软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2015,26(10):2656−2666 [doi: 10.13328/j.cnki.jos.004743]

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

P 盒为 *n*-MDS 矩阵的 SPS 模型差分概率的新上界*

刘国强, 金晨辉

(解放军信息工程大学,河南 郑州 450002)

通讯作者: 刘国强, E-mail: liuguoqiang87@hotmail.com

摘 要: 研究了 SPS 模型中的扩散变换为二元域上 *n*-MDS 矩阵对应的仿射变换构造时,差分概率的估计问题.首先给出任意给定一个差分对时,差分概率上界的估算公式,然后给出该类 SPS 模型差分概率的一个新上界.模拟实验结果表明,该上界比目前最好的上界更紧致.

关键词: 分组密码;差分分析;SPS 模型;差分概率;上界

中图法分类号: TP309

中文引用格式: 刘国强,金晨辉.P 盒为 *n*-MDS 矩阵的 SPS 模型差分概率的新上界.软件学报,2015,26(10):2656−2666. http://www.jos.org.cn/1000-9825/4743.htm

英文引用格式: Liu GQ, Jin CH. New upper bound on the maximum differential probability for SPS structure with P-box using *n*-MDS. Ruan Jian Xue Bao/Journal of Software, 2015,26(10):2656−2666 (in Chinese). http://www.jos.org.cn/1000-9825/4743.htm

New Upper Bound on the Maximum Differential Probability for SPS Structure with P-Box Using *n*-MDS

LIU Guo-Qiang, JIN Chen-Hui

(PLA Information Engineering University, Zhengzhou 450002, China)

Abstract: This paper investigates the upper bound on the maximum differential probability for SPS structure with P-box using *n*-MDS (maximum distance separable) matrix over the finite field *GF*(2). First, an estimation formula of differential probability for every fixed differential pair is presented. Then, a new upper bound on the maximum differential probability for SPS structure is described. The experimental analysis shows that the resulting upper bound is tighter than the best known upper bound.

Key words: block cipher; differential cryptanalysis; SPS structure; differential probability; upper bound

分组密码是一类重要且应用广泛的对称密码体制.从分组密码算法的设计模型来说,分组密码算法的设计模型主要分为:以 DES 算法[1]为代表的 Feistel 模型、以 CAST-256 算法[2]和 SMS4 算法[3]为代表的不平衡 Feistel 模型、以 Rijndael 算法[4]为代表的 SP 模型及以 IDEA 算法[5]为代表的 Lai-Massey 模型等.SP 模型是目前广泛使用的分组密码结构之一,很多著名的密码算法都采用这种结构,如 AES 算法[4]、ARIA 算法[6]、Serpent 算法[7]和 SAFER 算法[8]等.

差分分析和线性分析是两种对分组密码算法进行分析的最基本的手段.为了使 SP 模型更好地抵抗差分分析和线性分析,密码设计者希望构造差分分支数及线性分支数以尽可能大地扩散结构,从而增加差分及线性路径中活动 S 盒的个数.MDS 矩阵的差分和线性分支数均达到了最大值[9],故,利用 MDS 矩阵来构造分组密码的扩散结构是一种重要的方法,国内外的密码学者都对 MDS 矩阵的构造与密码特性进行了大量的研究[10−16].

本文研究了 SPS 模型差分概率上界的估计问题.在该问题的研究中,2000 年,Hong 等人在文献[17]中证明:当 P 变换的分支数达到最大值 m+1 时,2 轮 SP 网络差分概率的上界为 $p_{\max}^m$;当 P 变换的分支数达到次大值 m

* 基金项目: 国家自然科学基金(61272488, 61402523)
收稿时间: 2014-04-07; 修改时间: 2014-09-22; 定稿时间: 2014-10-14

时,2 轮 SP 网络差分概率的上界为 $p_{\max}^{m-1}$.2001 年,Kang 等人在文献[9]中证明了 2 轮 SP 网络差分概率的上界为 $p_{\max}^{B_d-1}$, 从而推广了 Hong 等人的结论,并据此给出了 2 轮 AES 算法的差分概率的上界为 2^{-24}.2002 年,Park 等人对类 Rijndael 结构的差分概率的上界进行了研究[18],指出,4 轮类 Rijndael 结构差分概率的上界为 1.06×2^{-96}.2003 年,Park 等人给出了 2 轮 SP 网络差分概率上界的估计公式[19],该上界是 SPS 模型迄今最紧的上界.对 SPS 模型差分概率的上界进行理论估计,可为 SP 网络、嵌套 SP 的 Feistel 结构等密码模型的可证明安全性提供理论支撑.在文献[20]中,Choy 等人利用 Park 给出的关于 SPS 模型差分概率上界的结论,给出了 E2 算法及 MCrypton 算法抵抗飞来去器[21]攻击的安全性.此外,针对 SP 网络的分组算法 ARIA,文献[22]对该算法差分概率进行了研究.Shirai 等人对嵌套 SP 结构的 Feistel 模型的差分概率的上界进行了研究[23],并指出,10 轮 Camellia 差分概率不会大于 2^{-128}.

针对 P 盒为 n-MDS 矩阵对应的仿射变换构造的扩散结构,本文给出了该类 SPS 模型差分概率的一个新上界.当 SPS 模型中的 S 盒均为仿射等价时,该上界等于 Park 等人给出的上界;当 S 盒是独立 S 盒时,我们的模拟实验结果说明,该上界一般比 Park 等人给出的上界更紧,从而说明使用独立的 S 盒可能获得比使用相同 S 盒获得更好的抗差分攻击的能力.

1 SPS 模型的简化

定义 1. 设 $S_i:\{0,1\}^n\to\{0,1\}^n$ 是双射,$S:[Z/(2^n)]^m\to[Z/(2^n)]^m$,使任意的$(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_m)\in[Z/(2^n)]^m$,有 $S(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_m)=(S_1(\boldsymbol{x}_1),\ldots,S_1(\boldsymbol{x}_m))$.再设 $P:\{0,1\}^{mn}\to\{0,1\}^{mn}$ 是二元域上的仿射双射,则称由 S 盒、P 盒、与密钥逐位模 2 加及 S 盒这 4 个变换复合的模型为 SPS 模型.

在分组密码中,S 盒有时设计为非线性变换与仿射变换的复合,如 AES 算法中的 S 盒.对于这类 S 盒构成的 SPS 模型,我们可将 S 盒中的仿射变换与扩散结构 P 看作一个整体,从而构成一个新的扩散结构 P_{new}.引理 1 给出了具体的约简关系.

引理 1. 设 $S_i:\{0,1\}^n\to\{0,1\}^n$ 是双射,$S:[Z/(2^n)]^m\to[Z/(2^n)]^m$ 使任意的$(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_n)\in[Z/(2^n)]^m$,有 $S(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_m)=(S_1(\boldsymbol{x}_1),\ldots,S_1(\boldsymbol{x}_m))$,且 $P:\{0,1\}^{mn}\to\{0,1\}^{mn}$ 是二元域上的仿射双射.再设 $T_i:\{0,1\}^n\to\{0,1\}^n$ 且存在仿射双射 $\varphi_i,\psi_i:\{0,1\}^n\to\{0,1\}^n$ 使 $S_i(\boldsymbol{x})=\psi_i(T_i(\varphi_i(\boldsymbol{x})))$,定义$\varphi=(\varphi_1,\ldots,\varphi_m),\psi=(\psi_1,\ldots,\psi_m),T=(T_1,\ldots,T_m),P_{new}:\{0,1\}^{mn}\to\{0,1\}^{mn}$ 使 $P_{new}(\boldsymbol{x})=\varphi\circ P\circ\psi(\boldsymbol{x})$,则有:

$$S(PS(\boldsymbol{x})\oplus\boldsymbol{k})=\psi T(P_{new}T\varphi(\boldsymbol{x})\oplus\varphi(\boldsymbol{k})\oplus\varphi(0)).$$

引理 1 说明采用扩散结构为 P、混淆层设计为 $T(\boldsymbol{x})=\psi(S(\varphi(\boldsymbol{x})))$的 TPT 模型,其差分概率的取值分布规律与采用扩散结构 $P_{new}(\boldsymbol{x})=\varphi(P(\psi(\boldsymbol{x})))$、混淆层为 $S(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_m)=(S_1(\boldsymbol{x}_1),\ldots,S_1(\boldsymbol{x}_m))$的 $SP_{new}S$ 模型的差分概率的取值分布规律相同,故下面只需研究 $SP_{new}S$ 的差分概率规律即可.例如:对于 S 盒为有限域上的仿射变换与仿射变换复合构成的 SPS 模型,我们只需假设 S 盒是有限域上的逆变换即可.即使 P 是 $GF(2^n)$上的线性变换,但 φ_i 和 ψ_i 可能只是二元域上的仿射变换而不是 $GF(2^n)$上的仿射变换,故 P_{new} 可能是二元域上的仿射变换而不是 $GF(2^n)$上的线性变换.因此,我们通常假设 $SP_{new}S$ 模型中的 P 盒 P_{new} 是二元域上的仿射变换,这说明定义 1 中对扩散结构 P 的定义具有一般性.

定义 2[21]. 设函数 $f:\{0,1\}^u\to\{0,1\}^v,\boldsymbol{\alpha}\in\{0,1\}^u,\boldsymbol{\beta}\in\{0,1\}^v$,则称 $p_f(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\#\{\boldsymbol{x}\in\{0,1\}^u:f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus\boldsymbol{\alpha})=\boldsymbol{\beta}\}/2^u$ 为 f 的差分对应$\boldsymbol{\alpha}\to\boldsymbol{\beta}$的差分概率,其中,#表示集合中元素的个数.

定义 3. 设 $f:\{0,1\}^{mn}\to\{0,1\}^{mn}$ 是仿射变换,$\boldsymbol{\alpha},\boldsymbol{\beta}\in\{0,1\}^{mn}$,则称 $DB_f^{(n)}=\min_{\boldsymbol{\alpha}\neq0}\{wt_n(\boldsymbol{\alpha})+wt_n(f(\boldsymbol{\alpha}))\}$ 为 f 的 n-差分分支数.这里,$wt_n(\boldsymbol{\alpha})$是$\boldsymbol{\alpha}=(\alpha_1,\ldots,\alpha_m)$中非零的 n 比特块的个数.

定义 4. 设 $f:\{0,1\}^{mn}\to\{0,1\}^{mn}$ 是仿射变换且 $f(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}\oplus f(0)$,当 f 的 n-差分分支数达到最大值 $m+1$ 时,则称 f 对应的变换矩阵 A 为 n 分块 MDS 矩阵,简记为 n-MDS 矩阵.

在本文中,在不引起歧义时,我们简称 n-差分分支数为 n-分支数.

2 预备知识

以下均假设所研究的SPS模型是定义1所定义的SPS模型,且其中的S盒都是有限域$GF(2^n)$上的逆变换,P是$\{0,1\}^{mn}$到自身的仿射变换.

引理2. 设$f(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}\oplus f(0)$,$\boldsymbol{A}$是$mn\times mn$二元矩阵,$\boldsymbol{E}$是$mn$级单位方阵.再设$\boldsymbol{A}\|\boldsymbol{E}=\boldsymbol{A}_1\|\ldots\|\boldsymbol{A}_{2m}$且诸$\boldsymbol{A}_i$是$mn\times n$矩阵,则矩阵$\boldsymbol{A}$的$n$-差分分支数$\geq d$的充要条件为$\boldsymbol{A}_1,\ldots,\boldsymbol{A}_{2m}$中任意$d-1$个矩阵的列向量全体构成的向量组均线性无关.

证明:

- 充分性

若$\boldsymbol{A}\|\boldsymbol{E}$的任意$d-1$个$n$-分块列在二元域上线性无关,则$\boldsymbol{A}\|\boldsymbol{E}$中至少$d$个$n$-分块列在二元域上才可能线性相关,从而任何重量小于d的向量$(\boldsymbol{X},\boldsymbol{Y})^T$都不能使$(\boldsymbol{A}\|\boldsymbol{E})(\boldsymbol{X},\boldsymbol{Y})^T=0$成立,即,$\boldsymbol{A}$的$n$-差分分支数$\geq d$.

- 必要性

若矩阵$\boldsymbol{A}$的n-差分分支数$\geq d$,则对任意非零的$\boldsymbol{X},\boldsymbol{Y}\in[Z/(2^n)]^m$,$wt_n(\boldsymbol{X})+wt_n(\boldsymbol{Y})$的最小值为$d$,其中$\boldsymbol{Y}=\boldsymbol{A}\boldsymbol{X}$.若$\boldsymbol{A}\|\boldsymbol{E}$存在$d-1$个$n$-分块列在二元域上线性相关,不妨设第$t_1,t_2,\ldots,t_{d-1}$个$n$-分块列线性相关,将这些$n$-分块列依次记为$\boldsymbol{z}_1,\boldsymbol{z}_2,\ldots,\boldsymbol{z}_{d-1}$,则存在$d-1$个$n$维0-1列向量$\boldsymbol{c}_1,\boldsymbol{c}_2,\ldots,\boldsymbol{c}_{d-1}\in Z/(2^n)$使得$\boldsymbol{c}_1\bullet\boldsymbol{z}_1\oplus\boldsymbol{c}_2\bullet\boldsymbol{z}_2\oplus\ldots\oplus\boldsymbol{c}_{d-1}\bullet\boldsymbol{z}_{d-1}=0$成立,其中,运算"$\bullet$"为$\boldsymbol{c}\bullet\boldsymbol{z}=\boldsymbol{c}^1\bullet\boldsymbol{z}^1\oplus\boldsymbol{c}^2\bullet\boldsymbol{z}^2\oplus\ldots\oplus\boldsymbol{c}^n\bullet\boldsymbol{z}^n$,$\boldsymbol{c}=(c^1,c^2,\ldots,c^n)\in Z/(2^n)$,$\boldsymbol{z}$为一个$n$-分块列,$\boldsymbol{z}^i$表示0-1块$\boldsymbol{z}$的第$i$列.$c^i\boldsymbol{z}^i$表示$c^i$与$\boldsymbol{z}^i$作数乘运算.

现构造$2mn$维列向量$(\boldsymbol{X}',\boldsymbol{Y}')^T=(0,\ldots,0,\boldsymbol{c}_1^T,0,\ldots,0,\boldsymbol{c}_2^T,0,\ldots,0,\boldsymbol{c}_{d-1}^T,0,\ldots,0)^T$,其中,诸$\boldsymbol{c}_i$及零元素均为$n$维0-1列向量,且$\boldsymbol{c}_i^T$为$(\boldsymbol{X}',\boldsymbol{Y}')^T$中的第$t_i$个$n$维向量,$i=1,2,\ldots,d-1$,则有:

$$(\boldsymbol{A}\|\boldsymbol{E})(\boldsymbol{X}',\boldsymbol{Y}')^T=\boldsymbol{c}_1\bullet\boldsymbol{z}_1\oplus\boldsymbol{c}_2\bullet\boldsymbol{z}_2\oplus\ldots\oplus\boldsymbol{c}_{d-1}\bullet\boldsymbol{z}_{d-1}=0.$$

此时,由$\boldsymbol{A}\|\boldsymbol{E}$中存在$d-1$个$n$-分块列在二元域上线性相关的假设,构造了向量重量$wt_n(\boldsymbol{X}')+wt_n(\boldsymbol{Y}')$为$d-1$的$\boldsymbol{X}',\boldsymbol{Y}'\in[Z/(2^n)]^m$,这与$\boldsymbol{A}$的$n$-差分分支数$\geq d$矛盾,故必要性成立. □

定理1. 设mn级二元矩阵$\boldsymbol{P}$是n-MDS矩阵,$t_1,t_2,\ldots,t_{2m}$是$1,2,\ldots,2m$的一个排列,则有:

(1) 存在二元域上的m^2个n级可逆方阵$\boldsymbol{e}_{i,j},i,j=1,2,\ldots,m$,使得任意的$\boldsymbol{X},\boldsymbol{Y}\in[GF/(2^n)]^m$,$\boldsymbol{Y}=\boldsymbol{P}\boldsymbol{X}$等价于对$1\leqslant i\leqslant m$,均有$\boldsymbol{z}_{t_i}=\overset{m}{\underset{j=1}{\oplus}}\boldsymbol{e}_{i,j}\boldsymbol{z}_{t_{m+j}}$.这里,列向量$\boldsymbol{z}_i$是$\boldsymbol{X}\|\boldsymbol{Y}$的第$i$个坐标;

(2) 如果$\boldsymbol{P}$是$GF(2^n)$上的m级方阵,则存在$GF(2^n)$上的非零元$\boldsymbol{e}_{i,j},i,j=1,2,\ldots,m$,使得任意的$\boldsymbol{X},\boldsymbol{Y}\in[GF/(2^n)]^m$,$\boldsymbol{Y}=\boldsymbol{P}\boldsymbol{X}$等价于对$1\leqslant i\leqslant m$,均有$\boldsymbol{z}_{t_i}=\overset{m}{\underset{j=1}{\oplus}}\boldsymbol{e}_{i,j}\boldsymbol{z}_{t_{m+j}}$,这里,列向量$\boldsymbol{z}_i$是$\boldsymbol{X}\|\boldsymbol{Y}$的第$i$个坐标.

证明:设$\boldsymbol{P}\|\boldsymbol{E}=\boldsymbol{\eta}_1\|\ldots\|\boldsymbol{\eta}_{2m}$且诸$\boldsymbol{\eta}_i$都是$mn\times n$二元矩阵,$\boldsymbol{X},\boldsymbol{Y}\in[GF/(2^n)]^m$,则$\boldsymbol{Y}=\boldsymbol{P}\boldsymbol{X}$等价于$(\boldsymbol{P}\|\boldsymbol{E})(\boldsymbol{X},\boldsymbol{Y})^T=0$.由于$\boldsymbol{z}_i$是$\boldsymbol{Z}=\boldsymbol{X}\|\boldsymbol{Y}$的第$i$坐标,故上式等价于$\overset{2m}{\underset{i=1}{\oplus}}\boldsymbol{\eta}_i\boldsymbol{z}_i=0$,即$\overset{m}{\underset{j=1}{\oplus}}\boldsymbol{\eta}_{t_j}\boldsymbol{z}_{t_j}=\overset{2m}{\underset{j=m+1}{\oplus}}\boldsymbol{\eta}_{t_j}\boldsymbol{z}_{t_j}$,亦即:

$$(\boldsymbol{\eta}_{t_1},\ldots,\boldsymbol{\eta}_{t_m})(\boldsymbol{z}_{t_1},\ldots,\boldsymbol{z}_{t_m})^T=(\boldsymbol{\eta}_{t_{m+1}},\ldots,\boldsymbol{\eta}_{t_{2m}})(\boldsymbol{z}_{t_{m+1}},\ldots,\boldsymbol{z}_{t_{2m}})^T.$$

由$\boldsymbol{P}$的n-分支数为$m+1$,故由引理2可知,矩阵$\boldsymbol{A}=(\boldsymbol{\eta}_{t_1},\boldsymbol{\eta}_{t_2},\ldots,\boldsymbol{\eta}_{t_m})$是可逆矩阵,因而上式等价于:

$$(\boldsymbol{z}_{t_1},\ldots,\boldsymbol{z}_{t_m})^T=\boldsymbol{A}^{-1}(\boldsymbol{\eta}_{t_1},\ldots,\boldsymbol{\eta}_{t_m})(\boldsymbol{z}_{t_{m+1}},\ldots,\boldsymbol{z}_{t_{2m}})^T=(\boldsymbol{A}^{-1}\boldsymbol{\eta}_{t_1},\ldots,\boldsymbol{A}^{-1}\boldsymbol{\eta}_{t_m})(\boldsymbol{z}_{t_{m+1}},\ldots,\boldsymbol{z}_{t_{2m}})^T\overset{def}{=}(\boldsymbol{e}_{i,j})_{m\times m}(\boldsymbol{z}_{t_{m+1}},\ldots,\boldsymbol{z}_{t_{2m}})^T,$$

其中,$\boldsymbol{e}_{i,j}$是二元域上的n级方阵.这说明$\boldsymbol{Y}=\boldsymbol{P}\boldsymbol{X}$等价于对$1\leqslant i\leqslant m$,均有$\boldsymbol{z}_{t_i}=\overset{m}{\underset{j=1}{\oplus}}\boldsymbol{e}_{i,j}\boldsymbol{z}_{t_{m+j}}$.下证诸$\boldsymbol{e}_{i,j}$都是二元域上的可逆矩阵.

假设$\boldsymbol{e}_{i_0,j_0}$不是二元域上的可逆矩阵,则存在$c\in\{0,1\}^n\backslash\{0\}$,使得$\boldsymbol{e}_{i_0,j_0}\boldsymbol{c}=0$.构造$\boldsymbol{Z}=(z_1,\ldots,z_{2m})$,使得对于$i\in\{1,2,\ldots,2m\}$,有:

$$\boldsymbol{z}_{t_i}=\begin{cases}\boldsymbol{c}, & \text{若}i=m+t_0\\ 0, & \text{若}i>m\text{且}i\neq m+t_0\\ \boldsymbol{e}_{i,j_0}\boldsymbol{c}, & \text{若}1\leqslant i\leqslant m\end{cases},$$

则 $1\leqslant i\leqslant m$,均有 $\boldsymbol{z}_{t_i}=\bigoplus_{j=1}^{m}\boldsymbol{e}_{i,j}\boldsymbol{z}_{t_{m+j}}$. 令 $\boldsymbol{X},\boldsymbol{Y}\in[GF/(2^n)]^m$,使得 $\boldsymbol{Z}=\boldsymbol{X}\|\boldsymbol{Y}$,则由已证结论可知 $\boldsymbol{Y}=\boldsymbol{PX}$.由于 $\boldsymbol{e}_{i_0,j_0}\boldsymbol{c}=0$, 因而 $\boldsymbol{Z}$ 的非零块的个数$\leqslant m$,这与 $\boldsymbol{P}$ 是 n-MDS 矩阵矛盾.该矛盾说明,诸 $\boldsymbol{e}_{i,j}$ 都是二元域上的可逆矩阵.

显然,当 $\boldsymbol{P}$ 是 $GF(2^n)$上的 m 级方阵时,诸 $\boldsymbol{\eta}_i$ 都是 $GF(2^n)$上的 m 维列向量,只需将 m 级矩阵与向量的乘法换为有限域 $GF(2^n)$上乘法,直接沿用上述证明即可证明后一结论. □

由定理 1 的证明可知,矩阵$(\boldsymbol{e}_{i,j})_{m\times m}$只与矩阵 $\boldsymbol{P}$ 和排列 $t_1,t_2,\ldots,t_{2m}$ 有关,故以下称定理 1 中,以 n 级可逆方阵 $\boldsymbol{e}_{i,j}$ 为元素的矩阵$(\boldsymbol{e}_{i,j})_{m\times m}$为由矩阵 $\boldsymbol{P}$ 和排列 $t_1,t_2,\ldots,t_{2m}$ 决定的矩阵.

下面先给出排序定理的一个推广形式.

引理 3[24]. 设对 $1\leqslant i\leqslant m$,均有 $0\leqslant a_{i,1}\leqslant a_{i,2}\leqslant\ldots\leqslant a_{i,n}$.如果对任意的 $i,b_{i,1},b_{i,2},\ldots,b_{i,n}$ 均是 $a_{i,1},a_{i,2},\ldots,a_{i,n}$ 的一个排列,则有 $\sum_{j=1}^{n}\prod_{i=1}^{m}b_{i,j}\leqslant\sum_{j=1}^{n}\prod_{i=1}^{m}a_{i,j}$. 再设 $j_0=\min\left\{j:\prod_{i=1}^{m}a_{i,j}>0\right\}$, 则上式等号成立的充要条件是:对任意的 $j\geqslant j_0$ 和任意的 i,均有 $b_{i,j}=a_{i,j}$.

3 给定差分对应的差分概率估计

当 P 是 n-MDS 矩阵构造的扩散变换时,下面我们将给出给定一个差分对应$\boldsymbol{\alpha}\to\boldsymbol{\beta}$时,其差分概率上界的估计问题.由于 SPS 模型的差分路径 $\boldsymbol{\alpha}\xrightarrow{S_{(1)}}\boldsymbol{A}\xrightarrow{P}\boldsymbol{PA}\xrightarrow{S_{(2)}}\boldsymbol{\beta}$ 的概率为

$$p_{S_{(1)}}(\boldsymbol{\alpha}\to\boldsymbol{A})p_{S_{(2)}}(\boldsymbol{PA}\to\boldsymbol{\beta})=p_{S_{(1)}}(\boldsymbol{\alpha}\to\boldsymbol{A})p_{S_{(2)}^{-1}}(\boldsymbol{\beta}\to\boldsymbol{PA}),$$

因而,SPS 模型一条差分路径的概率分析可以转化为 S 变换 $S_{(1)}\,\|\,S_{(2)}^{-1}$ 的一个差分对应 $\boldsymbol{\alpha}\,\|\,\boldsymbol{\beta}\xrightarrow{S_{(1)}\|S_{(2)}^{-1}}\boldsymbol{A}\|\boldsymbol{PA}$ 的概率分析,此时,叙述和研究起来更加简捷.

定理 2. 设扩散变换 P 为 n-MDS 矩阵对应的仿射变换构造且 P 的分支数为 $m+1$,$\boldsymbol{\alpha}\|\boldsymbol{\beta}=(\boldsymbol{\alpha}_1,\ldots,\boldsymbol{\alpha}_m,\boldsymbol{\beta}_1,\ldots,\boldsymbol{\beta}_m)\in[Z/(2^n)]^m\backslash\{0\}$.再设 S_i 在输入差为$\boldsymbol{\alpha}_i$ 时所有差分对应的概率从大到小依次为 $p_{i,0},\ldots,p_{i,2^n-1}$,$S_i$ 在输出差为$\boldsymbol{\beta}_i$ 时所有差分对应的概率从大到小依次为 $p_{m+i,0},\ldots,p_{m+i,2^n-1}$,定义变换 $T=(T_1,T_2,\ldots,T_{2m})$,使得:

$$T_i=\begin{cases}S_i, & \text{若}1\leqslant i\leqslant m\\ S_i^{-1}, & \text{若}m+1\leqslant i\leqslant 2m\end{cases},$$

则有:

(1) $p_{\mathrm{SPS}}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\leqslant\min\left\{\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{i,j}\right]:\Omega\text{是}\Lambda\text{的}m+1\text{元子集}\right\}$,其中,$\Lambda$是$\boldsymbol{\alpha}\|\boldsymbol{\beta}$的非零坐标构成的集合;

(2) 对 $1\leqslant i\leqslant 2m$,记 r_i 是 S_i 的能达到输入差为 $\boldsymbol{\gamma}_{t_i}$ 时的最大差分概率的输出差的个数,$wt_n(\boldsymbol{\alpha})+wt_n(\boldsymbol{\beta})\geqslant m+2$,如果 $p_{SPS}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\neq 0$ 且情形(1)中的等号成立,则存在$\boldsymbol{\alpha}\|\boldsymbol{\beta}$的非零坐标 $\boldsymbol{\gamma}_{t_1},\boldsymbol{\gamma}_{t_2},\ldots,\boldsymbol{\gamma}_{t_{m+2}}$,使得:

$$\#\{\boldsymbol{\xi}:p_{T_{t_{m+2}}}(\boldsymbol{\gamma}_{t_{m+2}}\to\boldsymbol{\xi})\neq 0\}\leqslant\min\{1+C_{r_i}^2:1\leqslant i\leqslant m+1\}.$$

证明:

(1) 设 $wt_n(\boldsymbol{\alpha})+wt_n(\boldsymbol{\beta})\leqslant m$,则对任意的 $\boldsymbol{A},\boldsymbol{B}\in[Z/(2^n)]^m$,由 S 是双射可知:当 $p_S(\boldsymbol{\alpha}\to\boldsymbol{A})>0$ 时,有 $wt_n(\boldsymbol{A})=wt_n(\boldsymbol{\alpha})$;当 $p_S(\boldsymbol{B}\to\boldsymbol{\beta})>0$ 时,有 $wt_n(\boldsymbol{B})=wt_n(\boldsymbol{\beta})$.因而:

$$wt_n(\boldsymbol{A})+wt_n(\boldsymbol{B})=wt_n(\boldsymbol{\alpha})+wt_n(\boldsymbol{\beta})\leqslant m.$$

再由$\boldsymbol{\alpha}\|\boldsymbol{\beta}\neq 0$ 可知 $\boldsymbol{A}\|\boldsymbol{B}\neq 0$,因而 $\boldsymbol{A}\neq 0$,从而由 $\boldsymbol{P}$ 的差分分支数为 $m+1$ 可知 $\boldsymbol{B}\neq\boldsymbol{PA}$.

这说明 $\boldsymbol{B}=\boldsymbol{PA}$ 蕴涵 $p_S(\boldsymbol{\alpha}\to\boldsymbol{A})p_S(\boldsymbol{\beta}\to\boldsymbol{B})=0$,故有:

$$p_{\mathrm{SPS}}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\sum_{\boldsymbol{A},\boldsymbol{B}}p_S(\boldsymbol{\alpha}\to\boldsymbol{A})p_P(\boldsymbol{A}\to\boldsymbol{B})p_S(\boldsymbol{B}\to\boldsymbol{\beta})=\sum_{\boldsymbol{A}\in[Z/(2^n)]^m,\boldsymbol{B}=\boldsymbol{PA}}p_S(\boldsymbol{\alpha}\to\boldsymbol{A})p_S(\boldsymbol{B}\to\boldsymbol{\beta})=0.$$

故,此时本定理成立.现设 $wt_n(\boldsymbol{\alpha})+wt_n(\boldsymbol{\beta})\geqslant m+1$,定义 $T=(T_1,T_2,\ldots,T_{2m})$,使得:

$$T_i=\begin{cases}S_i, & \text{若}1\leqslant i\leqslant m\\ S_i^{-1}, & \text{若}m+1\leqslant i\leqslant 2m\end{cases}.$$

对任意的 $\boldsymbol{A}\in[Z/(2^n)]^m$,令$\boldsymbol{\gamma}=\boldsymbol{\alpha}\|\boldsymbol{\beta}$,则有:

$$p_{\mathrm{SPS}}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\sum_{\boldsymbol{A}\in[Z/(2^n)]^m,\boldsymbol{B}=\boldsymbol{PA}}\left(\prod_{i=1}^{m}p_{S_i}(\boldsymbol{\alpha}_i\to\boldsymbol{A}_i)\right)\left(\prod_{i=1}^{m}p_{S_i}(\boldsymbol{B}_i\to\boldsymbol{\beta}_i)\right)=\sum_{\boldsymbol{A}\in[Z/(2^n)]^m}p_T(\boldsymbol{\gamma}\to\boldsymbol{A}\|\boldsymbol{PA}).$$

设 $\boldsymbol{\gamma}_{t_1},\boldsymbol{\gamma}_{t_2},\ldots,\boldsymbol{\gamma}_{t_{m+1}}$ 都非零,即$\Omega=\{i_1,i_2,\ldots,i_{m+1}\}$是$(\boldsymbol{\gamma}_1,\boldsymbol{\gamma}_2,\ldots,\boldsymbol{\gamma}_{2m})$的非零分量的坐标构成的集合$\Lambda$的一个 $m+1$ 元子集.再设 n 级可逆方阵 $\boldsymbol{e}_{i,j}$ 为元素的矩阵,$(\boldsymbol{e}_{i,j})_{m\times m}$ 为由矩阵 $\boldsymbol{P}$ 和排列 $t_1,t_2,\ldots,t_{2m}$ 决定的矩阵,则由定理 1 可知:对任意 $H=(\boldsymbol{C}_{t_{m+2}},\ldots,\boldsymbol{C}_{t_{2m}})\in[Z/(2^n)]^{m-1}$ 及任意$\boldsymbol{\varepsilon}\in Z/(2^n)$,当 $1\leqslant i\leqslant m$ 时,令:

$$C_{t_i}^{(H)}(\boldsymbol{\varepsilon})=\begin{cases}\boldsymbol{C}_{t_i}, & \text{若}i\geqslant m+2\\ \boldsymbol{\varepsilon}, & \text{若}i=m+1\\ \boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}\oplus\overset{m}{\underset{j=2}{\oplus}}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}, & \text{若}i\leqslant m\end{cases},$$

则 $C_{t_1}^{(H)}(\boldsymbol{\varepsilon}),\ldots,C_{t_{2m}}^{(H)}(\boldsymbol{\varepsilon})$ 使 $C_{t_i}^{(H)}(\boldsymbol{\varepsilon})=\overset{m}{\underset{j=1}{\oplus}}\boldsymbol{e}_{i,j}C_{t_{m+j}}^{(H)}(\boldsymbol{\varepsilon})$ 对 $1\leqslant i\leqslant m$ 均成立.故,存在 $\boldsymbol{A}\in Z/(2^n)$,使得:

$$(C_{t_1}^{(H)}(\boldsymbol{\varepsilon}),\ldots,C_{t_{2m}}^{(H)}(\boldsymbol{\varepsilon}))=\boldsymbol{A}\|\boldsymbol{PA}.$$

由定理 1 还可知,上述 $C_{t_1}^{(H)}(\boldsymbol{\varepsilon}),\ldots,C_{t_{2m}}^{(H)}(\boldsymbol{\varepsilon})$ 是满足 $\boldsymbol{C}=\boldsymbol{A}\|\boldsymbol{PA}$ 和 $(C_{t_{m+2}}(\boldsymbol{\varepsilon}),\ldots,C_{t_{2m}}(\boldsymbol{\varepsilon}))=\boldsymbol{H}$ 的唯一 $\boldsymbol{C}$.

这说明,在 $\boldsymbol{H}=(\boldsymbol{C}_{t_{m+2}},\ldots,\boldsymbol{C}_{t_{2m}})\in[Z/(2^n)]^{m-1}$ 给定时,满足 $\boldsymbol{C}=\boldsymbol{A}\|\boldsymbol{PA}$ 和 $(C_{t_{m+2}}(\boldsymbol{\varepsilon}),\ldots,C_{t_{2m}}(\boldsymbol{\varepsilon}))=\boldsymbol{H}$ 的 $\boldsymbol{C}$ 与 $Z/(2^n)$中的$\boldsymbol{\varepsilon}$一一对应,因而:

$$\begin{aligned}p_{\mathrm{SPS}}(\boldsymbol{\alpha}\to\boldsymbol{\beta})&=\sum_{\boldsymbol{A}\in[Z/(2^n)]^m}p_T(\boldsymbol{\gamma}\to\boldsymbol{A}\|\boldsymbol{PA})\\&=\sum_{\boldsymbol{C}_{t_{m+2}},\ldots,\boldsymbol{C}_{t_{2m}}\in Z/(2^n)}\ \sum_{\substack{\boldsymbol{C}_{t_1},\ldots,\boldsymbol{C}_{t_{m+1}}\in Z/(2^n)\\ \boldsymbol{C}=\boldsymbol{A}\|\boldsymbol{PA}}}\left[\prod_{i=1}^{m+1}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{C}_{t_i})\right]\\&=\sum_{\boldsymbol{C}_{t_{m+2}},\ldots,\boldsymbol{C}_{t_{2m}}\in Z/(2^n)}\left[\prod_{i=m+2}^{2m}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{C}_{t_i})\sum_{\varepsilon=0}^{2^n-1}\left[\prod_{i=1}^{m+1}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to C_{t_i}^{(H)}(\boldsymbol{\varepsilon}))\right]\right].\end{aligned}$$

由于当$\boldsymbol{\varepsilon}$遍历 $\{0,1\}^n$ 时,对于 $1\leqslant i\leqslant m$, $C_{t_i}^{(H)}(\boldsymbol{\varepsilon})$ 均遍历 $\{0,1\}^n$,因而对 $0\leqslant i\leqslant m+1$, $p_T(\boldsymbol{\gamma}_{t_i}\to C_{t_i}^{(H)}(0))$, $p_T(\boldsymbol{\gamma}_{t_i}\to C_{t_i}^{(H)}(1)),\ldots,p_T(\gamma_{t_i}\to C_{t_i}^{(H)}(2^n-1))$ 是 $p_{t_i,0},p_{t_i,1},\ldots,p_{t_i,2^n-1}$ 的一个排列 $q_{t_i,0},q_{t_i,1},\ldots,q_{t_i,2^n-1}$,故,由引理 3 可知:

$$\sum_{\varepsilon=0}^{2^n-1}\left(\prod_{i=1}^{m+1}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to C_{t_i}^{(H)}(\boldsymbol{\varepsilon}))\right)=\sum_{j=0}^{2^n-1}\left[\prod_{i=1}^{m+1}q_{t_i,j}\right]\leqslant\sum_{j=0}^{2^n-1}\left[\prod_{i=1}^{m+1}p_{t_i,j}\right]=\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{i,j}\right].$$

于是有:

$$\begin{aligned}p_{\mathrm{SPS}}(\boldsymbol{\alpha}\to\boldsymbol{\beta})&=\sum_{\boldsymbol{C}_{t_{m+2}},\ldots,\boldsymbol{C}_{t_{2m}}\in Z/(2^n)}\left[\prod_{i=m+2}^{2m}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{C}_{t_i})\sum_{\varepsilon=0}^{2^n-1}\prod_{i=1}^{m+1}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to C_{t_i}^{(H)}(\boldsymbol{\varepsilon}))\right]\\&=\sum_{\boldsymbol{C}_{t_{m+2}},\ldots,\boldsymbol{C}_{t_{2m}}\in Z/(2^n)}\left[\left(\prod_{i=m+2}^{2m}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{C}_{t_i})\right)\sum_{\boldsymbol{\varepsilon}=0}^{2^n-1}\left(\prod_{i\in\Omega}q_{i,j}\right)\right]\\&\leqslant\sum_{\boldsymbol{C}_{t_{m+2}},\ldots,\boldsymbol{C}_{t_{2m}}\in Z/(2^n)}\left[\left(\prod_{i=m+2}^{2m}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{C}_{t_i})\right)\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{i,j}\right]\right]\\&=\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{i,j}\right]\sum_{\boldsymbol{C}_{t_{m+2}},\ldots,\boldsymbol{C}_{t_{2m}}\in Z/(2^n)}\left(\prod_{i=m+2}^{2m}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{C}_{t_i})\right)\\&=\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{i,j}\right]\prod_{i=m+2}^{2m}\sum_{\boldsymbol{C}_{t_i}\in Z/(2^n)}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{C}_{t_i}).\end{aligned}$$

再遍历集合Ω,即证:

$$p_{\mathrm{SPS}}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\leqslant\min\left\{\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{i,j}\right]:\Omega\text{是}\Lambda\text{的}m+1\text{元子集}\right\}.$$

这说明本定理之情形(1)成立.

(2) 设Ω是Λ的 m+1 元子集,使得 $p_{SPS}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{i,j}\right]\neq 0$, 则由情形(1)的证明可知,情形(1)中不等式成立的充要条件是:对任意的 $\boldsymbol{H}=(\boldsymbol{C}_{t_{m+2}},...,\boldsymbol{C}_{t_{2m}})\in[Z/(2^n)]^{m-1}$,当 $\prod_{i=m+2}^{2m}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{C}_{t_i})\neq 0$ 时,均有:

$$\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{i,j}\right]=\sum_{\boldsymbol{\varepsilon}=0}^{2^n-1}\left(\prod_{i=1}^{m+1}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to C_{t_i}^{(H)}(\boldsymbol{\varepsilon}))\right)=\sum_{\boldsymbol{\varepsilon}=0}^{2^n-1}\left(\prod_{i=1}^{m+1}p_{T_{t_i}}\left(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}\right)\right)\tag{*}$$

记 $j_0=\min_{1\leqslant i\leqslant m+1}\#\{\boldsymbol{\xi}:p_{T_i}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{\xi})\neq 0\}$,再由引理 3 得知,公式(*)等价于 $p_{T_{t_i}}\left(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}\right),\boldsymbol{\varepsilon}\in Z/(2^n)$ 的前 j_0 个大值按大小排列的顺序与 i 无关,即, $p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{b}),\boldsymbol{b}\in Z/(2^n)$ 的前 j_0 个大值按大小排列的顺序与 i 无关.

由于 $wt_n(\boldsymbol{\alpha})+wt_n(\boldsymbol{\beta})\geqslant m+2$ 且 $\boldsymbol{\gamma}_{t_{m+2}}\neq 0$, 故由 S 是双射可知:当 $p_{T_{t_{m+2}}}(\boldsymbol{\gamma}_{t_{m+2}}\to\boldsymbol{C}_{t_{m+2}})\neq 0$ 时,一定有 $\boldsymbol{C}_{t_{m+2}}\neq 0$. 设 $\boldsymbol{\xi}_1=0$ 且 $\boldsymbol{C}_{t_{m+2}}\oplus\boldsymbol{\xi}_1,\boldsymbol{C}_{t_{m+2}}\oplus\boldsymbol{\xi}_2,...,\boldsymbol{C}_{t_{m+2}}\oplus\boldsymbol{\xi}_k$ 是使得 $p_{T_{t_{m+2}}}(\boldsymbol{\gamma}_{t_{m+2}}\to\boldsymbol{\eta})\neq 0$ 的所有输出差$\boldsymbol{\eta}$,再设 $\boldsymbol{\varepsilon}_1,\boldsymbol{\varepsilon}_2,...,\boldsymbol{\varepsilon}_{r_i}$ 是使

$$p_{T_{t_i}}\left(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}\right)=\max\{p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{b}):\boldsymbol{b}\in Z/(2^n)\}$$

成立的所有$\boldsymbol{\varepsilon}$.对任意的 $\boldsymbol{H}=(\boldsymbol{C}_{t_{m+3}},...,\boldsymbol{C}_{t_{2m}})\in[Z/(2^n)]^{m-2}$ 及任意的$\boldsymbol{\varepsilon}\in Z/(2^n)$,$1\leqslant u\leqslant k$,当 $1\leqslant i\leqslant m$ 时,令:

$$C_{t_i}^{(H)}(\boldsymbol{\varepsilon},u)=\begin{cases}\boldsymbol{C}_{t_i}, & \text{若}i\geqslant m+3\\ \boldsymbol{\varepsilon}, & \text{若}i=m+1\\ \boldsymbol{C}_{t_i}\oplus\boldsymbol{\xi}_u, & \text{若}i=m+2\\ \boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}\oplus\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u, & \text{若}i\leqslant m\end{cases},$$

则 $C_{t_1}^{(H)}(\boldsymbol{\varepsilon},u),...,C_{t_{2m}}^{(H)}(\boldsymbol{\varepsilon},u)$ 使 $C_{t_i}^{(H)}(\boldsymbol{\varepsilon},u)=\mathop{\oplus}_{j=1}^{m}\boldsymbol{e}_{i,j}C_{t_{m+j}}^{(H)}(\boldsymbol{\varepsilon},u)$ 对 $1\leqslant i\leqslant m$ 均成立.由于 $p_{T_{t_{m+2}}}(\boldsymbol{\gamma}_{t_{m+2}}\to\boldsymbol{C}_{t_{m+2}})\neq 0$ 等价于 $p_{T_{t_{m+2}}}(\boldsymbol{\gamma}_{t_{m+2}}\to C_{t_i}^{(H)}(\boldsymbol{\varepsilon},u))\neq 0$, 故, $\prod_{i=m+2}^{2m}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to\boldsymbol{C}_{t_i})\neq 0$ 等价于 $\prod_{i=m+2}^{2m}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to C_{t_i}^{(H)}(\boldsymbol{\varepsilon},u))\neq 0$.

现考察在形如 $\boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}\oplus\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u$ 的输出差中,哪些能使 T_{t_i} 在输入差是 $\boldsymbol{\gamma}_{t_i}$ 时的差分概率达到最大.设 $\boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}\oplus\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u$ 使 T_{t_i} 在输入差是 $\boldsymbol{\gamma}_{t_i}$ 时的差分概率达到最大,则由$\boldsymbol{\varepsilon}_v$ 的定义可知,该假设等价于 $\boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}\oplus\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u\in\left\{\boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}_v\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}:1\leqslant v\leqslant r_{t_i}\right\}$, 因而等价于存在$1\leqslant v\leqslant r_{t_i}$ 使得:

$$\boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}\oplus\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u=\boldsymbol{e}_{i,1}\boldsymbol{\varepsilon}_v\oplus\mathop{\oplus}_{j=2}^{m}\boldsymbol{e}_{i,j}\boldsymbol{C}_{t_{m+j}}.$$

即 $\boldsymbol{\varepsilon}=\boldsymbol{\varepsilon}_v\oplus\boldsymbol{e}_{i,1}^{-1}\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u$,亦即 $\boldsymbol{\varepsilon}\in\{\boldsymbol{\varepsilon}_v\oplus\boldsymbol{e}_{i,1}^{-1}\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u:1\leqslant v\leqslant r_{t_i}\}$.

因而, $\{\boldsymbol{\varepsilon}_v\oplus\boldsymbol{e}_{i,1}^{-1}\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u:1\leqslant v\leqslant r_{t_i},1\leqslant u\leqslant k\}$ 是使 T_{t_i} 在输入差是 $\boldsymbol{\gamma}_{t_i}$ 时的差分概率达到最大的所有输出差.

由于当 $1\leqslant u\leqslant k$ 时 $\prod_{i=m+2}^{2m}p_{T_{t_i}}(\boldsymbol{\gamma}_{t_i}\to C_{t_i}^{(H)}(\boldsymbol{\varepsilon},u))\neq 0$, 故由公式(*)对 $(C_{t_{m+2}}^{(H)}(\boldsymbol{\varepsilon},u),...,C_{t_{2m}}^{(H)}(\boldsymbol{\varepsilon},u))$ 成立可知:

$$\{\boldsymbol{\varepsilon}_v\oplus\boldsymbol{e}_{i,1}^{-1}\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u:1\leqslant v\leqslant r_{t_i},1\leqslant u\leqslant k\}=\{\boldsymbol{\varepsilon}_u:1\leqslant u\leqslant r_{t_i}\}.$$

设 $1\leqslant u\leqslant k$,则 $\forall v:1\leqslant v\leqslant r_{t_i}$, 存在 $w:1\leqslant w\leqslant r_{t_i}$, 使得 $\boldsymbol{\varepsilon}_v\oplus\boldsymbol{e}_{i,1}^{-1}\boldsymbol{e}_{i,2}\boldsymbol{\xi}_u=\boldsymbol{\varepsilon}_w$. 于是, $\boldsymbol{\xi}_u=(\boldsymbol{e}_{i,1}^{-1}\boldsymbol{e}_{i,2})^{-1}(\boldsymbol{\varepsilon}_w\oplus\boldsymbol{\varepsilon}_v)$, 因而:

$$\boldsymbol{\xi}_u\in\{\boldsymbol{e}_{i,2}^{-1}\boldsymbol{e}_{i,1}(\boldsymbol{\varepsilon}_w\oplus\boldsymbol{\varepsilon}_v):1\leqslant w,v\leqslant r_{t_i}\}.$$

故 $k\leqslant 1+C_{r_i}^2$, 即, $T_{t_{m+2}}$ 在输入差为 $\boldsymbol{\gamma}_{t_{m+2}}$ 时非零输出差的个数$\leqslant 1+C_{r_i}^2$, 故 $T_{t_{m+2}}$ 在输入差分 $\boldsymbol{\gamma}_{t_{m+2}}$ 时非零输出

差的个数 $\leqslant \min\{1+C_{r_i}^2 : 1\leqslant i\leqslant m+1\}$, 即,情形(2)成立.

对于 AES 算法的 S 盒, $\#\{\boldsymbol{\xi}: p_{T_{t_{m+2}}}(\boldsymbol{\gamma}_{t_{m+2}}\to\boldsymbol{\xi})\neq 0\}=127$ 且 r_i=1,因而定理 2 之情形(2)的条件:

$$\#\{\boldsymbol{\xi}: p_{T_{t_{m+2}}}(\boldsymbol{\gamma}_{t_{m+2}}\to\boldsymbol{\xi})\neq 0\}\leqslant \min\{1+C_{r_i}^2 : 1\leqslant i\leqslant m+1\}$$

不成立.一般地,为保证 S 盒的差分均匀性,密码算法中的 S 盒一般都使 r_i 很小甚至为 1,因而,条件:

$$\#\{\boldsymbol{\xi}: p_{T_{t_{m+2}}}(\boldsymbol{\gamma}_{t_{m+2}}\to\boldsymbol{\xi})\neq 0\}\leqslant \min\{1+C_{r_i}^2 : 1\leqslant i\leqslant m+1\}$$

通常都不成立,这说明 SPS 模型的重量大于分支数的差分对应的概率一般达不到定理 2 给出的上界. □

若 SPS 模型的扩散结构 P 是分支数为 B_d 的 n-MDS 矩阵,则计算根据定理 2 之情形(1)给出的差分对应 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 的差分概率上界的计算复杂度为 $2^n\times C_{wt_n(\boldsymbol{\alpha})+wt_n(\boldsymbol{\beta})}^{B_d}$. 例如:对于以扩散结构 P 是 $GF(2^8)$上 4×4 的 MDS 矩阵为例,计算差分对应上界的计算复杂度最大为 $2^8\times C_8^5=2^{13.8}$.

4 SPS 模型差分概率的新上界

记 SPS 模型差分概率的上界为 B_{SPS},下面我们将给出 B_{SPS} 的估计公式.

引理 4[19]. 设实数序列 $\{x_i^{(j)}\}_{i=1}^n$, $1\leqslant j\leqslant m$,则有:

$$\sum_{i=1}^{n}|x_i^{(1)}\cdots x_i^{(m)}|\leqslant \max\left\{\sum_{i=1}^{n}|x_i^{(1)}|^m,\ldots,\sum_{i=1}^{n}|x_i^{(m)}|^m\right\},$$

其中,等号成立的充要条件为:对任意的 $j,k\in\{1,2,\ldots,m\}$, $1\leqslant i\leqslant n$,均有 $|x_i^{(j)}|=|x_i^{(k)}|$ 成立.

注:文献[19]中仅给出了本文引理 4 中不等号成立的证明,而等号成立的充要条件并没有进行证明.

定理 3. 设扩散变换 P 为 n-MDS 矩阵对应的仿射变换 $f(\boldsymbol{x})=\boldsymbol{P}\boldsymbol{x}\oplus\boldsymbol{b}$ 构成,且分支数为 m+1, $\boldsymbol{\gamma}=(\boldsymbol{\gamma}_1,\boldsymbol{\gamma}_2,\ldots,\boldsymbol{\gamma}_{2m})\in[Z/(2^n)]^{2m}$.如果 S_i 在输入差为 $\boldsymbol{\gamma}_i$ 时差分对应概率从大到小依次为 $p_{\boldsymbol{\gamma}_i,0}^{(i)},\ldots,p_{\boldsymbol{\gamma}_i,2^n-1}^{(i)}$, S_i 在输出差为 $\boldsymbol{\gamma}_i$ 时差分对应概率从大到小依次为 $p_{\boldsymbol{\gamma}_i,0}^{(m+i)},\ldots,p_{\boldsymbol{\gamma}_i,2^n-1}^{(m+i)}$,则有:

(1) SPS 模型非平凡差分对应的概率上界为

$$B_{\mathrm{SPS}}=\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\ \min_{\Omega\subseteq\Lambda_{\boldsymbol{\gamma}},|\Omega|=B_d}\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{\boldsymbol{\gamma}_i,j}^{(i)}\right].$$

这里,$\Lambda_{\boldsymbol{\gamma}}$是由$\boldsymbol{\gamma}$的非零坐标构成的集合;

(2) $B_{\mathrm{SPS}}\leqslant \max_{1\leqslant i\leqslant 2m}\ \max_{\boldsymbol{u}\in\{0,1\}^n\setminus\{0\}}\sum_{j=1}^{2^n-1}\{p_{\boldsymbol{u},j}^{(i)}\}^{B_d}$;

(3) $B_{\mathrm{SPS}}=\max_{1\leqslant i\leqslant 2m}\ \max_{\boldsymbol{u}\in\{0,1\}^n\setminus\{0\}}\sum_{j=1}^{2^n-1}\{p_{\boldsymbol{u},j}^{(i)}\}^{B_d}$ 成立的必要条件为:存在使 $wt(\boldsymbol{x})\geqslant B_d$ 的 $\boldsymbol{x}\in[Z/(2^n)]^{2m}$,向量 $\boldsymbol{x}$ 的非零坐标序号对应的 S 盒的在给定输入差时差分概率的大小排序都相同;充分条件为:对任意的 $i,k\in\{1,2,\ldots,2m\}$及任意的 $\boldsymbol{u}\in\{0,1\}^n$, $j\in\{0,1,\ldots,2^n-1\}$,均有 $p_{\boldsymbol{u},j}^{(i)}=p_{\boldsymbol{u},j}^{(k)}$,即:任意两个 S 盒,在给定输入差时,差分概率的大小排序都相同.

证明:

(1) 设 $\boldsymbol{\alpha}||\boldsymbol{\beta}=\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\setminus\{0\}$, $\Lambda_{\boldsymbol{\gamma}}$是$\boldsymbol{\gamma}$的非零坐标构成的集合.设 $p_{\mathrm{SPS}}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\neq 0$,则 $wt(\boldsymbol{\gamma})\geqslant B_d$.记$\Omega$为$\Lambda_{\boldsymbol{\gamma}}$的一个 B_d 元子集,则由定理 2 之情形(1)可知:

$$p_{\mathrm{SPS}}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\leqslant \min_{\Omega\subseteq\Lambda_{\boldsymbol{\gamma}},|\Omega|=B_d}\left\{\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{\boldsymbol{\gamma}_i,j}^{(i)}\right]\right\}\leqslant \max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\ \min_{\Omega\subseteq\Lambda_{\boldsymbol{\gamma}},|\Omega|=B_d}\left\{\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{\boldsymbol{\gamma}_i,j}^{(i)}\right]\right\};$$

(2) 由引理 4 可知,对使$|\Omega|=B_d$的$\Omega\subseteq\Lambda_{\boldsymbol{\gamma}}$有:

$$\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{\boldsymbol{\gamma}_i,j}^{(i)}\right]\leqslant \max_{i\in\Omega}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}\leqslant \max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}.$$

即:

$$\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{\boldsymbol{\gamma}_i,j}^{(i)}\right]\leqslant\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}\tag{I}$$

故有:

$$\min_{\Omega\subseteq\Lambda_{\boldsymbol{\gamma}},|\Omega|=B_d}\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{\boldsymbol{\gamma}_i,j}^{(i)}\right]\leqslant\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}\tag{II}$$

进而有:

$$\begin{aligned}B_{\mathrm{SPS}}&=\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\min_{\Omega\subseteq\Lambda_{\boldsymbol{\gamma}},|\Omega|=B_d}\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{\boldsymbol{\gamma}_i,j}^{(i)}\right]\\&\leqslant\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}\\&=\max_{\boldsymbol{u}\in\{0,1\}^n}\max_{1\leqslant i\leqslant 2m}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{u},j}^{(i)}]^{B_d}\end{aligned}\tag{III}$$

事实上,设 $1\leqslant i\leqslant 2m$ 和 $\boldsymbol{r}_i\neq 0$,使得 $\max\limits_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\max\limits_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum\limits_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}=\sum\limits_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}$,则有:

$$\sum_{j=0}^{2^n-1}[p_{r_i,j}^{(i)}]^{B_d}\leqslant\max_{\boldsymbol{u}\in\{0,1\}^n}\max_{1\leqslant i\leqslant 2m}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{u},j}^{(i)}]^{B_d}.$$

即:

$$\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\setminus\{0\}}\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}\leqslant\max_{\boldsymbol{u}\in\{0,1\}^n}\max_{1\leqslant i\leqslant 2m}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{u},j}^{(i)}]^{B_d};$$

反之,设 $\boldsymbol{v}\neq 0$ 和 $1\leqslant i\leqslant 2m$,使得 $\max\limits_{\boldsymbol{u}\in\{0,1\}^n}\max\limits_{1\leqslant i\leqslant 2m}\sum\limits_{j=0}^{2^n-1}[p_{\boldsymbol{u},j}^{(i)}]^{B_d}=\sum\limits_{j=0}^{2^n-1}[p_{\boldsymbol{v},j}^{(i)}]^{B_d}$,令 $\boldsymbol{r}=(\boldsymbol{r}_1,\boldsymbol{r}_2,\ldots,\boldsymbol{r}_{2m})\in\{0,1\}^{2m}$,使 $\boldsymbol{r}_i=\boldsymbol{v}$ 对 $1\leqslant i\leqslant 2m$ 成立,则有:

$$\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}\geqslant\max_{1\leqslant i\leqslant 2m,\boldsymbol{r}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{r_i,j}^{(i)}]^{B_d}=\sum_{j=0}^{2^n-1}[p_{\boldsymbol{v},j}^{(i)}]^{B_d}.$$

因而

$$\sum_{j=0}^{2^n-1}[p_{\boldsymbol{v},j}^{(i)}]^{B_d}\leqslant\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}.$$

即:

$$\max_{\boldsymbol{u}\in\{0,1\}^n}\max_{1\leqslant i\leqslant 2m}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{u},j}^{(i)}]^{B_d}\leqslant\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}.$$

这说明:

$$\max_{\boldsymbol{u}\in\{0,1\}^n}\max_{1\leqslant i\leqslant 2m}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{u},j}^{(i)}]^{B_d}=\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\setminus\{0\}}\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}.$$

(3) 由于情形(2)中的等式成立等价于公式(III)中的等式成立,即,存在使 $wt(\boldsymbol{x})\geqslant B_d$ 的 $\boldsymbol{x}\in[Z/(2^n)]^{2m}$,使得:

$$\min_{\Omega\subseteq\Lambda_{\boldsymbol{x}},|\Omega|=B_d}\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{\boldsymbol{x}_i,j}^{(i)}\right]=\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d};$$

又由公式(II)对使$|\Omega|=B_d$的$\Omega\subseteq\Lambda_{\boldsymbol{x}}$都成立,即:

$$\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{\boldsymbol{x}_i,j}^{(i)}\right]\leqslant\max_{1\leqslant i\leqslant 2m,\boldsymbol{x}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{x}_i,j}^{(i)}]^{B_d}\leqslant\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}$$

对使$|\Omega|=B_d$的$\Omega\subseteq\Lambda_{\boldsymbol{x}}$都成立,因而公式(III)成立等价于对使$|\Omega|=B_d$的$\Omega\subseteq\Lambda_{\boldsymbol{x}}$,都有:

$$\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{x_i,j}^{(i)}\right]=\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d} \tag{IV}$$

- 必要性

设情形(2)成立,则由公式(I)和 $\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{x_i,j}^{(i)}\right]\leqslant\max_{1\leqslant i\leqslant 2m,\boldsymbol{x}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{x_i,j}^{(i)}]^{B_d}\leqslant\max_{\boldsymbol{\gamma}\in[Z/(2^n)]^{2m}\text{且}wt(\boldsymbol{\gamma})\geqslant B_d}\max_{1\leqslant i\leqslant 2m,\boldsymbol{\gamma}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{\boldsymbol{\gamma}_i,j}^{(i)}]^{B_d}$,从而由公式(IV)可知 $\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{x_i,j}^{(i)}\right]=\max_{1\leqslant i\leqslant 2m,\boldsymbol{x}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{x_i,j}^{(i)}]^{B_d}$;

再由引理 4 可知:对$\forall i,k\in\Omega$及$j\in\{0,1,\ldots,2^n-1\}$,均有 $p_{\boldsymbol{x}_i,j}^{(i)}=p_{\boldsymbol{x}_k,j}^{(k)}$,即,向量 $\boldsymbol{x}$ 的非零坐标序号对应的 S 盒的在给定输入差 $\boldsymbol{x}_k$ 时差分概率的大小排序都相同.

- 充分性

设存在重量$\geqslant B_d$的向量$\boldsymbol{x}$,使$\boldsymbol{x}$的非零坐标序号对应的 S 盒的差分概率的大小排序都相同,则由引理 4 可知,对使$|\Omega|=B_d$的$\Omega\subseteq\Lambda_{\boldsymbol{x}}$及$\forall t$,均有:

$$\sum_{j=0}^{2^n-1}\left[\prod_{i\in\Omega}p_{x_i,j}^{(i)}\right]=\max_{i\in\Omega}\sum_{j=0}^{2^n-1}[p_{x_i,j}^{(i)}]^{B_d}=\sum_{j=0}^{2^n-1}[p_{x_t,j}^{(t)}]^{B_d}=\max_{1\leqslant i\leqslant 2m,\boldsymbol{x}_i\neq 0}\sum_{j=0}^{2^n-1}[p_{x_i,j}^{(i)}]^{B_d}.$$

即,公式(I)中的等号对使$|\Omega|=B_d$的$\Omega\subseteq\Lambda_{\boldsymbol{x}}$均成立,因而公式(II)对 $\boldsymbol{x}$ 成立. □

目前,SPS 模型差分概率最好的上界是 2003 年由 Park 等人在文献[19]中给出的上界:

$$\max\left\{\max_{1\leqslant i\leqslant m}\max_{\boldsymbol{u}\in\{0,1\}^n}\sum_{j=1}^{2^n-1}\{p_{\boldsymbol{u},j}^{(i)}\}^{B_d},\max_{1\leqslant i\leqslant m}\max_{\boldsymbol{u}\in\{0,1\}^n}\sum_{j=1}^{2^n-1}\{p_{j,\boldsymbol{u}}^{(i)}\}^{B_d}\right\},$$

其中,B_d为线性变换的分支数,$p_{\boldsymbol{u},j}^{(i)}$为第 i 个 S 盒输入差为 $\boldsymbol{u}$、输出差为 j 时的差分概率.由定理 3 之情形(3)可知:若 SPS 模型中各个 S 盒的差分概率从大到小的排列完全相同时,本文给出的上界与文献[19]给出的上界在数值上是相同的.

当SPS模型中各个S盒的差分概率从大到小的排列不完全相同时,我们通过计算机模拟实验考察了本文给出的上界与文献[19]的上界进行比较的情况.当 m=4 时,对于 8 进 8 出的随机 S 盒,我们随机生成了 700 个满足最大差分概率为 8/256 且最大 Walsh 谱的绝对值为 60/256 的 S 盒,并在 m=4 时任取其中 8 个分别作为 SPS 模型中的 8 个 S 盒,共进行 2^{16} 组实验.实验结果如图 1 所示.实验结果表明:当 m=4 时,对于 8 进 8 出的随机 S 盒,本文给出的 SPS 模型差分概率的上界大致为文献[19]给出的上界的一半.这也说明,在设计 SP 网络的 S 层时,若使得 S 层中各个 S 盒的差分分布不同,可能会使 SP 网络获得更好的差分性质.

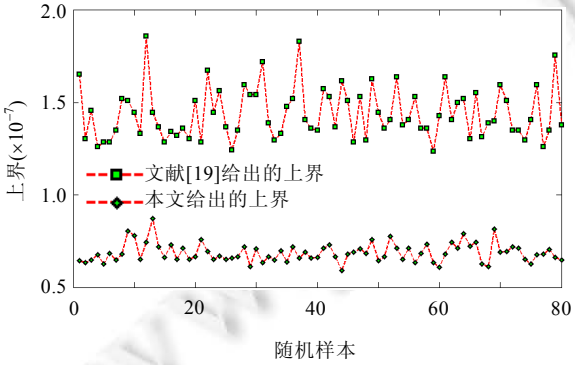

Fig.1 The upper bound of SPS structure with randomly chosen S-boxes in this paper and in Ref.[19]

图 1 本文与文献[19]针对随机 S 盒构成的 SPS 模型差分概率上界的对比图

5 结束语

本文对 P 盒为 *n*-MDS 矩阵的 SPS 模型差分概率上界的估计问题进行了研究.首先从给定的差分对应入手,给出了其差分概率上界的估计公式,并给出了当差分对应的重量大于分支数时,其差分概率达到该上界的一个必要条件;然后给出了 SPS 模型输入与输出差分遍历所有的可能差分对时,该类 SPS 模型差分概率的一个新上界;最后,利用计算机模拟实验对 Park 等人给出的上界与本文给出的上界进行了对比.实验结果表明:当 S 盒是独立不同的 S 盒时,该上界比 Park 等人给出的上界更紧,从而说明使用独立的 S 盒可能获得比使用相同 S 盒获得更好的抗差分攻击的能力.本文的研究丰富了 SPS 模型差分概率的分析结果,为基于该模型设计的分组密码算法的可证明安全性提供了理论支撑.

References:

[1] National Bureau of Standards. Data Encryption Standard, FIPS publication. No. 46, U. S. Department of Commerce, 1977.

[2] Adams C, Gilchrist J. The CAST-256 encryption algorithm. RFC 2612, 1999.

[3] Specification of SMS4, Block cipher for WLAN products-SMS4. 2006. http://www.oscca.gov.cn/UpFile/200621016423197990.pdf

[4] Daemen J, Rijmen V, Wrote; Gu DW, Xu SB, Trans. The Design of Rijindeal AES: The Advanced Encryption Standard. Beijing: Tsinghua University Press, 2002. 34−41 (in Chinese).

[5] Lai XJ, Massey JL. A proposal for a new block encryption standard. In: Proc. of the Cryptology Eurocrypt'90. LNCS 473, Berlin: Springer-Verlag, 1991. 389−404. [doi: 10.1007/3-540-46877-3_35]

[6] Kwon D, Kim J, Park S. New block cipher: ARIA. In: Proc. of the Information Security and Cryptology ICISC 2003. LNCS 2971, Berlin: Springer-Verlag, 2004. 432−445. [doi: 10.1007/978-3-540-24691-6_32]

[7] Anderson R, Biham E, Knudsen L. Serpent: A proposal for the advanced encryption standard. NIST AES Proposal, 2000,1(46): 83−87. http://aes.nist.gov

[8] Massey JL, Khachatrian GH, Kuregian MK. Nomination of SAFER+ as candidate algorithm for the advanced encryption standard (AES). In: Proc. of the 1st Advanced Encryption Standard Canditate Conf. 1998. 1−14. http://www.nist.gov

[9] Kang JS, Hong S, Lee S, Lim J. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks. ETRI Journal, 2001,23(4):158−167. [doi: 10.4218/etrij.01.0101.0402]

[10] Cui T, Jin CH. Construction of involution Cauchy-Hadamard type MDS matrices. Journal of Electronics & Information Technology, 2010,32(2):500−503 (in Chinese with English abstract).

[11] Guo L, Zheng HR, Fu ZQ, Wang Y. New construction methods for MDS matrices and involution MDS matrices. Application Research of Computers, 2013 (in Chinese with English abstract). http://www.cnki.net/kcms/detail/51.1196.TP.20130809.1753.022.html [doi: 10.3969/j.issn.1001-3695.2014.01.052]

[12] Sajadieh M, Dakhilalian M, Mala H, Omoomi B. On construction of involutory MDS matrices from vandermonde matrices in $GF(2^q)$. Designs, Codes and Cryptography, 2012,64(3):287−308. [doi: 10.1007/s10623-011-9578-x]

[13] Gupta K C, Ray IG. On constructions of involutory MDS matrices. In: Proc. of the AFRICACRYPT 2013. LNCS 7918, Springer-Verlag, 2013. 43−60. [doi: 10.1007/978-3-642-38553-7_3]

[14] Berger TP. Construction of recursive MDS diffusion layers from Gabidulin codes. In: Proc. of the INDOCRYPT 2013. LNCS 8250, Springer-Verlag, 2013. 274−285. [doi: 10.1007/978-3-319-03515-4_18]

[15] Gupta KC, Ray IG. On constructions of MDS matrices from companion matrices for lightweight cryptography. In: Proc. of the Security Engineering and Intelligence Informatics. LNCS 8128, Springer-Verlag, 2013. 29−43. [doi: 10.1007/978-3-642-40588-4_3]

[16] Cao JK, Li YQ, Cao SJ. Linear branch structure and bit level linear representation of MDS matrix. Journal of Information Engineering University, 2013,14(3):289−291,311 (in Chinese with English abstract). [doi: 10.3969/j.issn.1671-0673.2013.03.006]

[17] Hong S, Lee S, Lim J, Sung J, Cheon D, Cho I. Provable security against differential and linear cryptanalysis for the SPN structure. In: Proc. of the 7th Int'l Workshop, Fast Software Encryption 2000. LNCS 1978, New York, Berlin: Springer-Verlag, 2001. 273−283. [doi: 10.1007/3-540-44706-7_19]

[18] Park S, Sung SH, Chee S, Yoon E, Lim J. On the security of Rijndael-like structures against differential and linear cryptanalysis. In: Zheng Y, ed. Proc. of the ASIACRYPT 2002. LNCS 2501, 2002. 176−191. [doi: 10.1007/3-540-36178-2_11]

[19] Park S, Sung SH, Lee S, Lim J. Improving the upper bound on the maximum differential and the maximum linear hull probability for SPN structures and AES. In: Proc. of the 10th Int'l Workshop, Fast Software Encryption 2003. LNCS 2887, Berlin: Springer-Verlag, 2003. 247−260. [doi: 10.1007/978-3-540-39887-5_19]

[20] Choy J, Khoo K. New applications of differential bounds of the SDS structure. In: Proc. of the Information Security. LNCS 5222, 2008. 367−384. [doi: 10.1007/978-3-540-85886-7_26]

[21] Wu WL, Feng DG, Zhang WT. Design and Analysis of Block Cipher. Beijing: Tsinghua University Press, 2009. 229−234 (in Chinese).

[22] Guo JS, Zhang L, Luo W. Differential property of block cipher ARIA. Journal of Information Engineering University, 2013,14(2): 141−152 (in Chinese with English abstract). [doi: 10.3969/j.issn.1671-0673.2013.02.003]

[23] Shirai T, Kanamaru S, Abe G. Improved upper bounds of differential and linear characteristic probability for camellia. In: Daemen J, Rijmen V, eds. Proc. of the FSE 2002. LNCS 2365, 2002. 128−142. [doi: 10.1007/3-540-45661-9_10]

[24] Li ZQ. Dissemination of the ordered permutation rule. Journal of Guangxi Teachers Education University (Natural Science Edition), 1998,15(2):106−109 (in Chinese with English abstract).

附中文参考文献:

[4] Daemen J,Rijmen V,著;谷大武,徐胜波,译.高级加密标准(AES)算法——Rijndael 的设计.北京:清华大学出版社,2003.34−41.

[10] 崔霆,金晨辉.对合 Cauchy-Hadamard 型 MDS 矩阵的构造.电子与信息学报,2010,32(2):500−503.

[11] 郭磊,郑浩然,傅增强,王月.MDS 矩阵和对合 MDS 矩阵的新构造方法.计算机应用研究,2013. http://www.cnki.net/kcms/detail/51.1196.TP.20130809.1753.022.html [doi: 10.3969/j.issn.1001-3695.2014.01.052]

[16] 曹进克,李云强,曹守见.MDS 矩阵变换的线性分支结构和比特级线性表示.信息工程大学学报,2013,14(3):289−291,311. [doi: 10.3969/j.issn.1671-0673.2013.03.006]

[21] 吴文玲,冯登国,张文涛.分组密码的设计与分析.北京:清华大学出版社,2000.

[22] 郭建胜,张磊,罗伟.ARIA 的差分性质研究.信息工程大学学报,2013,14(2):141−152. [doi: 10.3969/j.issn.1671-0673.2013.02.003]

[24] 李致权.排序定理的推广.广西师范学院学报(自然科学版),1998,15(2):106−109.

刘国强(1986－),男,湖南浏阳人,博士生,主要研究领域为密码学.

金晨辉(1965－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.