一类新的基于元胞自动机的 S 盒的密码学性质研究

关杰，黄俊君
（解放军战略支援部队信息工程大学密码工程学院，河南 郑州 450001）

摘 要：通过实验找到了一类新的基于元胞自动机的 S 盒，分析了该 S 盒的置换性质，证明了其仅在规模为 5 时是一个置换。通过构造差分矩阵的方法给出了该 S 盒的非平凡差分转移概率与差分矩阵的秩之间的关系，从而得到其取值范围。证明了对输入差分进行循环移位不改变其对应的非平凡差分转移概率，从而给出其在规模为 5 时取最大和最小非平凡差分转移概率的充要条件，彻底解决了此时该 S 盒的差分对应的结构和计数问题。

关键词：元胞自动机；S 盒；置换性质；差分分析
中图分类号：TN918.1
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019101

Research on cryptographic properties of a new S-box based on cellular automaton

GUAN Jie, HUANG Junjun
Institute of Cryptography Engineering, Information Engineering University, Zhengzhou 450001, China

Abstract: A new S-box based on cellular automata was found by experiments. The permutation properties of the S-box were analyzed, which proved that the S-box was a permutation only when the size of lattice was 5. Then the relation between the nontrivial difference transition probability of the S-box and the rank of the difference matrix was proved by constructing the difference matrix. And it was proved that the cyclic shift of input differential would not change the corresponding nontrivial differential transition probability, and obtained the sufficient and necessary conditions about the maximum and minimum nontrivial differential transition probabilities when the size of lattice was 5. Then the problem of the difference distribution of the S-box in this situation is completely solved.

Key words: cellular automaton, S-box, permutation property, differential analysis

1 引言

基于元胞自动机（CA, cellular automaton）的 S 盒[1]因其良好的密码学性质及较低的实现成本被广泛应用到许多密码算法中，其中最典型的是已经作为 SHA-3 标准[2]之一的 Keccak 杂凑函数[3]。本文选用了一个作用域范围仅为 3 个元胞的局部规则，从而使该算法的 S 盒有着极小的软件实现成本及硬件实现消耗。目前，接触到的其他利用元胞自动机的局部规则定义 S 盒的密码都使用了与 Keccak 杂凑函数的 S 盒相同的局部规则，如 Panama[4]、Subterranean[5]和 3Way[6]。除了这些 S 盒外，还有一些密码算法使用的 S 盒是 Keccak 杂凑算法的 S 盒的仿射变换，如 Ascon[7]。

本文通过实验找到了一类新的基于元胞自动机的 S 盒，并对这一类 S 盒的密码学性质进行研究，该类 S 盒相比 Keccak 杂凑函数的 S 盒差分性质更好，并且在输入输出规模为 5 时也是一个置换，因此这一类新的 S 盒有潜力代替 Keccak 杂凑函数的 S 盒，为密码设计者提供设计参考。

收稿日期：2018−11−22；**修回日期**：2019−04−01
基金项目：国家自然科学基金资助项目（No.61572516, No.61272041, No.61272488）
Foundation Item: The National Natural Science Foundation of China (No.61572516, No.61272041, No.61272488)

2　基本概念

2.1　S 盒的密码学性质

在分组密码的设计中，最通用的设计准则就是香农提出的混乱和扩散原则[8]。在实际的设计过程中通常使用 S 盒来提供混乱效果，在很多密码中 S 盒都是唯一的非线性环节。一个 m 进 n 出的 S 盒可以用映射 F：$Z_2^m \to Z_2^n$ 表示，其中，m、n 都是正整数。

置换性质[9]和差分性质是 S 盒重要的密码学性质，具有良好差分性质及满足置换条件的 S 盒将有更广泛的应用场景。下面给出置换和差分的定义。

定义 1[10]　设 $F:Z_2^n \to Z_2^n$，若对任意 $\boldsymbol{X}$、$\boldsymbol{X}^* \in Z_2^n$ 且 $\boldsymbol{X} \neq \boldsymbol{X}^*$，有 $F(\boldsymbol{X}) \neq F(\boldsymbol{X}^*)$，称 F 是一个置换。

定义 2[11]　设 $F:Z_2^n \to Z_2^n$，$\boldsymbol{X}$、$\boldsymbol{\alpha}$、$\boldsymbol{\beta} \in Z_2^n$，那么称

$$p_F(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = \frac{1}{2^n} \#\{\boldsymbol{X} \mid \boldsymbol{\beta} = F(\boldsymbol{X}) \oplus F(\boldsymbol{X} \oplus \boldsymbol{\alpha})\}$$

为 F 在输入差分为 $\boldsymbol{\alpha}$，输出差分为 $\boldsymbol{\beta}$ 下的差分转移概率，其中，$\#\{\cdot\}$ 代表集合中元素的个数。

2.2　元胞自动机

元胞自动机是一种广泛应用在不同领域，用来模拟和分析复杂离散问题的并行运算模型。一个 CA 可以表示为一个由元胞（cell）组成的元胞空间（lattice）。在每一步状态更新中，元胞空间中的每一个元胞根据局部规则（local rule）同步更新状态。CA 中所有元胞的状态从原有状态到一步更新后的状态之间的映射可以用全局规则（global rule）来表示。事实上，如果经过合理的设计及选取，全局规则可以是一个具有良好密码学性质的非线性映射，即本文要研究的基于 CA 的 S 盒。根据划分的不同，CA 有很多分类，本文仅考虑一种可以用作 S 盒的一维布尔型循环边界 CA，这种 CA 的定义如下。

可以把元胞空间看作是等间隔排列在直线上的一系列完全相同的元胞，且每个元胞的状态均取自集合 $Z_2 = \{0,1\}$。

设 Z^* 为整数集合，假设元胞空间的规模为 n 且 $n \in Z^*$，即该 CA 由 n 个元胞组成，那么所有元胞的状态可以用一行有限的符号序列来表示，当其中每一个符号取特定状态就可以构成一个状态序列，称每个这样的状态序列为 CA 的一个构型。构型中的每一个元胞是用取自 Z_2 的状态来表示的，例如构型 $\boldsymbol{X}$ 可以表示为 $\boldsymbol{X} = (x_0, x_1, x_2, \cdots, x_{n-1})$，其中，$x_i \in Z_2$，$i \in \{0,1,2,\cdots,n-1\}$。

在一次状态更新中，设更新前的构型为 $\boldsymbol{X}$，那么更新后的构型完全由 $\boldsymbol{X}$ 决定，记为 $\boldsymbol{X}'$。其中，$\boldsymbol{X}'$ 中第 i 个元胞 x_i' 的状态由 $\boldsymbol{X}$ 的 x_i 及其右边不超过 $r(r \leqslant n-1)$ 个元胞的状态决定，即

$$x_i' = f(x_i, x_{i+1}, \cdots, x_{i+r})$$

其中，$f:Z_2^{r+1} \to Z_2$ 与元胞空间的规模 n 及元胞的位置 i 无关，称为 CA 的局部规则；r 为邻域半径；$(x_{i+1}, \cdots, x_{i+r})$ 为第 i 个元胞的右邻域。最后通过 f 可以推导出 $\boldsymbol{X}$ 到 $\boldsymbol{X}'$ 的映射，称作全局规则，其与元胞空间的规模 n 有关，记作 $F^n:Z_2^n \to Z_2^n$。

下面，给出一维布尔型循环边界 CA 的定义，如定义 3 所示。

定义 3[12]　映射 $F^n:Z_2^n \to Z_2^n$ 为一维布尔型循环边界 CA，其中，$n \in Z^*$ 为元胞空间的规模，存在 $r>0$ 及 $f:Z_2^{r+1} \to Z_2$，对 CA 的任意构型 $\boldsymbol{X} = (x_0, x_1, x_2, \cdots, x_{n-1})$，有

$$\begin{aligned} F^n(x_0, x_1, \cdots, x_{n-1}) = (&f(x_0, \cdots, x_r), \\ &f(x_1, \cdots, x_{r+1}), \cdots, f(x_{n-r}, \cdots, x_0), \\ &\cdots, f(x_{n-1}, \cdots, x_{r-1})) \end{aligned}$$

其中，r 为 CA 的邻域半径，f 为 CA 的局部规则，F^n 为 CA 的全局规则。

图 1 是一维布尔型循环边界 CA 的示例，其元胞空间的规模 $n=5$，局部规则可表示为 $f(x_0, x_1, x_2) = x_0 \oplus x_1 x_2 \oplus x_2$，且其邻域半径 $r=2$。可以看到，在这种循环边界的 CA 中，其元胞空间可以看作一个首尾相接的环，最开始的元胞接在最后一个元胞后，因此在更新最后 r 个元胞的状态时，会从最开始的 r 个元胞中选取部分作为其右邻域的一部分。在图 1 中，CA 向量的最右侧用最开始的 $r=2$ 个元胞接上，在最后 2 个元胞更新时可以作为其右邻域。

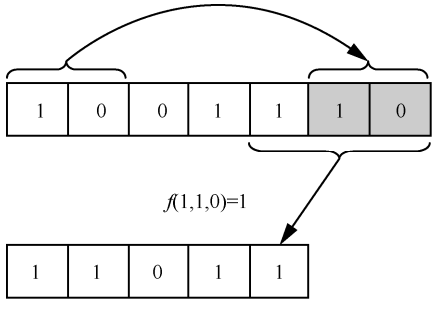


图 1　一维布尔型循环边界 CA 示例

图 1 中的 CA 的局部规则就是用于 Keccak 的非

线性变换 χ，本文将该 CA 的局部规则记为 f_K，全局规则记为 F_K^n。

接下来，本文将给出 CA 的一个重要性质。本文所有运算都是在模 n 上进行的。

定理 1 CA 的平移不变性。设 $F^n:Z_2^n\to Z_2^n$ 为一个 CA，其局部规则为 $f:Z_2^{r+1}\to Z_2$，其中 $n\in Z^*, r>0$ 且 $n>r$，设 $\boldsymbol{X}\in Z_2^n$ 为该 CA 的构型，令 $\sigma_k(\boldsymbol{X})$ 为对 $\boldsymbol{X}$ 循环左移 k 位，那么 $\forall \boldsymbol{X}$、$\forall k\in Z_n$ 均有 $F(\sigma_k(\boldsymbol{X}))=\sigma_k(F(\boldsymbol{X}))$。

证明 令 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})$，那么 $\sigma_k(\boldsymbol{X})=(x_k,x_{k+1},\cdots,x_{k-1})$，所以有

$$\begin{aligned}&F(\sigma_k(\boldsymbol{X}))=(f(x_k,\cdots,x_{r+k}),f(x_{k+1},\cdots,x_{r+k+1}),\\&\cdots,f(x_{k-1},\cdots,x_{r+k-1}))=\sigma_k(f(x_0,\cdots,x_r),\\&f(x_1,\cdots,x_{r+1}),\cdots,f(x_{n-1},\cdots,x_{r-1}))=\sigma_k(F(\boldsymbol{X}))\end{aligned}$$

故结论成立，证毕。

在一般的 CA 中，局部规则对第 i 个元胞 x_i 的作用域为 $(x_{i-r},\cdots,x_{i-1},x_i,x_{i+1},\cdots,x_{i+r})$，不仅跟右邻域相关，还与左邻域相关。但是根据定理 1 可知，把 CA 的构型经过平移后可以与上文介绍的 CA 的局部规则一样，仅与右邻域相关而不改变其置换性质和差分性质。

2.3 一类新的基于 CA 的 S 盒

由于用全局规则就可以唯一地表示一个 CA，而一个 CA 经过合理地设计后，可以使全局规则成为一个密码学性质良好的非线性变换，从而可以用作密码环节中的 S 盒。为了找到密码学性质良好的基于 CA 的 S 盒，本文通过实验穷举了规模为 5 的所有 CA 并从中筛选出一个 CA。该 CA 具有良好的差分性质且满足置换条件，然后本文将其在不同的规模下的情况抽象成一类 CA。

下面，给出本文要研究的这一类新的基于 CA 的 S 盒的定义。

定义 4 设 $n\geqslant 5$，映射 $F^n:Z_2^n\to Z_2^n$ 为一类 CA，其局部规则为 $f:Z_2^5\to Z_2$ 且满足

$$f(x_0,x_1,x_2,x_3,x_4)=x_0(x_1\oplus x_2)\oplus x_4$$

将这类 CA 记作 F_{new}^n，局部规则记为 f_{new}。

3 F_{new}^n 的置换性质分析

置换性质是 S 盒一个重要的密码学性质，满足置换性质的 S 盒在很多密码体制中实现数据变换，具有广泛的应用场景。

引理 1 对于元胞空间规模 n 为偶数的 CA，设局部规则为 $f(x_0,x_1,\cdots,x_r)$ 且 $r<n$，若 r 为奇数，有 $f(\underbrace{0,1,\cdots,0,1}_{\text{“0,1”循环的序列}})=f(\underbrace{1,0,\cdots,1,0}_{\text{“1,0”循环的序列}})$；若 r 为偶数，有 $f(\underbrace{0,1,\cdots,0,1,0}_{\text{“0,1”循环的序列}})=f(\underbrace{1,0,\cdots,1,0,1}_{\text{“1,0”循环的序列}})$，那么该 CA 的全局规则 F^n 必然不是一个置换。

证明 设 $\boldsymbol{X}$、$\boldsymbol{X}^*\in Z_2^n$，如果能够找到 $\boldsymbol{X}\neq\boldsymbol{X}^*$，使得 $F(\boldsymbol{X})=F(\boldsymbol{X}^*)$，那么 F 不是一个置换。由于 n 为偶数，本文令 $\boldsymbol{X}=\underbrace{(0,1,0,1,\cdots,0,1)}_{\frac{n}{2}\text{对“0,1”}}$，令 $\boldsymbol{X}^*=\underbrace{(1,0,1,0,\cdots,1,0)}_{\frac{n}{2}\text{对“1,0”}}$，若 r 为奇数，有

$$\begin{aligned}&F^n(\boldsymbol{X})=(f(0,1,\cdots,0,1),f(1,0,\cdots,1,0),\cdots,\\&f(0,1,\cdots,0,1),f(1,0,\cdots,1,0))=(f(1,0,\cdots,1,0),\\&f(0,1,\cdots,0,1),\cdots,f(1,0,\cdots,1,0),f(0,1,\cdots,0,1))=\\&F^n(\boldsymbol{X}^*)\end{aligned}$$

若 r 为偶数，有

$$\begin{aligned}&F^n(\boldsymbol{X})=(f(0,1,\cdots,0,1,0),f(1,0,\cdots,1,0,1),\cdots,\\&f(0,1,\cdots,0,1,0),f(1,0,\cdots,1,0,1))=(f(1,0,\cdots,1,0,1),\\&f(0,1,\cdots,0,1,0),\cdots,f(1,0,\cdots,1,0,1),f(0,1,\cdots,0,1,0))=\\&F^n(\boldsymbol{X}^*)\end{aligned}$$

显然，此处 $\boldsymbol{X}\neq\boldsymbol{X}^*$，但有 $F^n(\boldsymbol{X})=F^n(\boldsymbol{X}^*)$。所以此时全局规则 F^n 不是一个置换，证毕。

事实上，Keccak 中的非线性映射的全局规则 F_K^n 在 n 为偶数时不是一个置换，因为 F_K^n 对应的局部规则 f_K 有 $f_K(0,1,0)=f_K(1,0,1)=0$，根据引理 1 即得。

引理 2 设 $n\geqslant 6$ 且 n 为奇数，对于 $\boldsymbol{X}=(1,0,1,0,\cdots,1,0,1)\in Z_2^n$，有 $F_{\text{new}}^n(\boldsymbol{X})=(0,0,\cdots,0,1,1,1,1)$；对于 $\boldsymbol{X}=(1,1,1,1,0,0,1,0,\cdots,0)\in Z_2^n$，也有 $F_{\text{new}}^n(\boldsymbol{X})=(0,0,\cdots,0,1,1,1,1)$。

证明 首先，令 $\boldsymbol{X}=(1,0,1,0,\cdots,1,0,1)$，令 $\boldsymbol{X}'=F_{\text{new}}^n(\boldsymbol{X})=(x_0',x_1',\cdots,x_{n-1}')$，那么有

$$x_k'=\begin{cases}f_{\text{new}}(1,0,1,0,1), k=0,2,4,\cdots,n-5\\f_{\text{new}}(0,1,0,1,0), k=1,3,5,\cdots,n-6\end{cases}$$

而 $f_{\text{new}}(1,0,1,0,1)=f_{\text{new}}(0,1,0,1,0)=0$，所以

$x'_i=0$，$i=\{0,1,2,\cdots,n-5\}$。又因为

$(x'_{n-4},x'_{n-3},x'_{n-2},x'_{n-1})=(f_{\text{new}}(0,1,0,1,1),f_{\text{new}}(1,0,1,1,0),$
$f_{\text{new}}(0,1,1,0,1),f_{\text{new}}(1,1,0,1,0))=(1,1,1,1)$

所以 $\boldsymbol{X}'=F^n_{\text{new}}(\boldsymbol{X})=(0,0,\cdots,0,1,1,1,1)$。

当 $n=7$ 时，令 $\boldsymbol{X}=(1,1,1,1,0,0,1)$，容易验证 $F^7_{\text{new}}(\boldsymbol{X})=(0,0,0,1,1,1,1)$ 成立；当 $n=9$ 时，令 $\boldsymbol{X}=(1,1,1,1,0,0,1,0,0)$，同样有 $F^9_{\text{new}}(\boldsymbol{X})=$ (0,0,0,0,0,1,1,1,1) 成立；当 $n\geqslant 11$ 时，令 $\boldsymbol{X}=(1,1,1,1,0,0,1,0,\cdots,0)$，$\boldsymbol{X}'=F^n_{\text{new}}(\boldsymbol{X})=$ $(x'_0,x'_1,\cdots,x'_{n-1})$，验证有 $x'_i=0$，$i=0,1,2,\cdots,6$。又因为

$(x'_{n-4},x'_{n-3},x'_{n-2},x'_{n-1})=(f_{\text{new}}(0,0,0,0,1),$
$f_{\text{new}}(0,0,0,1,1),f_{\text{new}}(0,0,1,1,1),f_{\text{new}}(0,1,1,1,1))=(1,1,1,1)$

最后，因为 $x'_i=f_{\text{new}}(0,0,0,0,0)=0$，$7\leqslant i\leqslant n-5$。所以 $\boldsymbol{X}'=F^n_{\text{new}}(\boldsymbol{X})=(0,0,\cdots,0,1,1,1,1)$ 在 $n\geqslant 11$ 时成立。

综上所述，结论成立，证毕。

定理 2　设 $\boldsymbol{X},\boldsymbol{X}^*,\boldsymbol{Y}=F^n_{\text{new}}(\boldsymbol{X}),\boldsymbol{Y}^*=F^n_{\text{new}}(\boldsymbol{X}^*)\in Z_2^n$，当 $n=5$ 时，F^n_{new} 是置换；当 $n\geqslant 6$ 时，F^n_{new} 不是置换。

证明　对于 F^5_{new}，容易验证遍历 32 个输入 $\boldsymbol{X}$ 会有对应 32 个不同的输出 Y，即对于任意的 $\boldsymbol{X}\neq\boldsymbol{X}^*$，必然有 $\boldsymbol{Y}\neq\boldsymbol{Y}^*$，所以 F^5_{new} 是置换。

下面，分 2 种情况讨论 $n\geqslant 6$ 时 F^n_{new} 不是一个置换。

情况 1　$n\geqslant 6$ 且 n 为偶数，此时由 $f_{\text{new}}(x_0,x_1,x_2,x_3,x_4)=x_0(x_1\oplus x_2)\oplus x_4$ 得

$$f_{\text{new}}(0,1,0,1,0)=f_{\text{new}}(1,0,1,0,1)=0$$

所以根据引理 1 可知，当 n 为偶数时 F^n_{new} 不是一个置换。

情况 2　$n\geqslant 6$ 且 n 为奇数，由引理 2 可以构造 $\boldsymbol{X}=(1,0,1,0\cdots,1,0,1)$，有 $F^n_{\text{new}}(\boldsymbol{X})=(0,0,\cdots,\ 0,1,1,1,1)$，同时可以构造 $\boldsymbol{X}^*=(1,1,1,1,0,0,1,0,\cdots,0)$，也有 $F^n_{\text{new}}(\boldsymbol{X}^*)=(0,0,\cdots,0,1,1,1,1)=F^n_{\text{new}}(\boldsymbol{X})$。因为 $\boldsymbol{X}\neq\boldsymbol{X}^*$，但是 $F^n_{\text{new}}(\boldsymbol{X})=F^n_{\text{new}}(\boldsymbol{X}^*)$，所以此时 F^n_{new} 也不是一个置换。

综上所述可知，当 $n\geqslant 6$ 时，F^n_{new} 均不是一个置换，证毕。

4　F^n_{new} 的差分性质分析

差分性质是 S 盒最基础的性质之一。为了研究 F^n_{new} 的差分性质，本文首先介绍 F^n_{new} 的差分矩阵的概念，然后找到 F^n_{new} 的差分转移概率与差分矩阵之间的关系，从而得到 F^n_{new} 的非平凡差分转移概率的取值范围。

令 $n\in Z^*$，设 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})\in Z_2^n$，记 $F^n_{\text{new}}(\boldsymbol{X})$ 的输入差分为 $\boldsymbol{\alpha}\in(\alpha_0,\alpha_1,\cdots,\alpha_{n-1})\in Z_2^n$，输出差分为 $\boldsymbol{\beta}\in(\beta_0,\beta_1,\cdots,\beta_{n-1})\in Z_2^n$，由于 $f_{\text{new}}(x_0,x_1,x_2,x_3,x_4)=x_0(x_1\oplus x_2)\oplus x_4$，那么输入差分和输出差分之间满足如式(1)所示的等式。

$$\begin{aligned}\beta_i=&\big(x_i(x_{i+1}\oplus x_{i+2})\oplus x_{i+4}\big)\oplus\big((x_i\oplus\alpha_i)\\&(x_{i+1}\oplus\alpha_{i+1}\oplus x_{i+2}\oplus\alpha_{i+2})\oplus(x_{i+4}\oplus\alpha_{i+4})\big)=\\&x_i(\alpha_{i+1}\oplus\alpha_{i+2})\oplus x_{i+1}\alpha_i\oplus x_{i+2}\alpha_i\oplus\\&(\alpha_i\alpha_{i+1}\oplus\alpha_i\alpha_{i+2}\oplus\alpha_{i+4})\end{aligned}\tag{1}$$

其中，$i\in\{0,1,\cdots,n-1\}$，且下标的运算均是模 n 上的运算。

本文把 n 位输入差分和输出差分的关系用 n 个式子组成的方程组来表示，如式(2)所示。

$$\begin{cases}\beta_0=x_0(\alpha_1\oplus\alpha_2)\oplus x_1\alpha_0\oplus x_2\alpha_0\oplus\\(\alpha_0\alpha_1\oplus\alpha_0\alpha_2\oplus\alpha_4)\\\beta_1=x_1(\alpha_2\oplus\alpha_3)\oplus x_2\alpha_1\oplus x_3\alpha_1\oplus\\(\alpha_1\alpha_2\oplus\alpha_1\alpha_3\oplus\alpha_5)\\\quad\vdots\\\beta_{n-1}=x_{n-1}(\alpha_0\oplus\alpha_1)\oplus x_0\alpha_{n-1}\oplus\\x_1\alpha_{n-1}\oplus(\alpha_{n-1}\alpha_0\oplus\alpha_{n-1}\alpha_1\oplus\alpha_3)\end{cases}\tag{2}$$

该差分方程组对应的 n 维系数矩阵就是 F^n_{new} 的差分矩阵，记为 $\boldsymbol{A}$，如式(3)所示。

$$\boldsymbol{A}=\begin{bmatrix}\alpha_1\oplus\alpha_2&\alpha_0&\alpha_0&0&\cdots&0&0&0\\0&\alpha_2\oplus\alpha_3&\alpha_1&\alpha_1&\cdots&0&0&0\\\vdots&\vdots&\vdots&\vdots&\ddots&\vdots&\vdots&\vdots\\0&0&0&0&\cdots&\alpha_{n-2}\oplus\alpha_{n-1}&\alpha_{n-3}&\alpha_{n-3}\\\alpha_{n-2}&0&0&0&\cdots&0&\alpha_{n-1}\oplus\alpha_0&\alpha_{n-2}\\\alpha_{n-1}&\alpha_{n-1}&0&0&\cdots&0&0&\alpha_0\oplus\alpha_1\end{bmatrix}=\begin{bmatrix}\boldsymbol{A}_0\\\boldsymbol{A}_1\\\vdots\\\boldsymbol{A}_{n-1}\end{bmatrix}\tag{3}$$

其中，$\boldsymbol{A}_i\left(i\in\{0,1,2,\cdots,n-1\}\right)$ 表示 $\boldsymbol{A}$ 的第 i 行。另外，$\boldsymbol{A}$ 仅与 F_{new}^n 的输入差分相关。

定理 3 设 $n\geqslant 5$，对于 F_{new}^n，任意输入差分 $\boldsymbol{\alpha}\neq 0$ 及输出差分 $\boldsymbol{\beta}$，若差分转移概率 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\neq 0$，那么一定有 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\dfrac{1}{2^r}$，其中 $r=\text{rank}(\boldsymbol{A})$ 表示 $\boldsymbol{A}$ 的秩。

证明 设 F_{new}^n 的输入 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})$，输入差分及输出差分分别为 $\boldsymbol{\alpha}=(\alpha_0,\alpha_1,\cdots,\alpha_{n-1})\neq(0,0,\cdots,0)$ 和 $\boldsymbol{\beta}=(\beta_0,\beta_1,\cdots,\beta_{n-1})$。其中，$x_i$、$\alpha_i$、$\beta_i\in\{0,1\}$，$i\in\{0,1,2,\cdots,n-1\}$。由式(1)可得

$$\begin{bmatrix}y_0\\y_1\\\vdots\\y_{n-1}\end{bmatrix}=\begin{bmatrix}\alpha_1\oplus\alpha_2 & \alpha_0 & \alpha_0 & 0 & \cdots & 0 & 0 & 0\\0 & \alpha_2\oplus\alpha_3 & \alpha_1 & \alpha_1 & \cdots & 0 & 0 & 0\\\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\0 & 0 & 0 & 0 & \cdots & \alpha_{n-2}\oplus\alpha_{n-1} & \alpha_{n-3} & \alpha_{n-3}\\\alpha_{n-2} & 0 & 0 & 0 & \cdots & 0 & \alpha_{n-1}\oplus\alpha_0 & \alpha_{n-2}\\\alpha_{n-1} & \alpha_{n-1} & 0 & 0 & \cdots & 0 & 0 & \alpha_0\oplus\alpha_1\end{bmatrix}\begin{bmatrix}x_0\\x_1\\\vdots\\x_{n-1}\end{bmatrix}\tag{4}$$

即 $\boldsymbol{Y}^{\mathrm{T}}=\boldsymbol{A}\boldsymbol{X}^{\mathrm{T}}$，其中，$\boldsymbol{X}^{\mathrm{T}}$ 和 $\boldsymbol{Y}^{\mathrm{T}}$ 分别表示 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$ 的转置。

若 $\boldsymbol{X}\in\left\{\boldsymbol{X}|\boldsymbol{\beta}=F_{\text{new}}^n(\boldsymbol{X})\oplus F_{\text{new}}^n(\boldsymbol{X}\oplus\boldsymbol{\alpha})\right\}$，即 X 是使关系式 $\boldsymbol{\beta}=F_{\text{new}}^n(\boldsymbol{X})\oplus F_{\text{new}}^n(\boldsymbol{X}\oplus\boldsymbol{\alpha})$ 成立的一个解，那么对于每一位 α_i 和 β_i，x_i 也使其关系式成立，所以 $\boldsymbol{X}$ 就是 $\boldsymbol{Y}^{\mathrm{T}}=\boldsymbol{A}\boldsymbol{X}^{\mathrm{T}}$ 的一个解；此外，若 $\boldsymbol{X}$ 是 $\boldsymbol{Y}^{\mathrm{T}}=\boldsymbol{A}\boldsymbol{X}^{\mathrm{T}}$ 的一个解，显然也有 $\boldsymbol{X}\in\left\{\boldsymbol{X}|\boldsymbol{\beta}=F_{\text{new}}^n(\boldsymbol{X})\oplus F_{\text{new}}^n(\boldsymbol{X}\oplus\boldsymbol{\alpha})\right\}$。所以 $\#\{\boldsymbol{X}|\boldsymbol{\beta}=F(\boldsymbol{X})\oplus F(\boldsymbol{X}\oplus\boldsymbol{\alpha})\}$ 就等于 $\boldsymbol{Y}^{\mathrm{T}}=\boldsymbol{A}\boldsymbol{X}^{\mathrm{T}}$ 解的个数。设 $r=\text{rank}(\boldsymbol{A})$ 是方程组系数矩阵的秩，$\boldsymbol{X}_0$ 为其一个特解，那么所有的解为

$$\boldsymbol{X}=\boldsymbol{X}_0\oplus k_1\eta_1\oplus k_2\eta_2\oplus\cdots\oplus k_{n-r}\eta_{n-r}$$

其中，$k_i\in\{0,1\}$，η_i 是方程组线性无关的基础解系，$i\in\{1,2,\cdots,n-r\}$。遍历所有的 k_i 可以得到所有方程组的解，所以解的个数为 2^{n-r} 个，也就是说 $\#\left\{\boldsymbol{X}|\boldsymbol{\beta}=F(\boldsymbol{X})\oplus F(\boldsymbol{X}\oplus\boldsymbol{\alpha})\right\}=2^{n-r}$。所以有

$$p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{\#\left\{\boldsymbol{X}|\boldsymbol{\beta}=F(\boldsymbol{X})\oplus F(\boldsymbol{X}\oplus\boldsymbol{\alpha})\right\}}{2^n}=\frac{1}{2^r}$$

证毕。

定理 3 给出了 F_{new}^n 的差分转移概率与 $r=\text{rank}(\boldsymbol{A})$ 之间的关系。而 $\boldsymbol{A}$ 仅与输入差分相关，给定一个输入差分 $\boldsymbol{\alpha}\neq 0$ 便可以确定此时的差分转移矩阵，从而得到 r，那么对于任意 $\boldsymbol{\beta}$ 都有 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\dfrac{1}{2^r}$ 或 0。而由差分转移概率的定义可知，$\sum_{k=0}^{2^n-1}p_{F_{\text{new}}^n}\left(\boldsymbol{\alpha}\to\boldsymbol{\beta}^{(k)}\right)=1$，其中 $\boldsymbol{\beta}^{(k)}\left(k\in\{0,1,\cdots,2^n-1\}\right)$ 是全部 2^n 个不同的输出差分。所以存在 2^r 个 $\boldsymbol{\beta}^{(k)}$ 使 $p_{F_{\text{new}}^n}\left(\boldsymbol{\alpha}\to\boldsymbol{\beta}^{(k)}\right)=\dfrac{1}{2^r}$，其余的 2^n-2^r 个 $\boldsymbol{\beta}^{(k)}$ 使 $p_{F_{\text{new}}^n}\left(\boldsymbol{\alpha}\to\boldsymbol{\beta}^{(k)}\right)=0$。

$$\beta_i\oplus(\alpha_i\alpha_{i+1}\oplus\alpha_i\alpha_{i+2}\oplus\alpha_{i+4})=x_i(\alpha_{i+1}\oplus\alpha_{i+2})\oplus x_{i+1}\alpha_i\oplus x_{i+2}\alpha_i$$

令 $y_i=\beta_i\oplus(\alpha_i\alpha_{i+1}\oplus\alpha_i\alpha_{i+2}\oplus\alpha_{i+4}),i\in\{0,1,2,\cdots,n-1\},y_i\in\{0,1\}$。则有

$$y_i=x_i(\alpha_{i+1}\oplus\alpha_{i+2})\oplus x_{i+1}\alpha_i\oplus x_{i+2}\alpha_i,i\in\{0,1,2,\cdots,n-1\}$$

对于确定的 α_i 及 β_i，本文可以得到方程组 $y_i=x_i(\alpha_{i+1}\oplus\alpha_{i+2})\oplus x_{i+1}\alpha_i\oplus x_{i+2}\alpha_i$ 系数的值及 y_i 的值，所以该方程组就是 Z_2 上的非齐次线性方程组，并且其系数矩阵即为 F_{new}^n 的差分转移矩阵 $\boldsymbol{A}$。将该非齐次线性方程组用矩阵形式表示，如式(4)所示。

接下来，本文利用定理 3 给出的关系，通过研究 F_{new}^n 的差分转移矩阵的秩，得到 F_{new}^n 的非平凡差分转移概率的取值范围。

定理 4 设 $n\geqslant 5$，对于 F_{new}^n，任意输入差分 $\boldsymbol{\alpha}$ 及输出差分 $\boldsymbol{\beta}$，若差分转移概率 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})$ 不为0和1，那么 $\dfrac{1}{2^{n-1}}\leqslant p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\leqslant\dfrac{1}{8}$。

证明 设 F_{new}^n 的输入 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})$，输入差分 $\boldsymbol{\alpha}=(\alpha_0,\alpha_1,\cdots,\alpha_{n-1})$，输出差分 $\boldsymbol{\beta}=(\beta_0,\beta_1,\cdots,\beta_{n-1})$。

首先，对任意选定的 $\boldsymbol{\alpha}\neq 0$ 及输出差分 $\boldsymbol{\beta}$，若存在 $\boldsymbol{X}$ 满足 $\boldsymbol{\beta}=F(\boldsymbol{X})\oplus F(\boldsymbol{X}\oplus\boldsymbol{\alpha})$，则显然 $\boldsymbol{X}\oplus\boldsymbol{\alpha}$

满足此式，所以$\#\{\boldsymbol{X}\mid\boldsymbol{\beta}=F(\boldsymbol{X})\oplus F(\boldsymbol{X}\oplus\boldsymbol{\alpha})\}$非零时必为偶数。故当差分转移概率$p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\dfrac{\#\{\boldsymbol{X}\mid\boldsymbol{\beta}=F(\boldsymbol{X})\oplus F(\boldsymbol{X}\oplus\boldsymbol{\alpha})\}}{2^n}$非零时，其最小值为$\dfrac{1}{2^{n-1}}$，所以$p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\geqslant\dfrac{1}{2^{n-1}}$显然成立。

下面将证明对任意的$\boldsymbol{\alpha}=(\alpha_0,\alpha_1,\cdots,\alpha_{n-1})\neq 0$，$\boldsymbol{A}$的秩$r\geqslant 3$。由于$\boldsymbol{\alpha}\neq 0$，那么不妨设其中的一位$\alpha_i=1, i\in\{0,1,2,\cdots,n-1\}$。在$\boldsymbol{A}$中有 3 行与$\alpha_i$相关，分别是$\boldsymbol{A}_{i-2},\boldsymbol{A}_{i-1},\boldsymbol{A}_i$。$\begin{bmatrix}\boldsymbol{A}_{i-2}\\ \boldsymbol{A}_{i-1}\\ \boldsymbol{A}_i\end{bmatrix}$经过初等变换后可以得到$\begin{bmatrix}\alpha_{i-1}\oplus\alpha_i & \alpha_{i-2} & \alpha_{i-2} & 0 & 0 & \cdots & 0\\ 0 & \alpha_i\oplus\alpha_{i+1} & \alpha_{i-1} & \alpha_{i-1} & 0 & \cdots & 0\\ 0 & 0 & \alpha_{i+1}\oplus\alpha_{i+2} & \alpha_i & \alpha_i & \cdots & 0\end{bmatrix}$。若$\boldsymbol{A}_{i-2},\boldsymbol{A}_{i-1},\boldsymbol{A}_i$线性无关，则$\begin{bmatrix}\boldsymbol{A}_{i-2}\\ \boldsymbol{A}_{i-1}\\ \boldsymbol{A}_i\end{bmatrix}$的秩即为 3，那么显然有$\boldsymbol{A}$的秩$r\geqslant 3$；若$\boldsymbol{A}_{i-2},\boldsymbol{A}_{i-1},\boldsymbol{A}_i$线性相关，则存在不全为 0 的$k_0,k_1,k_2\in\{0,1\}$使$k_0\boldsymbol{A}_{i-2}+k_1\boldsymbol{A}_{i-1}+k_2\boldsymbol{A}_i=0$，表示为线性方程组，如式(5)所示。

$$\begin{cases}k_0\alpha_{i-1}+k_0\alpha_i=0\\ k_0\alpha_{i-2}+k_1\alpha_i+k_1\alpha_{i+1}=0\\ k_0\alpha_{i-2}+k_1\alpha_{i-1}+k_2\alpha_{i+1}+k_2\alpha_{i+2}=0\\ k_1\alpha_{i-1}+k_2\alpha_i=0\\ k_2\alpha_i=0\end{cases}\tag{5}$$

由$k_2\alpha_i=0$可知$k_2=0$。下面分别讨论α_{i-1}取值为 0 和 1 这 2 种情况。

情形 1　若$\alpha_{i-1}=0$，由$k_0\alpha_{i-1}+k_0\alpha_i=0$得$k_0=0$。因为$k_0$、$k_1$、$k_2$不全为 0，所以必有$k_1=1$。那么由$k_0\alpha_{i-2}+k_1\alpha_i+k_1\alpha_{i+1}=0$得$\alpha_{i+1}=\alpha_i=1$，最后根据$k_0\alpha_{i-2}+k_1\alpha_{i-1}+k_2\alpha_{i+1}+k_2\alpha_{i+2}=0$有$\alpha_{i-1}=0$。考虑$\boldsymbol{A}_{i-2},\boldsymbol{A}_i,\boldsymbol{A}_{i+1}$，经初等变换后有

$$\begin{bmatrix}\boldsymbol{A}_{i-2}\\ \boldsymbol{A}_i\\ \boldsymbol{A}_{i+1}\end{bmatrix}=\begin{bmatrix}1 & \alpha_{i-2} & \overline{\alpha_{i-2}} & 0 & 0 & 0 & \cdots & 0\\ 0 & 0 & \overline{\alpha_{i+2}} & 1 & 1 & 0 & \cdots & 0\\ 0 & 0 & 0 & \alpha_{i+2}\oplus\alpha_{i+3} & 1 & 1 & \cdots & 0\end{bmatrix}$$

其中，$\overline{\alpha_{i+2}}$是α_{i+2}的补，可以看到此时$\boldsymbol{A}_{i-2},\boldsymbol{A}_i,\boldsymbol{A}_{i+1}$线性无关，所以$\boldsymbol{A}$的秩$r\geqslant 3$。

情形 2　若$\alpha_{i-1}=1$，由$k_1\alpha_{i-1}+k_2\alpha_i=0$知$k_1=0$。因为$k_0$、$k_1$、$k_2$不全为 0，所以必有$k_0=1$。再由$k_0\boldsymbol{\alpha}_{i-1}+k_0\boldsymbol{\alpha}_i=0$得$\boldsymbol{\alpha}_{i-1}=\boldsymbol{\alpha}_i=1$，最后由$k_0\boldsymbol{\alpha}_{i-2}+k_1\boldsymbol{\alpha}_i+k_1\boldsymbol{\alpha}_{i+1}=0$有$\boldsymbol{\alpha}_{i-2}=0$。此时考虑$\boldsymbol{A}_{i-3},\boldsymbol{A}_{i-1},\boldsymbol{A}_i$，经初等变换后有

$$\begin{bmatrix}\boldsymbol{A}_{i-3}\\ \boldsymbol{A}_{i-1}\\ \boldsymbol{A}_i\end{bmatrix}=\begin{bmatrix}1 & \alpha_{i-3} & \overline{\alpha_{i-3}} & 0 & 0 & 0 & \cdots & 0\\ 0 & 0 & \overline{\alpha_{i+1}} & 1 & 1 & 0 & \cdots & 0\\ 0 & 0 & 0 & \alpha_{i+1}\oplus\alpha_{i+2} & 1 & 1 & \cdots & 0\end{bmatrix}$$

可以看到，此时$\boldsymbol{A}_{i-3}$、$\boldsymbol{A}_{i-1}$、$\boldsymbol{A}_i$线性无关，所以$\boldsymbol{A}$的秩$r\geqslant 3$。

经过上面讨论可知，对任意输入差分$\boldsymbol{\alpha}\neq 0$，$\boldsymbol{A}$的秩$r\geqslant 3$。根据定理 3，任取输出差分$\boldsymbol{\beta}$，若$p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\neq 0$，则必有$p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\dfrac{1}{2^r}\leqslant\dfrac{1}{8}$，证毕。

5　F_{new}^5的差分分布

本节要解决F_{new}^5所有输入差分对应的非平凡差分转移概率的分布情况。首先给出 2 个一般性的结论，如定理 5 和定理 6 所示。

定理 5　设$n\geqslant 5$，对于F_{new}^n，任意输入差分$\boldsymbol{\alpha}\neq\boldsymbol{0}$及输出差分$\boldsymbol{\beta},\boldsymbol{\beta}'\in Z_2^n$，设$\sigma_k(\boldsymbol{\alpha})$为对$\boldsymbol{\alpha}$循环左移$k$位，那么令$\boldsymbol{\alpha}'=\sigma_k(\boldsymbol{\alpha}),\forall k\in\{1,2,\cdots,n-1\}$，若$p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\neq 0$且$p_{F_{\text{new}}^n}(\boldsymbol{\alpha}'\to\boldsymbol{\beta}')\neq 0$，则$p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=p_{F_{\text{new}}^n}(\boldsymbol{\alpha}'\to\boldsymbol{\beta}')$。

证明　不妨先设$k=1$，对$\boldsymbol{\alpha}=(\alpha_0,\alpha_1,\cdots,\alpha_{n-1})$，有$\boldsymbol{\alpha}'=(\alpha_1,\alpha_2,\cdots,\alpha_{n-1},\alpha_0)$。记$F_{\text{new}}^n$在输入差分为$\boldsymbol{\alpha}$与$\boldsymbol{\alpha}'$时的差分转移矩阵分别为$\boldsymbol{A}^a$和$\boldsymbol{A}^{a'}$。那么有$\boldsymbol{A}^a=$

$$\begin{bmatrix}\alpha_1\oplus\alpha_2 & \alpha_0 & \alpha_0 & 0 & \cdots & 0 & 0 & 0\\ 0 & \alpha_2\oplus\alpha_3 & \alpha_1 & \alpha_1 & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \cdots & \alpha_{n-2}\oplus\alpha_{n-1} & \alpha_{n-3} & \alpha_{n-3}\\ \alpha_{n-2} & 0 & 0 & 0 & \cdots & 0 & \alpha_{n-1}\oplus\alpha_0 & \alpha_{n-2}\\ \alpha_{n-1} & \alpha_{n-1} & 0 & 0 & \cdots & 0 & 0 & \alpha_0\oplus\alpha_1\end{bmatrix}$$

在Z_2上对其进行初等变换可以转化为

$$\begin{bmatrix}\alpha_2\oplus\alpha_3 & \alpha_1 & \alpha_1 & 0 & \cdots & 0 & 0 & 0\\ 0 & \alpha_3\oplus\alpha_4 & \alpha_2 & \alpha_2 & \cdots & 0 & 0 & 0\\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & 0 & \cdots & \alpha_{n-1}\oplus\alpha_0 & \alpha_{n-2} & \alpha_{n-2}\\ \alpha_{n-1} & 0 & 0 & 0 & \cdots & 0 & \alpha_0\oplus\alpha_1 & \alpha_{n-1}\\ \alpha_0 & \alpha_0 & 0 & 0 & \cdots & 0 & 0 & \alpha_1\oplus\alpha_2\end{bmatrix}=\boldsymbol{A}^{a'}$$

因为初等变化不改变矩阵的秩，所以必有$\text{rank}(\boldsymbol{A}^a)=\text{rank}(\boldsymbol{A}^{a'})=r$。根据定理 3，若$p_{F_{\text{new}}^n}(\boldsymbol{\alpha}\to$

$\boldsymbol{\beta}) \neq 0$ 且 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha}' \to \boldsymbol{\beta}') \neq 0$，则 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = p_{F_{\text{new}}^n}(\boldsymbol{\alpha}' \to \boldsymbol{\beta}') = \frac{1}{2^r}$。所以 $k=1$ 时定理成立。

另外只需将上面的 $\boldsymbol{\alpha}$ 替换成 $\sigma_1(\boldsymbol{\alpha})$，$\boldsymbol{\alpha}'$ 替换成 $\sigma_2(\boldsymbol{\alpha})$，就有 $k=2$ 时成立。同样地，k 为其他值时定理均成立，证毕。

定理 6 设 $n \geqslant 5$，对于 F_{new}^n，给定输入差分 $\boldsymbol{\alpha} = (\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) \neq 0$，设 $\boldsymbol{\alpha}$ 的汉明重量为 $w(\boldsymbol{\alpha})$，对于任意输出差分 $\boldsymbol{\beta}$，若 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) \neq 0$，那么当 $w(\boldsymbol{\alpha})=1$ 时，$p_{F_{\text{new}}^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = \frac{1}{8}$；当 $w(\boldsymbol{\alpha}) = n-1$ 或 n 时，$p_{F_{\text{new}}^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = \frac{1}{2^{n-1}}$。

证明 当 $w(\boldsymbol{\alpha})=1$ 时，考虑 $\boldsymbol{\alpha}' = (0,0,\cdots,0,1)$ 时的情况，即 $\boldsymbol{\alpha}'_{n-1}=1$ 而其余位置均为 0。此时将 $\boldsymbol{A} = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 1 & 1 & \cdots & 0 & 0 & 0 \end{bmatrix}$ 在 Z_2 上进行初等变换，可以得到有 3 行非零的阶梯型矩阵 $\begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}$，所以此时 $\boldsymbol{A}$ 的秩 $r=3$，由定理 3 可知，对于任意输出差分 β，若 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha}' \to \boldsymbol{\beta}) \neq 0$，有 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha}' \to \boldsymbol{\beta}) = \frac{1}{2^r} = \frac{1}{8}$。又由定理 5，若 $w(\boldsymbol{\alpha})=1$，必然存在 $k \in \{0,1,2,\cdots,n-1\}$ 使得 $\boldsymbol{\alpha} = \sigma_k(\boldsymbol{\alpha}')$，所以 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) \neq 0$ 时就有 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = \frac{1}{8}$。

当 $w(\boldsymbol{\alpha}) = n-1$ 时，同样地，考虑 $\boldsymbol{\alpha}' = (0,1,\cdots,1,1)$ 时的情况，即 $\boldsymbol{\alpha}'_0 = 0$ 而其余位置均为 1。此时 $\boldsymbol{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$，在 Z^2 上进行初等变换，可以得到有 $n-1$ 行非零的阶梯型矩阵 $\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 1 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$，所以 $\boldsymbol{A}$ 的秩 $r=n-1$。由定理 3 可知，存在 2^{n-1} 个不同的 $\boldsymbol{\beta}$ 使 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = \frac{1}{2^{n-1}}$。又由定理 5，若 $w(\boldsymbol{\alpha}) = n-1$，必然存在 $k \in \{0,1,2,\cdots,n-1\}$ 使 $\boldsymbol{\alpha} = \sigma_k(\boldsymbol{\alpha}')$，所以 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) \neq 0$ 时就有 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha}' \to \boldsymbol{\beta}) = \frac{1}{2^{n-1}}$。

当 $w(\boldsymbol{\alpha}) = n$ 时，相应的 $\boldsymbol{A} = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 1 & 0 & \cdots & 0 \\ & & & \ddots & & & \\ 1 & 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 1 & 0 & 0 & 0 & \cdots & 0 \end{bmatrix}$ 在 Z^2 上对其进行初等变换，可以得到有 $n-1$ 行非零的阶梯型矩阵 $\begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ & & & \ddots & & & \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$，所以 $\boldsymbol{A}$ 的秩 $r=n-1$。由定理 3 可知，存在 2^{n-1} 个不同的 $\boldsymbol{\beta}$ 使 $p_{F_{\text{new}}^n}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = \frac{1}{2^{n-1}}$，证毕。

由定理 6 可知，F_{new}^5 在输入差分 α 的汉明重量 $w(\alpha)=1$ 时，对应的非平凡差分转移概率 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = \frac{1}{8}$；当 $w(\boldsymbol{\alpha})=4$ 和 $w(\boldsymbol{\alpha})=5$ 时，对应的非平凡差分转移概率 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha} \to \boldsymbol{\beta}) = \frac{1}{2^{5-1}} = \frac{1}{16}$。

根据定理 5 可知，循环移位等价的 2 个输入差分对应的非平凡差分转移概率是相等的。从而本文可以根据循环移位等价将 $w(\boldsymbol{\alpha})=2$ 和 $w(\boldsymbol{\alpha})=3$ 时的 $\boldsymbol{\alpha}$ 进行分类。

F_{new}^5 的输入差分 $\boldsymbol{\alpha}$ 在 $w(\boldsymbol{\alpha})=2$ 时根据循环移位等价可以分为 $\{\sigma_k(5) \mid k \in Z\} = \{5,9,10,18,20\}$ 和 $\{\sigma_k(3) \mid k \in Z\} = \{3,6,12,17,24\}$ 2 类。在 $w(\boldsymbol{\alpha})=3$ 时也可以分为 $\{\sigma_k(11) \mid k \in Z\} = \{11,13,21,22,26\}$ 和 $\{\sigma_k(7) \mid k \in Z\} = \{7,14,19,25,29\}$ 两类。由定理 5 可

知，同一类中的输入差分对应相同的非平凡差分转移概率。经验证可知，$\{\sigma_k(5)\,|\,k\in Z\}$ 和 $\{\sigma_k(11)\,|\,k\in Z\}$ 对应的非平凡差分转移概率 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{16}$，记这 2 个集合的并集为 $\Omega_1=\{5,9,10,18,20,11,13,21,22,26\}$；而 $\{\sigma_k(3)\,|\,k\in Z\}$ 和 $\{\sigma_k(7)\,|\,k\in Z\}$ 对应的非平凡差分转移概率 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{8}$，记这 2 个集合的并集为 $\Omega_2=\{3,6,12,17,24,7,14,19,25,29\}$。至此本文已经得到 F_{new}^5 的输入差分 $\boldsymbol{\alpha}$ 在 $w(\boldsymbol{\alpha})=2$ 和 $w(\boldsymbol{\alpha})=3$ 时对应的非平凡差分转移概率情况。

接下来，给出 F_{new}^5 在取到最大非平凡差分转移概率和最小非平凡差分转移概率时的充要条件。

定理 7　设 F_{new}^5 的输入差分为 $\boldsymbol{\alpha}$，其汉明重量为 $w(\boldsymbol{\alpha})$，对任意 $\boldsymbol{\beta}\in Z_5$，如果 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\neq 0$，当且仅当 $\boldsymbol{\alpha}\in\Omega_1\cup\{\boldsymbol{\alpha}|w(\boldsymbol{\alpha})=4\&\ \ w(\boldsymbol{\alpha})=5\}$ 时，$p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{16}$；当且仅当 $\boldsymbol{\alpha}\in\Omega_2\cup\{\boldsymbol{\alpha}|\ w(\boldsymbol{\alpha})=1\}$ 时，$p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{8}$。

证明　由于 $w(\boldsymbol{\alpha})\in\{0,1,2,3,4,5\}$。当 $w(\boldsymbol{\alpha})=0$ 时，$p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=0$ 或 1；由定理 6，当 $w(\boldsymbol{\alpha})=4$ 或 $w(\boldsymbol{\alpha})=5$ 时，若 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\neq 0$，则有 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{16}$，而当 $w(\boldsymbol{\alpha})=1$ 时，若 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\beta)\neq 0$，则有 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{8}$；又根据上面的讨论，当 $w(\boldsymbol{\alpha})=2$ 或 $w(\boldsymbol{\alpha})=3$ 时，若 $\boldsymbol{\alpha}\in\Omega_1$，则其对应的非平凡差分转移概率 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{16}$，而若 $\boldsymbol{\alpha}\in\Omega_2$，则其对应的非平凡差分转移概率 $p_{F_{\text{new}}^5}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{8}$。

由定理 4 可知，F_{new}^5 的最小非平凡差分转移概率和最大非平凡差分转移概率分别为 $\frac{1}{16}$ 和 $\frac{1}{8}$。综上讨论 $\boldsymbol{\alpha}$ 的所有情况可知，当且仅当 $\boldsymbol{\alpha}\in\Omega_1\cup\{\boldsymbol{\alpha}|w(\boldsymbol{\alpha})=4\&w(\boldsymbol{\alpha})=5\}$ 时，$\boldsymbol{\alpha}$ 对应的非平凡差分转移概率为 F_{new}^5 可取到的最小值 $\frac{1}{16}$；当且仅当 $\boldsymbol{\alpha}\in\Omega_2\cup\{\boldsymbol{\alpha}|w(\boldsymbol{\alpha})=1\}$ 时，α 对应的非平凡差分转移概率为 F_{new}^5 可取到的最大值 $\frac{1}{8}$，证毕。

最后本文给出 F_{new}^5 和 F_K^5 的差分转移概率的计数，具体如表 1 所示。通过观察 F_{new}^5 和 F_K^5 的差分转移概率的计数可以发现，F_{new}^5 比 F_K^5 有更小的非平凡差分转移概率。另外，F_{new}^5 的差分转移概率为 0 的情况相比 F_K^5 要少，这说明 F_{new}^5 相比 F_K^5 差分分布更加均匀，因此该 S 盒的差分性质比 Keccak 的 S 盒更好。

表 1　F_{new}^5 和 F_K^5 的差分转移概率计数

差分转移概率	F_{new}^5	F_K^5
1	1	1
$\frac{1}{4}$	0	20
$\frac{1}{8}$	120	120
$\frac{1}{16}$	256	176
0	647	707

6　结束语

虽然目前有许多密码已经使用了基于元胞自动机的 S 盒，但都使用了 Keccak 的局部规则或者仿射变换。本文通过实验找到了一类新的基于元胞自动机的 S 盒并研究了其置换性质和差分性质，证明了该类 S 盒在规模为 5 时是一个置换，并且其非平凡差分转移概率的取值范围为 $\left[\frac{1}{2^{n-1}},\frac{1}{8}\right]$，而 Keccack 的 S 盒的非平凡差分转移概率的取值范围则为 $\left[\frac{1}{2^{n-1}},\frac{1}{4}\right]$[13]。另外，本文进一步研究了该类 S 盒在规模为 5 时的差分分布情况，给出了该类 S 盒在取到最大和最小非平凡差分转移概率时的充要条件。最后通过比较 F_{new}^5 和 F_K^5 的差分转移概率的计数情况可以发现，F_{new}^5 相比 F_K^5 差分分布更加均匀。所以该类 S 盒有着比 Keccak 类 S 盒更好的差分性质。接下来的工作重点是从理论上研究这类 S 盒抵抗线性分析以及立方攻击[14]等各类攻击方法的效果。

参考文献：

[1] MARIOT L, PICEK S, LEPORATI A, et al. Cellular automata based S-boxes[J]. Cryptography and Communications, 2019, 11(1):41-62.

[2] NIST. Announcing request for candidate algorithm nominations for a new cryptographic hash algorithm (SHA-3) family[EB]. Gaithersburg: National Institute of Standards and Technology, 2007.

[3] BERTONI G, DAEMEN J, PEETERS M, et al. The KECCAK reference, SHA-3 competition (round 3)[EB]. STMicroelectronics, NXP Semiconductors, 2011.

[4] DAEMEN J, CLAPP C S K. Fast hashing and stream encryption with PANAMA[C]//International Workshop on FAST Software Encryption. Springer-Verlag, 1998:60-74.

[5] CLAESEN L, DAEMEN J, GENOE M, et al. Subterranean: a 600 Mbit/s cryptographic VLSI chip[C]//IEEE International Conference on Computer Design: VLSI in Computers and Processors. IEEE, 1993:610-613.

[6] DAEMEN J, GOVAERTS R, VANDEWALLE J. A new approach to block cipher design[C]//Fast Software Encryption. Cambridge Security Workshop, 1993:18-32.

[7] DOBRAUNING C, EICHLSEDER M, MENDEL F, et al. Ascon v1.2: submission to the CAESAR competition [EB]. Institute for Applied Information Processing and Communications，Infineon Technologies Austria AG, 2016.

[8] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[9] NAJI A W, HAMEED S A, ZAIDAN B B, et al. Novel framework for hidden data in the image page within executable file using computation between advanced encryption standard and distortion techniques[J]. International Journal of Computer Science and Information Security, 2009, 3(1): 73-78.

[10] PIEPRZYK J, FINKELSTEIN G. Towards effective nonlinear cryptosystem design[J]. IEE Proceedings E-Computers and Digital Techniques, 2005, 135(6):325-335.

[11] 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. Cryptography[M]. Beijing: Higher Education Press, 2009.

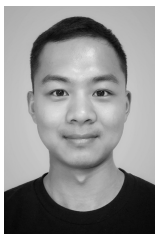
[12] 江志松. 元胞自动机的语法复杂性[D]. 苏州: 苏州大学, 2001.
JIANG Z S. The grammatical complexity of cellular automata[D]. Suzhou: Suzhou University, 2001.

[13] 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 Q N, LI Y Q, JIANG S J, et al. Research on differential properties of Keccak-like nonlinear transform[J]. Journal on Communications, 2012,33(9):140-146.

[14] DINUR I, MORAWIECKI P, PIEPRZYK J, et al. Cube attacks and cube-attack-like cryptanalysis on the round-reduced Keccak sponge function[J]. Theory and Application of Cryptographic Techniques, 2015: 733-761.

[作者简介]

关杰（1974– ），女，河南郑州人，博士，解放军战略支援部队信息工程大学教授、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（1995– ），男，浙江上虞人，解放军战略支援部队信息工程大学硕士生，主要研究方向为对称密码设计与分析。