Keccak类S盒的线性性质研究

关 杰 黄俊君*

(战略支援部队信息工程大学 郑州 450001)

摘 要：该文将Keccak的S盒一般化为n元Keccak类S盒，研究了Keccak类S盒的线性性质。证明了这类S盒的相关优势的取值都为0或2^{-k}，其中$k \in Z$且$0 \le k \le \lfloor 2^{-1}n \rfloor$，并且对于此范围内的任意$k$，都存在输入输出掩码使得相关优势取到$2^{-k}$；证明了当输出掩码确定时，其非平凡相关优势都相等；给出了非平凡相关优势为最大值2^{-1}时的充要条件与计数，解决了这类S盒的Walsh谱分布规律问题。

关键词：哈希函数；Keccak；S盒；线性性质

中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2020)07-1790-06

DOI: 10.11999/JEIT190570

Research on Linear Properties of Keccak-like S-box

GUAN Jie HUANG Junjun

(*PLA SSF Information Engineering University, Zhengzhou* 450001, *China*)

Abstract: In this paper, the S-box of Keccak is generalized into n-variable Keccak-like S-box, and the linear properties of n-variable Keccak-like S-box is studied. It is proved that all the values of correlation advantages of this kind of S-box are 0 or 2^{-k}, where $k \in Z$ and $0 \le k \le \lfloor 2^{-1}n \rfloor$, and for any k in this range, there is an input mask and an output mask that make the correlation advantage be 2^{-k}. Furthermore, it is proved that when the output mask is fixed, the values of the nontrivial correlation advantages of the S-box are determined. Then, the necessary and sufficient condition are given when the count for the nontrivial correlation advantage is the maximum value 2^{-1}. Finally, the value distribution of the Walsh spectrum of Keccak-like S-box is presented.

Key words: Hash function; Keccak; S-box; Linear properties

1 引言

Keccak[1]是美国国家标准与技术协会(NIST)公布的新一代哈希函数标准SHA-3[2]的获胜算法,其轻量级及高效性使其有众多应用场景[3]。对Keccak的结构进行系统研究与深入挖掘可以进一步理解其设计思想，把握Keccak的密码学性质，具有重要的理论价值。通过立方攻击及其变式对缩减轮速的Keccak的分析也是目前的研究热点[4]。

Keccak中唯一的非线性变换是χ变换，其非线性环节本质上是一个5进5出的S盒。许多其他密码算法也用到了这类S盒，例如通过对Keccak的χ变换进行改造，文献[5]提出一种新的3进3出的S盒，文献[6]采用了类似的17进17出S盒，文献[7]也使用了这类19进19出的S盒。通过将这类S盒一般化为n元Keccak类S盒并研究其密码学性质可以有效评估该编码环节的安全强度，有助于加强对该编码环节的认识与把握。

元胞自动机在密码学中有许多的应用，由于其能够从简单的规则中产生复杂、随机的模式，通过一定的组合可以实现分组密码的混淆盒扩散[8]，也可以构造成伪随机数生成器[9]。类似Keccak的S盒也被叫做基于元胞自动机的S盒[10,11]，由于其良好的密码学性质及较低的实现代价已经被广泛应用到许多密码算法中。通过PEIGEN平台[12]可以找到满足设计者需求的S盒，而寻找轻量级及密码学性质良好的基于元胞自动机的S盒[13,14]可以为密码设计者在不同的应用场景提供更多的参考。通过研究n元Keccak类S盒也有助于增加对基于元胞自动机的S盒的认识，为研究其他类似的S盒的密码学性质提供解决思路和方法。

文献[15]对n元Keccak类S盒的差分性质进行了研究，基本上解决了Keccak类S盒的差分性质问

收稿日期：2019-07-29；改回日期：2020-04-19；网络出版：2020-04-29
*通信作者： 黄俊君 hjj7752@outlook.com
基金项目：国家自然科学基金(61572516, 61272041, 61272488)
Foundation Items: The National Natural Science Foundation of China (61572516, 61272041, 61272488)

题。文献[16]中对n元Keccak类S盒的线性性质进行分析仅得到其最大非平凡相关优势。本文解决了n元Keccak类S盒的Walsh谱分布规律问题。

2　基本概念

定义1[15]　设$F^n: Z_2^n \to Z_2^n$, $X=(x_0,x_1,\cdots,x_{n-1}), Y=(y_0,y_1,\cdots,y_{n-1}) \in Z_2^n$，那么Keccak的$\chi$变换即为$f(x_0,x_1,x_2)=x_0\oplus x_1x_2\oplus x_2$，若$F^n$满足：$y_i=x_i\oplus x_{i+1}x_{i+2}\oplus x_{i+2}$, $0\le i<n$, $n\ge 3$，则称F^n为n元Keccak类S盒。注意上式的下标运算在模n上进行。

定义2[17]　设$F^n: Z_2^n \to Z_2^n$, $f: Z_2^n \to Z_2$, $X,\eta,\mu,w\in Z_2^n$，那么称$\rho_F(\eta\to\mu)=W_{(F)}(\eta\to\mu)=\frac{1}{2^n}\sum_{X\in Z_2^n}(-1)^{\eta\cdot X\oplus\mu\cdot F(X)}$为$F$在$(\eta,\mu)$点的Walsh谱。称$\eta$为输入掩码，$\mu$为输出掩码，并称$\eta\to\mu$为$F$的一个线性逼近，$|\rho_F(\eta\to\mu)|$为该线性逼近的相关优势。称$\rho_f(w)=W_{(f)}(w)=\frac{1}{2^n}\sum_{X\in Z_2^n}(-1)^{f(X)\oplus w\cdot X}$为$f$在$w$点的Walsh谱，$|\rho_f(w)|$为$f$与线性组合$w\cdot X$的相关优势。

对于$f: Z_2^n \to Z_2^n$, $X=(x_0,x_1,\cdots,x_{n-1})\in Z_2^n$，记$p(f(X)=0)=\frac{1}{2^n}\#\{X\in Z_2^n: f(X)=0\}$。若$X'=(x'_0,x'_1,\cdots,x'_{n-1})\in Z_2^n$为一个定值，则记

$$\begin{aligned}&p\left(f(X)=0\middle|\left(x_{i_0},x_{i_1},\cdots,x_{i_{k-1}}\right)\right.\\&=\left.\left(x'_{i_0},x'_{i_1},\cdots,x'_{i_{k-1}}\right)\right)\\&=\frac{1}{2^{n-k}}\#\{X\in Z_2^n: f(X)\\&=0,\left(x_{i_0},x_{i_1},\cdots,x_{i_{k-1}}\right)=\left(x'_{i_0},x'_{i_1},\cdots,x'_{i_{k-1}}\right)\}\end{aligned}\tag{1}$$

其中，$0\le i_0<i_1<i_2<\cdots<i_{k-1}\le n-1$且都为整数，$0\le k\le n$。另外，记$f\left|_{\left(x_{i_0},x_{i_1},\cdots,x_{i_{k-1}}\right)}\right.: Z_2^{n-k}\to Z_2$为当$f$的输入中的分量$(x_{i_0},x_{i_1},\cdots,x_{i_{k-1}})$取作定值时的一个布尔函数。

定义3[17]　设$f: Z_2^n\to Z_2$, $X\in Z_2^n$，若有$p(f(X)=0)=p(f(X)=1)=1/2$，称$f(X)$是平衡函数。

引理1描述了平衡函数的Walsh谱特征，并给出计算$f(X)$在0点的Walsh谱的方法。引理2是布尔函数相关优势的能量守恒性质，说明了任一布尔函数$f(X)$与所有线性组合$w\cdot X$的相关优势平方和恒为1。

引理1[17]　设$f: Z_2^n\to Z_2$, $X\in Z_2^n$则有：$\rho_f(0)=2p(f(X)=0)-1=p(f(X)=0)-p(f(X)=1)$。而$f$是平衡函数的充要条件是$\rho_f(0)=W_{(f)}(0)=0$。

引理2[17]　设$f: Z_2^n\to Z_2$是布尔函数，则有：$\sum_{w\in Z_2^n}[\rho_f(w)]^2=1$。

3　Keccak类S盒的线性性质分析

在本节，将n元Keccak类S盒记为F^n，其输入和输出分别为$X=(x_0,x_1,\cdots,x_{n-1})$, $Y=(y_0,y_1,\cdots,y_{n-1})\in Z_2^n$且$n\ge 3$，由定义1知$y_i=x_i\oplus x_{i+1}x_{i+2}\oplus x_{i+2}$，注意$i\in\{0,1,\cdots,n-1\}$且所有下标运算均在模$n$上进行。由Walsh谱的定义易得

$$\begin{aligned}\rho_{F^n}(\eta\to\mu)&=\frac{1}{2^n}\sum_{X\in Z_2^n}(-1)^{\eta\cdot X\oplus\mu\cdot Y}\\&=\frac{1}{2^n}\sum_{X\in Z_2^n}(-1)^{\bigoplus_{i=0}^{n-1}[(\eta_i\oplus\mu_i\oplus\mu_{i+3})x_i\oplus\mu_ix_{i+1}x_{i+2}]}\end{aligned}\tag{2}$$

下面本文将$\oplus_{i=0}^{n-1}[(\eta_i\oplus\mu_i\oplus\mu_{i+3})x_i\oplus\mu_ix_{i+1}x_{i+2}]$记为$f^*_{\eta,\mu}: Z_2^n\to Z_2$，那么由定义2即知$\rho_{F^n}(\eta\to\mu)=\rho_{f^*_{\eta,\mu}}(0)$。

引理3　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

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

那么$\rho_f(0)=0$。

如果一个布尔函数满足引理3的条件，即说明该布尔函数的结构中存在独立的线性变量，显然这个布尔函数必然平衡。通过引理3可以容易地得到定理1，即对于Keccak类S盒的Walsh谱，给出了其满足引理3条件时η,μ的结构，即给出了0点谱值对应的η,μ的一个充分条件。

定理1　对于$\eta,\mu\in Z_2^n$，若存在$0\le i_0\le n-1$使得$\eta_{i_0}\oplus\mu_{i_0}\oplus\mu_{i_0+3}=1$且$\mu_{i_0-2}=0$，$\mu_{i_0-1}=0$，那么$\rho_{F^n}(\eta\to\mu)=0$。

设$w(\mu)$为μ的汉明重量，通过定理1容易得到Keccak类S盒在$w(\mu)=0$时相关优势取0和1时的充分必要条件，即推论1。

推论1　$\forall\eta\in Z_2^n$且$n\ge 3$，当$w(\mu)=0$时，有以下结论成立：

(1) 若$\eta\ne 0$，则$|\rho_{F^n}(\eta\to\mu)|=0$；

(2) 若$\eta=0$，则$|\rho_{F^n}(\eta\to\mu)|=1$。

设$\boldsymbol{\alpha}=(\alpha_0,\alpha_1,\cdots,\alpha_{m-1})\in Z_2^m$，$m\in Z^+$，那么记$\overline{\boldsymbol{\alpha}}=(\alpha_0\oplus 1,\alpha_1\oplus 1,\cdots,\alpha_{m-1}\oplus 1)$，称$\overline{\boldsymbol{\alpha}}$为$\boldsymbol{\alpha}$的补。

引理4　设$n\ge 3$，$\eta\in Z_2^n$，$w(\mu)=n$，

$$\boldsymbol{\alpha}=\begin{cases}\left(\bigoplus_{i=1}^{(n-3)/2}\eta_{2i+1},\bigoplus_{i=2}^{(n-3)/2}\eta_{2i+1},\cdots,\eta_{n-2}\right)\in Z_2^{(n-1)/2},\\ n\text{为奇数}\\ \left(\bigoplus_{i=1}^{(n-2)/2}\eta_{2i},\bigoplus_{i=2}^{(n-2)/2}\eta_{2i},\cdots,\eta_{n-2}\right)\in Z_2^{(n-2)/2},\\ n\text{为偶数}\end{cases}$$

($n=3$时取$\boldsymbol{\alpha}=(\eta_{n-2})$)。那么当$n$为奇数时，若$(x_2,x_4,\cdots,x_{n-1})\ne\boldsymbol{\alpha}$和$\overline{\boldsymbol{\alpha}}$，则$\rho_{f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})}\right.}(0)$

$=0$；当n为偶数时，若$(x_3,x_5,\cdots,x_{n-1})\neq\boldsymbol{\alpha}$和$\overline{\boldsymbol{\alpha}}$，则$\rho_{f^*_{\eta,\mu}\left|_{(x_3,x_5,\cdots,x_{n-1})}\right.}(0)=0$。

证 明 由于$w(\mu)=n$，那么$f^*_{\eta,\mu}=\oplus_{i=0}^{n-1}(x_ix_{i+1}\oplus\eta_ix_i)$。考虑$n$为奇数时，当$f^*_{\eta,\mu}$的输入中有分量$(x_2,x_4,\cdots,x_{n-1})$确定为定值$(x'_2,x'_4,\cdots,x'_{n-1})$时有

$$\begin{aligned}f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})}\right.&=x_0x_1\oplus(\eta_2x'_2\oplus\eta_4x'_4\oplus\cdots\\&\oplus\eta_{n-1}x'_{n-1})\oplus((\eta_0\oplus x'_{n-1})x_0\oplus(\eta_1\oplus x'_2)x_1\oplus\cdots\\&\oplus(\eta_3\oplus x'_2\oplus x'_4)x_3\oplus\cdots\\&\oplus(\eta_{n-2}\oplus x'_{n-3}\oplus x'_{n-1})x_{n-2})\end{aligned}\tag{4}$$

观察式(4)可知，$f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})}\right.$2次项部分为$x_0x_1$，常数部分为$(\eta_2x'_2\oplus\eta_4x'_4\oplus\cdots\oplus\eta_{n-1}x'_{n-1})$，剩余的为线性部分。假设其线性部分$x_i,i\geq3$的系数都为0，那么

$$\begin{cases}\eta_3\oplus x'_2\oplus x'_4=0\\\eta_5\oplus x'_4\oplus x'_6=0\\\vdots\\\eta_{n-4}\oplus x'_{n-5}\oplus x'_{n-3}=0\\\eta_{n-2}\oplus x'_{n-3}\oplus x'_{n-1}=0\end{cases}$$

$$\Rightarrow\begin{cases}x'_2=\eta_3\oplus\eta_5\oplus\cdots\oplus\eta_{n-2}\oplus x'_{n-1}\\x'_4=\eta_5\oplus\eta_7\oplus\cdots\oplus\eta_{n-2}\oplus x'_{n-1}\\\vdots\\x'_{n-5}=\eta_{n-4}\oplus\eta_{n-2}\oplus x'_{n-1}\\x'_{n-3}=\eta_{n-2}\oplus x'_{n-1}\end{cases}\tag{5}$$

所以当$x'_{n-1}=0$时，有$(x'_2,x'_4,\cdots,x'_{n-1})=\left(\oplus_{i=1}^{(n-3)/2}\eta_{2i+1},\oplus_{i=2}^{(n-3)/2}\eta_{2i+1},\cdots,\eta_{n-2}\right)=\boldsymbol{\alpha}$；当$x'_{n-1}=1$时，则有$(x'_2,x'_4,\cdots,x'_{n-1})=\left(\oplus_{i=1}^{(n-3)/2}\eta_{2i+1}\oplus1,\oplus_{i=2}^{(n-3)/2}\eta_{2i+1}\oplus1,\cdots,\eta_{n-2}\oplus1\right)=\overline{\boldsymbol{\alpha}}$。如果$(x_2,x_4,\cdots,x_{n-1})\neq\boldsymbol{\alpha}$和$\overline{\boldsymbol{\alpha}}$，说明其至少存在一个线性项$x_i,i\geq3$的系数不为0，那么$f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})}\right.$满足引理3的条件，有$\rho_{f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})}\right.}(0)=0$。而$n$为偶数时可以类似证明。 证毕

引理5 设$X=(x_0,x_1,\cdots,x_{n-1},x_n)\in Z_2^{n+1}$，$f(X)=\oplus_{i=0}^{n-1}x_ix_{i+1}\oplus L(X)$，其中$L(X)=\oplus_{i=0}^{n}k_ix_i$，$k_i\in\{0,1\}$，则当$n=1,2$时，对任意$L(X)$，$f(X)$与$f(X)\oplus x_0\oplus x_n$有相同的平衡性。

引理5仅需穷举$n=1,2$时$f(X)$与$f(X)\oplus x_0\oplus x_n$在0点的Walsh谱值即可证明。接下来通过引理4和引理5可以进一步证得定理2，给出了Keccak类S盒在$w(\mu)=n$时其非平凡相关优势的取值。

定理2 对于$F^n,\forall\eta$及$n\geq3$，若$w(\mu)=n$，则$|\rho_{F^n}(\eta\to\mu)|=0$或$1/2^{\left\lfloor\frac{n-1}{2}\right\rfloor}$。

证明 设$X\in Z_2^n$，若$w(\mu)=n$且n为奇数(n为偶数时可类似证得)，则$f^*_{\eta,\mu}=\oplus_{i=0}^{n-1}[\eta_ix_i\oplus x_{i+1}x_{i+2}]$。由Walsh谱的定义及引理1有

$$\begin{aligned}\rho_{F^n}(\eta\to\mu)&=\rho_{f^*_{\eta,\mu}}(0)=p\left(f^*_{\eta,\mu}(X)=0\right)\\&\quad-p\left(f^*_{\eta,\mu}(X)=1\right)\\&=\sum_{a\in\{0,1\}}\frac{1}{2}\left[p\left(f^*_{\eta,\mu}(X)=0\mid x_{n-1}=a\right)\right.\\&\quad\left.-p\left(f^*_{\eta,\mu}(X)=1\mid x_{n-1}=a\right)\right]\\&=\frac{1}{2}\sum_{a\in\{0,1\}}\left[\frac{1}{2^{n-1}}\#\left\{X\in Z_2^n:f^*_{\eta,\mu}(X)=0,\right.\right.\\&\quad\left.x_{n-1}=a\right\}-\frac{1}{2^{n-1}}\#\{X\in Z_2^n:\\&\quad\left.\left.f^*_{\eta,\mu}(X)=1,x_{n-1}=a\right\}\right]\\&=\frac{1}{2}\left(\rho_{f^*_{\eta,\mu}|_{x_{n-1}=0}}(0)+\rho_{f^*_{\eta,\mu}|_{x_{n-1}=1}}(0)\right)\\&=\frac{1}{2^2}\left(\rho_{f^*_{\eta,\mu}\left|_{(x_{n-3},x_{n-1})=(0,0)}\right.}(0)\right.\\&\quad+\rho_{f^*_{\eta,\mu}\left|_{(x_{n-3},x_{n-1})=(0,1)}\right.}(0)\\&\quad+\rho_{f^*_{\eta,\mu}\left|_{(x_{n-3},x_{n-1})=(1,0)}\right.}(0)\\&\quad\left.+\rho_{f^*_{\eta,\mu}\left|_{(x_{n-3},x_{n-1})=(1,1)}\right.}(0)\right)\end{aligned}\tag{6}$$

继续按照这样的方法分解直到

$$\begin{aligned}\rho_{F^n}(\eta\to\mu)&=\frac{1}{2^{\frac{n-1}{2}}}\sum_{(x_2,x_4,\cdots,x_{n-1})\in Z_2^{(n-1)/2}}\\&\quad\cdot\rho_{f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})}\right.}(0)\\&=\frac{1}{2^{\frac{n-1}{2}}}\left(\rho_{f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})=\boldsymbol{\alpha}}\right.}(0)\right.\\&\quad+\rho_{f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})=\overline{\boldsymbol{\alpha}}}\right.}(0)\\&\quad+\sum_{(x_2,x_4,\cdots,x_{n-1})\neq\boldsymbol{\alpha},\overline{\boldsymbol{\alpha}}}\\&\quad\left.\cdot\rho_{f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})}\right.}(0)\right)\end{aligned}\tag{7}$$

由引理4可知，若$(x_2,x_4,\cdots,x_{n-1})\neq\boldsymbol{\alpha}$和$\overline{\boldsymbol{\alpha}}$，则$\rho_{f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})}\right.}(0)=0$，所以此时有

$$\begin{aligned}\rho_{F^n}(\eta\to\mu)&=\frac{1}{2^{\frac{n-1}{2}}}\left(\rho_{f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})=\boldsymbol{\alpha}}\right.}(0)\right.\\&\quad\left.+\rho_{f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})=\overline{\boldsymbol{\alpha}}}\right.}(0)\right)\end{aligned}\tag{8}$$

又根据引理4中的式(4)，将$\boldsymbol{\alpha}$与$\overline{\boldsymbol{\alpha}}$代入有

$$\left.\begin{aligned}f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})=\boldsymbol{\alpha}}\right.&=x_0x_1\oplus\eta_0x_0\\&\oplus\left(\mathop{\oplus}_{i=0}^{(n-3)/2}\eta_{2i+1}\right)x_1\oplus K_1\\f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})=\overline{\boldsymbol{\alpha}}}\right.&=f^*_{\eta,\mu}\left|_{(x_2,x_4,\cdots,x_{n-1})=\boldsymbol{\alpha}}\right.\\&\oplus x_0\oplus x_1\oplus K_2\end{aligned}\right\}\tag{9}$$

其中，K_1和K_2表示常数部分，不影响布尔函数的平衡性。所以根据引理5，$f^*_{\eta,\mu}\big|_{(x_2,x_4,\cdots,x_{n-1})=\boldsymbol{\alpha}}$与$f^*_{\eta,\mu}\big|_{(x_2,x_4,\cdots,x_{n-1})=\overline{\boldsymbol{\alpha}}}$有相同的平衡性，因此两式同为0或同不为0，那么$|\rho_{F^n}(\eta\to\mu)|=0$或$1/2^{\frac{n-1}{2}}$。证毕

引理6　设$n\ge 2$，$\forall(k_0,\cdots,k_{n-1})\in Z_2^n$，$X=(x_0,\cdots,x_{n-1})\in Z_2^n$，$f(X)=\oplus_{i=0}^{n-2}(x_ix_{i+1}\oplus k_ix_i)\oplus k_{n-1}x_{n-1}$，那么$|\rho_f(0)|=0$ 或$1/2^{\lfloor\frac{n}{2}\rfloor}$。

证明　这里不妨设n为奇数，类似定理2的证明有：

$$\begin{aligned}\rho_f(0)&=\frac{1}{2}\left(\rho_f\big|_{x_{n-2}=0}(0)+\rho_f\big|_{x_{n-2}=1}(0)\right)=\cdots\\&=\frac{1}{2^{\frac{n}{2}-1}}\sum_{(x_2,x_4,\cdots,x_{n-2})\in Z_2^{(n-2)/2}}\rho_f\big|_{(x_2,x_4,\cdots,x_{n-2})}(0)\end{aligned}\tag{10}$$

记$\boldsymbol{\beta}=\left(\oplus_{i=1}^{(n-2)/2}k_{2i+1},\oplus_{i=2}^{(n-2)/2}k_{2i+1},\cdots,k_{n-1}\right)$（注意$n=2$时取$\boldsymbol{\beta}=(k_{n-1})$），设$(x_2,x_4,\cdots,x_{n-2})=(x'_2,x'_4,\cdots,x'_{n-2})$时，那么$f\big|_{(x_2,x_4,\cdots,x_{n-2})}$的线性部分为

$$\begin{aligned}&(k_0x_0\oplus(k_1\oplus x'_2)x_1\oplus(k_3\oplus x'_2\oplus x'_4)x_3\oplus\cdots\\&\oplus(k_{n-1}\oplus x'_{n-2})x_{n-1})\end{aligned}\tag{11}$$

假设$x_i,i\ge 3$的系数都为0，可得$(x_2,x_4,\cdots,x_{n-2})=\boldsymbol{\beta}$。那么当$(x_2,x_4,\cdots,x_{n-2})\ne\boldsymbol{\beta}$时，$f\big|_{(x_2,x_4,\cdots,x_{n-2})}$满足引理3的条件，则$\rho_{f\big|_{(x_2,x_4,\cdots,x_{n-2})}}(0)=0$。同理$n$为奇数时类似得当$(x_3,x_5,\cdots,x_{n-2})\ne\boldsymbol{\beta}$时，$\rho_{f\big|_{(x_3,x_5,\cdots,x_{n-2})}}(0)=0$。又由引理5易知$\rho_{f\big|_{(x_3,x_5,\cdots,x_{n-2})=\beta}}(0)=0$或$\pm1/2$而$\rho_{f\big|_{(x_2,x_4,\cdots,x_{n-2})=\boldsymbol{\beta}}}(0)=\pm1/2$。

所以

$$\begin{aligned}\rho_f(0)&=\begin{cases}\dfrac{1}{2^{\frac{n-3}{2}}}\rho_{f\big|_{(x_3,x_5,\cdots,x_{n-2})=\beta}}(0)&,n=2l-1\\[2mm]\dfrac{1}{2^{\frac{n}{2}-1}}\rho_{f\big|_{(x_2,x_4,\cdots,x_{n-2})=\beta}}(0)&,n=2l-2\end{cases}\\&=\begin{cases}\pm\dfrac{1}{2^{\frac{n-1}{2}}}\text{或}0,n=2l-1\\[2mm]\pm\dfrac{1}{2^{\frac{n}{2}}},n=2l-2\end{cases}\end{aligned}\tag{12}$$

其中，$l\ge 2$且$l\in Z$。因此$|\rho_f(0)|=0$或$1/2^{\lfloor\frac{n}{2}\rfloor}$。证毕

引理7　设$n\ge 3$，$\alpha_2,\alpha_3,\cdots,\alpha_n$均取非负整数，那么若$2\le 2\cdot\alpha_2+3\cdot\alpha_3+\cdots+n\cdot\alpha_n\le n$，则必有$\lfloor 2/2\rfloor\cdot\alpha_2+\lfloor 3/2\rfloor\cdot\alpha_3+\cdots+\lfloor n/2\rfloor\cdot\alpha_n\in[1,\lfloor n/2\rfloor]$且能取到$[1,\lfloor n/2\rfloor]$中所有整数。

引理7不难证明，考察了$\lfloor 2/2\rfloor\cdot\alpha_2+\lfloor 3/2\rfloor\cdot\alpha_3+\cdots+\lfloor n/2\rfloor\cdot\alpha_n$的取值范围，将在下面定理3证明中引用。

定理3　对于F^n，$\forall\eta$及$n\ge 3$，若$1\le w(\mu)\le n-1$，则$|\rho_{F^n}(\eta\to\mu)|=0$ 或$1/2^k$，$k\in Z$且$1\le k\le\lfloor n/2\rfloor$，并且对于任意$k$，必存在$\eta,\mu\in Z_2^n$使得$|\rho_{F^n}(\eta\to\mu)|=1/2^k$。

证明　当$1\le w(\mu)\le n-1$时，假设$f^*_{\eta,\mu}$不满足引理3条件，那么

$$\begin{aligned}f^*_{\eta,\mu}(X)=&\left[\bigoplus_{i=i_1}^{i'_1}(x_ix_{i+1}\oplus k_ix_i)\oplus k_{i'_1+1}x_{i'_1+1}\right]\\&\oplus\left[\bigoplus_{i=i_2}^{i'_2}(x_ix_{i+1}\oplus k_ix_i)\oplus k_{i'_2+1}x_{i'_2+1}\right]\\&\oplus\cdots\oplus\left[\bigoplus_{i=i_j}^{i'_j}(x_ix_{i+1}\oplus k_ix_i)\oplus k_{i'_j+1}x_{i'_j+1}\right]\\\overset{\text{记作}}{=}&f_1^*(x_{i_1},\cdots,x_{i'_1+1})\\&\oplus f_2^*(x_{i_2},\cdots,x_{i'_2+1})\oplus\cdots\\&\oplus f_j^*(x_{i_j},\cdots,x_{i'_j+1})\end{aligned}\tag{13}$$

其中，对$\forall i$，$k_i\in\{0,1\}$，且$0\le i_1\le i'_1<i_2-1,i_2\le i'_2<i_3-1,\cdots,i_{j-1}\le i'_{j-1}<i_j-1,i_j\le i'_j\le n-1$，$1\le j\le\left\lfloor\dfrac{n}{2}\right\rfloor$，所以$f_1^*,f_2^*,\cdots,f_j^*$是相互独立的。因此有

$$\begin{aligned}&\rho_{F^n}(\eta\to\mu)=\rho_{f^*_{\eta,\mu}}(0)\\&=\frac{1}{2^n}\sum_{X\in Z_2^n}(-1)^{f^*_{\eta,\mu}(X)}=\frac{1}{2^n}\sum_{X\in Z_2^n}\\&(-1)^{f_1^*(x_{i_1},\cdots,x_{i'_1+1})\oplus f_2^*(x_{i_2},\cdots,x_{i'_2+1})\oplus\cdots\oplus f_j^*(x_{i_j},\cdots,x_{i'_j+1})}\\&=\left[\frac{1}{2^{i'_1-i_1+2}}\sum_{(x_{i_1},\cdots,x_{i'_1+1})\in Z_2^{i'_1-i_1+2}}(-1)^{f_1^*(x_{i_1},\cdots,x_{i'_1+1})}\right]\\&\cdots\left[\frac{1}{2^{i'_j-i_j+2}}\sum_{(x_{i_j},\cdots,x_{i'_j+1})\in Z_2^{i'_j-i_j+2}}(-1)^{f_j^*(x_{i_j},\cdots,x_{i'_j+1})}\right]\\&=\rho_{f_1^*}(0)\cdots\rho_{f_j^*}(0)\end{aligned}\tag{14}$$

由引理6知$\forall 1\le l\le j$，$\left|\rho_{f_l^*}(0)\right|=0$或$1/2^{\left\lfloor\frac{i'_j-i_j+2}{2}\right\rfloor}$，$|\rho_{F^n}(\eta\to\mu)|\ne 0$时必有所有的$\rho_{f_l^*}(0)$都非0。

显然对$\forall 1\le l\le j$，有$2\le i'_l-i_l+2\le n$，记$\alpha_2,\alpha_3,\cdots,\alpha_n$分别为$\{i'_1-i_1+2,i'_2-i_2+2,\cdots,i'_j-i_j+2\}$中值为$2,3,\cdots,n$的个数，显然也有$2\le 2\cdot\alpha_2+3\cdot\alpha_3+\cdots+n\cdot\alpha_n\le n$。所以

$$\begin{aligned}|\rho_{F^n}(\eta\to\mu)|&=\left|\rho_{f_1^*}(0)\right|\cdots\left|\rho_{f_j^*}(0)\right|\\&=\left(\frac{1}{2^{\lfloor\frac{2}{2}\rfloor}}\right)^{\alpha_2}\left(\frac{1}{2^{\lfloor\frac{3}{2}\rfloor}}\right)^{\alpha_3}\cdots\left(\frac{1}{2^{\lfloor\frac{n}{2}\rfloor}}\right)^{\alpha_n}\\&=\frac{1}{2^{\left(\lfloor\frac{2}{2}\rfloor\cdot\alpha_2+\lfloor\frac{3}{2}\rfloor\cdot\alpha_3+\cdots+\lfloor\frac{n}{2}\rfloor\cdot\alpha_n\right)}}\end{aligned}\tag{15}$$

由引理7即知$\lfloor 2/2\rfloor\cdot\alpha_2+\lfloor 3/2\rfloor\cdot\alpha_3+\cdots+\lfloor n/2\rfloor\cdot\alpha_n\in[1,\lfloor n/2\rfloor]$且能取到$[1,\lfloor n/2\rfloor]$中所有整数。因此

$|\rho_{F^n}(\eta\to\mu)|=0$或$1/2^k$, $k\in Z$且$1\le k\le\lfloor n/2\rfloor$，并且对于任意$k$，必存在$\eta,\mu\in Z_2^n$使得$|\rho_{F^n}(\eta\to\mu)|=1/2^k$。 证毕

定理3给出了Keccak类S盒在$1\le w(\mu)\le n-1$时其非平凡相关优势的取值。下面的定理4整合了推论1，定理2和定理3的结论，给出了Keccak类S盒相关优势的取值形式以及非平凡相关优势的最大最小值。

定理 4 对于F^n, $\forall\eta,\mu\in Z_2^n$及$n\ge3$，均有$|\rho_{F^n}(\eta\to\mu)|=0$或$1/2^k$, $k\in Z$且$0\le k\le\lfloor n/2\rfloor$，并且对于任意$k$，必存在$\eta,\mu\in Z_2^n$使得$|\rho_{F^n}(\eta\to\mu)|=1/2^k$。

证明 由推论1，$w(\mu)=0$时有$|\rho_{F^n}(\eta\to\mu)|=0$或1，且$\eta=0$时就有$|\rho_{F^n}(\eta\to\mu)|=1$；由定理2，$w(\mu)=n$时，$|\rho_{F^n}(\eta\to\mu)|=0$或$1/2^{\lfloor\frac{n-1}{2}\rfloor}$，由引理2即知必存在$\eta$使$|\rho_{F^n}(\eta\to\mu)|=1/2^{\lfloor\frac{n-1}{2}\rfloor}$；再由定理3，$1\le w(\mu)\le n-1$时，$|\rho_{F^n}(\eta\to\mu)|=0$或$1/2^{\left(\lfloor\frac{2}{2}\rfloor\cdot\alpha_2+\lfloor\frac{3}{2}\rfloor\cdot\alpha_3+\cdots+\lfloor\frac{n}{2}\rfloor\cdot\alpha_n\right)}$，且$\lfloor2/2\rfloor\cdot\alpha_2+\lfloor3/2\rfloor\cdot\alpha_3+\cdots+\lfloor n/2\rfloor\cdot\alpha_n$可以取到$[1,\lfloor n/2\rfloor]$中每一个整数。综上，结论成立。 证毕

定理4给出了Keccak类S盒的非平凡相关优势的结构，接下来进一步研究其计数问题。

定理5 对于$\forall\eta,\eta',\mu\in Z_2^n$, $n\ge3$，则若$\rho_{F^n}(\eta\to\mu)\ne0$且$\rho_{F^n}(\eta'\to\mu)\ne0$，则必有$|\rho_{F^n}(\eta\to\mu)|=|\rho_{F^n}(\eta'\to\mu)|$。

证明 若$w(\mu)=0$或n，根据推论1和定理2结论显然成立；

若$1\le w(\mu)\le n-1$，由定理3知当确定μ后，对于$\forall\eta$，若$f^*_{\eta,\mu}$不满足引理3的条件，则$|\rho_{F^n}(\eta\to\mu)|=1/2^{\left(\lfloor\frac{2}{2}\rfloor\cdot\alpha_2+\lfloor\frac{3}{2}\rfloor\cdot\alpha_3+\cdots+\lfloor\frac{n}{2}\rfloor\cdot\alpha_n\right)}$。而$\alpha_2,\alpha_3,\cdots,\alpha_n$的值由$\mu$决定，所以当$\rho_{F^n}(\eta\to\mu)\ne0$且$\rho_{F^n}(\eta'\to\mu)\ne0$时，有$|\rho_{F^n}(\eta\to\mu)|=|\rho_{F^n}(\eta'\to\mu)|$。综上，结论成立。 证毕

定理5说明了F^n的每一个输出掩码都对应了唯一一个非零相关优势，即当F^n的输出掩码确定时，此时F^n的非零相关优势便得以确定。通过该定理，当μ确定时，将$\rho_{F^n}(\eta\to\mu)$经过一定的变换转换为某一个函数在η点的Walsh谱，再由引理2可以得到每一个μ对应的非平凡相关优势的计数，具体见下面的推论2。

推论 2 对于$\forall\mu\in Z_2^n$，必存在$\eta^*\in Z_2^n$使得$|\rho_{F^n}(\eta^*\to\mu)|\ne0$，那么

$$\#\{\eta\in Z_2^n:|\rho_{F^n}(\eta\to\mu)|\ne0\}=\frac{1}{|\rho_{F^n}(\eta^*\to\mu)|^2} \tag{16}$$

证明 取定$\mu\in Z_2^n$，记$h(X)=\oplus_{i=0}^{n-1}[(\mu_i\oplus\mu_{i+3})x_i\oplus\mu_ix_{i+1}x_{i+2}]$，任取$\eta\in Z_2^n$，根据式(2)有

$$\begin{aligned}\rho_{F^n}(\eta\to\mu)&=\frac{1}{2^n}\sum_{X\in Z_2^n}(-1)^{\overset{n-1}{\underset{i=0}{\oplus}}[(\eta_i\oplus\mu_i\oplus\mu_{i+3})x_i\oplus\mu_ix_{i+1}x_{i+2}]}\\&=\frac{1}{2^n}\sum_{X\in Z_2^n}(-1)^{h(X)\oplus\eta\cdot X}=\rho_h(\eta)\end{aligned} \tag{17}$$

由引理2即知$\sum_{\eta\in Z_2^n}[\rho_h(\eta)]^2=1$，所以不可能对所有的$\eta\in Z_2^n$都有$|\rho_{F^n}(\eta\to\mu)|=0$，即可以找到$\eta^*\in Z_2^n$使得$|\rho_{F^n}(\eta^*\to\mu)|\ne0$。又根据定理5，当取定$\mu$时，对$\forall\eta\in Z_2^n$有$|\rho_{F^n}(\eta\to\mu)|=0$或$|\rho_{F^n}(\eta^*\to\mu)|$，即$|\rho_h(\eta)|=0$或$|\rho_{F^n}(\eta^*\to\mu)|$，那么

$$\begin{aligned}\sum_{\eta\in Z_2^n}[\rho_h(\eta)]^2&=\sum_{\eta\in Z_2^n\text{且}|\rho_h(\eta)|=0}[\rho_h(\eta)]^2\\&\quad+\sum_{\eta\in Z_2^n\text{且}\rho_h(\eta)=|\rho_{F^n}(\eta^*\to\mu)|}[\rho_h(\eta)]^2\\&=\sum_{\eta\in Z_2^n\text{且}\rho_h(\eta)=|\rho_{F^n}(\eta^*\to\mu)|}[\rho_h(\eta)]^2\\&=\#\{\eta\in Z_2^n:|\rho_{F^n}(\eta\to\mu)|\ne0\}\\&\quad\times|\rho_{F^n}(\eta^*\to\mu)|^2=1\end{aligned} \tag{18}$$

因此有$\#\{\eta\in Z_2^n:|\rho_{F^n}(\eta\to\mu)|\ne0\}=1/|\rho_{F^n}(\eta^*\to\mu)|^2$。 证毕

在研究S盒的线性性质时，其最大非平凡相关优势的结构和计数是需要重点关注的问题。接下来通过定理6给出了Keccak类S盒的非平凡相关优势取到最大值$\frac{1}{2}$时(η,μ)的充分必要条件及计数。定理6可根据之前的推论1、定理2、定理3分别讨论$w(\mu)=0, w(\mu)=n, 1\le w(\mu)\le n-1$时的情况证得。

定理6 对于F^n, $n\ge3$, $\eta=(\eta_0,\eta_1,\cdots,\eta_{n-1})$, $\mu=(\mu_0,\mu_1,\cdots,\mu_{n-1})\in Z_2^n$，则当且仅当$(\eta,\mu)$满足下列条件之一时有$|\rho_{F^n}(\eta\to\mu)|=1/2$：

(1) $n=3$, $w(\mu)=3$, $\eta_0\oplus\eta_1\oplus\eta_2=1$；

(2) $n=4$, $w(\mu)=4$, $\eta_0=\eta_2$, $\eta_1=\eta_3$；

(3) $\forall n\ge3$, $w(\mu)=1$且$\mu_{i_0}=1$, $0\le i_0\le n-1$, $\eta_{i_0-3}=\eta_{i_0}=1$，且$\forall i\notin\{i_0-3,i_0,i_0+1,i_0+2\}$时有$\eta_i=0$；

(4) $\forall n\ge3, w(\mu)=2$且$\mu_{i_0}=\mu_{i_0+1}=1, 0\le i_0\le n-1$, $\eta_{i_0-3}=\eta_{i_0-2}=\eta_{i_0}=1$, $\eta_{i_0+1}\oplus\eta_{i_0+3}=1$，且$\forall i\notin\{i_0-3,i_0-2,i_0,i_0+1,i_0+2,i_0+3\}$时有$\eta_i=0$。

且满足$|\rho_{F^n}(\eta\to\mu)|=1/2$的$(\eta,\mu)$对数为$\begin{cases}8n+4, & n=3,4\\ 8n, & n\ge5\end{cases}$。

4　结束语

许多密码算法都使用了与Keccak的S盒类似的S盒，本文将这类S盒一般化为Keccak类S盒。为了更好地理解和应用这类S盒，文献[16]仅给出了Keccak类S盒最大非平凡相关优势为2^{-1}，而本文进一步研究了其线性性质，基本解决了Keccak类S盒的线性逼近的结构和计数问题。接下来需要做的工作是研究如文献中有更加复杂局部函数的基于元胞自动机的S盒的线性性质。

参 考 文 献

[1] BERTONI G, DAEMEN J, PEETERS M, *et al*. Keccak[C]. The 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, Athens, Greece, 2013: 313–314.

[2] NIST. Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family[EB/OL]. http://www.nist.gov/hash-competition, 2007.

[3] 王永娟, 王涛, 袁庆军, 等. 密码算法旁路立方攻击改进与应用[J]. 电子与信息学报, 2020, 42(5): 1087–1093. doi: 10.11999/JEIT181075.
WANG Yongjuan, WANG Tao, YUAN Qingjun, *et al*. Side channel cube attack improvement and application on cryptographic algorithm[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1087–1093. doi: 10.11999/JEIT181075.

[4] 赵军, 曾学文, 郭志川. 支持国产密码算法的高速PCIe密码卡的设计与实现[J]. 电子与信息学报, 2019, 41(10): 2402–2408. doi: 10.11999/JEIT190003.
ZHAO Jun, ZENG Xuewen, and GUO Zhichuan. Design and implementation of high speed PCIe cipher card supporting GM algorithms[J]. *Journal of Electronics & Information Technology*, 2019, 41(10): 2402–2408. doi: 10.11999/JEIT190003.

[5] DAEMEN J. Cipher and hash function design strategies based on linear and differential cryptanalysis[D]. [Ph.D. dissertation], Katholieke Universiteit Leuven, 1995: 23–58.

[6] BERTONI G M, DAEMEN J, PEETERS M, *et al*. RadioGatún, a belt-and-mill hash function[C]. The 2nd Cryptographic Hash Workshop, Santa Barbara, USA, 2006: 24–25.

[7] GUO Xu, SRIVASTAV M, HUANG Sinan, *et al*. ASIC implementations of five SHA-3 finalists[C]. 2012 Design, Automation & Test in Europe Conference & Exhibition, Dresden, Germany, 2012: 1006–1011.

[8] JOSHI P, MUKHOPADHYAY D, and ROYCHOWDHURY D. Design and analysis of a robust and efficient block cipher using cellular automata[C]. The 20th International Conference on Advanced Information Networking and Applications, Vienna, Austria, 2006: 67–71.

[9] MANZONI L and MARIOT L. Cellular automata pseudo-random number generators and their resistance to asynchrony[C]. The 13th International Conference on Cellular Automata for Research and Industry, Como, Italy, 2018: 428–437.

[10] PICEK S, MARIOT L, YANG Bohan, *et al*. Design of S-boxes defined with cellular automata rules[C]. The Computing Frontiers Conference, Siena, Italy, 2017: 409–414.

[11] MARIOT L, PICEK S, LEPORATI A, *et al*. Cellular automata based S-boxes[J]. *Cryptography and Communications*, 2019, 11(1): 41–62. doi: 10.1007/s12095-018-0311-8.

[12] BAO Zhenzhen, GUO Jian, LING San, *et al*. PEIGEN-a platform for evaluation, implementation, and generation of S-boxes[J]. *IACR Transactions on Symmetric Cryptology*, 2019(1): 330–394. doi: 10.13154/tosc.v2019.i1.330-394.

[13] GHOSHAL A, SADHUKHAN R, PATRANABIS S, *et al*. Lightweight and side-channel secure 4×4 S-boxes from cellular automata rules[J]. *IACR Transactions on Symmetric Cryptology*, 2018(3): 311–334. doi: 10.13154/tosc.v2018.i3.311-334.

[14] 关杰, 黄俊君. 一类新的基于元胞自动机的S盒的密码学性质研究[J]. 通信学报, 2019, 40(5): 192–200.
GUAN Jie and HUANG Junjun. Research on cryptographic properties of a new S-box based on cellular automaton[J]. *Journal on Communications*, 2019, 40(5): 192–200.

[15] 李倩男, 李云强, 蒋淑静, 等. Keccak类非线性变换的差分性质研究[J]. 通信学报, 2012, 33(9): 140–146.
LI Qiannan, LI Yunqiang, JIANG Shujing, *et al*. Research on differential properties of Keccak-like nonlinear transform[J]. *Journal on Communications*, 2012, 33(9): 140–146.

[16] 李倩男. Keccak类杂凑函数研究[D]. [硕士论文], 信息工程大学, 2013: 30–36.
LI Qiannan. Research on Keccak-like Hash function[D]. [Master Dissertation], The PLA Information Engineering University, 2013: 30–36.

[17] 金晨辉, 郑浩然, 张少武, 等. 密码学[M]. 北京: 高等教育出版社, 2009: 30–36.
JIN Chenhui, ZHENG Haoran, ZHANG Shaowu, *et al*. Cryptography[M]. Beijing: Higher Education Press, 2009: 30–36.

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

黄俊君：男，1995年生，硕士生，主要研究方向为对称密码设计与分析.

责任编辑：余　蓉