SIMON类非线性函数的线性性质研究

关 杰 卢健伟*

(战略支援部队信息工程大学 郑州 450001)

摘 要：SIMON算法是由美国国家安全局(NSA)在2013 年推出的一簇轻量级分组密码算法，具有实现代价低、安全性能好等优点，其轮函数采用了$F(x)=(x<<<a)\&(x<<<b)\oplus(x<<<c)$类型的非线性函数。该文研究了移位参数$(a,b,c)$一般化时SIMON类算法轮函数的线性性质，解决了这类非线性函数的Walsh谱分布规律问题，证明了其相关优势只可能取到0或2^{-k}，其中$k\in Z$且$0\le k\le\lfloor 2^{-1}n\rfloor$，并且对于特定条件下的每一个$k$，都存在相应的掩码对使得相关优势等于$2^{-k}$，给出了相关优势取到$2^{-1}$时的充分必要条件及掩码对的计数，给出了特定条件下非平凡相关优势取到最小值时的充分必要条件与掩码对的计数。

关键词：SIMON算法；线性性质；循环移位；S盒

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2021)11-3359-08

DOI: 10.11999/JEIT200999

Research on Linear Properties of SIMON Class Nonlinear Function

GUAN Jie LU Jianwei

(*Strategic Support Forces Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: SIMON algorithm is a group of lightweight block cipher algorithms introduced by the National Security Agency (NSA) in 2013. It has the advantages of low implementation cost and good security performance. Its round function adopts $F(x)=(x<<<a)\&(x<<<b)\oplus(x<<<c)$ type nonlinear function. In this paper, the linear properties of the round function of SIMON algorithm when the shift parameters (a, b, c) are generalized are studied. The problem of Walsh spectrum distribution of this kind of nonlinear function is solved, it is proved that the correlation advantage can only be equal to 0 or 2^{-k}, where $k\in Z$ and $0\le k\le\lfloor 2^{-1}n\rfloor$, and for each k under specific conditions, there are corresponding mask pairs so that the correlation advantage is equal to 2^{-k}. The necessary and sufficient conditions for the correlation advantage to be equal to 1/2 and the count of mask pairs are given. And the necessary and sufficient conditions for the nontrivial correlation advantage to be equal to the minimum value and the count of mask pairs under specific conditions are also given.

Key words: SIMON algorithm; Linear property; Cyclic shift; S-box

1 引言

随着技术的快速发展，信息处理功能已经可以在越来越小的嵌入式设备中实现。这类微型嵌入式设备的计算与存储能力十分有限，因此称为资源受限设备。传统密码在设计上主要考虑提高算法的安全性，没有考虑将算法应用于受限设备的情况。轻量级密码(LightWeight Cryptography, LWC)的诞生给这类设备所处理的信息提供了相应的保护，成为密码学研究的热点之一。

SIMON算法[1]是美国国家安全局(the National Security Agency, NSA)在2013年设计的一类基于Feistel结构的轻量级分组密码算法，该算法的轮函数为$F_{182}(x)=(x<<<1)\&(x<<<8)\oplus(x<<<2)$，只包含循环移位、按位与和异或这3类基本运算，因此软件与硬件的实现效果较好。自从SIMON算法提出以来，密码学者对其进行了大量分析。目前针对该算法的安全性分析主要包括差分分析[2–4]、线性分析[5–9]、不可能差分分析[10–12]、零相关分析[13–15]和积分分析[16,17]等。

SIMECK算法[18]是于2015年设计的一类轻量级分组密码算法，其结合了SIMON算法和 SPECK算法的优点，具有高效且低成本硬件实现的特点。该

收稿日期：2020-11-25；改回日期：2021-03-30；网络出版：2021-05-06
*通信作者： 卢健伟 lujianwei1997@163.com
基金项目：国家自然科学基金(61572516)
Foundation Item: The National Natural Science Foundation of China (61572516)

算法的轮函数为$F_{051}(x)=x\&(x<<<5)\oplus(x<<<1)$，同样沿用了SIMON算法轮函数的结构，将循环移位参数由(1,8,2)修改为(0,5,1)。

这些算法的轮函数均采用了如下形式的非线性函数$F_{abc}(x)=(x<<<a)\&(x<<<b)\oplus(x<<<c)$，该函数也是此类算法中唯一的非线性环节，它的密码学性质决定了算法的安全性，我们称此类函数为SIMON类非线性函数。目前关于SIMON类非线性函数的差分性质方面的结果较为完善，文献[3]找到了$F_{182}(x)$的差分分布规律，给出了差分转移概率的取值范围，解决了非0差分概率对应的输出差分的取值与计数问题。然而，线性性质方面的结果还较少，文献[5]给出了在$F_{182}(x)$的线性逼近式的2次项相互独立下相关系数取到0与$1/2^k$时掩码应满足的条件，但是当该线性逼近式的2次项相关时，掩码对与相关系数之间的关系没有彻底解决。

本文主要研究了移位参数一般化的SIMON类算法轮函数$F_{abc}(x)$的线性性质，给出了相关优势的取值范围，并且证明了对于该范围内的每一个相关优势，都可以找到对应的掩码对，解决了这类轮函数的Walsh谱分布规律问题，同时给出了非平凡相关优势取到2^{-1}与最小值的充分必要条件与计数情况，为SIMON系列算法与SIMECK算法等的线性安全性分析提供了理论基础。

本文组织架构如下：第2节介绍SIMON类算法轮函数、不相交2次型以及线性相关优势等基本概念，第3节给出SIMON类非线性函数的线性性质，第4节进行全文总结。

2 基本概念

定义1 设$F:Z_2^n\to Z_2^n$, $X=(x_0,x_1,\cdots,x_{n-1})$, $Y=F(X)=(y_0,y_1,\cdots,y_{n-1})\in Z_2^n$，若$F$的每一比特输出满足以下规则：$y_i=x_{i+a}\cdot x_{i+b}\oplus x_{i+c}$，其中 $0\le i,a,b,c<n$ ，即$F(x)=(x<<<a)\&(x<<<b)\oplus(x<<<c)$，其中$<<<$表示循环移位，$\&$表示按位AND操作，那么称为SIMON类非线性函数，记为F_s^n。(注：若无特殊说明，$n>\max\{a,b,c\}$，且下标运算都在模n上进行，另外不妨设$a<b$, $b-a\triangleq t$。)

定义2[19] 若$\deg(f)=2$，则布尔函数f是2次的。若一个2次布尔函数的常数项为0，那么称为2次型。记2次型$f(x_1,x_2,\cdots,x_n)=\bigoplus\limits_{1\le i\le j\le n}a_{i,j}x_ix_j=Q_f(x_1,x_2,\cdots,x_n)+L_f(x_1,x_2,\cdots,x_n)$ ，其中$a_{i,j}\in F_2$, Q_f包含了f的所有2次项，L_f包含了f的所有线性项。对于$i\in\{1,2,\cdots,n\}$，用$\sigma(f,x_i)$表示在Q_f中包含x_i的不同2次项的个数。

定义3[19] 给定2次型$f(x_1,x_2,\cdots,x_n)$，如果$\sigma(f,x_i)=\sigma(f,x_j)=1$，那么$x_ix_j$是独立的2次项。特别地，如果所有2次项都是独立的，那么称f是不相交的。

定义4[19] 给定两个布尔函数$f(x)$和$g(x)$，若存在一个可逆矩阵$\boldsymbol{M}$，使得$g(x)=f(x\boldsymbol{M})$成立，则称$f(x)$和$g(x)$是互为仿射等价的。

设$F:Z_2^n\to Z_2^n$, $f:Z_2^n\to Z_2$，称$\rho_F(\eta\to\mu)=W_{(F)}(\eta\to\mu)=\dfrac{1}{2^n}\sum\limits_{X\in Z_2^n}(-1)^{\eta\cdot X\oplus\mu\cdot F(X)}$为$F$在$(\eta,\mu)$点的Walsh谱，其中$X,\eta,\mu\in Z_2^n$，称$\eta$为输入掩码，$\mu$为输出掩码，$\eta\to\mu$为$F^n$的一个线性逼近，$|\rho_F(\eta\to\mu)|$为该线性逼近的相关优势，称$\rho_f(0)=\dfrac{1}{2^n}\sum\limits_{X\in Z_2^n}(-1)^{f(X)}$为$f$在0点的Walsh谱。

3 $F_{s'}^n$的线性性质

在本节，对于F，其输入和输出分别为$X=(x_0,x_1,\cdots,x_{n-1})$, $Y=(y_0,y_1,\cdots,y_{n-1})\in Z_2^n$，输入与输出掩码分别为$\eta=(\eta_0,\eta_1,\cdots,\eta_{n-1})$，$\mu=(\mu_0,\mu_1,\cdots,\mu_{n-1})$，由定义1可知

$$Y=F_{s'}^n(X)=(x_a\cdot x_b\oplus x_c,x_{a+1}\cdot x_{b+1}\oplus x_{c+1},\cdots,x_{n+a-1}\cdot x_{n+b-1}\oplus x_{n+c-1}) \tag{1}$$

由Walsh谱的定义易得

$$\begin{aligned}\rho_{F_{s'}^n}(\eta\to\mu)&=\frac{1}{2^n}\sum_{X\in F_2^n}(-1)^{\eta\cdot X\oplus\mu\cdot Y}\\&=\frac{1}{2^n}\sum_{X\in F_2^n}(-1)^{\bigoplus_{i=0}^{n-1}[(\eta_i\oplus\mu_{i-c})x_i\oplus\mu_ix_{i+a}x_{i+b}]}\end{aligned} \tag{2}$$

其中，$\bigoplus\limits_{i=0}^{n-1}[(\eta_i\oplus\mu_{i-c})x_i\oplus\mu_ix_{i+a}x_{i+b}]\triangleq f_{\eta,\mu}^*$，则$\rho_{F_{s'}^n}(\eta\to\mu)=\rho_{f_{\eta,\mu}^*}(0)$。

记$\mathrm{var}(f)$为布尔函数f中的变量集合，$|\mathrm{var}(f)|$为集合$\mathrm{var}(f)$的规模。例如，若$f=x_1x_2\oplus x_3$，则$\mathrm{var}(f)=\{x_1,x_2,x_3\}$, $|\mathrm{var}(f)|=3$。

引理 1[19] 设$f:Z_2^n\to Z_2$, $X=(x_0,x_1,\cdots,x_{n-1})\in Z_2^n$，若存在$x_i$, $i\in\{0,1,\cdots,n-1\}$使得

$$\begin{aligned}&f(x_0,x_1,\cdots,x_{i-1},x_i,x_{i+1},\cdots,x_{n-1})\\&\quad=x_i\oplus f(x_0,x_1,\cdots,x_{i-1},0,x_{i+1},\cdots,x_{n-1})\end{aligned} \tag{3}$$

那么$\rho_f(0)=0$。

引理 2[19] 若布尔函数$f(x)$和$g(x)$是互为仿射等价的，则$\rho_f(0)=\rho_g(0)$。

该引理揭示了对于一个布尔函数的输入变量进行可逆线性变换后，在0点的Walsh谱不变。Shi等人[19]给出了一个不相交化算法(算法1[19]，具体见附

录)，可以有效地将任意给定的2次布尔函数转换为不相交2次型。

$$\rho_f(0)=\begin{cases}(-1)^{\sum_{t=1}^{k}\mathrm{coe}_f(x_{i_{2t-1}})\mathrm{coe}_f(x_{i_{2t}})}\cdot 2^{-k}, & \{j_1,j_2,\cdots,j_s\}\subseteq\{i_1,i_2,\cdots,i_{2k}\}\\ 0, & \{j_1,j_2,\cdots,j_s\}\not\subset\{i_1,i_2,\cdots,i_{2k}\}\end{cases}\tag{4}$$

其中，$\mathrm{coe}_f(x^u)$表示x^u在f中的系数。

引理3提供了计算不相交2次型在0点的Walsh谱值的一种方法，其中k表示f中不同2次项的个数，根据算法1和引理3可以有效地计算出任意2次布尔函数在0点的Walsh谱值。

3.1 F_s^n谱值的取值范围

本文从$f_{\eta,\mu}^*$的结构入手，首先将$f_{\eta,\mu}^*$经过算法1后转化成的不相交2次型记为$\hat{f}$，由于$f_{\eta,\mu}^*$与$\hat{f}$是互为仿射等价的，由引理2可知两者在0点的Walsh谱值相等，再由引理3，分析k的取值等价于分析$\hat{f}$中不相交2次项的个数。为方便证明，将$w(\mu)$记为μ的汉明重量。

下面给出$F_{s'}^n$的Walsh谱取值范围及其证明。

定理1　对于$F_{s'}^n$，有以下结论成立：

(1)$\forall\eta,\mu\in Z_2^n$，均有$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=0$或$1/2^k$，其中$k\in Z$，且$0\le k\le\lfloor n/2\rfloor$；

(2)当n为偶数且t为奇数，或$t|\lfloor n/2\rfloor$时，对于区间$[0,\lfloor n/2\rfloor]$内任意的k，存在$\eta,\mu\in Z_2^n$使得$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^k$。

证明　(1)由引理2可知$\rho_{f_{\eta,\mu}^*}(0)=\rho_{\hat{f}}(0)$，由引理3易得$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=\left|\rho_{f_{\eta,\mu}^*}(0)\right|=\left|\rho_{\hat{f}}(0)\right|=0$或$1/2^k$，故对$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|$的取值证毕；由算法1的变换过程可知，$\mathrm{var}\left(f_{\eta,\mu}^*\right)\supseteq\mathrm{var}\left(\hat{f}\right)$，而$\hat{f}$是一个不相交2次型，故$k$必然不超过$\lfloor n/2\rfloor$，即$0\le k\le\lfloor n/2\rfloor$；

(2)以下采用构造式证明，首先证明当n为偶数且t为奇数时的情况，显然，只需证明对于区间内的每一个k，均可以找到相应的掩码对，以下均取$\eta_i=\mu_{i-c}$使得$f_{\eta,\mu}^*$中不出现线性项：

当$k=0$时，取$\mu=(0,0,\cdots,0)$，则$f_{\eta,\mu}^*=0$，此时$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1$；

当$k=1$时，取$\mu_0=1$，其余$\mu_i=0$，则$f_{\eta,\mu}^*=x_ax_b$，此时$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2$；

当$k=2$时，取$\mu_0=\mu_2=1$，其余$\mu_i=0$，则$f_{\eta,\mu}^*=x_ax_b\oplus x_{a+2}x_{b+2}$，此时$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^2$；

一般化，当$k=m$ $(m\in[2,\lfloor n/2\rfloor])$时，取$w(\mu)=m$且$\mu_0=\mu_2=\cdots=\mu_{2m-4}=\mu_{2m-2}=1$，其余$\mu_i=0$，则$f_{\eta,\mu}^*=\bigoplus_{i=0}^{m-1}x_{a+2i}x_{b+2i}$，其中$t$为奇数保证了上述每个$f_{\eta,\mu}^*$都是不相交2次型，此时

引理3[19]　对于不相交2次型$f=x_{i_1}x_{i_2}\oplus\cdots\oplus x_{i_{2k-1}}x_{i_{2k}}\oplus x_{j_1}\oplus\cdots\oplus x_{j_s}$，$f$在0点的Walsh谱值计算方法为

$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^m$，故$n$为偶数且$t$为奇数时，结论(2)成立。

其次证明当$t|\lfloor n/2\rfloor$时的情况，不妨记$m=\lfloor n/2t\rfloor$，当$k=0$时，取$\mu=(0,0,\cdots,0)$即可，下面按照k的取值范围，分成以下m种情况进行讨论：

情况1：当$1\le k\le t$时，取$w(\mu)=k$且$\mu_0=\mu_1=\cdots=\mu_{k-1}=1$，其余$\mu_i=0$，则$f_{\eta,\mu}^*=\bigoplus_{i=0}^{k-1}x_{a+i}x_{b+i}\triangleq f_{1,k}$，其中$f_{1,k}$的下标“$1,k$”表示在情况1中$\mu_0=\mu_1=\cdots=\mu_{k-1}=1$的掩码选取规则下对应的$f_{\eta,\mu}^*$，$t|\lfloor n/2\rfloor$保证了上述每个$f_{\eta,\mu}^*$都是不相交2次型，此时$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^k$；

情况2：当$t+1\le k\le 2t$时，在$f_{1,t}$的掩码选取规则下(由情况1可知，$f_{1,t}$的掩码选取规则为$\mu_0=\mu_1=\cdots=\mu_{t-1}=1$)，再取$\mu_{2t}=\mu_{2t+1}=\cdots=\mu_{t+k-1}=1$，则$f_{\eta,\mu}^*=f_{1,t}\oplus\bigoplus_{i=t+1}^{k}x_{a+t-1+i}x_{b+t-1+i}$，其中$\bigoplus_{i=t+1}^{k}x_{a+t-1+i}x_{b+t-1+i}\triangleq f_{2,k}$，显然$f_{1,t}$与$f_{2,k}$是不相交的，且各自均是不相交2次型，故$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^k$；

情况3：当$2t+1\le k\le 3t$时，在$f_{1,t}$与$f_{2,t}$的掩码选取规则下(即$\mu_0=\mu_1=\cdots=\mu_{t-1}=1$且$\mu_{2t}=\mu_{2t+1}=\cdots=\mu_{3t-1}=1$)，再取$\mu_{4t}=\mu_{4t+1}=\cdots=\mu_{2t+k-1}=1$，则$f_{\eta,\mu}^*=f_{1,t}\oplus f_{2,t}\oplus\bigoplus_{i=2t+1}^{k}x_{a+2t-1+i}x_{b+2t-1+i}$，其中$\bigoplus_{i=2t+1}^{k}x_{a+2t-1+i}x_{b+2t-1+i}\triangleq f_{3,k}$，显然$f_{1,t}$,$f_{2,t}$与$f_{3,k}$互不相交，且各自均是不相交2次型，故$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^k$；

以t为周期依次对μ取值，故当$(m-1)t+1\le k\le mt$时，在$f_{1,t}$,$f_{2,t}$,$\cdots$,$f_{m-1,(m-1)t}$的掩码选取规则下，再取$\mu_{2(m-1)t}=\mu_{2(m-1)t+1}=\cdots=\mu_{k+(m-1)t-1}=1$，则$f_{\eta,\mu}^*=\bigoplus_{i=1}^{m-1}f_{i,it}\oplus\bigoplus_{i=(m-1)t+1}^{k}x_{a+(m-1)t-1+i}x_{b+(m-1)t-1+i}$，其中$\bigoplus_{i=(m-1)t+1}^{k}x_{a+(m-1)t-1+i}x_{b+(m-1)t-1+i}\triangleq f_{m,mk}$，显然$\forall i,j\in[1,m-1]$，每个$f_{i,it}$都是不相交2次型，且$f_{i,it}$与$f_{j,jt}$互不相交，而$f_{m,mk}$也是不相交2次型，此时$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^k$，故当$t|\lfloor n/2\rfloor$时，结论(2)成立。　　证毕

定理 2 $\forall \eta \neq \eta', \mu \in Z_2^n$，若$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right|$与$\left|\rho_{F_{s'}^n}(\eta' \to \mu)\right|$均不为 0，则必有$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| = \left|\rho_{F_{s'}^n}(\eta' \to \mu)\right|$。

证明 $\forall \eta \neq \eta', \mu \in Z_2^n$, $f_{\eta,\mu}^*$与$f_{\eta',\mu}^*$的所有2次项相同，且$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| \neq 0$, $\left|\rho_{F_{s'}^n}(\eta' \to \mu)\right| \neq 0$，故$f_{\eta,\mu}^*$与$f_{\eta',\mu}^*$经过不相交化算法后得到的式子中，不相交的2次项均相同，且均不存在独立的单次项，由引理3，$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| = \left|\rho_{F_{s'}^n}(\eta' \to \mu)\right|$。 证毕

定理2说明了$F_{s'}^n$的输出掩码与非0相关优势之间的一一对应关系，即输出掩码取定后，不论输入掩码如何取值，非零相关优势始终相同，显然$F_{s'}^n$是一个多输出部分bent函数。为方便叙述，引入以下记号：对于函数$F: Z_2^n \to Z_2^n$，给定的$u \in Z_2^n$，若存在$t \in Z_2^n$使得对于任意的$s \in Z_2^n$，总有$\frac{1}{2^n}\sum_{X \in Z_2^n}(-1)^{u(F(x \oplus s) \oplus F(x))} \triangleq r_F(u,s) = (-1)^{t \cdot s}$或0，记$E = \left\{s \in Z_2^n | r_F(u,s) = (-1)^{t \cdot s}\right\}$，不妨设$E$中有$t$个不同的$s$，即$E = \{s_0, s_1, \cdots, s_{t-1}\}$，其中$s_i = (s_{i,0}, s_{i,1}, \cdots, s_{i,n-1})$，将满足$\forall i \in [0, t-1]$，均有$s_{i,j_0} = 0$的$j_0$的个数记为$k$，记$E^\perp = \{v \in Z_2^n | v \cdot s = 0, \forall s \in E\}$。

引理 4[20] $F^n: Z_2^n \to Z_2^n$是部分bent函数的充分必要条件是$\forall u \in Z_2^n$，存在$t \in Z_2^n$，使得

$$\left(\rho_{F^n}(t \oplus v \to u)\right)^2 = \begin{cases} 1/2^{n-k}, & v \in E^\perp \\ 0, & v \notin E^\perp \end{cases} \tag{5}$$

当μ取定时，可以将$\rho_{F_s}(\eta \to \mu)$转换为某一个函数关于η的函数值。当$w(\mu) \neq 0$时，必存在$\eta^* \in Z_2^n$使得$\left|\rho_{F_{s'}^n}(\eta^* \to \mu)\right| \neq 0$，由引理4，$\left|\rho_{F_{s'}^n}(\eta^* \to \mu)\right|^2 = 1/2^{n-k}$，且$\#\left\{\eta \in Z_2^n : \left|\rho_{F_{s'}^n}(\eta \to \mu)\right| \neq 0\right\} = \left|E^\perp\right| = 2^{n-k}$，其中$\left|E^\perp\right|$表示$E^\perp$的规模。下面得到$\mu$与非平凡相关优势的计数的对应关系，即推论1。

推论 1 当$w(\mu) \neq 0$时，必存在$\eta^* \in Z_2^n$使得$\left|\rho_{F_{s'}^n}(\eta^* \to \mu)\right| \neq 0$，那么

$$\#\left\{\eta \in Z_2^n : \left|\rho_{F_{s'}^n}(\eta \to \mu)\right| \neq 0\right\} = 1/\left|\rho_{F_{s'}^n}(\eta^* \to \mu)\right|^2$$

3.2 $F_{s'}^n$的掩码结构和计数

如果布尔函数f经过算法1后满足引理1的条件，说明不相交化后的布尔函数的结构中存在独立的线性变量，由引理2与引理3，显然$\rho_f(0) = 0$。下面给出$F_{s'}^n$在0点的谱值对应的充分条件。

定理3 对于$\eta, \mu \in Z_2^n$，若存在$0 \le i_0 \le n-1$使得$\eta_{i_0} \oplus \mu_{i_0-c} = 1$且满足以下条件之一：

(1)$\mu_{i_0-a} = \mu_{i_0-b} = 0$；

(2)$\eta_{i_0-2a+2b} \oplus \mu_{i_0-2a+2b-c} = 0$, $\mu_{i_0-a} = \mu_{i_0-2a+b} = 1$，其余$\mu_i = 0$；

则$\rho_{F_{s'}^n}(\eta \to \mu) = 0$。

证明 (1)$f_{\eta,\mu}^* = \bigoplus_{i=0}^{n-1}\left[(\eta_i \oplus \mu_{i-c})x_i \oplus \mu_i x_{i+a} x_{i+b}\right]$，已知存在$0 \le i_0 \le n-1$使得$\eta_{i_0} \oplus \mu_{i_0-c} = 1$，则$f_{\eta,\mu}^*$包含线性项$x_{i_0}$，当$\mu_{i_0-a} = \mu_{i_0-b} = 0$时，$f_{\eta,\mu}^*$中的所有2次项不包含$x_{i_0}$，故此时线性项$x_{i_0}$是独立的，由引理1可知，$\rho_{F_{s'}^n}(\eta \to \mu) = 0$，条件(1)成立；

(2)由于$\mu_{i_0-a} = \mu_{i_0-2a+b} = 1$且其余$\mu_i = 0$，则$f_{\eta,\mu}^* = x_{i_0} x_{i_0-a+b} \oplus x_{i_0-a+b} x_{i_0-2a+2b} \oplus x_{i_0} \oplus f_d$，其中$f_d$为除$x_{i_0}$以外剩余的线性项之和，已知$\eta_{i_0-2a+2b} \oplus \mu_{i_0-2a+2b-c} = 0$，则$f_d$不包含$x_{i_0-2a+2b}$，经过算法1后，得到$f_{\eta,\mu}^* = x_{i_0} x_{i_0-a+b} \oplus x_{i_0} \oplus x_{i_0-2a+2b} \oplus f_d$，此时$x_{i_0-2a+2b}$是独立的线性项，故$\rho_{F_{s'}^n}(\eta \to \mu) = 0$，条件(2)成立。 证毕

通过定理3容易得到在$w(\mu) = 0$时相关优势取0和1时的充分必要条件，即推论2。

推论 2 $\forall \eta \in Z_2^n$，当$w(\mu) = 0$时，有以下结论成立：

若$\eta \neq 0$，则$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| = 0$；

若$\eta = 0$，则$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| = 1$。

通过引理3中对于不相交2次项的个数分析，得出$w(\mu) = 1$时相关优势的取值情况，即引理5。

引理 5 $\forall \eta \in Z_2^n$，当$w(\mu) = 1$时，$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| = 0$或$1/2$。

证明 由于$w(\mu) = 1$，即存在$i_0 \in [0, n-1]$，使得$\mu_{i_0} = 1$，其余$\mu_i = 0$，则$f_{\eta,\mu}^* = x_{i_0}(x_{i_0+a} \oplus x_{i_0+b}) \oplus \bigoplus_{i=0}^{n-1}\left[(\eta_i \oplus \mu_{i-c})x_i\right]$，经过$x_{i_0+a} \leftarrow x_{i_0+a} \oplus x_{i_0+b}$线性变换后，显然$f_{\eta,\mu}^*$中只有一个2次项$x_{i_0} x_{i_0+a}$，由引理2和引理3，若存在$i_1 \in [0, n-1]$且$i_1 \notin \{i_0, i_0+a\}$，使得$\eta_{i_1} \oplus \mu_{i_1-c} = 1$，即$f_{\eta,\mu}^*$中存在独立的线性项，则$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| = 0$，否则$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| = 1/2$。 证毕

下面给出$w(\mu) = 2$时相关优势的取值情况，即引理6。

引理 6 $\forall \eta \in Z_2^n$, $w(\mu) = 2$（不妨令$\mu_{i_0} = \mu_{i_0+k} = 1$, $k \in [1, n-1]$），有以下结论：

（1）当$k \in \{t, n-t\}$时，$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| = 0$或$1/2$；

（2）当$k \notin \{t, n-t\}$时，$\left|\rho_{F_{s'}^n}(\eta \to \mu)\right| = 0$或$1/4$。

证 明　已知 $w(\mu)=2$,$\mu_{i_0}=\mu_{i_0+k}=1$，则 $f^*_{\eta,\mu}=x_{i_0+a}x_{i_0+b}\oplus x_{i_0+k+a}x_{i_0+k+b}\oplus f_d$，其中 $f_d=(\eta_{i_0+c}\oplus 1)x_{i_0+c}\oplus(\eta_{i_0+c+k}\oplus 1)x_{i_0+c+k}\oplus \bigoplus_{i=0,i\neq i_0+c,i_0+c+k}^{n-1}\eta_i x_i$ 表示所有线性项之和。

当 $k=t$ 时，$f^*_{\eta,\mu}=x_{i_0+a}x_{i_0+b}\oplus x_{i_0+b}x_{i_0+2b-a}\oplus f_d$，由算法1，经过线性变换 $x_{i_0+a}\leftarrow x_{i_0+a}\oplus x_{i_0+2b-a}$ 后，显然 $f^*_{\eta,\mu}$ 中只有一个2次项 $x_{i_0+a}x_{i_0+b}$，由引理2与引理3，$\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=0$ 或 $1/2$；

当 $k=n-t$ 时，$f^*_{\eta,\mu}=x_{i_0+a}x_{i_0+b}\oplus x_{i_0+2a-b}x_{i_0+a}\oplus f_d$，经过线性变换 $x_{i_0+b}\leftarrow x_{i_0+b}\oplus x_{i_0+2a-b}$ 后，$f^*_{\eta,\mu}$ 中只有一个2次项 $x_{i_0+a}x_{i_0+b}$，故 $\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=0$ 或 $1/2$；

每个变量 x_i 在 $f^*_{\eta,\mu}$ 的2次项中最多出现两次，故当 $k\notin\{t,n-t\}$ 时，$f^*_{\eta,\mu}$ 的两个2次型互不相交，即 $\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=0$ 或 $1/4$。　证毕

下面给出 $w(\mu)=n$ 时相关优势的取值情况，即引理7。

引理 7　当 $t|n$ 且 $n>t$ 时，取 $w(\mu)=n$，以下结论成立：若 $n=jt\,(j\geq 2)$，则 $\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=0$ 或 $1/2^{\lfloor(j-1)/2\rfloor t}$。

证 明　已知 $w(\mu)=n$，则 $f^*_{\eta,\mu}=\bigoplus_{i=0}^{t-1}x_ix_{i+t}\oplus\bigoplus_{i=t}^{n-1}x_ix_{i+t}\oplus f_d$，其中 $f_d=\bigoplus_{i=0}^{n-1}(\eta_i+1)x_i$ 表示所有线性项之和。当 $j=2$ 时，$\bigoplus_{j=t}^{n-1}x_{j+t}x_j=\bigoplus_{i=0}^{t-1}x_ix_{i+t}$，则 $f^*_{\eta,\mu}$ 中只存在线性项，若 $\forall i\in[0,n-1],\eta_i+1=0$，即 $f_d=0$，则 $\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=1$，否则，$\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=0$，故当 $j=2$ 时成立；当 $j\geq 3$ 时，$f^*_{\eta,\mu}$ 经过算法1变换后，$f^*_{\eta,\mu}=\bigoplus_{i=0}^{t-1}\bigoplus_{k=0}^{\lfloor(j-1)/2\rfloor}x_{2kt+i}x_{2kt+t+i}\oplus f_d{}'$，其中 $f_d{}'$ 表示线性变换后所有线性项之和，显然此时 $f^*_{\eta,\mu}$ 为不相交2次项，若 $f_d{}'$ 中存在独立的线性项，$\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=0$，否则 $\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=1/2^{\lfloor(j-1)/2\rfloor t}$。　证毕

在研究S盒的线性性质时，其最大非平凡相关优势点的结构和计数通常需要重点关注。接下来通过定理4给出 $F^n_{s'}$ 的非平凡相关优势取到最大值 $1/2$ 时的充分必要条件及计数。

定理4　对于 $F^n_{s'}$，当 a,b,c 两两不相等，tn，$t+c\neq a,b\,(\mathrm{mod}n)$，$t+b\neq c\,(\mathrm{mod}n)$ 时，$\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=1/2$ 当且仅当 (η,μ) 满足下列条件之一：

(1) $w(\mu)=1$，不妨令 $\mu_{i_0}=1$，则 $\eta_{i_0+c}=1$，且对于 $i\notin\{i_0+a,i_0+b\}$，$\eta_i=0$；

(2) $w(\mu)=2$，$\forall i_0\in[0,n-1]$ 使得 $\mu_{i_0}=\mu_{i_0+t}=1$，则 $\eta_{i_0+c}=\eta_{i_0+t+c}=1$，$\eta_{i_0+a}\oplus\eta_{i_0+2b-\mathrm{a}}=0$ 且 $\forall i\notin\{i_0+c,i_0+c+t,i_0+a,i_0+b,i_0+2b-\mathrm{a}\}$ 时 $\eta_i=0$；

(3) $w(\mu)=2$，$\forall i_0\in[0,n-1]$ 使得 $\mu_{i_0}=\mu_{i_0+n-t}=1$，则 $\eta_{i_0+c}=\eta_{i_0+n-t+c}=1$，$\eta_{i_0+a}\oplus\eta_{i_0+a+n-t}=0$ 且 $\forall i\notin\{i_0+c,i_0+n-t+c,i_0+a,i_0+b,i_0+a+n-t\}$ 时 $\eta_i=0$；

此时满足 $\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=1/2$ 的掩码对数为 $8n$。

证明　由引理2和引理3可知，$\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|=1/2$ 当且仅当 $f^*_{\eta,\mu}$ 经过算法1后得到的式子 $\hat{f}$ 中只有一个2次项，且不存在独立的单次项。

(1) 当 $w(\mu)=1$ 时，$\mu_{i_0}=1$，$f^*_{\eta,\mu}=x_{i_0+a}\cdot x_{i_0+b}\oplus(\eta_{i_0+c}\oplus 1)x_{i_0+c}\oplus\bigoplus_{i\neq i_0+c}(\eta_ix_i)$，由于 a,b,c 两两不相等，$f^*_{\eta,\mu}$ 中不存在独立的单次项当且仅当 $\eta_{i_0+c}=1$，且对于 $i\notin\{i_0+a,i_0+b\}$，$\eta_i=0$；

(2) 当 $w(\mu)=2$ 时，若取 $\mu_{i_0}=\mu_{i_0+k}=1$，其中 $k\in[1,t-1]\cup[t+1,n-t-1]\cup[n-t+1,n-1]$，显然 $x_{i_0+a}x_{i_0+b}$ 与 $x_{i_0+k+a}x_{i_0+k+b}$ 互不相交，即 $f^*_{\eta,\mu}$ 中有两个不相交2次项，由引理3，$\left|\rho_{F^n_{s'}}(\eta\to\mu)\right|\neq 1/2$。

若取 $k=t$，即 $\mu_{i_0}=\mu_{i_0+t}=1$ 时，$f^*_{\eta,\mu}=x_{i_0+b}(x_{i_0+a}\oplus x_{i_0+2b-a})\oplus(\eta_{i_0+c}\oplus 1)x_{i_0+c}\oplus(\eta_{i_0+t+c}\oplus 1)x_{i_0+t+c}\oplus\bigoplus_{i\neq i_0+c,i_0+t+c}(\eta_ix_i)$，由算法1的线性变换 $x_{i_0+a}\leftarrow x_{i_0+a}\oplus x_{i_0+2b-a}$ 可知，$\hat{f}$ 中不存在独立的线性项当且仅当 $\eta_{i_0+c}=\eta_{i_0+t+c}=1$，$\eta_{i_0+a}=\eta_{i_0+2b-\mathrm{a}}$ 且 $\forall i\notin\{i_0+a,i_0+b,i_0+2b-a\}$ 时 $\eta_i=0$。其中 a,b,c 两两不相等、$t+c\neq a,b\,(\mathrm{mod}n)$ 与 $t+b\neq a,c\,(\mathrm{mod}n)$ 保证了 $\{i_0+c,i_0+c+t,i_0+a,i_0+b,i_0+2b-a\}$ 中的元素互不相同，故条件(2)成立；

(3) 当 $w(\mu)=2$ 时，若取 $k=n-t$，即 $\mu_{i_0}=\mu_{i_0+n-t}=1$，$f^*_{\eta,\mu}=x_{i_0+a}(x_{i_0+b}\oplus x_{i_0+a+n-t})\oplus(\eta_{i_0+c}\oplus 1)x_{i_0+c}\oplus(\eta_{i_0+n-t+c}\oplus 1)x_{i_0+n-t+c}\oplus\bigoplus_{i\neq i_0+c,i_0+n-t+c}(\eta_ix_i)$，由算法1的线性变换 $x_{i_0+b}\leftarrow x_{i_0+b}\oplus x_{i_0+a+n-t}$ 可知，$\hat{f}$ 中不存在独立的线性项当且仅当 $\eta_{i_0+c}=\eta_{i_0+n-t+c}=1$，$\eta_{i_0+b}=\eta_{i_0+a+n-t}$ 且 $\forall i\notin\{i_0+a,i_0+b,i_0+a+n-t\}$ 时 $\eta_i=0$。其中 a,b,c 两两不相等、$t+c\neq a,b\,(\mathrm{mod}n)$ 与 $t+b\neq a,c\,(\mathrm{mod}n)$ 保证了 $\{i_0+c,i_0+n-t+c,i_0+a,i_0+b,i_0+a+n-t\}$ 中的元素互不相同，故条件(3)成立；

当 $2<w(\mu)\leq n$ 时，由于每个变量 x_i 在 $f^*_{\eta,\mu}$ 的

2次项中最多出现两次，由算法1可知，$t\backslash n$保证了$\hat{f}$中至少存在两个不相交2次项，即$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|\le 1/4$，此时不存在满足条件的掩码对；

下面考虑掩码对计数问题，由上述证明过程可知，一个输出掩码μ对应4个输入掩码η，故当$w(\mu)=1$时掩码对数为$4n$，当$w(\mu)=2$时，取遍i_0后，$\mu_{i_0}=\mu_{i_0+t}=1$与$\mu_{i_0}=\mu_{i_0+n-t}=1$包含的$\mu$的集合相同，故此时掩码对数为$4n$，总计$8n$。

证毕

定理4研究了最大非平凡相关优势点的结构和计数，但是最小非平凡相关优势点的结构和计数也是需要重点考虑的问题。下面给出特定条件下非平凡相关优势取到最小值的充分必要条件。

定理5 对于$F_{s'}^n$，n为偶数，t为奇数，$t\ne n/2$，当$w(\mu)=n/2$时，非平凡相关优势取到最小值$1/2^{n/2}$当且仅当μ的每个取值为1的比特位不相邻，即$\mu=(0101,\cdots,0101)$或$(1010,\cdots,1010)$，满足$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^{n/2}$的掩码对数为$2^{n+1}$。

证明 由引理2和引理3可知，非平凡相关优势取到最小值$1/2^{n/2}$当且仅当$f_{\eta,\mu}^*$经过算法1后得到的式子$\hat{f}$中有$n/2$个不相交的2次项，且不存在独立的线性项。由于$n/2$个不相交的2次项包含了$x_0,x_1,\cdots,x_{n-1}$这n个变量，故不存在独立的单次项，即对η的取值可以进行遍历。因此，当$w(\mu)=n/2$时，非平凡相关优势取到最小值问题可以转换为在n个不同的2次项$x_{i+a}x_{i+b}\,(i\in[0,n-1])$中，如何找出$n/2$个不相交的2次项的问题。由$f_{\eta,\mu}^*$的表达式可知，每个$\mu_i$决定了2次项$x_{i+a}x_{i+b}$是否出现在$f_{\eta,\mu}^*$中。

首先分析μ中有两个取值为1的比特位相邻的情况，即存在$i_0\in[0,n-1]$，使得$\mu_{i_0}=\mu_{i_0+1}=1$，则$f_{\eta,\mu}^*$中出现$x_{i_0+a}x_{i_0+b}\oplus x_{i_0+a+1}x_{i_0+b+1}$，由于$f_{\eta,\mu}^*$不相交，且每个变量$x_i$在$f_{\eta,\mu}^*$中最多出现两次，故$x_{i_0+a-t}x_{i_0+a}$，$x_{i_0+a+1-t}x_{i_0+a+1}$，$x_{i_0+b}x_{i_0+b+t}$与$x_{i_0+b+1}x_{i_0+b+1+t}$均不出现在$f_{\eta,\mu}^*$中($t\ne n/2$保证了$x_{i_0+a-t}\ne x_{i_0+b}$与$x_{i_0+a+1-t}\ne x_{i_0+b+1}$，即$x_{i_0+a-t}x_{i_0+a}$，$x_{i_0+a+1-t}x_{i_0+a+1}$，$x_{i_0+b}x_{i_0+b+t}$与$x_{i_0+b+1}x_{i_0+b+1+t}$互不相同)，而$f_{\eta,\mu}^*$中最多有$n$个2次项，$x_{i_0+a}x_{i_0+b}\oplus x_{i_0+a+1}x_{i_0+b+1}$已经提供了两个不相交的2次项，下面从剩余的$n-6$个2次项中找出$n/2-6$个不相交的2次项即可，显然这是不可能的，因为剩余$n$–6个2次项可以根据公共变量$x_{i_0+a+j}$进行两两配对，即$x_{i_0+a+j}x_{i_0+b+j}$与$x_{i_0+2a-b+j}x_{i_0+a+j}$（其中$j\in[2,n-1]$且$j\notin\{n-t,n-t+1,t,t+1\}$)是相交的，两者只能取一个才能保证$f_{\eta,\mu}^*$是不相交2次型，故剩余的$n-6$个2次项最多只能提供$n/2-3$个不相交的2次项，显然总共不相交的2次项至多为$n/2-1$，相关优势取不到最小值$1/2^{n/2}$。

当μ中取值为1的比特位均不相邻，即$\mu=(0101,\cdots,0101)$或$(1010,\cdots,1010)$时，$f_{\eta,\mu}^*=\bigoplus_{i=1}^{n/2}x_{2i}x_{2i+t}\oplus f_d$或$f_{\eta,\mu}^*=\bigoplus_{i=1}^{n/2}x_{2i-1}x_{2i+t-1}\oplus f_{d'}$，其中$f_d$与$f_{d'}$分别表示所有线性项之和，$t$为奇数保证了$f_{\eta,\mu}^*$中每个2次项的下标均是1奇1偶，即这$n/2$个不相交的2次项包含了$n$个全部变量，故不存在独立的线性项，显然这两个2次型都是不相交的，故$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^{n/2}$；对$\eta$的取值可以进行遍历，因此满足非平凡相关优势取到最小值$1/2^{n/2}$的掩码对数为2^{n+1}。

证毕

结合定理5，给出非平凡相关优势取到最小值$1/2^{n/2}$时的一个充分条件。

定理6 对于$F_{s'}^n$，n为偶数，t为奇数且$t\ne n/2$，当μ满足以下情况之一时，非平凡相关优势取到最小值$1/2^{n/2}$：当$w(\mu)=n/2+k$时(其中$k\in[0,n/2-1]$)，μ的取值如下：分别在$(0101,\cdots,0101)$或$(1010,\cdots,1010)$取值为0的$n/2$个比特位中任取k个进行翻转；

此时满足$\left|\rho_{F_{s'}^n}(\eta\to\mu)\right|=1/2^{n/2}$的$\mu$有$2^{n/2+1}-2$个。

证明 对于$F_{s'}^n$，由定理1可知，当n为偶数，t为奇数时，存在相应掩码对使得非平凡相关优势取到最小值$1/2^{n/2}$，由引理3可知，相关优势取到$1/2^{n/2}$的必要条件是$w(\mu)\ge n/2$，由定理5可知，当$k=0$时结论成立；当$w(\mu)=n/2+k$ (k取遍$[1,n/2-1]$)时，以$\mu=(0101,\cdots,0101)$为例，不妨将在$(0101,\cdots,0101)$中取值为0的比特位中进行翻转的位置设为$\mu_1^{2j_1},\mu_1^{2j_2},\cdots,\mu_1^{2j_k}$($\mu_1^{2j_i}$表示$\mu_1$的第$2j_i$个比特位)，其中$j_1,j_2,\cdots,j_k\in[0,n/2-1]$，当$\mu=(0101,\cdots,0101)$时，$f_{\eta,\mu}^*=\bigoplus_{i=0}^{n/2-1}x_{a+2i+1}x_{b+2i+1}\oplus f_d$(由于非平凡相关优势要取到最小值$1/2^{n/2}$，即$f_{\eta,\mu}^*$经过算法1变换后有$n/2$个不相交的2次项，这些2次项包含了$x_0,x_1,\cdots,x_{n-1}$所有变量，故不存在独立的线性项，为方便证明，下面将涉及的所有线性项之和均记为f_d)，对第$\mu_1^{2j_1},\mu_1^{2j_2},\cdots,\mu_1^{2j_k}$比特位进行翻转后

$$
\begin{aligned}
f_{\eta,\mu}^{*} &= \bigoplus_{i=1}^{k} x_{a+2j_i}x_{b+2j_i} \oplus \bigoplus_{i=0}^{n/2-1} x_{a+2i+1}x_{b+2i+1} \oplus f_d \\
&= \bigoplus_{i=1}^{k} \left(x_{a+2j_i}x_{b+2j_i} \oplus x_{b+2j_i}x_{b+2j_i+t}\right) \oplus \bigoplus_{v\neq(2j_i+t-1)/2\left(i\text{取遍}[1,k]\right),v=1}^{n/2-1} x_{a+2v+1}x_{b+2v+1} \oplus f_d, \\
&= \bigoplus_{i=1}^{k} \left(x_{b+2j_i}\left(x_{b+2j_i+t} \oplus x_{a+2j_i}\right)\right) \oplus \bigoplus_{v\neq(2j_i+t-1)/2\left(i\text{取遍}[1,k]\right),v=1}^{n/2-1} x_{a+2v+1}x_{b+2v+1} \oplus f_d。
\end{aligned}
$$

上述$f_{\eta,\mu}^{*}$依次经过k次线性变换$x_{b+2j_i+t} \leftarrow x_{b+2j_i+t} \oplus x_{a+2j_i}$（其中$i$依次取遍$1,2,\cdots,k$）后，$f_{\eta,\mu}^{*} = \bigoplus_{i=1}^{n/2} x_{b+2j_i}x_{b+2j_i+t} \oplus \bigoplus_{v\neq(2j_i+t-1)/2\left(i\text{取遍}[1,k]\right),v=1}^{n/2} x_{a+2v+1}x_{b+2v+1} \oplus f_d$，显然此时$f_{\eta,\mu}^{*}$是不相交2次型，有$n/2$个不相交2次项，且不存在独立的线性项，由引理3可知，$\left|\rho_{F_{s'}^{n}}(\eta \to \mu)\right| = 1/2^{n/2}$，由于翻转的比特位取遍$n/2$个取值为0的比特位，针对$\mu=(0101,\cdots,0101)$或$\mu=(1010,\cdots,1010)$进行比特翻转分别有$C_{n/2}^{k}$个$\mu$，总计$2\times C_{n/2}^{k}$；对$\mu$的计数进行求和，利用2项式定理可知，$2\sum_{i=0}^{n/2-1} C_{n/2}^{i} = 2^{n/2+1}-2$。　　证毕

表1给出当$n\in\{8,9\}$时SIMON类轮函数F_{182}与SIMECK类轮函数F_{051}的相关优势计数表。

表 1　$F_{abc}(x)$**相关优势计数表**

	$\lvert\rho\rvert$						
	0	1	1/2	1/4	1/8	1/16	1/32
F_{182}^{8}	48255	1	64	1280	8256	7680	0
F_{051}^{8}	48255	1	64	1280	8256	7680	0
F_{182}^{9}	207863	1	72	1728	15360	37120	0
F_{051}^{9}	207863	1	72	1728	15360	37120	0

实验数据表明，其相关优势情况均符合定理1，定理4与定理6(当n=8时，最小非平凡相关优势点的个数为$\left(2^{8/2+1}-2\right)\times 2^{8}=7680$)。由定理1可知，$F_{182}$与$F_{051}$可以取到的相关优势的取值范围是相同的。由表1可知，F_{182}与F_{051}的各个相关优势点分布情况相同，因此可以认为两者的线性分布均匀程度基本相同。

4　结束语

文献[5]仅给出了SIMON类轮函数的线性逼近式的2次项相互独立时的线性性质，然而2次项相关时的线性性质还未彻底解决。本文进一步研究了移位参数一般化下SIMON类算法轮函数的线性性质，利用算法1将相关优势取值问题转化为不相交2次型中2次项的个数问题，界定了相关优势的取值范围，证明了在特定条件下对于该范围内的每一个相关优势点均可找到对应的掩码对，证明了此类函数是多输出部分bent函数，给出了非平凡相关优势取到最大值1/2时掩码对的充要条件及计数，给出了特定条件下非平凡相关优势取到最小值的充分条件与掩码对的计数。研究表明，当n为偶数且t为奇数时，可以取到最小非平凡相关优势点。该研究成果为SIMON与SIMECK等算法的线性分析提供了理论基础。接下来需要做的工作是给出此类函数移位参数抵抗各类密码分析方法的选取准则，并应用于SIMON与SIMECK等算法的线性安全性分析。

5　附录

子程序1(PickIndex)给定2次布尔函数$f(x_1,x_2,\cdots,x_n)$，PickIndex(f)返回t，其中$t\in\{1,2,\cdots,n\}$是使得$\sigma(f,x_t)\geq\sigma(f,x_{t'}),\forall t'\in\{1,2,\cdots,n\}$成立的最小整数。

子程序2(Substitute)给定2次布尔函数$f(x)=f(x_1,x_2,\cdots,x_n)$，$\boldsymbol{M}$是一个$n\times n$的可逆矩阵，Substitute$(f,\boldsymbol{M})$返回布尔函数$f(x\boldsymbol{M})$。

不相交化算法[12]如表2所示。

表 2　**转变成不相交2次型算法(算法1)**

输入：2次型布尔函数$f(x)=f(x_1,x_2,\cdots,x_n)$

输出：可逆矩阵$\boldsymbol{M}$，不相交二次型$\hat{f}(x)$使得$\hat{f}(x)=f(x\boldsymbol{M})$

(1)　/*初始化*/

(2)　$\boldsymbol{M}\leftarrow\boldsymbol{I}$　　/*$\boldsymbol{I}$是$n\times n$的可逆矩阵*/

(3)　$\hat{f}(x)\leftarrow f(x_1,x_2,\cdots,x_n)$

(4)　$v\leftarrow$ PickIndex$\left(\hat{f}\right)$

(5)　/*不相交化*/

(6)　当$\sigma\left(\hat{f},x_v\right)\geq 2$时，执行

(7)　　$m\leftarrow\sigma\left(\hat{f},x_v\right)$　　/*$\hat{f}$中包含x_v的2次项个数*/

(8)　　在$\hat{f}$中找出所有的2次项$x_vx_{t_i}$满足$t_1<t_2<\cdots<t_m$

(9)　　$\hat{f}\leftarrow$ Substitute$\left(\hat{f},\boldsymbol{I}_{t_1\leftarrow t_1,t_2,\cdots,t_m}\right)$

(10)　　$\boldsymbol{M}\leftarrow\boldsymbol{I}_{t_1\leftarrow t_1,t_2,\cdots,t_m}\cdot\boldsymbol{M}$

(11)　　如果$\sigma\left(\hat{f},x_{t_1}\right)\geq 2$，执行

(12)　　　$k\leftarrow\sigma\left(\hat{f},x_{t_1}\right)$

(13)　　　在$\hat{f}$中找出所有的2次项$x_{t_1}x_{s_i}$满足$s_1<s_2<\cdots<s_m$，

续表2

(14) $\hat{f} \leftarrow \text{Substitute}\left(\hat{f}, \boldsymbol{I}_{v\leftarrow s_1,s_2,\cdots,s_k}\right)$

(15) $\boldsymbol{M} \leftarrow \boldsymbol{I}_{v\leftarrow s_1,s_2,\cdots,s_k} \cdot \boldsymbol{M}$

(16) 结束

(17) $v \leftarrow \text{PickIndex}\left(\hat{f}\right)$

(18) 结束

(19) 返回$\boldsymbol{M}$和$\hat{f}$

参 考 文 献

[1] BEAULIEU R, SHORS D, SMITH J, *et al*. The SIMON and SPECK lightweight block ciphers[C]. The 52nd Annual Design Automation Conference. San Francisco, USA, 2015: 1-6.

[2] WANG N, WANG X, JIA K, *et al*. Diffffferential attacks on reduced SIMON versions with dynamic key-guessing techniques[J]. *IACR Cryptology ePrint Archive*, 2014: 2014/448.

[3] 董向忠, 关杰. SIMON类算法轮函数的差分性质分析[J]. 密码学报, 2015, 2(3): 207–216. doi: 10.13868/j.cnki.jcr.000072.
DONG Xiangzhong, GUAN Jie. Analysis on diffffferential properties of the round function of SIMON family of block ciphers[J]. *Journal of Cryptologic Research*, 2015, 2(3): 207–216. doi: 10.13868/j.cnki.jcr.000072.

[4] SEYED MOJTABA DEHNAVI. Further Observations on SIMON and SPECK Block Cipher Families[J]. *Cryptography*, 2018, 3(1): 1. doi: 10.3390/cryptography3010001.

[5] 董向忠, 关杰. SIMON类算法轮函数的线性性质[J]. 山东大学学报(理学版), 2015, 50(9): 49–54.
DONG Xiangzhong, GUAN Jie. Linear properties of the round function of SIMON family of block ciphers[J]. 山东大学学报, 2015, 50(9): 49–54.

[6] ABDELRAHEEM N A, ALIZADEH J, ALKHZAIMI H A, *et al*. Improved linear cryptanalysis of reduced-round SIMON[EB/OL]. https://eprint.iacr.org/2014/681, 2014.

[7] CHEN H, WANG X. Improved linear hull attack on round-reduced SIMON with dynamic key-guessing techniques[C]. Fast Software Encryption—FSE 2016. Berlin, Germany, 2016: 428–449. doi: 10.1007/978-3-662-52993-5_22.

[8] SHI Danping, HU Lei, SUN Siwei, *et al*. Improved linear(hull) cryptanalysis of round-reduced versions of SIMON[J]. Science China (Information Sciences) 60.03(2017): 223–225. doi: 10.1007/s11432-015-0007-1.

[9] REHAM A and POORVI L. V linear cryptanalysis of reduced-round simon using super rounds[J]. *Cryptography*, 2020, 4(1): 9. doi: 10.3390/cryptography4010009.

[10] BOURA C, NAYA-PLASENCIA M, and SUDER V. Scrutinizing and improving impossible differential attacks: Applications to CLEFIA, Camellia, LBlock and Simon[C]. The 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, China, 2014: 179–199.

[11] 陈展, 王宁. SIMON算法的不可能差分分析[J]. 密码学报, 2015, 2(6): 505–514. doi: 10.13868/j.cnki.jcr.000097.
CHEN Zhan and WANG Ning. Impossible diffffferential cryptanalysis of reduced-round SIMON[J]. *Journal of Cryptologic Research*, 2015, 2(6): 505–514. doi: 10.13868/j.cnki.jcr.000097.

[12] KONDO K, SASAKI Y, TODO Y, *et al*. On the design rationale of SIMON block cipher: Integral attacks and impossible differential attacksagainst SIMON variants[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 2018, 101(1): 88–98.

[13] YU Xiaoli, WU Wenling, SHI Zhenqing, *et al*. Zero correlation linear cryptanalysis of reduced-round SIMON[J]. *Journal of Computer Science and Technology*, 2015, 30(6): 1358–1369. doi: 10.1007/s11390-015-1603-5.

[14] SUN L, FU K, and WANG M. Improved zero-correlation cryptanalysis on SIMON[C]. Information Security and Cryptology—INSCRYPT 2015. Beijing, China, 2015: 125–143.

[15] ZHANG Kai, Guanjie, HU Bin, *et al*. Security evaluation on Simeck against zero-correlation linear cryptanalysis[C]. IET Information Security, 2018, 12(1): 87–93. doi: 10.1049/iet-ifs.2016.0503.

[16] FU Kai, SUN Ling, and WANG Meiqin. New integral attacks on SIMON[J]. *IET Information Security*, 2017, 11(5): 277–286. doi: 10.1049/iet-ifs.2016.0241.

[17] CHU Zhihui, CHEN Huaifeng, WANG Xiaoyun, *et al*. Improved integral attacks on SIMON32 and SIMON48 with dynamic key-guessing techniques[J]. *Security and Communication Networks*, 2018: 5160237. doi: 10.1155/2018/5160237.

[18] YANG G, ZHU B, SUDER V, *et al*. The Simeck Family of Lightweight Block Ciphers[C]. Güneysu T, Handschuh H. (eds) Cryptographic Hardware and Embedded Systems, CHES 2015. Lecture Notes in Computer Science, vol 9293. Springer, Berlin, Germany, https://doi.org/10.1007/978-3-662-48324-4_16.

[19] SHI D, SUN S, SASAKI Y, *et al*. Correlation of Quadratic Boolean Functions: Cryptanalysis of All Versions of Full MORUS[M]. Advances in Cryptology–CRYPTO, 2019.

[20] 鞠桂枝, 赵亚群. 多输出部分Bent函数若干性质的研究[J]. 工程数学学报, 2005(6): 183–186.

关 杰：女，1974年生，教授，博士生导师，研究方向为密码理论和密码算法分析.

卢健伟：男，1997年生，硕士生，研究方向为对称密码设计与分析.

责任编辑：余 蓉