一般 SPT 模型的抗差分和线性攻击安全性研究

刘凤梅，陈连俊，李春祥，李艳梅，张国双
（信息保障技术重点实验室，北京 100072）

摘　要：为安全高效地在序列密码设计中应用 SP 网络，研究了一般 SPT 模型的抗差分攻击和线性攻击的能力，其中，S 和 T 表示 2 个不同的可实现压缩的混淆层，P 代表扩散层。给出了 P 为最佳扩散层时 SPT 模型的最大差分概率上界，给出了 P 为最佳扩散层且 S 和 T 均平衡时的最大线性逼近优势和最大线性包优势的上界，从而部分解决了该模型的抗差分和线性攻击安全性评估问题。

关键词：分支数；差分概率；线性优势；线性逼近优势；线性包优势
中图分类号：TN918　　**文献标识码：**A　　**文章编号：**1000-436X(2012)01-0120-08

Security against differential and linear cryptanalysis for general SPT models

LIU Feng-mei, CHEN Lian-jun, LI Chun-xiang, LI Yan-mei, ZHANG Guo-shuang
(Science and Technology on Information Assurance Laboratory, Beijing 100072, China)

Abstract: To use SP network in stream ciphers safely and efficiently, the ability against differential and linear cryptanalysis of SPT models was studied, where S and T denote different layers for substitution, in which compression could be achieved, and P denotes the layer for permutation. The upper bound of the maximum differentiality was given when the branch number of P was optimal, and the upper bound of the maximum linear approximation probability and the maximum linear hull probability are given when the branch number of P was optimal and when S and T were balanced. As a consequence, the problem about evaluating the security against differential and linear cryptanalysis for general SPT models was resolved partially.

Key words: branch number; differential probability; linear probability; linear approximation probability; linear hull probability

1　引言

差分攻击和线性攻击是对分组密码最有效的 2 种攻击方法，研究和评估密码算法抵抗差分攻击和线性攻击的能力，是密码设计者和分析者必须考虑的问题[1~3]。SPS 模型（如图 1 和图 2 所示）是分组密码的一个基本模型[3~5]，它主要是由混淆层－扩散层－混淆层组成，通常会在第 2 层混淆之前异或加入轮密钥。对于分组密码来讲，为了保证其能够解密，一般要求每个 S_i（$1 \le i \le n$）都是置换且上下 2 个混淆层是完全一样的。

近年来，在序列密码的设计中，人们也广泛应用将混淆和扩散分层实现的设计理念[6~8]。与分组密码不同的是，对于序列密码，在采用 SP 网络时，由于其解密机制不同于分组密码，且可以使用压缩环节来实现输入多输出少的功能，因此在“混淆层－扩散层－混淆层”这一设计模型中，上下 2 个混淆层可以不一样，也不需要其中 S 盒都是置换。具体来说，序列密码中利用分组密码的迭代思想时既可以先迭代最后再压缩[6]，也可以边迭代边压缩[7]。因

收稿日期：2011-01-19；修回日期：2011-04-26

此，在序列密码的设计中，为同时且高效地实现迭代和压缩(多输入少输出)，可以使用更加一般的 SPT 模型（如图 3 和图 4 所示），这里 S 和 T 表示 2 个不同的混淆层，而且每个 S 或 T 都不必是置换。这就需要对 SPT 模型抗已知攻击的能力进行评估，弄清一般 SPT 模型抵抗差分攻击和抵抗线性攻击的能力。

对于 SPS 模型的抗差分攻击和抗线性攻击的安全性问题，一直是受到密码学者关注，也已有了完善的结果 [9~13]。但对于更一般的可实现压缩功能的 SPT 模型的抗差分攻击能力和抗线性攻击能力却未见研究。本文正是在这一背景需求下进行研究的，通过分析，本文克服了 S 变换和 T 变换的非双射性给证明过程带来的困难，给出了一般 SPT 模型

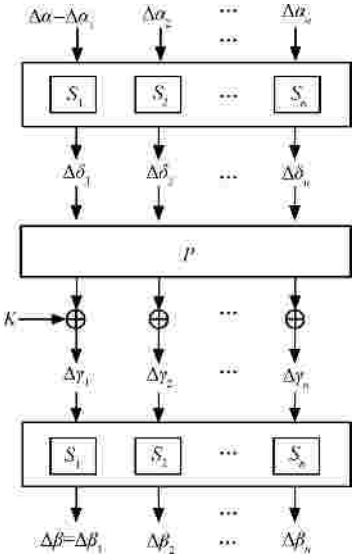

图 1　SPS 模型(差分路径)

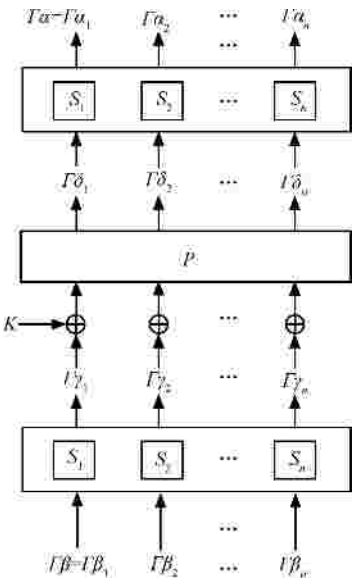

图 2　SPS 模型(线性路径)

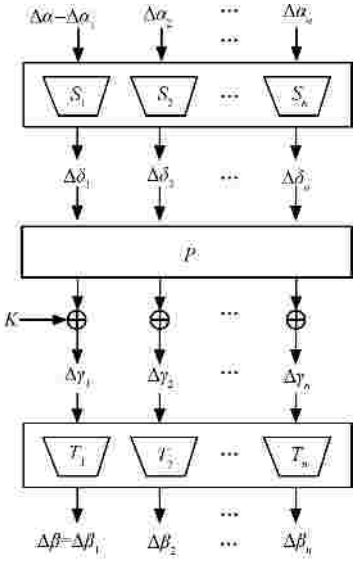

图 3　SPT 模型(差分路径)

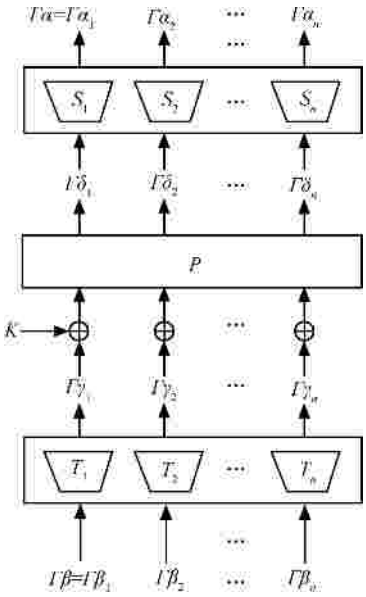

图 4　SPT 模型(线性路径)

在 P 为最佳扩散层时抗差分攻击和线性攻击（S 变换和 T 变换平衡时）能力估计的结果，这对于该模型在序列密码设计中的应用有重要的意义。

本文第 2 节给出了相关定义和已有的结论；在第 3 节中，研究了如图 3 所示的一般 SPT 模型在 P 为最佳扩散层时抗差分攻击的安全性问题，给出了该模型的最大差分概率上界。

在第 4 节中，研究了如图 4 所示的一般 SPT 模型在 P 为最佳扩散层且 S 变换及 T 变换平衡时抗线性攻击的安全性问题，给出了类似于 SPS 模型的最大线性逼近优势的上界和最大线性包优势的上界。

2 相关定义和已有结论

图 3 和图 4 中各记号约定如下。

设 m, m_1, m', n **为 4 个正整数，且** $m \geq m' \geq m_1$。$S_i : \mathrm{GF}(2)^m \to \mathrm{GF}(2)^{m'}$，$T_i : \mathrm{GF}(2)^{m'} \to \mathrm{GF}(2)^{m_1}$，$i = 1, \cdots, n$。

记 $\Delta a = (\Delta a_1, \Delta a_2, \cdots, \Delta a_n)$，$\Delta b = (\Delta b_1, \Delta b_2, \cdots, \Delta b_n)$，$\Delta d = (\Delta d_1, \Delta d_2, \cdots, \Delta d_n)$，$\Delta g = (\Delta g_1, \Delta g_2, \cdots, \Delta g_n)$，**其中，** $\Delta a_i \in \mathrm{GF}(2)^m$，$\Delta b_i \in \mathrm{GF}(2)^{m_1}$，$\Delta d_i, \Delta g_i \in \mathrm{GF}(2)^{m'}$，$i = 1, \cdots, n$。

记 $Ga = (Ga_1, Ga_2, \cdots, Ga_n)$，$Gb = (Gb_1, Gb_2, \cdots, Gb_n)$，$Gd = (Gd_1, Gd_2, \cdots, Gd_n)$，$Gg = (Gg_1, Gg_2, \cdots, Gg_n)$，**其中，** $Ga_i \in \mathrm{GF}(2)^m$，$Gb_i \in \mathrm{GF}(2)^{m_1}$，$Gd_i \in \mathrm{GF}(2)^{m'}$，$Gg_i \in \mathrm{GF}(2)^{m'}$，$i = 1, \cdots, n$。

以 $wt(\Delta a)$ **表示** Δa **的包重量，即** $wt(\Delta a) = \#\{i \mid \Delta a_i \neq 0\}$; $wt(Ga)$ **表示** Ga **的包重量；以** $\boldsymbol{M}^{\mathrm{T}}$ **表示矩阵** $\boldsymbol{M}$ **的转置。**

$P : (\mathrm{GF}(2)^{m'})^n \to (\mathrm{GF}(2)^{m'})^n$ **为线性变换，且其扩散性达到最佳，即其分支数**[12] $\min_{Gg \neq 0}\{wt(Gd) + wt(Gg)\} = \min_{\Delta d \neq 0}\{wt(\Delta d) + wt(\Delta g)\} = n + 1$，**此时称** P **为最佳扩散层。**

设密钥 K **的各分位是相互独立且服从均匀分布的。**

定义 1 设映射 $S : \mathrm{GF}(2)^m \to \mathrm{GF}(2)^{m'}$，$\Delta x \in \mathrm{GF}(2)^m$，$\Delta y \in \mathrm{GF}(2)^{m'}$，$S$ 的差分概率[9]定义如下：

$$DP^S(\Delta x \to \Delta y) = \frac{\#\{x \in \mathrm{GF}(2)^m \mid S(x) \oplus S(x \oplus \Delta x) = \Delta y\}}{2^m}$$

记 $DP^S = \max_{\Delta x \neq 0, \Delta y} DP^S(\Delta x \to \Delta y)$ **为映射** S **的最大差分概率。**

很容易有引理 1~引理 4。

引理 1 设 Δa_i 和 Δd_i 分别为映射 S_i 的输入差和输出差，则有 $\Delta a_i = 0 \Rightarrow \Delta d_i = 0$；又若 S_i 是双射，则 $\Delta a_i \neq 0 \Leftrightarrow \Delta d_i \neq 0$。

引理 2 设 Δd 和 Δg 分别为 P 的输入差和输出差，且 P 的分支数为 $n+1$，则有 $wt(\Delta d) + wt(\Delta g) \geq n + 1$。

引理 3 设 P 对应于矩阵 $\boldsymbol{M} = (m_{ij})_{n \times n}$，$m_{ij} \in \mathrm{GF}(2^{m'})$，即 $P(d) = d \cdot M$，则 $\Delta g = \Delta d \cdot M$。

引理 4 对于任意 $1 \leq i \leq n$，$DP^{S_i}(\Delta a_i \to \Delta d_i)$

$$= \begin{cases} DP^{S_i}(\Delta a_i \to \Delta d_i) \leq 1, & \text{若} \Delta a_i \neq 0, \Delta d_i \neq 0 \\ DP^{S_i}(\Delta a_i \to 0) \leq 1, & \text{若} \Delta a_i \neq 0, \Delta d_i = 0 \\ 0, & \text{若} \Delta a_i = 0, \Delta d_i \neq 0 \\ 1, & \text{若} \Delta a_i = 0, \Delta d_i = 0 \end{cases}$$

引理 5[10] 设 $n \times n$ 矩阵 $\boldsymbol{M}$ 对应于变换 P，则 P 的分支数为 $n+1$，当且仅当对于任意 $1 \leq k \leq n$，$\boldsymbol{M}$ 的 $k \times k$ 子矩阵的秩为 k（此时，$\boldsymbol{M}^{\mathrm{T}}$ 的 $k \times k$ 子矩阵的秩也为 k）。

引理 6[10] 设图 1 中 $S_i\ (i = 1, \cdots, n)$ 均为置换且 P 为最佳扩散层，记 $r = \max_{1 \leq i, j \leq n} DP^{S_i}$，则图 1 所示模型 SPS 的最大差分概率上界为 r^n。

定义 2 设映射 $S : \mathrm{GF}(2)^m \to \mathrm{GF}(2)^{m'}$，$Gx \in \mathrm{GF}(2)^m$，$Gy \in \mathrm{GF}(2)^{m'}$，$S$ 的线性优势[9]定义为

$$LP^S(Gy \to Gx) = \left(\frac{\#\{x \in \mathrm{GF}(2)^m \mid Gx \cdot x = Gy \cdot S(x)\}}{2^{m-1}} - 1 \right)^2$$

其中， $Gx \cdot x$ **表示** Gx **和** x **的点积。** S **的最大线性优势定义为**

$$LP^S = \max_{Gx, Gy \neq 0} LP^S(Gy \to Gx)$$

根据 Walsh **谱**[14]**的定义，有**

$$LP^S(Gy \to Gx) = Walsh_S(Gy, Gx)^2 @ \left(\frac{1}{2^m} \sum_{x \in \mathrm{GF}(2)^m} (-1)^{Gy \cdot S(x) \oplus Gx \cdot x} \right)^2$$

通常考察图 4 所示模型 SPT **的 2 种线性优势。**

定义 3 （SPT **的线性逼近优势**）[9]**设** $Ga \in \mathrm{GF}(2)^m$，$Gd, Gg \in \mathrm{GF}(2)^{m'}$，$Gb \in \mathrm{GF}(2)^{m_1}$，$SPT$ **的线性逼近优势定义为**

$$LAP^{SPT}(Gb \to Ga) = \max_{Gg} \prod_{i=1}^{n} LP^{T_i}(Gb_i \to Gg_i) LP^{S_i}(Gd_i \to Ga_i)$$

SPT **的最大线性逼近优势定义为**

$$LAP^{SPT}_{\max} = \max_{Gb \neq 0, Ga} LAP^{SPT}(Gb \to Ga)$$

定义 4 （SPT **的线性包优势**）[9]**设** $Ga \in \mathrm{GF}(2)^m$，$Gd, Gg \in \mathrm{GF}(2)^{m'}$，$Gb \in \mathrm{GF}(2)^{m_1}$，$SPT$ **的线性包优势定义为**

$$LP^{SPT}(Gb \to Ga)$$

$$= \sum_{Gg_1,\cdots,Gg_n}\left[\prod_{i=1}^{n} LP^{T_i}(Gb_i \to Gg_i)\prod_{i=1}^{n} LP^{S_i}(Gd_i \to Ga_i)\right]$$

SPT 的最大线性包优势定义为

$$LP_{\max}^{SPT} = \max_{Gb\neq 0,Ga} LP^{SPT}(Gb \to Ga)$$

引理 7[9]　设图 2 中的 S_i，$i=1,\cdots,n$ 均为置换，且 P 为最佳扩散层，记 $r = \max\limits_{1\le i,j\le n} LP^{S_i}$，则图 2 所示模型 *SPS* 的最大线性逼近优势 $LAP_{\max}^{SPS} \le r^{n+1}$，最大线性包优势 $LP_{\max}^{SPS} \le r^{n}$。

引理 8[14]　设映射 $S:\mathrm{GF}(2)^m \to \mathrm{GF}(2)^{m'}$，则 S 平衡当且仅当对任意 $Gy\in\mathrm{GF}(2)^{m'}$ 且 $Gy\neq 0$，都有 $Walsh_S(Gy,0)=0$。

由 Walsh 谱的定义及引理 8 有以下推论。

推论 1　设映射 $S:\mathrm{GF}(2)^m \to \mathrm{GF}(2)^{m'}$ 为平衡的，$Gx\in\mathrm{GF}(2)^m$，$Gy\in\mathrm{GF}(2)^{m'}$，则 S 的线性优势有如下性质：

$$LP^{S}(Gy \to Gx) = \begin{cases} LP^{S}(Gy \to Gx) \le 1, & \text{若 } Gy\neq 0,\ Gx\neq 0 \\ 0, & \text{若 } Gy\neq 0,\ Gx=0 \\ 0, & \text{若 } Gy=0,\ Gx\neq 0 \\ 1, & \text{若 } Gy=0,\ Gx=0 \end{cases}$$

引理 9[14]　Parseval 等式：

$$\sum_{Gx\in\mathrm{GF}(2)^m} LP^{S}(Gy\to Gx) = \sum_{Gx\in\mathrm{GF}(2)^m} Walsh_S(Gy,Gx)^2 = 1$$

引理 10[10]　设 P 对应于矩阵 $\boldsymbol{M}=(m_{ij})_{n\times n}$，$m_{ij}\in GF(2^{m'})$，即 $P(d)=d\cdot\boldsymbol{M}$。如果 $LP^{P}(Gg\to Gd)=1$，则 $Gd=Gg\cdot\boldsymbol{M}^{\mathrm{T}}$。

3　SPT 模型的抗差分攻击性

引理 11　设 $n\times n$ 矩阵 $\boldsymbol{M}$ 对应于变换 P（即 $P(d)=d\cdot\boldsymbol{M}$），且 P 是最佳扩散层，$\Delta g=\Delta d\cdot\boldsymbol{M}$。再设 $wt(\Delta d)=j$，$\{i_1,\cdots,i_j\}$ 为 Δd 的非零分位的序号构成的集合，$s\ge 1$，$wt(\Delta g)=n-s+1$ 且 $\Delta g_1=\cdots=\Delta g_{s-1}=0$。则 $\Delta d_{i_1},\cdots,\Delta d_{i_j}$ 可由 $\Delta d_{i_s},\cdots,\Delta d_{i_j}$ 唯一决定。

证明　若 $s=1$，结论显然成立。设 $s>1$。取 $\boldsymbol{M}$ 的子矩阵 $\boldsymbol{M}'=\begin{pmatrix} m_{1i_1} & m_{2i_1} & \cdots & m_{s-1i_1} \\ \vdots & \vdots & \vdots & \vdots \\ m_{1i_{s-1}} & m_{2i_{s-1}} & \cdots & m_{s-1i_{s-1}} \\ m_{1i_s} & m_{2i_s} & \cdots & m_{s-1i_s} \\ \vdots & \vdots & \vdots & \vdots \\ m_{1i_j} & m_{2i_j} & \cdots & m_{s-1i_j} \end{pmatrix}$，记 $\Delta d'=(\Delta d_{i_1},\cdots,\Delta d_{i_j})$，则由题设知 $\Delta d\cdot\boldsymbol{M}$ 的第 $1\sim s-1$ 列 $=\Delta d'\cdot\boldsymbol{M}'$，再由 $\Delta g=\Delta d\cdot\boldsymbol{M}$ 知 $\Delta d'\cdot\boldsymbol{M}'=(\Delta g_1,\cdots,\Delta g_{s-1})=0$。

记

$$\boldsymbol{M}_1=\begin{pmatrix} m_{1i_1} & m_{2i_1} & \cdots & m_{s-1i_1} \\ & \cdots & & \\ m_{1i_{s-1}} & m_{2i_{s-1}} & \cdots & m_{s-1i_{s-1}} \end{pmatrix},\quad \boldsymbol{M}_2=\begin{pmatrix} m_{1i_s} & m_{2i_s} & \cdots & m_{s-1i_s} \\ & \cdots & & \\ m_{1i_j} & m_{2i_j} & \cdots & m_{s-1i_j} \end{pmatrix}$$

则由 P 的分支数是 $n+1$ 和引理 5 知，$\boldsymbol{M}_1$ 可逆，且 $(\Delta d_{i_1},\cdots,\Delta d_{i_{s-1}})=(\Delta d_{i_s},\cdots,\Delta d_{i_j})\boldsymbol{M}_2\boldsymbol{M}_1^{-1}$，即 $\Delta d_{i_1},\cdots,\Delta d_{i_{s-1}}$ 由 $\Delta d_{i_s},\cdots,\Delta d_{i_j}$ 决定，故 $\Delta d_{i_1},\cdots,\Delta d_{i_j}$ 由 $\Delta d_{i_s},\cdots,\Delta d_{i_j}$ 决定。#

下面将借助引理 11，克服由 S_i 和 T_i 的非双射性引发的非零输入差可能产生零输出差的特性给研究过程造成的困难，获得下述结论。

定理 1　设图 3 中 P 为最佳扩散层，记 $r_d=\max\limits_{1\le i,j\le n}(DP^{S_i},DP^{T_j})$。则图 3 所示模型 *SPT* 的输出差非零时的最大差分概率上界为 $r_d^{\,n}$。

证明　本证明所用符号如图 3 所示。设 $wt(\Delta a)=k$，$\Delta b\neq 0$，且 $wt(\Delta b)=n-s+1$，不失一般性，不妨设 $\Delta a_1\neq 0,\cdots,\Delta a_k\neq 0$，$\Delta b_{i_1}\neq 0,\cdots,\Delta b_{i_{n-s+1}}\neq 0$。

假设密钥 K 的各分位是相互独立且服从均匀分布的，则可认为 SPT 模型中各层输入的各路彼此是独立的，且 Δa 与 Δg 独立，因而

$$DP(\Delta a \to \Delta b)$$

$$= \sum_{\Delta d_1,\cdots,\Delta d_n}\left(\prod_{i=1}^{n} DP^{S_i}(\Delta a_i \to \Delta d_i)\prod_{i=1}^{n} DP^{T_i}(\Delta g_i \to \Delta b_i \mid \Delta a)\right)$$

$$= \sum_{\Delta d_1,\cdots,\Delta d_n}\left(\prod_{i=1}^{n} DP^{S_i}(\Delta a_i \to \Delta d_i)\prod_{i=1}^{n} DP^{T_i}(\Delta g_i \to \Delta b_i)\right)$$

$$= \sum_{\Delta d_1} DP^{S_1}(\Delta a_1 \to \Delta d_1)\cdots\sum_{\Delta d_k} DP^{S_k}(\Delta a_k \to \Delta d_k)\cdot \sum_{\Delta d_{k+1}} DP^{S_{k+1}}(0 \to \Delta d_{k+1})\cdots$$

$$\sum_{\Delta d_n}\left(DP^{S_n}(0\to\Delta d_n)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)\right)$$

由引理 4，有

$$\sum_{\Delta d_n}\left(DP^{S_n}(0\to\Delta d_n)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)\right)$$

$$=\sum_{\Delta d_n\neq 0}\left(DP^{S_n}(0\to\Delta d_n)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)\right)+$$

$$DP^{S_n}(0\to 0)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)$$

$$=DP^{S_n}(0\to 0)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)$$

$$=\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)$$

依此类推：

$$DP(\Delta a\to\Delta b)=\sum_{\Delta d_1,\cdots,\Delta d_k}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)\right)\tag{1}$$

将所有可能的（即所有正概率差分路径上的）Δd 所在集合记为 M_d，则式(1)中的求和实际上是对 $\Delta d\in M_d$ 求和。

对 M_d 中元素进行分类。记 $M_{k_1,s_1}=\{\Delta d\mid \Delta d\in M_d,\ wt(\Delta d)=k_1$，且对于 $\Delta g=\Delta d\cdot \boldsymbol{M},\ wt(\Delta g)=n-s_1+1\}$，记所有可能的 (k_1,s_1) 所在的集合为 G。则 $M_d=\bigcup_{(k_1,s_1)\in\Gamma}M_{k_1,s_1}$ 为诸 M_{k_1,s_1} 的不交并。注意 $\Delta d\neq 0$（否则 $\Delta b=0$）且任意 Δd 的非零位一定包含于 $\{1,\cdots,k\}$，故 $1\le k_1\le k$。又由 P 的分支数为 $n+1$ 和引理 2 可知 $k_1\ge s_1\ge 1$。故式(1)求和可化为

$$DP(\Delta a\to\Delta b)=\sum_{(k_1,s_1)\in G}\sum_{\Delta d\in M_{k_1,s_1}}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)\right)\tag{2}$$

下面估计

$$\sum_{\Delta d\in M_{k_1,s_1}}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)\right)\tag{3}$$

对于 $\Delta d\in M_{k_1,s_1}$，设 $\Delta g=\Delta d\cdot \boldsymbol{M}$，且其非零位为 $\{j_1,\cdots,j_{n-s_1+1}\}\subseteq\{1,\cdots,n\}$。则由引理 1 知，当 $\Delta g_i=0$ 时 $\Delta b_i=0$，故 $n-s_1+1\ge n-s+1$，即 $s\ge s_1$，且 $\{j_1,\cdots,j_{n-s_1+1}\}\supseteq\{i_1,\cdots,i_{n-s+1}\}$。结合引理 4，有

$$\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)\le\prod_{i=1}^{n-s_1+1}DP^{T_{j_i}}(\Delta g_{j_i}\to\Delta b_{j_i})\le r_d^{\,n-s_1+1}$$

故式(3)可化为

$$\sum_{\Delta d\in M_{k_1,s_1}}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)\right)\le r_d^{\,n-s_1+1}\sum_{\Delta d\in M_{k_1,s_1}}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\right)\tag{4}$$

对于 $\Delta d\in M_{k_1,s_1}$，假设其非零位为 $t_1,\cdots,t_{k_1}$，则 $\{t_1,\cdots,t_{k_1}\}\subseteq\{1,2,\cdots,k\}$。为方便起见，将指标集 $\{1,2,\cdots,k\}$ 重新编号，即记 $\{1,2,\cdots,k\}=\{t_1,\cdots,t_{k_1},t_{k_1+1},\cdots,t_k\}$，则

$$\sum_{\Delta d\in M_{k_1,s_1}}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\right)=\sum_{\substack{\Delta d\in M_{k_1,s_1}\\ \Delta d_{t_1},\cdots,\Delta d_{t_{k_1}}}}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\right)$$

又由引理 11，$\Delta d_{t_1},\cdots,\Delta d_{t_{k_1}}$ 由 $\Delta d_i, i\in\{t_{s_1},t_{s_1+1},\cdots,t_{k_1}\}$ 决定，故上式为

$$\sum_{\substack{\Delta d\in M_{k_1,s_1}\\ \Delta d_{t_1},\cdots,\Delta d_{t_{k_1}}}}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\right)\le r_d^{\,s_1-1}\sum_{\substack{\Delta d\in M_{k_1,s_1}\\ \Delta d_{t_{s_1}},\cdots,\Delta d_{t_{k_1}}}}\left(\prod_{i=s_1}^{k_1}DP^{S_{t_i}}(\Delta a_{t_i}\to\Delta d_{t_i})\right)$$

则式(4)可化为

$$\sum_{\Delta d\in M_{k_1,s_1}}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to\Delta b_i)\right)\le r_d^{\,n}\sum_{\substack{\Delta d\in M_{k_1,s_1}\\ \Delta d_{t_{s_1}},\cdots,\Delta d_{t_{k_1}}}}\left(\prod_{i=s_1}^{k_1}DP^{S_{t_i}}(\Delta a_{t_i}\to\Delta d_{t_i})\right)$$

此即为式(3)的估计，进而由式(2)可知：

$$DP(\Delta a\to\Delta b)\le r_d^{\,n}\sum_{(k_1,s_1)\in G}\sum_{\substack{\Delta d\in M_{k_1,s_1}\\ \Delta d_{t_{s_1}},\cdots,\Delta d_{t_{k_1}}}}\left(\prod_{i=s_1}^{k_1}DP^{S_{t_i}}(\Delta a_{t_i}\to\Delta d_{t_i})\right)$$

$$\le r_d^{\,n}\sum_{\Delta d\in M_d\Delta d_i\neq 0}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\right)$$

$$\le r_d^{\,n}\sum_{\Delta d_1,\cdots,\Delta d_k\neq 0}\left(\prod_{i=1}^{k}DP^{S_i}(\Delta a_i\to\Delta d_i)\right)$$

再注意 $\sum_{\Delta d_{i_j}}DP^{S_{i_j}}(\Delta a_{i_j}\to\Delta d_{i_j})\le 1$，因此上式进一步放大为；

$$DP(\Delta a\to\Delta b)\le r_d^{\,n}$$

因此图 3 所示模型 SPT 的输出差非零时的最大差分概率上界为 $r_d^{\,n}$。

定理 2　设图 3 所示模型 SPT 中 P 为最佳扩散层，其输入差为 Δa 且 $wt(\Delta a)=k$，记 $r_d=\max_{1\le i,j\le n}(DP^{S_i},DP^{T_j})$。则 $DP(\Delta a\to 0)\le r_d^{\,k}+r_d^{\,n}$。

证明　同定理 1 证明，将所有可能的 Δd 所在集合记为 M_d，则 M_d 中可能含有 0（S 为压缩变换时），同样的推理可以得到

$$DP(\Delta a\to\Delta b)=$$

$$\sum_{\Delta d\in M_d}\left(\prod_{i=1}^{n}DP^{S_i}(\Delta a_i\to\Delta d_i)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to 0)\right)$$

$$=\sum_{\Delta d\in M_d-\{0\}}\left(\prod_{i=1}^{n}DP^{S_i}(\Delta a_i\to\Delta d_i)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to 0)\right)+\prod_{i=1}^{n}DP^{S_i}(\Delta a_i\to 0)$$

类似于定理 1 可证

$$\sum_{\Delta d\in M_d-\{0\}}\left(\prod_{i=1}^{n}DP^{S_i}(\Delta a_i\to\Delta d_i)\prod_{i=1}^{n}DP^{T_i}(\Delta g_i\to 0)\right)\le r_d^{\,n}$$

而易知 $\prod_{i=1}^{n}DP^{S_i}(\Delta a_i\to 0)\le r_d^{\,k}$，故 $DP(\Delta a\to 0)\le r_d^{\,k}+r_d^{\,n}$。#

4　SPT 模型的抗线性攻击性

定理 3　设图 4 中 P 为最佳扩散层且 S_i,T_i，$i=1,\cdots,n$ 均为平衡映射，记 $r_l=\max_{1\le i,j\le n}(LP^{S_i},LP^{T_j})$。则图 4 所示模型 SPT 的最大线性逼近优势 $LAP_{\max}^{SPT}\le r_l^{\,n+1}$。

证明　设 $wt(Gb)=k\ge 1$，$Gb_1\neq 0,\cdots,Gb_k\neq 0$，$Gb_{k+1}=0,\cdots,Gb_n=0$，$wt(Ga)=n-s+1$，$s\ge 1$，$Ga\neq 0$，且设 $Ga_{i_s}\neq 0,\cdots,Ga_{i_n}\neq 0$，$Ga_{i_1}=0,\cdots,Ga_{i_{s-1}}=0$。此时，SPT 的线性逼近优势为

$$LAP^{SPT}(Gb\to Ga)=$$

$$\max_{\Gamma g}\prod_{i=1}^{n}LP^{T_i}(Gb_i\to Gg_i)LP^{S_i}(Gd_i\to Ga_i)$$

首先考察使得 $\prod_{i=1}^{n}LP^{T_i}(Gb_i\to Gg_i)LP^{S_i}(Gd_i\to Ga_i)\neq 0$ 的 Gg。

若 $\prod_{i=1}^{n}LP^{T_i}(Gb_i\to Gg_i)LP^{S_i}(Gd_i\to Ga_i)\neq 0$，则对任意 $i=1,\cdots,n$，都有：

$LP^{T_i}(Gb_i\to Gg_i)\neq 0$ 且 $LP^{S_i}(Gd_i\to Ga_i)\neq 0$。

已知 $Gb_1\neq 0,\cdots,Gb_k\neq 0$，$Gb_{k+1}=0,\cdots,Gb_n=0$，及 $Ga_{i_s}\neq 0,\cdots,Ga_{i_n}\neq 0$，$Ga_{i_1}=0,\cdots,Ga_{i_{s-1}}=0$，考虑到 T_i、S_i 平衡，由推论 1 有，$Gg_1\neq 0,\cdots,Gg_k\neq 0$ 且 $Gg_{k+1}=0,\cdots,Gg_n=0$；$Gd_{i_s}\neq 0,\cdots,Gd_{i_n}\neq 0$，$Gd_{i_1}=0,\cdots,Gd_{i_{s-1}}=0$。

因此，非零的 $\prod_{i=1}^{n}LP^{T_i}(Gb_i\to Gg_i)LP^{S_i}(Gd_i\to Ga_i)$ 即为 $k+n-s+1$ 个 $LP(LP^{T_i}(Gb_i\to Gg_i)$ 或 $LP^{S_i}(Gd_i\to Ga_i)$ 都计为一个 LP)的乘积。再考虑到每个 LP 的上界为 r_l，故

$$\prod_{i=1}^{n}LP^{T_i}(Gb_i\to Gg_i)LP^{S_i}(Gd_i\to Ga_i)\le r_l^{\,k+n-s+1}$$

又由变换 P 的分支数为 $n+1$，故 $k+n-s+1\ge n+1$，而 $0<r_l\le 1$，故 $r_l^{\,k+n-s+1}\le r_l^{\,n+1}$，即

$$LAP^{SPT}(Gb\to Ga)=\max_{Gg}\prod_{i=1}^{n}LP^{T_i}(Gb_i\to Gg_i)LP^{S_i}(Gd_i\to Ga_i)\le r_l^{\,n+1},$$

注意在题设条件下，整个 SPT 模型是平衡的，由推论 1 知 $LAP^{SPT}(Gb\to 0)=0$，因此 $LAP_{\max}^{SPT}=\max_{Gb\neq 0,Ga}LAP^{SPT}(Gb\to Ga)\le r_l^{\,n+1}$。

引理 12　设矩阵 $\boldsymbol{M}$ 对应于变换 P，$Gd=Gg\cdot\boldsymbol{M}^{\mathrm{T}}$，$wt(Gd)=n-s+1$，$wt(Gg)=k$（则 $k\ge s\ge 1$），再设 $Gg_{i_1}\neq 0,\cdots,Gg_{i_k}\neq 0$，$Gd_1=\cdots=Gd_{s-1}=0$，则存在指标集 $\{i_1,\cdots,i_{s-1}\}$ 使得 $Gg_{i_1}\neq 0,\cdots,Gg_{i_{s-1}}\neq 0$，且 $Gg_{i_1},\cdots,Gg_{i_k}$ 由 $Gg_{i_s},\cdots,Gg_{i_k}$ 决定。

证明　结合引理 5 和引理 10，对矩阵 $\boldsymbol{M}^{\mathrm{T}}$ 利用类似于引理 11 的证明方法即可得证。#

定理 4　设图 4 中 $S_i,T_i,i=1,\cdots,n$ 均为平衡函数且 P 为最佳扩散层，记 $r_l=\max_{1\le i,j\le n}(LP^{S_i},LP^{T_j})$。则图 4 所示模型 SPT 的最大线性包优势 $LP_{\max}^{SPT}\le r_l^{\,n}$。

证明 设 $wt(Gb)=k\geq 1$，$Gb_1\neq 0,\cdots,Gb_k\neq 0$，$Gb_{k+1}=0,\cdots,Gb_n=0$，$wt(Ga)=n-s+1$，$s\geq 1$，$Ga_{i_s}\neq 0,\cdots,Ga_{i_n}\neq 0$，$Ga_{i_1}=0,\cdots,Ga_{i_{s-1}}=0$。同定理 3 在题设条件下，只需考察 $Ga\neq 0$ 时的情形。

由线性包优势的定义：

$$LP^{SPT}(Gb\to Ga)=\sum_{Gg_1,\cdots,Gg_n}\left[\prod_{i=1}^{n}LP^{T_i}(Gb_i\to Gg_i)\prod_{i=1}^{n}LP^{S_i}(Gd_i\to Ga_i)\right] \tag{5}$$

观察式(5)可见，首先应排除使得 $\prod_{i=1}^{n}LP^{T_i}(Gb_i\to Gg_i)=0$，或者 $\prod_{i=1}^{n}LP^{S_i}(Gd_i\to Ga_i)=0$ 的 Gg_i 求和部分。

已知 $Gb_1\neq 0,\cdots,Gb_k\neq 0$，$Gb_{k+1}=0,\cdots,Gb_n=0$，考虑到 T_i 平衡，由推论 1，若 $\prod_{i=1}^{n}LP^{T_i}(Gb_i\to Gg_i)\neq 0$，则 $Gg_1\neq 0,\cdots,Gg_k\neq 0$ 且 $Gg_{k+1}=0,\cdots,Gg_n=0$。再注意 $LP^{T_i}(0\to 0)=1$，故式(5)可化为

$$LP^{SPT}(Gb\to Ga)=\sum_{Gg_1\neq 0,\cdots,Gg_k\neq 0}\prod_{i=1}^{k}LP^{T_i}(Gb_i\to Gg_i)\prod_{i=1}^{n}LP^{S_i}(Gd_i\to Ga_i) \tag{6}$$

又已知 $Ga_{i_s}\neq 0,\cdots,Ga_{i_n}\neq 0$，$Ga_{i_1}=0,\cdots,Ga_{i_{s-1}}=0$，考虑到 S_i 平衡，同样若 $\prod_{i=1}^{n}LP^{S_i}(Gd_i\to Ga_i)\neq 0$，则 $Gd_{i_s}\neq 0,\cdots,Gd_{i_n}\neq 0,Gd_{i_1}=0,\cdots,Gd_{i_{s-1}}=0$。

因此对于给定的 Gg，且 Gg 的非零位为 $\{1,\cdots,k\}$，假设 $Gd=Gg\cdot M^{\mathrm{T}}$ 的非零位集合为 $\{j_1,\cdots,j_{n-s_1+1}\}$。那么当 $\{j_1,\cdots,j_{n-s_1+1}\}\neq\{i_s,i_{s+1},\cdots,i_n\}$ 时，$\prod_{i=1}^{n}LP^{S_i}(Gd_i\to Ga_i)=0$。

由以上分析，若记：

$$G=\left\{Gg\,\middle|\,Gg_i\begin{cases}\neq 0,\ i\in\{1,\cdots,k\}\\ =0,\ \text{否则}\end{cases}\right.$$ 且对于 $Gd=Gg\cdot M^{\mathrm{T}}$ 有：$Gd_i\begin{cases}\neq 0,\ i\in\{i_s,\cdots,i_n\}\\ =0,\ i\in\{i_1,\cdots,i_{s-1}\}\end{cases}\Bigg\}$

则式(6)可化为

$$LP^{SPT}(Gb\to Ga)=\sum_{Gg\in G}\prod_{i=1}^{k}LP^{T_i}(Gb_i\to Gg_i)\prod_{j=s}^{n}LP^{S_{i_j}}(Gd_{i_j}\to Ga_{i_j}) \tag{7}$$

因此只需考察 G 中的 Gg。对于 $Gg\in G$，由引理 12 可知，存在指标集 $\{j_s,\cdots,j_k\}\subseteq\{1,\cdots,k\}$，使得 $Gg_1,\cdots,Gg_k$ 由 $Gg_{j_s},\cdots,Gg_{j_k}$ 决定。因此由式(7)得：

$$\begin{aligned}&LP^{SPT}(Gb\to Ga)\\ &\leq\sum_{Gg_{j_s}\neq 0,\cdots,Gg_{j_k}\neq 0}\prod_{i=s}^{k}LP^{T_{j_i}}(Gb_{j_i}\to Gg_{j_i})r_l^{\,s-1}r_l^{\,n-s+1}\\ &=r_l^{\,n}\sum_{Gg_{j_s}\neq 0,\cdots,Gg_{j_k}\neq 0}\prod_{i=s}^{k}LP^{T_{j_i}}(Gb_{j_i}\to Gg_{j_i})\\ &=r_l^{\,n}\sum_{Gg_{j_s}\neq 0}LP^{T_{j_s}}(Gb_{j_s}\to Gg_{j_s})\cdots\sum_{Gg_{j_k}\neq 0}LP^{T_{j_k}}(Gb_{j_k}\to Gg_{j_k})\end{aligned} \tag{8}$$

由引理 10 的 Parseval 等式知 $\sum_{Gg_{j_i}\neq 0}LP^{T_{j_i}}(Gb_{j_i}\to Gg_{j_i})\leq 1$，$i=s,\cdots,k$。故由式(8)有：$LP^{SLT}(Gb\to Ga)\leq r_l^{\,n}$。因此 SPT 的最大线性包优势：

$$LP_{\max}^{SPT}=\max_{Gb\neq 0,Ga}LP^{SPT}(Gb\to Ga)\leq r_l^{\,n}$$

注：在对 SPT 模型最大线性逼近优势和最大线性包优势上界的估计中，其中所用 S 变换和 T 变换的平衡性是最关键的。

5 结束语

SPS 网络是分组密码的一个基本模型，能够同时实现压缩功能的 SPT 模型是该模型的推广，在序列密码的设计中具有重要的应用价值。本文在 P 为最佳扩散层的条件下，研究了该模型的抗差分攻击的安全性和抗线性攻击（S 和 T 平衡）的安全性，分别给出了其差分概率的上界、最大线性逼近优势的上界和最大线性包优势的上界，这些结论对于序列密码的设计和分析具有现实的意义。在今后的工作中，还将研究该模型在更宽松条件下的抗差分和线性攻击性能，并研究更加紧致的上界。

参考文献：

[1] KIM J S, LEE C H, SUNG J C, *et al*. Seven new block cipher structures with provable security against differential cryptanalysis[J]. IEICE Trans Fundamentals, 2008,92(10): 3047-3058.

[2] SU B Z, WU W L, ZHANG W T. Security of the SMS4 block cipher against differential cryptanalysis[J]. Journal of Computer Science and Technology, 2011,26(1): 130-138.

[3] 张文涛, 卿斯汉, 吴文玲. 嵌套 Feistel 结构的 SP 型分组密码的可证明安全性[J]. 计算机研究与发展, 2004, 41(8): 1389-1397.
ZHANG W T, QIN S H, WU W L. Provable security for SPN block ciphers containing feistel structure[J]. Journal of Computer Research and Development, 2004,41(8): 1389-1397.

[4] 魏悦川, 孙兵, 李超. FOX 密码的不可能差分攻击[J]. 通信学报, 2010, 31(9): 24-29.
WEI Y C, SUN B, LI C. Impossible differential attacks on FOX[J]. Journal on Communication, 2010, 31(9): 24-29.

[5] KELIHER L. Refined analysis of bounds related to linear and differential cryptanalysis for the AES[A]. AES 2004, LNCS 3373[C]. 2005. 42-57.

[6] BIRYUKOV A. Design of a new stream cipher-LEX, new stream cipher designs[A]. LNCS 4986[C]. 2008. 48-56.

[7] DAEMEN J, KITSOS P. The self-synchronizing stream cipher: MOUSTIQUE, new stream cipher designs[A]. LNCS 4986[C]. 2008. 210-223.

[8] DE Cannière C，PRENAAL B, TRIVIUM. New stream cipher designs[A]. LNCS 4986[C]. 2008.244-266.

[9] KANG J S, HONG S, LEE S, *et al*. Practical and provable security against differential and linear cryptanalysis for the substitution- permutation networks[J]. ETRI Journal, 2001, 23(4):158-167.

[10] HONG S, LEE S, LIM J, *et al*. Provable security against differential and linear cryptanalysis for the SPN structure[A]. FSE 2000, LNCS 1978[C]. 2001. 273-283.

[11] 吕述望, 范修斌, 王昭顺等. 完全映射及其密码学应用[M]. 合肥: 中国科学技术大学出版社, 2008.
LV S W, FAN X B, WANG Z S, *et al*. Complete Mapping and Application in Cryptography[M]. Hefei: University of Science and Technology of China Press, 2008.

[12] 吴文玲, 冯登国, 张文涛. 分组密码的设计与分析(第 2 版)[M]. 北京: 清华大学出版社, 2009.
WU W L, FENG D G, ZHANG W T, The Design and Analysis of Block Ciphers(Second Edition)[M]. Beijing: Tsinghua University Press, 2009.

[13] KELIHER L, MEIJER H, TAVARES S. New method for upper bounding the maximum average linear hull probability for SPNs[A]. EUROCRYPT 2001, LNCS 2045[C]. 2001. 420-436.

[14] 金晨辉, 郑浩然, 张少武等. 密码学[M]. 北京: 高等教育出版社, 2009.
JIN C H, ZHENG H R, ZHANG S W, *et al*. Cryptology[M]. Beijing: Higher Education Press, 2009.

作者简介：

刘凤梅（1974-），女，河南郸城人，博士，信息保障技术重点实验室副研究员，主要研究方向为密码理论与应用。

陈连俊（1965-），男，四川达县人，博士，信息保障技术重点实验室研究员，主要研究方向为密码理论与应用。

李春祥（1956-），男，河北成安人，信息保障技术重点实验室研究员，主要研究方向为密码理论与应用。

李艳梅（1977-），女，河北三河人，信息保障技术重点实验室助理研究员，主要研究方向为密码理论与应用。

张国双（1982-），男，河北临城人，信息保障技术重点实验室助理研究员，主要研究方向为密码理论与应用。