两类扩散结构特征向量的研究与应用

崔 霆* 金晨辉
(信息工程大学电子技术学院 郑州 450004)

摘 要：SP(Substitution & Permutation)模型是分组密码常用模型之一。该文提出了基于扩散结构特征向量构造SP模型高概率差分传递链和线性逼近链的方法。利用该方法构造了ARIA算法6轮概率为2^{-168}的差分传递链，并构造了仅使用一个S盒的6轮弱化ARIA算法达到概率上界2^{-144}的差分传递链。结果表明，SP模型的设计者应当尽量选择特征向量个数较少且不含低重量特征向量的扩散结构。此外，该文还给出了准对合 MDS(Maximum Distance Separable)矩阵及循环移位矩阵的特征值以及特征向量计数公式。

关键词：SP 模型；ARIA 密码算法；扩散结构；特征向量；计数
中图分类号：TN918.1 **文献标识码**： A **文章编号**：1009-5896(2011)-04-0854-04
DOI: 10.3724/SP.J.1146.2010.00837

Research and Application for Characteristic Vectors of Two Kinds of Diffusion Structures

Cui Ting Jin Chen-hui
(*Electronic Technology Institute*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: SP (Substitution & Permutation) structure is often used in block ciphers. This paper provides a method which could construct high probability differential trails and linear trails by using characteristic vectors of the diffusion layer. By this method some differential trails of ARIA can be constructed, these trails could reach probability 2^{-168} for 6 rounds. And for 6 rounds reduced ARIA, who only employs a single S box, some differential trails can be got which could reach the highest probability 2^{-144}. The results show that the SP cipher designers should choose those diffusion layers with fewer characteristic vectors as possible. And diffusion layers should never have low weight characteristic vectors. Additionally, the characteristic value as well as the count value of quasi-involution MDS matrices and cyclic shift matrices are provided.

Key words: SP (Substitution & Permutation) structure; ARIA cipher; Diffusion layer; Characteristic vector; Count value

1 引言

差分密码分析和线性密码分析是目前分析分组密码最基本，也是最有效的两种分析方法。由于实施这两种攻击需要构造密码算法高概率差分传递链(线性逼近链)，因此人们提出分支数的概念来估计迭代型分组密码差分传递链(线性逼近链)的概率[1–3]。需要指出的是，分支数仅给出了上述两种链的概率上界，却并未给出相应链的构造方法。而后者恰恰是密码设计者和分析者关心的问题：若能构造达到概率上界的差分传递链(线性逼近链)，就可以用最小的代价完成差分分析(线性分析)工作。然而，目前关于高概率差分传递链和线性逼近链的构造方法尚不成熟，尤其当算法迭代次数较多时，构造高概率差分传递链(线性逼近链)较为困难，因此希望构造的高概率差分传递链(线性逼近链)最好满足周期性，从而在算法迭代次数较多时，仅通过串联周期链就能构造出新的链。

本文首先将指出，利用P盒的特征向量可能能构造出SP模型的高概率差分传递链，其后，本文将给出利用P盒特征向量构造SP模型[2]周期为1的高概率差分传递链的方法。作为该方法的应用实例，本文将构造ARIA算法6轮概率为2^{-168}，同时达到活动指标下界的差分传递链以及仅使用一个S盒的弱化ARIA算法达到概率上界2^{-144}的6轮差分传递链。本文的结果说明，在设计时仅考虑扩散结构的分支数是不够的，特征向量也需要引起人们的格外重视，SP模型的设计者最好选择那些特征向量个数较少，同时特征向量的重量较大的P变换。进一步地，我们将分析两类常见扩散结构的特征值，并给出其特征向量计数公式，从而为SP模型中P变换的选择提供参考。

2010-08-09 收到，2010-12-07 改回
河南省杰出青年科学基金(0312001800)资助课题
*通信作者：崔霆 cuiting_1209@yahoo.com.cn

2　预备知识

约定：α_i 为向量 $\boldsymbol{\alpha}$ 的第 i 个分量；$\oplus$ 为逐位异或运算；$\lfloor x \rfloor$ 表示对实数 x 下取整；$\lceil x \rceil$ 表示对实数 x 上取整；$\boldsymbol{M}^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{M}$ 的转置；# 表示集合中元素的个数；$\boldsymbol{E}_k$ 为 k 阶单位矩阵；$\partial f(x)$ 为多项式 $f(x)$ 的次数。

定义 1[4]　设 $\boldsymbol{M}$ 是 $\mathrm{GF}(2^n)$ 上的 $m\times m$ 矩阵，若存在 $\lambda\in\mathrm{GF}(2^n)$，使得 $\mathrm{GF}(2^n)$ 上的 m 维非零向量 $\boldsymbol{\eta}$，有 $\boldsymbol{M}\boldsymbol{\eta}=\lambda\cdot\boldsymbol{\eta}$ 成立，则称 λ 为 f 的一个特征值，称 $\boldsymbol{\eta}$ 为属于特征值 λ 的特征向量。特别地，属于特征值 1 的特征向量称作不动向量。

定义 2[5]　设 $S_0,\cdots,S_{m-1}:\{0,1\}^n\to\{0,1\}^n$ 为非线性双射，$P:\{0,1\}^{mn}\to\{0,1\}^{mn}$ 为线性双射，$k=(k_0,\cdots,k_{m-1})$ 为圈子密钥，则称采用轮函数为 $F(x,k)=P(S_0(x_0\oplus k_0),\cdots,S_{m-1}(x_{m-1}\oplus k_{m-1}))$ 的密码模型为 SP 模型。

定义 3[5]　设函数 $f:Z_2^u\to Z_2^v$，令 $\Delta X\in Z_2^u$，$\Delta Y\in Z_2^v$，则称 $p_f(\Delta X\to\Delta Y)=(1/2^u)\#\{X\in Z_2^u:f(X)\oplus f(X\oplus\Delta X)=\Delta Y\}$ 为 f 的差分对应 $\Delta X\to\Delta Y$ 的概率。

定义 4[3]　设 $f(x)=\boldsymbol{A}x$，且 $\boldsymbol{A}$ 是 $\mathrm{GF}(2^n)$ 上的 $m\times m$ 矩阵，则分别称 $D_f=\min\{W(\boldsymbol{\alpha})+W(\boldsymbol{A}\boldsymbol{\alpha}):\boldsymbol{\alpha}\in[\mathrm{GF}(2^n)]^m\setminus\{0\}\}$ 和 $L_f=\min\{W(\boldsymbol{A}^{\mathrm{T}}\boldsymbol{\alpha})+W(\boldsymbol{\alpha}):\boldsymbol{\alpha}\in[\mathrm{GF}(2^n)]^m\setminus\{0\}\}$ 为 $\boldsymbol{A}$ 的差分分支数和线性分支数。

对 $\mathrm{GF}(2^n)$ 上 $m\times m$ 矩阵 $\boldsymbol{A}$，其差分分支数达到最大值 $m+1$ 等价于其线性分支数达到最大值 $m+1$。此时称 $\boldsymbol{A}$ 为 MDS 矩阵。

3　SP 模型基于特征向量的差分传递链构造

本节仅给出 SP 模型基于特征向量的差分传递链构造方法。对线性逼近链，有类似的结论成立。

定理 1　在 SP 模型中，设 $S_0,\cdots,S_{m-1}:\{0,1\}^n\to\{0,1\}^n$ 为非线性双射，$P:\boldsymbol{x}\mapsto\boldsymbol{M}_{m\times m}\boldsymbol{x}$ 为 $[\mathrm{GF}(2^n)]^m\to[\mathrm{GF}(2^n)]^m$ 矩阵 $\boldsymbol{M}$ 定义的线性双射，若 $0\neq\lambda\in\mathrm{GF}(2^n)$ 为 $\boldsymbol{M}$ 的特征值，且 $\boldsymbol{\alpha}=(\alpha_0,\cdots,\alpha_{m-1})$ 是属于 λ 的特征向量。则若对 $0\le i\le m-1$，均有 $p_{S_i}(\lambda\alpha_i\to\alpha_i)>0$，则 r 轮 S-P 模型存在概率为 $\prod_{a_i\neq0}p_{S_i}^r(\lambda\alpha_i\to\alpha_i)$ 的差分传递链。

证明　对 S 层而言，输入差分为 $\lambda\boldsymbol{\alpha}$，输出差分为 $\boldsymbol{\alpha}$ 的概率为 $\prod_{i=0}^{m-1}p_{S_i}(\lambda\alpha_i\to\alpha_i)$。注意到对 S 盒而言，当其输入差为 0 时，输出差以概率 1 为 0，即 $\prod_{a_i=0}p_{S_i}(\lambda\alpha_i\to\alpha_i)=1$；另由 P 是线性变换知 $p_P(\boldsymbol{\alpha}\to\lambda\boldsymbol{\alpha})=1$，故 $p(\lambda\boldsymbol{\alpha}\xrightarrow{S}\boldsymbol{\alpha}\xrightarrow{P}\lambda\boldsymbol{\alpha})=\prod_{a_i\neq0}p_{S_i}(\lambda\alpha_i\to\alpha_i)$。故对 r 轮 SP 模型有 $p_{r\text{-SPN}}(\lambda\boldsymbol{\alpha}\xrightarrow{S}\cdots\xrightarrow{S}\boldsymbol{\alpha})=\prod_{a_i\neq0}p_{S_i}^r(\lambda\alpha_i\to\alpha_i)$。　证毕

备注 1：由分支数定义，若 $\boldsymbol{\alpha}$ 是 $\boldsymbol{M}$ 的特征向量，则 $\boldsymbol{\alpha}$ 的非零块个数(以下称作重量)至少为 $\lceil D_f\rceil/2$。

定理 1 实际上给出了周期为 1 的差分传递链的构造方法。定理 1 给出的差分传递链的概率大小取决于 3 个要素：(1)当 P 盒具有特征向量 $\boldsymbol{\alpha}=(\alpha_0,\cdots,\alpha_{m-1})$ 时，诸 S 盒的差分对应是否与之匹配成功，即当 $p_P((\alpha_0,\cdots,\alpha_{m-1})\to(\lambda\alpha_0,\cdots,\lambda\alpha_{m-1}))=1$ 时，是否有诸 $p_{S_i}(\lambda\alpha_i\to\alpha_i)>0$；(2)特征向量 $\boldsymbol{\alpha}=(\alpha_0,\cdots,\alpha_{m-1})$ 中不为零的 α_i 个数；(3)与特征向量相匹配的诸 S 盒差分概率 $p_{S_i}(\lambda\alpha_i\to\alpha_i)$ 取值。

因此，在 P 盒的选择上，我们需要尽可能选择特征向量较少的 P 变换，且该变换的低重量特征向量应该尽量少。若对低重量的 $(\alpha_0,\cdots,\alpha_{m-1})$ 有 $p_P((\alpha_0,\cdots,\alpha_{m-1})\to(\lambda\alpha_0,\cdots,\lambda\alpha_{m-1}))=1$，那么就必须限制诸 $p_{S_i}(\lambda\alpha_i\to\alpha_i)$ 均较小。

作为定理 1 的应用，本文考察了 ARIA 算法的 P 变换。该算法具体描述可参考文献[6]。

实验发现，ARIA 算法的 P 变换仅有特征值 1，且存在 $2^{17}-1$ 个不动向量。由备注 1 可知，所有不动向量的最小重量为 4，并且这样的不动向量有 $7\times2^{10}-1$ 个。因此，我们考虑利用重量为 4 的不动向量来构造差分传递链和线性逼近链。

S_1,S_1^{-1} 仅在 $0xc5\to0xc5$ 的差分概率达到最大值 2^{-6}，S_2,S_2^{-1} 仅在 $0x5a\to0x5a$ 的差分概率达到最大值 2^{-6}，然而，P 变换的所有特征向量均不能与上述两个 S 盒的差分匹配成整体的差分传递链。

如果不再限制 $S_1,S_1^{-1},S_2,S_2^{-1}$ 形如 $\Delta X\to\Delta X$ 的非平凡差分的概率达到最大值，则可以找到 P 盒重量为 4 的特征向量与这些 S 盒的差分对应相匹配(此时诸 S 盒差分对应概率均为 2^{-7})。因此，对 6 轮 ARIA 算法可以构造概率为 $2^{-7\times4\times6}=2^{-168}$ 的差分传递链。

如果将 S_2,S_2^{-1} 替换成 S_1,S_1^{-1}(将 S_1,S_1^{-1} 替换成 S_2,S_2^{-1})，则可找出与 S 盒差分 $0xc5\to0xc5$ ($0x5a\to0x5a$)匹配的重量为 4 的特征向量，由此可以构造出概率为 $2^{-6\times4\times6}=2^{-144}$ 的差分传递链。这与文献[6]给出的理论上界是一致的。

定理 1 有效的前提是 P 盒必须存在特征向量。一般而言，P 盒的特征向量越多，则 S 盒与之匹配成功的概率就会越大，那么攻击者构造出相应的差分传递链的选择就会更多。下面将给出两类常用扩散结构的特征向量计数。

4　两类扩散结构的特征值及特征向量计数

定义 5　设 $\boldsymbol{A}$ 是 $\mathrm{GF}(2^n)$ 上的 m 阶矩阵，若存在 $\mu\in\mathrm{GF}(2^n)$，使得 $(\mu\cdot\boldsymbol{A})^2=\boldsymbol{E}_m$，则称 $\boldsymbol{A}$ 为 $\mathrm{GF}(2^n)$ 上

的 m 阶准对合矩阵，称 μ 为 $\boldsymbol{A}$ 的对合因子。

引理 1[2] 有限域 $\mathrm{GF}(2^n)$ 上的矩阵是 MDS 矩阵当且仅当它的任一子矩阵都是满秩矩阵。

准对合矩阵囊括了一大批特殊矩阵。文献[7]指出，Hadamard 矩阵是准对合矩阵；文献[2]构造的一类特殊的 Cauchy 矩阵也被设计者证明是准对合 MDS 矩阵；由于对合矩阵显然是准对合矩阵，而 ARIA[6]，Anubis[8]等算法的线性变换是对合矩阵，因此也均是准对合矩阵。下面的定理给出了准对合 MDS 矩阵的特征值和特征向量的计数。

定理 2 设 $\boldsymbol{A}$ 是 $\mathrm{GF}(2^n)$ 上的 m 阶准对合 MDS 矩阵，μ 为 $\boldsymbol{A}$ 的对合因子，则 $\boldsymbol{A}$ 存在唯一的特征值 μ^{-1}，且 $\boldsymbol{A}$ 有 $2^{n(m-\lfloor m/2\rfloor)}-1$ 个特征向量。

证明 一方面 $(\mu\cdot\boldsymbol{A})^2=\boldsymbol{E}$ 等价于 $\boldsymbol{A}^2=\mu^{-2}\boldsymbol{E}$，故有 $(\mu^{-1}\boldsymbol{E}\oplus\boldsymbol{A})^2=\mu^{-2}\boldsymbol{E}\oplus\boldsymbol{A}^2=0$，因此行列式 $\left|\mu^{-1}\boldsymbol{E}\oplus\boldsymbol{A}\right|=0$，故 μ^{-1} 为 $\boldsymbol{A}$ 的特征值；另一方面，假设 $\boldsymbol{A}$ 另有特征值 λ，令 $\boldsymbol{\xi}_\lambda$ 为属于特征值 λ 的特征向量，则 $\boldsymbol{\xi}_\lambda=\boldsymbol{E}\boldsymbol{\xi}_\lambda=(\mu\boldsymbol{A})^2\boldsymbol{\xi}_\lambda=\mu^2\lambda^2\boldsymbol{\xi}_\lambda$，故有 $\mu^2\lambda^2=1$，也即 $(\mu\lambda\oplus1)^2=0$ 故 $\lambda=\mu^{-1}$。因此 μ^{-1} 是 $\boldsymbol{A}$ 的唯一的特征值。

同时，由于 $\boldsymbol{A}$ 的特征向量恰是方程组 $(\boldsymbol{A}\oplus\mu^{-1}\boldsymbol{E})\boldsymbol{X}=0$ 的非 0 解。只需证 $\mathrm{rank}(\boldsymbol{A}\oplus\mu^{-1}\boldsymbol{E})=\lfloor m/2\rfloor$：由 $(\mu^2\boldsymbol{A}^2)\oplus\boldsymbol{E}=(\mu\boldsymbol{A}\oplus\boldsymbol{E})(\mu\boldsymbol{A}\oplus\boldsymbol{E})=0$ 知，$(\mu\boldsymbol{A}\oplus\boldsymbol{E})$ 的列向量均为线性方程组 $(\mu\boldsymbol{A}\oplus\boldsymbol{E})\boldsymbol{X}=0$ 的解，故 $(\mu\boldsymbol{A}\oplus\boldsymbol{E})$ 之秩不超过 $(\mu\boldsymbol{A}\oplus\boldsymbol{E})\boldsymbol{X}=0$ 解空间的维数。故 $2\times\mathrm{rank}(\boldsymbol{A}\oplus\mu^{-1}\cdot\boldsymbol{E})=2\times\mathrm{rank}(\mu\boldsymbol{A}\oplus\boldsymbol{E})\le m$，即 $\mathrm{rank}(\boldsymbol{A}\oplus\mu^{-1}\cdot\boldsymbol{E})\le\lfloor m/2\rfloor$；另一方面，当 $m=1$ 时，显然有 $\mathrm{rank}(\boldsymbol{A}\oplus\mu^{-1}\cdot\boldsymbol{E})\ge\lfloor m/2\rfloor$，当 $m\ge2$ 时，不妨设 $\boldsymbol{A}=\begin{bmatrix}\boldsymbol{A}_0 & \boldsymbol{A}_1\\ \boldsymbol{A}_2 & \boldsymbol{A}_3\end{bmatrix}$，这里 $\boldsymbol{A}_0$ 为 $\lfloor m/2\rfloor\times\lfloor m/2\rfloor$ 块，$\boldsymbol{A}_1$ 为 $\lfloor m/2\rfloor\times(m-\lfloor m/2\rfloor)$ 块。则 $\boldsymbol{A}\oplus\mu^{-1}\boldsymbol{E}_m=\begin{bmatrix}\boldsymbol{A}_0\oplus\mu^{-1}\boldsymbol{E}_{\lfloor m/2\rfloor} & \boldsymbol{A}_1\\ \boldsymbol{A}_2 & \boldsymbol{A}_3\oplus\mu^{-1}\boldsymbol{E}_{m-\lfloor m/2\rfloor}\end{bmatrix}$，故 $\mathrm{rank}(\boldsymbol{A}\oplus\mu^{-1}\boldsymbol{E}_m)\ge\mathrm{rank}\boldsymbol{A}_1$。又 $\boldsymbol{A}$ 是 MDS 矩阵，故由引理 1 知 $\boldsymbol{A}_1$ 中的任意 $\lfloor m/2\rfloor\times\lfloor m/2\rfloor$ 子块满秩，故 $\mathrm{rank}\boldsymbol{A}_1\ge\lfloor m/2\rfloor$。即 $\mathrm{rank}(\boldsymbol{A}\oplus\mu^{-1}\boldsymbol{E}_m)\ge\mathrm{rank}\boldsymbol{A}_1\ge\lfloor m/2\rfloor$。故 $\mathrm{rank}(\boldsymbol{A}\oplus\mu^{-1}\boldsymbol{E})=\lfloor m/2\rfloor$。

综上，有 $\mathrm{rank}(\boldsymbol{A}\oplus\mu^{-1}\boldsymbol{E})=\lfloor m/2\rfloor$，因而 $(\boldsymbol{A}\oplus\mu^{-1}\boldsymbol{E})\boldsymbol{X}=0$ 解空间的维数恰为 $m-\lfloor m/2\rfloor$，故方程组 $(\boldsymbol{A}\oplus\mu^{-1}\boldsymbol{E})\boldsymbol{X}=0$ 有 $2^{n(m-\lfloor m/2\rfloor)}-1$ 个非 0 解。

证毕

推论 1 设 $\boldsymbol{A}$ 是 $\mathrm{GF}(2^n)$ 上的 m 阶准对合 MDS 矩阵，μ 为 $\boldsymbol{A}$ 的对合因子，则当 m 为偶数时，$\boldsymbol{A}$ 所有的特征向量添加全零向量后恰为 $\boldsymbol{A}\oplus\mu^{-1}\cdot\boldsymbol{E}$ 的列向量张成的向量空间。

除了准对合矩阵之外，循环移位矩阵也是一类常见的扩散结构，AES 算法[9]就采用了这样的矩阵设计列混合变换(实验表明，AES 算法的列混合变换仅有特征值 1，且特征向量空间维数为 1，对应的特征向量重量均为 4)。下面我们对循环移位矩阵的特征值与特征向量进行研究。

定义 6[1] 设 $\boldsymbol{C}=(c_{i,j})_{m\times m}$ 是 $\mathrm{GF}(2^n)$ 上的矩阵，满足 $c_{i,j}=c_{(j-i)\bmod m}$，则称 $\boldsymbol{C}$ 为循环移位矩阵，记作 $\boldsymbol{C}=\mathrm{circ}(c_0,c_1,\cdots,c_{m-1})$。将 $c(x)=\bigoplus_{i=0}^{m-1}c_ix^i$ 称作 $\boldsymbol{C}$ 的变换多项式。

引理 2[10] 有限域 $\mathrm{GF}(2^n)$ 上的多项式环 $\mathrm{GF}(2^n)[x]$ 模理想 $(x^m\oplus1)$ 所得的商环与 $\mathrm{GF}(2^n)$ 上所有的 $m\times m$ 循环移位矩阵构成的矩阵环同构。

定理 3 设 $\mathrm{GF}(2^n)$ 上矩阵 $\boldsymbol{C}=\mathrm{circ}(c_0,c_1,\cdots,c_{m-1})$ 的变换多项式为 $c(x)=\bigoplus_{i=0}^{m-1}c_ix^i$。$\mu\in\mathrm{GF}(2^n)$ 为 $\boldsymbol{C}$ 的特征值当且仅当 $\partial\gcd(c(x)\oplus\mu,x^m\oplus1)\ge1$，且当 $\partial\gcd(c(x)\oplus\mu,x^m\oplus1)\ge1$ 时，属于 μ 的特征值恰有 $2^{\partial[\gcd(c(x)\oplus\mu,x^m\oplus1)]\times n}-1$ 个。

证明 由定义 1，μ 为 $\boldsymbol{C}$ 的特征值当且仅当方程组 $(\boldsymbol{C}\oplus\mu\boldsymbol{E})\boldsymbol{X}=0$ 存在非 0 解。由引理 2，循环移位矩阵 $\boldsymbol{C}\oplus\mu\boldsymbol{E}$ 不满秩，等价于 $\boldsymbol{C}\oplus\mu\boldsymbol{E}$ 的变换多项式 $c'(x)=(c_0\oplus\mu)\oplus\bigoplus_{i=1}^{m-1}c_ix^i=c(x)\oplus\mu$ 与 $x^m\oplus1$ 不互素，即 $\partial\gcd(c(x)\oplus\mu,x^m\oplus1)\ge1$。

以下证明方程组 $(\boldsymbol{C}\oplus\mu\boldsymbol{E})\boldsymbol{X}=0$ 非零解的个数。

设 $\boldsymbol{X}=(x_0,\cdots,x_{m-1})^{\mathrm{T}}\in\mathrm{GF}(2^n)^m$ 为 $(\boldsymbol{C}\oplus\mu\boldsymbol{E})\boldsymbol{X}=0$ 的解，设 $\gcd(c'(x),x^m\oplus1)=p(x)$，因而存在 $s(x),t(x)\in\mathrm{GF}(2^n)[x]$，使得 $c'(x)=p(x)s(x)$ 和 $x^m\oplus1=p(x)t(x)$ 同时成立，且 $\gcd(s(x),t(x))=1$。

对 $0\le i\le m-1$，令 $z_i=x_{(m-1-i)\bmod m}$。可验证 $(\boldsymbol{C}\oplus\mu\boldsymbol{E})\boldsymbol{X}=0$ 等价于 $(\boldsymbol{C}\oplus\mu\boldsymbol{E})\mathrm{circ}(z_0,\cdots,z_{m-1})=0$，令 $z(x)=\bigoplus_{i=0}^{m-1}z_ix_i\in\mathrm{GF}(2^n)[x]/(x^m\oplus1)$，则由引理 2 知，$(\boldsymbol{C}\oplus\mu\boldsymbol{E})\mathrm{circ}(z_0,\cdots,z_{m-1})=0$ 等价于 $c'(x)z(x)=0\bmod(x^m\oplus1)$。因而方程组 $(\boldsymbol{C}\oplus\mu\boldsymbol{E})\boldsymbol{X}=0$ 的解和使得 $c'(x)z(x)=0\bmod(x^m\oplus1)$ 成立的 $z(x)$ 一一对应，即 $p(x)t(x)\mid p(x)s(x)z(x)$。由 $\gcd(s(x),t(x))=1$ 知 $t(x)\mid z(x)$，也即存在 $b(x)=\bigoplus_{i=0}^{m-1}b_ix^i\in\mathrm{GF}(2^n)[x]$，使得 $z(x)=t(x)b(x)$。

设 $\partial p(x)=r$。由 $x^m\oplus1=p(x)t(x)$ 知，$\partial p(x)=r$ 等价于 $\partial t(x)=m-r$，又 $z(x)\in\mathrm{GF}(2^n)[x]/(x^m\oplus1)$，故由 $z(x)=t(x)b(x)$ 知，$b(x)$ 的次数最多为 $(m-1)-(m-r)=r-1$，故 $b(x)$ 有 2^{nr} 种取值。又 $t(x)$ 固定，由式 $z(x)=t(x)b(x)$ 知，$z(x)$ 有 2^{nr} 种取值，也即线性

方程组 $(\boldsymbol{C}\oplus\mu\boldsymbol{E})\boldsymbol{X}=0$ 的解有 2^{nr} 个。因此，$(\boldsymbol{C}\oplus\mu\boldsymbol{E})\boldsymbol{X}=0$ 的非零解有 $2^{nr}-1$ 个。　　证毕

备注 2：设 $\boldsymbol{C}=\mathrm{circ}(c_0,c_1,\cdots,c_{m-1})$ 是 $\mathrm{GF}(2^n)$ 上的循环移位矩阵，并令 $\boldsymbol{X}=(1,\cdots,1)^{\mathrm{T}}$，注意到有 $\boldsymbol{CX}=\left(\bigoplus_{i=0}^{m-1}c_i,\cdots,\bigoplus_{i=0}^{m-1}c_i\right)^{\mathrm{T}}$，故 $\bigoplus_{i=0}^{m-1}c_i$ 必为 $\boldsymbol{C}$ 的特征值。

5　结束语

本文提出了基于 SP 模型特征向量来构造差分传递链的方法，并构造了 ARIA 算法达到活动指标下界的差分传递链以及仅使用一个 S 盒的弱化 ARIA 算法的概率达到理论上界的差分传递链。本文的结果说明，特征向量需要引起密码设计者的重视。设计者最好选择那些特征向量个数较少，同时没有低重量特征向量的 P 变换。最后，本文给出了准对合 MDS 矩阵和循环移位矩阵的特征值，并给出了特征向量计数公式。本文的研究结果为 SP 模型的设计与分析提供了一些参考。对其他密码模型是否有类似的分析结果，则是下一步需要研究的问题。

参 考 文 献

[1] Wang Nian-ping and Jin Chen-hui. Security evaluation against differential and linear cryptanalyses for Feistel ciphers. *Frontiers of Computer Science in China*, 2009, 3(12): 494–502.

[2] Youssef A, Mister S, and Tavares S. On the design of linear transformations for substitution permutation encryption networks. Workshop on Selected Areas in Cryptography-SAC'97, Ottawa, Workshop record, 1997: 40–48.

[3] Kang Ju-sung, Hong Seo-khie, and Lee Sang-jin, *et al.*. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks. *ETRI Journal*, 2001, 23(4): 158–167.

[4] 北京大学数学系几何与代数教研室代数小组. 高等代数(第 2 版). 北京: 高等教育出版社, 1988: 296–298.

[5] 金晨辉, 郑浩然, 张少武等. 密码学. 北京: 高等教育出版社, 2009, 11: 175–176.

[6] Kwon Daesung, Kim Jaesung, and Park Sangwoo, *et al.*. New block cipher: ARIA. ICISC 2003, 2004, LNCS 2971: 432–445.

[7] Xiao L and Heys H M. Hardware design and analysis of block cipher components. Proceedings of the 5th International Conference on Information Security and Cryptology-ICISC'02. 2003, LNCS 2587: 164–181.

[8] Biryukov A and Nikolić I. Automatic search for related-key differential characteristics in byte-oriented block ciphers: application to AES, Camellia, Khazad and Others. EUROCRYPT 2010. 2010, LNCS 6110: 322–344.

[9] Biryukov A and Khovratovich D. Related-key cryptanalysis of the full AES-192 and AES-256. ASIACRYPT 2009. 2009, LNCS 5912: 1–18.

[10] 王念平, 金晨辉, 余昭平. 对合型列混合变换的研究. 电子学报, 2005, 33(10): 1917–1920.

Wang N P, Jin C H, and Yu Z P. Research on involution-typed mixcolumn transform. *Acta Electronica Sinica*, 2005, 33(10): 1917–1920.

崔　霆：　男，1985 年生，博士生，研究方向为密码学.

金晨辉：　男，1965 年生，教授，博士生导师，研究方向为密码学与信息安全.