明文和经过 7 轮加密后的密文, 然后计算属于 M_J 同一陪集的不同密文对数量, 对于典型三维 SPN 型密码该数值以概率 1 为 2^{nl-1} 的倍数, 可具体描述为如下定理.

定理 9. 对于固定集合 I 和 J (这里假设 $|I|=1$), 设 D_I 和 M_J 分别表示一个类对角子空间和一个混淆子空间. 给定 D_I 的任意一个陪集 $D_I\oplus a$, $a\in D_I^{\perp}$, 考虑属于该陪集的所有 $2^{n\times l\times s}$ 个明文以及相应的经过 7 轮加密后的密文, 记为 (p^i,c^i), $i=0,1,\ldots,2^{n\times l\times s}-1$, 其中 $p^i\in D_I\oplus a$, $c^i=R^7(p^i)$, 则满足 $c^i\oplus c^j\in M_J(i\neq j)$ 的不同密文对 (c^i,c^j) 的数量 n:

$$n:=\left|\left\{(p^i,c^i),(p^j,c^j)|\forall p^i,p^j\in D_I\oplus a,\ p^i<p^j,\ c^i\oplus c^j\in M_J\right\}\right|$$

为 2^{nl-1} 的倍数. 其中“<”定义为: 给定两个不同的明文 t^1 和 t^2, $t^1<t^2$ 表示存在 $k\in\{0,1,\ldots,l-1\}$, $i\in\{0,1,\ldots,n-1\}$, $j\in\{0,1,\ldots,m-1\}$, 使得: (1) 对于所有满足 $p+n\cdot q+n\cdot m\cdot r<i+n\cdot j+n\cdot m\cdot k$ 的 $r\in\{0,1,\ldots,l-1\}$, $p\in\{0,1,\ldots,n-1\}$, $q\in\{0,1,\ldots,m-1\}$ 有 $t^1_{r,p,q}=t^2_{r,p,q}$; (2) $t^1_{k,i,j}<t^2_{k,i,j}$.

4 定理证明

4.1 定理 6 的证明

在本节中, 我们将给出定理 6 的一个详细证明. 如上所述, 证明引理 2 就足以证明定理 6, 所以我们只考虑引

理 2 的证明即可. 通过采用 Grassi 等人证明 AES 的“8 倍性质”的思想[14], 我们对引理 2 进行了证明; 此外, 在 AES 的“8 倍性质”证明中用到了列混淆矩阵为 MDS 矩阵的性质, 但下述证明表明列混淆矩阵不必为 MDS 矩阵, 即该性质与列混淆矩阵的差分分支数无关.

为简单起见, 这里假设 $I=\{0\}$ (其他情况亦可类似进行考虑). 首先考虑属于 M_0 同一陪集 $M_0\oplus a$, $a\in M_0^{\perp}$ 的两个元素 p^1 和 p^2, 则由混淆子空间的定义可知存在 $x_1,x_2,\ldots,x_n\in F_{2^s}$ 和 $x'_1,x'_2,\ldots,x'_n\in F_{2^s}$ 使得 (下面两个公式中从左到右的列索引分别为 $(0-l_0) \bmod m$、$(0-l_1) \bmod m$ 和 $(0-l_{n-1}) \bmod m$):

$$p^1=a\oplus\begin{bmatrix}\cdots & c_{1,1}\cdot x_1 & \cdots & c_{1,2}\cdot x_2 & \cdots & c_{1,n}\cdot x_n & \cdots\\ \cdots & c_{2,1}\cdot x_1 & \cdots & c_{2,2}\cdot x_2 & \cdots & c_{2,n}\cdot x_n & \cdots\\ & & & & & & \\ \cdots & c_{n,1}\cdot x_1 & \cdots & c_{n,2}\cdot x_2 & \cdots & c_{n,n}\cdot x_n & \cdots\end{bmatrix},$$

$$p^2=a\oplus\begin{bmatrix}\cdots & c_{1,1}\cdot x'_1 & \cdots & c_{1,2}\cdot x'_2 & \cdots & c_{1,n}\cdot x'_n & \cdots\\ \cdots & c_{2,1}\cdot x'_1 & \cdots & c_{2,2}\cdot x'_2 & \cdots & c_{2,n}\cdot x'_n & \cdots\\ & & & & & & \\ \cdots & c_{n,1}\cdot x'_1 & \cdots & c_{n,2}\cdot x'_2 & \cdots & c_{n,n}\cdot x'_n & \cdots\end{bmatrix}.$$

且对于 p^1 和 p^2, 由列混淆矩阵的差分分支数定义可知, 若 $x_i\neq 0$ 或 $x'_i\neq 0$, 则对应列中至少有 $r-1$ 个元素非零. 下面可记 p^1 和 p^2 分别由 $\langle x_1,x_2,\ldots,x_n\rangle$ 和 $\langle x'_1,x'_2,\ldots,x'_n\rangle$ 生成, 然后根据 $\langle x_1,x_2,\ldots,x_n\rangle$ 和 $\langle x'_1,x'_2,\ldots,x'_n\rangle$ 的 n 种不同取值情况分别进行考虑.

第 1 种情况: $\langle x_1,x_2,\ldots,x_n\rangle$ 和 $\langle x'_1,x'_2,\ldots,x'_n\rangle$ 中只有一个变量不相等.

假设 $x_1\neq x'_1,x_2=x'_2,\ldots,x_n=x'_n$ (其他情况类似), 则有 $p^1\oplus p^2\in C_{(0-l_0) \bmod m}$. 由 $p^1\oplus p^2\in C_{(0-l_0) \bmod m}$ 可直接得到 $R(p^1)\oplus R(p^2)\in M_{(0-l_0) \bmod m}$, 再结合引理 1 可知只有 $|J|>r-2$ 时 $R(p^1)\oplus R(p^2)\in D_J$ 才有可能成立. 为了更详细地进行分析, 我们具体计算了 $SR\circ SB(p^1)\oplus SR\circ SB(p^2)$ 的第 $(0-l_0-l_0) \bmod m+1$ 列:

$$(SR\circ SB(p^1)\oplus SR\circ SB(p^2))_{\cdot,(0-l_0-l_0) \bmod m}=\begin{pmatrix}S(c_{1,1}\cdot x_1\oplus a')\oplus S(c_{1,1}\cdot x'_1\oplus a')\\ 0\\ \vdots\\ 0\end{pmatrix}.$$

随后再进行列混淆操作即可得到 $R(p^1)\oplus R(p^2)$ 的第 $(0-l_0-l_0) \bmod m+1$ 列: $MC\circ(SR\circ SB(p^1)\oplus SR\circ SB(p^2))_{\cdot,(0-l_0-l_0) \bmod m}$. 然后考虑两种情况: 若 $S(c_{1,1}\cdot x_1\oplus a')\oplus S(c_{1,1}\cdot x'_1\oplus a')=0$, 则该列值全为 0; 若 $S(c_{1,1}\cdot x_1\oplus a')\oplus S(c_{1,1}\cdot x'_1\oplus a')\neq 0$, 则根据列混淆矩阵的差分分支数定义可知, 该列中至少有 $r-1$ 个元素非零, 即至多有 $n-(r-1)$ 个元素可为 0. 最后对满足 $|J|>r-2$ 的不同 J 分别构建关于 x_1,x'_1 的方程组求解即可. 当存在满足相应方程组的 p^1 和 p^2 时, 那么将 p^1 和 p^2 中的 $x_2,\ldots,x_n$ 的取值换成任意值仍然成立, 因此在这种情况下属于 D_J 的同一陪集的不同密文对数量一定为 $(2^s)^{n-1}$ 的倍数 (也包括 0).

第 i 种情况: $\langle x_1,x_2,\ldots,x_n\rangle$ 和 $\langle x'_1,x'_2,\ldots,x'_n\rangle$ 中有 i 个变量不相等 ($2\leqslant i\leqslant n$).

假设 $x_1\neq x'_1,\ldots,x_i\neq x'_i,x_{i+1}=x'_{i+1},\ldots,x_n=x'_n$ (其他情况类似), 则有 $p^1\oplus p^2\in C_{(0-l_0) \bmod m,\ldots,(0-l_{i-1}) \bmod m}$. 由 $p^1\oplus p^2\in C_{(0-l_0) \bmod m,\ldots,(0-l_{i-1}) \bmod m}$ 可直接得到 $R(p^1)\oplus R(p^2)\in M_{(0-l_0) \bmod m,\ldots,(0-l_{i-1}) \bmod m}$, 再结合引理 1 可知只有 $|J|>r-i-1$ 时 $R(p^1)\oplus R(p^2)\in D_J$ 才有可能成立. 若假设对于特定的 $x_{i+1},\ldots,x_n$ 存在两个元素 p^1 (由 $\langle x_1,x_2,\ldots,x_i\rangle$ 生成) 和 p^2 (由 $\langle x'_1,x'_2,\ldots,x'_i\rangle$ 生成) 满足 $R(p^1)\oplus R(p^2)\in D_J$, 则有由以下 $2^{i-1}-1$ 对元素生成的 $\hat{p}^1$ 和 $\hat{p}^2$ 也满足 $R(\hat{p}^1)\oplus R(\hat{p}^2)\in D_J$:

$\langle x'_1,x_2,x_3,\ldots,x_i\rangle$ 和 $\langle x_1,x'_2,x'_3,\ldots,x'_i\rangle$

$\langle x_1,x'_2,x_3,\ldots,x_i\rangle$ 和 $\langle x'_1,x_2,x'_3,\ldots,x'_i\rangle$

…

该结论是由 $R(p^1)\oplus R(p^2)=R(\hat{p}^1)\oplus R(\hat{p}^2)$ 保证的, 其中 $\hat{p}^1$ 和 $\hat{p}^2$ 这两个元素的存在性是由我们考虑的是 M_0 的完整陪集这一事实确保的, 那么此时属于 D_J 的同一陪集的不同密文对数量一定为 2^{i-1} 的倍数.

下面我们考虑是否存在 $x_1,x'_1,\ldots,x_i,x'_i$ 可以使得 $R(p^1)\oplus R(p^2)\in D_J$ 成立, 与第 1 种情况类似可以考虑 $SR\circ SB(p^1)\oplus SR\circ SB(p^2)$ 的每一列, 每一列中至多有 i 个关于 $x_1,x'_1,\ldots,x_i,x'_i$ 的元素, 随后再进行列混淆操作即可得到 $R(p^1)\oplus R(p^2)$ 的各列值. 然后考虑 $i+1$ 种情况: 若 $SR\circ SB(p^1)\oplus SR\circ SB(p^2)$ 的列中所有值均为 0, 则列混淆操作后该

列值全为 0; 若 $SR\circ SB(p^1)\oplus SR\circ SB(p^2)$ 的列中有一个值非零, 则列混淆操作后该列中至少有 $r-1$ 个元素非零, 即至多有 $n-(r-1)$ 个元素可为 0; 依此类推, 若 $SR\circ SB(p^1)\oplus SR\circ SB(p^2)$ 的列中有 i 个值非零, 则列混淆操作后该列中至少有 $r-i$ 个元素非零, 即至多有 $n-(r-i)$ 个元素可为 0. 最后对满足 $|J|>r-i-1$ 的不同 J 分别构建关于 $x_1,x_1',\ldots,x_i,x_i'$ 的方程组求解即可. 若方程组有解, 则对于任意的 $x_{i+1},\ldots,x_n$, 由 $\langle x_1,x_2,\ldots,x_i\rangle$ 和 $\left\langle x_1',x_2',\ldots,x_i'\right\rangle$ 的 2^{i-1} 个组合所生成的所有 (p^1,p^2) 对均满足 $R(p^1)\oplus R(p^2)\in D_J$. 因此在这种情况下属于 D_J 的同一陪集的不同密文对数量一定为 $2^{i-1}\cdot(2^s)^{n-i}$ 的倍数 (也包括 0).

综上所述, 对于给定的 J, 分别将不同情况下属于 D_J 的同一陪集的不同密文对数量相加, 即可得到总数量 n. 依据上述 n 种情况的分析可知, 分别存在 $N_1,N_2,\ldots,N_n\in\mathbb{N}$ 可以使得 $n=N_1\cdot(2^s)^{n-1}+N_2\cdot 2\cdot(2^s)^{n-2}+\ldots+N_n\cdot 2^{n-1}=2^{n-1}\cdot(N_1\cdot 2^{(n-1)(s-1)}+N_2\cdot 2^{(n-2)(s-1)}+\ldots+N_n)$ (对于与 $|J|$ 取值不相符的情况或方程组无解的情况, N_i 值均为 0), 即 n 为 2^{n-1} 的倍数, 即证明了引理.

进而考虑典型二维 SPN 型密码的 5 轮子空间迹: $D_I\oplus a\xrightarrow[prob.1]{R^2(\cdot)}M_I\oplus b\xrightarrow{R(\cdot)}D_J\oplus c\xrightarrow[prob.1]{R^2(\cdot)}M_J\oplus d$. 由引理 2 可知, 满足中间轮 $M_I\oplus b\xrightarrow{R(\cdot)}D_J\oplus c$ 的不同密文对数量一定为 2^{n-1} 的倍数, 然后通过逆向扩展两轮可以以概率 1 将 M_I 的陪集映射为 D_I 的陪集, 而通过正向扩展两轮可以以概率 1 将 D_J 的陪集映射为 M_J 的陪集, 即证明了定理 6. 对于 $|I|=2,3,\ldots$ 的情况, 也有类似的定理和证明, 这里不再详细描述.

4.2 定理 9 的证明

由定理 7 可知, D_I 的任意一个陪集经过 3 轮轮变换后会以概率 1 映射为 M_I 的一个陪集, 故定理 9 中的 7 轮性质可以描述为: $D_I\oplus a\xrightarrow[prob.1]{R^3(\cdot)}M_I\oplus b\xrightarrow{R(\cdot)}D_J\oplus c\xrightarrow[prob.1]{R^3(\cdot)}M_J\oplus d$, 则定理 9 的证明核心即转换为中间轮变换 $M_I\to D_J$. 与第 4.1 节中引理 2 的证明类似, 这里同样考虑属于 M_0 同一陪集 $M_0\oplus a$, $a\in M_0^{\perp}$ 的两个元素 p^1 和 p^2, 则由混淆子空间的定义可知存在 $x_1^1,\ldots,x_n^1,\ldots,x_1^l,\ldots,x_n^l\in F_{2^s}$ 和 $\bar{x}_1^1,\ldots,\bar{x}_n^1,\ldots,\bar{x}_1^l,\ldots,\bar{x}_n^l\in F_{2^s}$ 使得:

$$p^1=a\oplus\begin{bmatrix}\cdots & c_{1,1}\cdot x_1^1 & \cdots & c_{1,n}\cdot x_n^1 & \cdots & c_{1,1}\cdot x_1^i & \cdots & c_{1,n}\cdot x_n^i & \cdots & c_{1,1}\cdot x_1^l & \cdots & c_{1,n}\cdot x_n^l & \cdots\\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots\\ \cdots & c_{n,1}\cdot x_1^1 & \cdots & c_{n,n}\cdot x_n^1 & \cdots & c_{n,1}\cdot x_1^i & \cdots & c_{n,n}\cdot x_n^i & \cdots & c_{n,1}\cdot x_1^l & \cdots & c_{n,n}\cdot x_n^l & \cdots\end{bmatrix},$$

$$p^2=a\oplus\begin{bmatrix}\cdots & c_{1,1}\cdot \bar{x}_1^1 & \cdots & c_{1,n}\cdot \bar{x}_n^1 & \cdots & c_{1,1}\cdot \bar{x}_1^i & \cdots & c_{1,n}\cdot \bar{x}_n^i & \cdots & c_{1,1}\cdot \bar{x}_1^l & \cdots & c_{1,n}\cdot \bar{x}_n^l & \cdots\\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots\\ \cdots & c_{n,1}\cdot \bar{x}_1^1 & \cdots & c_{n,n}\cdot \bar{x}_n^1 & \cdots & c_{n,1}\cdot \bar{x}_1^i & \cdots & c_{n,n}\cdot \bar{x}_n^i & \cdots & c_{n,1}\cdot \bar{x}_1^l & \cdots & c_{n,n}\cdot \bar{x}_n^l & \cdots\end{bmatrix}.$$

记 p^1 和 p^2 分别由 $\left\langle x_1^1,\ldots,x_n^1,\ldots,x_1^l,\ldots,x_n^l\right\rangle$ 和 $\left\langle \bar{x}_1^1,\ldots,\bar{x}_n^1,\ldots,\bar{x}_1^l,\ldots,\bar{x}_n^l\right\rangle$ 生成, 然后根据 $\left\langle x_1^1,\ldots,x_n^1,\ldots,x_1^l,\ldots,x_n^l\right\rangle$ 和 $\langle \bar{x}_1^1,\ldots,\bar{x}_n^1,\ldots,\bar{x}_1^l,\ldots,\bar{x}_n^l\rangle$ 的 nl 种不同取值情况分别进行考虑, 则依照第 4.1 节中的证明结果可知: 属于 D_J 的同一陪集的不同密文对数量一定为 2^{nl-1} 的倍数.

进而考虑典型三维 SPN 型密码的 7 轮子空间迹: $D_I\oplus a\xrightarrow[prob.1]{R^3(\cdot)}M_I\oplus b\xrightarrow{R(\cdot)}D_J\oplus c\xrightarrow[prob.1]{R^3(\cdot)}M_J\oplus d$. 已知满足中间轮 $M_I\oplus b\xrightarrow{R(\cdot)}D_J\oplus c$ 的不同密文对数量一定为 2^{nl-1} 的倍数, 然后通过逆向扩展 3 轮可以以概率 1 将 M_I 的陪集映射为 D_I 的陪集, 而通过正向扩展 3 轮可以以概率 1 将 D_J 的陪集映射为 M_J 的陪集, 即证明了定理 9.

5 实验分析

在第 4 节中我们已经对本文研究的 SPN 型密码的子空间迹性质进行了证明, 但为了更直观地呈现本文提出的子空间迹性质, 在本节中我们选择了一些算法来进行验证. 对于典型二维 SPN 型密码, 我们以 PHOTON 算法的内部置换和 Rijndael 算法的小规模版本为例做了具体的实验; 对于典型三维 SPN 型密码, 我们选择了 3D 算法和 Saturnin 算法作为实例, 并在其相应的小规模版本上进行了实验.

5.1 PHOTON 置换

PHOTON 是 Guo 等人提出的一种基于海绵结构的轻量级哈希函数[17], 并在 ISO/IEC 29192-5: 2016 中被标准

化. PHOTON 算法共包含 5 个哈希函数, 分别对应 5 个不同的内部置换. PHOTON 置换采用典型二维 SPN 型密码的设计原则, 其状态可以表示为 F_{2^s} 上的一个 $n\times n$ 二维数组, 5 个置换可分别记为: PHOTON_{100}: $s=4$, $n=5$; PHOTON_{144}: $s=4$, $n=6$; PHOTON_{196}: $s=4$, $n=7$; PHOTON_{256}: $s=4$, $n=8$; PHOTON_{288}: $s=8$, $n=6$ (考虑到实现的复杂度, 这里不考虑最后一种置换). 置换的轮函数由以下 4 个操作组成.

(1) AddConstants: 将固定常数与状态第 1 列元素进行异或.

(2) SubCells: 对状态的每个元素应用 S 盒变换, 算法中使用了两种类型的 S 盒: PRESENT 的 4 比特 S 盒以及 AES 的 8 比特 S 盒.

(3) ShiftRows: 对于状态的每一行 i, 分别将其对应行元素循环左移 i 个位置.

(4) MixColumnsSerial: 通过左乘一个 $n\times n$ 的 MDS 矩阵对状态逐列进行线性变换.

利用 C/C++实现, 我们分别在 4 个 PHOTON 置换上进行了实验. 根据定理 6, 对于固定集合 I 和 J, 首先需要选择 D_I 的任意一个陪集, 即所需数据量为 $2^{|I|\times 4n}$, 所以我们取 $|I|=1$, 否则数据复杂度太大; 此外, 对于任意两个不同的密文, 其属于 M_J 的同一陪集的概率为 $2^{-n\times n\times 4+|J|\times 4n}=2^{-(n-|J|)\times 4n}$, 则 2^{4n} 个密文中属于 M_J 的同一陪集的不同密文对数量约为 $C_{2^{4n}}^2\times 2^{-(n-|J|)\times 4n}$, 所以我们取 $|J|=n-1$, 否则该值较小, 不易判断, 综上所述, 实验选择 $|I|=1$, $|J|=n-1$. 首先随机选择 D_I 的任意一个陪集, 即 2^{4n} 个明文, 并用 5 轮的 PHOTON 置换对 2^{4n} 个明文进行加密得到密文, 然后计算密文中属于 M_J 同一陪集的不同密文对数量 N, 由于 $M_J=MC(ID_J)$, 所以对密文进行判断时采用 $MC^{-1}(c)$ 进行判断更容易, 如对于每次实验, 在计算属于 M_J 同一陪集的密文对数量时可以选择以 $x=MC^{-1}(c)_{0,j}+2^4\times MC^{-1}(c)_{1,(j-1)\bmod n}+\ldots+(2^4)^{n-1}\times MC^{-1}(c)_{n-1,(j-n+1)\bmod n}$, $j=\{0,1,\ldots,n-1\}\backslash J$ 作为密文索引, 若两个密文具有相同的索引即属于 M_J 的同一陪集, 最后判断值 N 是否为 2^{n-1} 的倍数. 此外, 由于 $|J|=n-1$, M_J 自然有 n 种不同的选择, 若对 M_J 的 n 种情况都进行考虑即相当于进行 n 次实验. 对于 PHOTON_{100}、PHOTON_{144} 和 PHOTON_{196}, 因为复杂度较小, 所以我们对 n 个不同的 I 和 n 个不同的 J 均进行了实验, 结果分别如表 1–表 3 所示; 对于 PHOTON_{256}, 因为复杂度变大, 实验所需时间较长, 所以我们只对 $I=\{0\}$ 及其相应的 n 个不同的 J 进行了实验, 实验结果如表 4 所示.

表 1 置换 PHOTON_{100} 上的实验结果

D_I	变量	$M_{1,2,3,4}$	$M_{0,2,3,4}$	$M_{0,1,3,4}$	$M_{0,1,2,4}$	$M_{0,1,2,3}$
D_0	N	516208	533520	525312	517440	521264
	N mod 16	0	0	0	0	0
D_1	N	517968	515696	513488	529856	517584
	N mod 16	0	0	0	0	0
D_2	N	519248	516544	525040	523632	532128
	N mod 16	0	0	0	0	0
D_3	N	529904	514944	520832	527232	513600
	N mod 16	0		0	0	0
D_4	N	513536	516640	515376	516816	517600
	N mod 16	0	0	0	0	0

表 2 置换 PHOTON_{144} 上的实验结果

D_I	变量	$M_{1,2,3,4,5}$	$M_{0,2,3,4,5}$	$M_{0,1,3,4,5}$	$M_{0,1,2,4,5}$	$M_{0,1,2,3,5}$	$M_{0,1,2,3,4}$
D_0	N	8378624	8379392	8357248	8367744	8452256	8413056
	N mod 32	0	0	0	0	0	0
D_1	N	8438880	8395744	8381792	8449920	321344	8518304
	N mod 32	0	0	0	0	0	0
D_2	N	8448608	8383712	8413184	8411584	8332128	8375808
	N mod 32	0	0	0	0	0	0

表 2 置换 PHOTON_{144} 上的实验结果 (续)

D_I	变量	$M_{1,2,3,4,5}$	$M_{0,2,3,4,5}$	$M_{0,1,3,4,5}$	$M_{0,1,2,4,5}$	$M_{0,1,2,3,5}$	$M_{0,1,2,3,4}$
D_3	N	8 390 144	8 408 512	8 390 688	8 414 656	8 438 080	8 365 280
	N mod 32	0	0	0	0	0	0
D_4	N	8 495 040	8 374 080	8 366 272	8 365 568	8 300 736	8 295 552
	N mod 32	0	0	0	0	0	0
D_5	N	8 462 432	8 339 232	8 327 360	8 306 272	8 401 856	8 375 232
	N mod 32	0	0	0	0	0	0

表 3 置换 PHOTON_{196} 上的实验结果

D_I	变量	$M_{1,2,3,4,5,6}$	$M_{0,2,3,4,5,6}$	$M_{0,1,3,4,5,6}$	$M_{0,1,2,4,5,6}$	$M_{0,1,2,3,5,6}$	$M_{0,1,2,3,4,6}$	$M_{0,1,2,3,4,5}$
D_0	N	134 566 464	134 187 584	134 304 512	134 220 160	134 359 360	134 181 760	134 402 880
	N mod 64	0	0	0	0	0	0	0
D_1	N	134 456 768	134 016 960	133 697 280	135 032 640	134 029 632	134 180 352	134 531 392
	N mod 64	0	0	0	0	0	0	0
D_2	N	134 248 064	134 950 272	133 915 328	133 856 064	134 192 192	134 660 800	134 026 112
	N mod 64	0	0	0	0	0	0	0
D_3	N	134 073 664	133 995 840	133 867 136	134 150 528	134 090 240	134 644 224	134 199 872
	N mod 64	0	0	0	0	0	0	0
D_4	N	134 383 616	134 596 160	133 856 384	133 594 176	134 218 752	134 218 240	133 837 248
	N mod 64	0	0	0	0	0	0	0
D_5	N	133 993 728	134 548 032	133 994 880	133 794 944	134 947 520	134 588 096	134 590 592
	N mod 64	0	0	0	0	0	0	0
D_6	N	134 146 816	133 919 040	134 016 320	134 173 440	134 545 600	133 429 504	134 250 624
	N mod 64	0	0	0	0	0	0	0

表 4 置换 PHOTON_{256} 上的实验结果 (D_0)

变量	$M_{1,2,3,4,5,6,7}$	$M_{0,2,3,4,5,6,7}$	$M_{0,1,3,4,5,6,7}$	$M_{0,1,2,4,5,6,7}$	$M_{0,1,2,3,5,6,7}$	$M_{0,1,2,3,4,6,7}$	$M_{0,1,2,3,4,5,7}$	$M_{0,1,2,3,4,5,6}$
N	2 150 950 144	2 149 393 920	2 149 082 368	2 144 953 600	2 144 202 880	2 147 714 816	2 144 700 928	2 148 163 840
N mod 128	0	0	0	0	0	0	0	0

5.2 Rijndael 算法

Rijndael 算法是由比利时学者 Daemen 等人共同设计的迭代型分组密码算法[2], 是 AES 算法的前身, 其分组长度和密钥长度可设定为 32 比特的任意倍数, 其中最小值为 128 比特, 最大值为 256 比特. 对于分组长度分别为 128、192 和 256 比特的 3 个算法, 其状态可分别表示为 4×4、4×6、4×8 的二维数组, 其中数组的每个元素为一个字节. 算法轮函数由 SubBytes、ShiftRows、MixColumns、AddRoundKey 这 4 个操作组成, 其中只有行移位操作与现在的 AES 算法不同, 3 个算法的循环右移数分别为: $(0,1,2,3)$、$(0,1,2,3)$ 和 $(0,1,3,4)$.

利用 C/C++实现, 我们同样在上述 3 个 Rijndael 算法的小规模版本上进行了实验, 这里的小规模版本是参考 AES 的小规模版本将 Rijndael 算法中的 8 比特元素改为 4 比特元素得到的, 使用小规模版本的目的是减小复杂度以便于实现. 与第 5.1 节中对 PHOTON 置换的分析类似, 这里同样选择 $|I|=1$, $|J|=m-1$. 首先随机选择 D_I 的任意一个陪集, 即 2^{16} 个明文, 并用随机生成的密钥对 2^{16} 个明文进行 5 轮加密得到密文, 然后计算密文中属于 M_J 同一陪集的不同密文对数量 N, 计算过程同样与 PHOTON 置换类似, 最后判断该值是否为 8 的倍数. 对于 3 个小规模版本的 Rijndael 算法, 我们对 m 个不同的 I 和 m 个不同的 J 均进行了实验, 结果分别如表 5–表 7 所示.

表 5 小规模 Rijndael-128 上的实验结果

D_I	变量	$M_{1,2,3}$	$M_{0,2,3}$	$M_{0,1,3}$	$M_{0,1,2}$
D_0	N	32256	27968	30656	28352
	N mod 8	0	0	0	0
D_1	N	33792	29312	31424	31616
	N mod 8	0	0	0	0
D_2	N	31808	29888	32000	28736
	N mod 8	0	0	0	0
D_3	N	29568	32128	31936	29824
	N mod 8	0	0	0	0

表 6 小规模 Rijndael-192 上的实验结果

D_I	变量	$M_{1,2,3,4,5}$	$M_{0,2,3,4,5}$	$M_{0,1,3,4,5}$	$M_{0,1,2,4,5}$	$M_{0,1,2,3,5}$	$M_{0,1,2,3,4}$
D_0	N	30208	31680	31528	30528	30480	30544
	N mod 8	0	0	0	0	0	0
D_1	N	30864	30128	30064	31472	31528	30784
	N mod 8	0	0	0	0	0	0
D_2	N	30208	32768	32160	30784	30000	30544
	N mod 8	0	0	0	0	0	0
D_3	N	30560	30424	31296	30952	30488	32448
	N mod 8	0	0	0	0	0	0
D_4	N	30432	30968	29936	30448	30800	31168
	N mod 8	0	0	0	0	0	0
D_5	N	30144	31912	30528	30968	30816	28544
	N mod 8	0	0	0	0	0	0

表 7 小规模 Rijndael-256 上的实验结果

D_I	变量	$M_{1,2,3,4,5,6,7}$	$M_{0,2,3,4,5,6,7}$	$M_{0,1,3,4,5,6,7}$	$M_{0,1,2,4,5,6,7}$	$M_{0,1,2,3,5,6,7}$	$M_{0,1,2,3,4,6,7}$	$M_{0,1,2,3,4,5,7}$	$M_{0,1,2,3,4,5,6}$
D_0	N	30944	32256	0	32384	30496	0	0	0
	N mod 8	0	0	0	0	0	0	0	0
D_1	N	0	30720	30208	0	31232	30816	0	0
	N mod 8	0	0	0	0	0	0	0	0
D_2	N	0	0	31232	32768	0	34240	30688	0
	N mod 8	0	0	0	0	0	0	0	0
D_3	N	0	0	0	30528	34048	0	34304	30752
	N mod 8	0	0	0	0	0	0	0	0
D_4	N	30912	0	0	0	30976	32640	0	30784
	N mod 8	0	0	0	0	0	0	0	0
D_5	N	34048	30944	0	0	0	30784	32704	0
	N mod 8	0	0	0	0	0	0	0	0
D_6	N	0	28160	30592	0	0	0	30720	33408
	N mod 8	0	0	0	0	0	0	0	0
D_7	N	31616	0	32896	31424	0	0	0	31104
	N mod 8	0	0	0	0	0	0	0	0

5.3 3D 算法

3D 算法是 Nakahara 在 CANS 2008 上提出的一个分组密码算法[18], 其设计思想源于 AES 算法, 算法的分组规模和密钥规模均为 512 比特, 其状态可表示为 $4\times4\times4$ 的字节立方体, 算法轮函数由轮密钥加、置换层、行移位和列混淆这 4 个操作组成.

(1) 轮密钥加 k_i: 将轮密钥与每轮的输入直接异或.

(2) 置换层 γ: 将数据的每个字节都进行相同的 S 盒操作, 其中 S 盒采用 AES 的 S 盒.

(3) 行移位 θ_1,θ_2: θ_1 对立方体的每个 slice 进行 AES 的行移位变换; θ_2 对立方体的每个 sheet 进行 AES 的行移位变换; 其中 θ_1 作用于奇数轮, θ_2 作用于偶数轮.

(4) 列混淆 π: 采用 Aunbis 密码中的 4×4 MDS 矩阵对数据的每一列进行相乘操作.

为了便于实现, 我们将 3D 算法的规模缩减为 $2\times4\times4$, 并参考 AES 的小规模版本将其中的 8 比特元素改为 4 比特元素, 然后在该小规模版本上进行了实验. 与前面的分析类似, 这里也选择 $|I|=1$, $|J|=3$. 首先随机选择 D_I 的任意一个陪集, 即 2^{32} 个明文, 并用随机生成的密钥对 2^{32} 个明文进行 7 轮加密得到密文, 然后计算密文中属于 M_J 同一陪集的不同密文对数量 N, 最后判断该值是否为 128 的倍数, 对于 $I=\{0\}$ 及其相应的 4 个不同的 J 的实验结果如表 8 所示.

表 8 小规模 3D-2-4-4 上的实验结果 (D_0)

变量	$M_{1,2,3}$	$M_{0,2,3}$	$M_{0,1,3}$	$M_{0,1,2}$
N	36293312512	28068904960	31490363392	34395812352
N mod 128	0	0	0	0

5.4 Saturnin 算法

Saturnin 算法是 NIST 轻量级密码算法征集的第 2 轮候选算法之一[19], 是基于自行设计的分组密码 Saturnin 而设计的轻量级密码算法, 其中分组密码 Saturnin 的设计思想源于 AES 算法, 其分组规模和密钥规模均为 256 比特, 状态可表示为 $4\times4\times4$ 的半字节立方体, 算法轮函数由 S 盒层、半字节置换、线性层、半字节置换的逆、轮密钥异或这 5 个操作组成.

(1) S 盒层 S: 对数据的偶数索引半字节和奇数索引半字节分别应用两个不同的 4 比特 S 盒.

(2) 半字节置换 SR_r: 对于偶数轮, SR_r 是恒等变换; 对于奇数轮, 若 $r \bmod 4=1$, $SR_r=SR_{\text{slice}}$, 即对数据的每个 slice 进行相同的行移位操作, 可描述为 $(x,y,z)\xrightarrow{SR_{\text{slice}}}(x+y \bmod 4,y,z)$, 若 $r \bmod 4=3$, $SR_r=SR_{\text{sheet}}$, 即对数据的每个 sheet 进行相同的行移位操作, 可描述为 $(x,y,z)\xrightarrow{SR_{\text{sheet}}}(x,y,z+y \bmod 4)$, 如图 1 所示.

(3) 线性层 MC: 对数据的每一列并行应用一个线性变换, 具体细节可参考设计文档.

(4) 半字节置换的逆 SR_r^{-1}: 应用该轮对应的半字节置换 SR_r 的逆运算.

(5) 轮密钥异或: 对于奇数轮, 将状态与一个轮密钥进行异或.

针对 Saturnin 算法, 由于其轮函数与第 3.1 节中定义的典型三维 SPN 型密码的轮函数不完全一致, 故其子空间迹性质不能直接套用第 3.3 节中的定理 9, 但由于轮函数中的 SR_r^{-1} 和 S 操作顺序可交换, 故连续两轮轮函数 $S\to SR_{\text{slice}}/SR_{\text{sheet}}\to MC\to SR_{\text{slice}}^{-1}\big/SR_{\text{sheet}}^{-1}\to S\to MC$ (忽略轮密钥异或操作) 可等价为 $S\to SR_{\text{slice}}/SR_{\text{sheet}}\to MC\to S\to SR_{\text{slice}}^{-1}/SR_{\text{sheet}}^{-1}\to MC$, 然后分析该等价轮函数依旧可以得到算法的一个 7 轮性质, 即: 属于 slice 子空间 $Slice_I$ 的同一陪集的所有明文经过 7 轮加密得到的密文中属于子空间 $MC(D_J)$ 的同一陪集的不同密文对数量一定为 2^{15} 的倍数, 该 7 轮性质可以具体描述为:

$$Slice_I\oplus a\xrightarrow[prob.1]{R^4(\cdot)}MC(Sheet\text{-}ID_I)\oplus b\xrightarrow{R(\cdot)}D_J\oplus c\xrightarrow[prob.1]{R^2(\cdot)}MC(D_J)\oplus d,$$

其中, $Slice_I$ 表示一个 slice 子空间 (即一个或多个 slice), $Sheet\text{-}ID_I$ 表示 sheet 面上的类反对角子空间, 即 $SR_{\text{sheet}}(Slice_I)$. 针对 Saturnin 算法, 我们同样在缩小规模版本上进行了验证, 实验结果与理论分析保持一致.

最后, 由于本文提出的针对 SPN 型密码的通用子空间迹性质是一个概率为 1 的性质, 为了呈现其优势, 针对实验验证的 4 个算法: PHOTON 置换、Rijndael 算法、3D 算法、Saturnin 算法, 我们将本文提出的子空间迹性质与现有的概率为 1 的区分器进行了比较, 如表 9 所示. 结果表明, 子空间迹性质基本能达到现有的概率为 1 的区分器的相同长度, 特别地, 针对 3D 密码, 可以给出一个更好的 7 轮区分器.

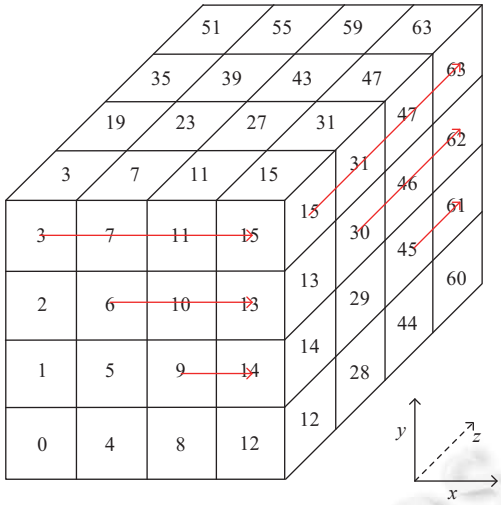

图 1 Saturnin 算法内部状态的三维表示

表 9 与现有的概率为 1 的区分器的比较

算法	轮数	区分器类型	相关文献
PHOTON置换	5	不可能差分区分器	[20]
	5	子空间迹性质	本文第5.1节
Rijndael算法	⩽6	不可能差分区分器	[21]
	⩽6	积分区分器	[22]
	5	子空间迹性质	本文第5.2节
3D算法	6	不可能差分区分器	[23]
	6.25	积分区分器	[24]
	7	子空间迹性质	本文第5.3节
Saturnin算法	7	不可能差分区分器	[19]
	7	子空间迹性质	本文第5.4节

6 总 结

本文针对典型二维 SPN 型密码和典型三维 SPN 型密码的子空间迹进行了研究, 并得到了以下两条通用性质: 1) 针对一个状态可形式化为 $n\times m$ 二维数组 (假设 $n\leqslant m$) 的典型二维 SPN 型密码, 属于类对角子空间 D_I 的同一陪集的所有明文经过 5 轮加密得到的密文中属于混淆子空间 M_J 的同一陪集的不同密文对数量一定为 2^{n-1} 的倍数; 2) 针对一个状态可形式化为 $l\times n\times m$ 三维数组 (假设 $n\leqslant m$) 的典型三维 SPN 型密码, 属于类对角子空间 D_I 的同一陪集的所有明文经过 7 轮加密得到的密文中属于混淆子空间 M_J 的同一陪集的不同密文对数量一定为 2^{nl-1} 的倍数. 该性质与密钥、S 盒以及列混淆矩阵的细节均无关, 且适用于所有此类 SPN 型密码, 所以在实际应用中, 针对此类典型 SPN 型密码我们可以根据其子空间迹性质直接得到一个 5 轮或 7 轮区分器, 进而进行分析.

References:

[1] Feistel H. Cryptography and computer privacy. Scientific American, 1973, 228(5): 15–23. [doi: 10.1038/scientificamerican0573-15]

[2] Daemen J, Rijmen V. The Design of Rijndael. Berlin: Springer, 2002. [doi: 10.1007/978-3-662-04722-4]

[3] Wu WL, Zhang L, Zheng YF, Li LC. The block cipher uBlock. Journal of Cryptologic Research, 2019, 6(6): 690 –703 (in Chinese with English abstract). [doi: 10.13868/j.cnki.jcr.000334]

[4] Shannon CE. Communication theory of secrecy systems. The Bell System Technical Journal, 1949, 28(4): 656–715. [doi: 10.1002/j.1538-7305.1949.tb00928.x]

[5] Lai XJ, Massey JL. A proposal for a new block encryption standard. In: Proc. of the 1991 Workshop on the Theory and Application of Cryptographic Techniques. Aarhus: Springer, 1991. 389–404. [doi: 10.1007/3-540-46877-3_35]

[6] Vaudenay S. On the Lai-Massey scheme. In: Proc. of the 1999 Int'l Conf. on the Theory and Application of Cryptology and Information Security. Singapore: Springer, 1999. 8–19. [doi: 10.1007/978-3-540-48000-6_2]

[7] Leander G, Abdelraheem MA, Alkhzaimi H, Zenner E. A cryptanalysis of PRINTcipher: The invariant subspace attack. In: Proc. of the 31st Annual Cryptology Conf. Santa Barbara: Springer, 2011. 206–221. [doi: 10.1007/978-3-642-22792-9_12]

[8] Leander G, Minaud B, Rønjom S. A generic approach to invariant subspace attacks: Cryptanalysis of Robin, iSCREAM and Zorro. In: Proc. of the 34th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Sofia: Springer, 2015. 254–283. [doi: 10.1007/978-3-662-46800-5_11]

[9] Liu YW, Rijmen V. New observations on invariant subspace attack. Information Processing Letters, 2018, 138: 27–30. [doi: 10.1016/j.ipl.

2018.01.015]
[10] Todo Y, Leander G, Sasaki Y. Nonlinear invariant attack: Practical attack on full SCREAM, iSCREAM, and Midori64. Journal of Cryptology, 2019, 32(4): 1383–1422. [doi: 10.1007/s00145-018-9285-0]
[11] Beierle C, Canteaut A, Leander G, Rotella Y. Proving resistance against invariant attacks: How to choose the round constants. In: Proc. of the 37th Annual Int'l Cryptology Conf. Santa Barbara: Springer, 2017. 647–678. [doi: 10.1007/978-3-319-63715-0_22]
[12] Wei YZ, Ye T, Wu WL, Pasalic E. Generalized nonlinear invariant attack and a new design criterion for round constants. IACR Trans. on Symmetric Cryptology, 2018, 2018(4): 62–79. [doi: 10.13154/tosc.v2018.i4.62-79]
[13] Grassi L, Rechberger C, Rønjom S. Subspace trail cryptanalysis and its applications to AES. IACR Trans. on Symmetric Cryptology, 2017, 2016(2): 192–225. [doi: 10.13154/tosc.v2016.i2.192-225]
[14] Grassi L, Rechberger C, Rønjom S. A new structural-differential property of 5-round AES. In: Proc. of the 36th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Paris: Springer, 2017. 289–317. [doi: 10.1007/978-3-319-56614-6_10]
[15] Boura C, Canteaut A, Coggia D. A general proof framework for recent AES distinguishers. IACR Trans. on Symmetric Cryptology, 2019, 2019(1): 170–191. [doi: 10.13154/tosc.v2019.i1.170-191]
[16] Cui T, Jin CH. Finding impossible differentials for Rijndael-like and 3D-like structures. KSII Trans. on Internet and Information Systems, 2013, 7(3): 509–521. [doi: 10.3837/tiis.2013.03.006]
[17] Guo J, Peyrin T, Poschmann A. The PHOTON family of lightweight hash functions. In: Proc. of the 31st Annual Cryptology Conf. Santa Barbara: Springer, 2011. 222–239. [doi: 10.1007/978-3-642-22792-9_13]
[18] Nakahara Jr J. 3D: A three-dimensional block cipher. In: Proc. of the 7th Int'l Conf. Hong Kong: Springer, 2008. 252–267. [doi: 10.1007/978-3-540-89641-8_18]
[19] Canteaut A, Duval S, Leurent G, Naya-Plasencia M, Perrin L, Pornin T, Schrottenloher A. Saturnin: A suite of lightweight symmetric algorithms for post-quantum security. IACR Trans. on Symmetric Cryptology, 2020, 2020(S1): 160–207. [doi: 10.13154/tosc.v2020.iS1.160-207]
[20] Shen X, Liu GQ, Sun B, Li C. Impossible differentials of SPN ciphers. In: Proc. of the 12th Int'l Conf. on Information Security and Cryptology. Beijing: Springer, 2017. 47–63. [doi: 10.1007/978-3-319-54705-3_4]
[21] Liu Y, Shi YF, Gu DW, Dai B, Zhao FY, Li W, Liu ZQ, Zeng ZQ. Improved impossible differential cryptanalysis of large-block Rijndael. Science China Information Sciences, 2019, 62(3): 32101. [doi: 10.1007/s11432-017-9365-4]
[22] Li YJ, Wu WL. Improved integral attacks on Rijndael. Journal of Information Science and Engineering, 2011, 27(1): 2031–2045.
[23] Xie ZM, Chen SZ, Lu LZ. Impossible differential cryptanalysis of 11-round 3D cipher. Journal of Electronics & Information Technology, 2014, 36(5): 1215–1220 (in Chinese with English abstract). [doi: 10.3724/SP.J.1146.2013.00948]
[24] Wang MY, Tang XH, Li C, Qu LJ. Square attacks on 3D cipher. Journal of Electronics & Information Technology, 2010, 32(1): 157–161 (in Chinese with English abstract). [doi: 10.3724/SP.J.1146.2008.01846]

附中文参考文献:

[3] 吴文玲, 张蕾, 郑雅菲, 李灵琛. 分组密码uBlock. 密码学报, 2019, 6(6): 690–703. [doi: 10.13868/j.cnki.jcr.000334]
[23] 谢作敏, 陈少真, 鲁林真. 11轮3D密码的不可能差分攻击. 电子与信息学报, 2014, 36(5): 1215–1220. [doi: 10.3724/SP.J.1146.2013.00948]
[24] 王美一, 唐学海, 李超, 屈龙江. 3D密码的Square攻击. 电子与信息学报, 2010, 32(1): 157–161. [doi: 10.3724/SP.J.1146.2008.01846]

宋蝉(1997－), 女, 博士生, 主要研究领域为认证加密算法的分析与设计.

吴文玲(1966－), 女, 博士, 研究员, 博士生导师, 主要研究领域为对称密码算法的设计与分析.

张蕾(1981－), 女, 博士, 副研究员, 主要研究领域为分组密码算法的设计与分析.