一类动态 S 盒的构造与差分性质研究

刘国强* 金晨辉
(解放军信息工程大学密码工程学院 郑州 450004)

摘 要：该文对有限域的逆与仿射变换复合得到的动态 S 盒进行了研究。首先给出了动态 S 盒变换差分概率的刻画方法，并给出了动态 S 盒变换的差分对应是不可能差分对应的充分必要条件及不可能差分的个数。接着给出了动态 S 盒变换最大差分概率的上界及可达性。最后利用模拟实验的方法研究了由随机 S 盒来构造的动态 S 盒的差分性质。理论和实验分析都表明，这类动态 S 盒变换具有远好于单个 S 盒的差分特性。

关键词：密码学；分组密码；动态 S 盒；差分分析
中图分类号： TN918.1 **文献标识码**： A **文章编号**：1009-5896(2014)01-0074-08
DOI: 10.3724/SP.J.1146.2013.00416

Investigation on Construction and Differential Property of a Class of Dynamic S-box

Liu Guo-qiang Jin Chen-hui
(*Cryptography Engineering Institute*, *Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: This paper discusses the dynamic S-boxes using the combination of inversion mapping and an affine transformation over the finite field. First, a definition of differential probability for dynamic S-box is provided. Necessary and sufficient conditions of impossible differentials in dynamic S-box and the number of impossible differentials are presented. Then, an upper bound on the maximum differential probability of dynamic S-box is proved, and the accessibility of this bound is presented. Finally, the differential properties of dynamic S-box consisting of randomly chosen S-boxes are researched by simulation experiments. The theoretical and experimental analyses show that dynamic S-box is better than single S-box in differential properties.

Key words: Cryptography; Block cipher; Dynamic S-box; Differential cryptanalysis

1 引言

分组密码算法是现代密码学中一个重要的研究方向，其诞生和发展有着广泛的实用背景和重要的理论意义。S 盒是许多分组密码的唯一非线性模块，因此它的密码强度将直接影响整个分组密码的安全强度。S 盒的设计准则包括差分均匀性、非线性度、代数次数及项数分布等。要构造满足所有准则的 S 盒是非常困难的事情，目前 S 盒的设计主要采用随机选取并测试、利用密码结构、数学函数构造等方式。利用数学函数构造 S 盒通常能从理论上证明 S 盒的某些密码特性，并可以使用户相信没有陷门[1]。

有限域上乘法求逆变换构造的 S 盒能使最大差分概率和最大的 Walsh 谱的绝对值均很小，因而很多著名的分组密码算法都采用该变换作为 S 盒，例如 SHARK[2], SQUARE[3], AES[4]及 SMS4[5]等。然而在这些分组密码算法中，S 盒都是固定不变的。可以设想，如果能够根据密钥等可变因素决定 S 盒的选用，则密码算法的差分分布和线性分布将与密钥等可变因素有关，因而将显著提高密码算法的安全强度。目前，已有一些针对分组密码动态选择 S 盒的研究。2007 年，殷新春等人[6]对 Rijndael 算法的字节代替变换进行改进，提出了一种基于密钥控制的多 S 盒的 Rijndael 算法。2011 年，文献[7]提出了一种基于 CA(Cellular Automata)的 S 盒构造方法并对其密码学性质进行了分析。同年，Stoianov[8]构造了与 AES 中 S 盒性质相似的两个新的 S 盒，并在加解密过程中与 AES 的 S 盒、逆 S 盒一起动态选择使用。除此之外，文献[9–11]均给出了各种不同的动态 S 盒的构造方法。还有一些算法通过引入密钥因素构造秘密 S 盒提高算法的安全性。1990 年，Merkle[12]提出了带秘密 S 盒的 Khufu 算法。1994 年，Schneier[13]提出了一个 16 轮的 Feistel 密码算法，该算法中的 S 盒由密钥随机生成。2001 年，Biryukov 和 Shamir[14]研究了 S 盒与 P 盒都与密钥相关且未知的一种迭代模型 SASAS。2003 年，IBM, Intel,

2013-04-01 收到，2013-07-02 改回
国家自然科学基金(61272488, 61272041)资助课题
*通信作者：刘国强 liuguoqiang87@hotmail.com

Matsushita 和 Toshiba[15]发布一种用于 DVD 加密的 10 轮 Feistel 密码算法 C2, C2 算法中的 S 盒为 8 进 8 出的秘密 S 盒。2010 年，Kundsen 等人[16]提出了一个轻量级分组密码算法 $\mathrm{PRINT}_{\mathrm{CIPHER}}$，该算法在 S 盒前引入了与密钥相关的置换。文献[17]指出，$\mathrm{PRINT}_{\mathrm{CIPHER}}$ 的秘密置换与 S 盒可看作为从 32 个 S 盒中按密钥进行选择的动态 S 盒。而对于具有良好密码学性质的 S 盒的构造方面，文献[18–23]均给出了不同的构造方法。

本文针对各 S 盒均是有限域 $\mathrm{GF}(2^n)$上的乘法逆与仿射变换复合的情形，以使不可能差分对应的个数和最大差分转移概率尽量小为目标，研究了动态 S 盒变换的设计问题。本文首先给出了动态 S 盒变换的差分概率的刻画方法，给出了动态 S 盒变换的差分对应是不可能差分对应的充分必要条件及不可能差分的个数。接着给出了动态 S 盒变换最大差分概率的上界及可达性，并对随机 S 盒构造的动态 S 盒的差分性质进行了分析。

2　动态 S 盒的基本结构

本文若无特别说明，均以 $\boldsymbol{A}\boldsymbol{\alpha}$ 表示矩阵 $\boldsymbol{A}$ 与向量 $\boldsymbol{\alpha}$ 相乘，以 $\boldsymbol{\alpha}\times\boldsymbol{\beta}$ 表示向量 $\boldsymbol{\alpha}$ 对应的多项式与向量 $\boldsymbol{\beta}$ 对应的多项式相乘。

定义 1　设 $S_i:\{0,1\}^n\to\{0,1\}^n, i\in\{0,1\}^m$，则称 $\{S_i\}_{i=0}^{2^m-1}$ 为动态 S 盒，并称动态 S 盒由 $S_0,S_2,\cdots,S_{2^m-1}$ 构成。

不失一般性，本文总假设控制参数服从均匀分布。下面研究如何定义动态 S 盒 $\{S_i\}_{i=0}^{2^m-1}$ 的差分概率分布问题。

假设在密码算法的一条差分路径中的活动 S 盒分别为 $S_{k_1},S_{k_2},\cdots,S_{k_t}$，且 S_{k_i} 的输入差和输出差分别为 α_i 和 β_i，则该差分路径的差分概率为

$$p_{(k_1,\cdots,k_t)}=\prod_{i=1}^{t}p_{S_{k_i}}(\alpha_i\to\beta_i)\tag{1}$$

因而在 $k_1,k_2,\cdots,k_t$ 相互独立且都在 $\{0,1\}^m$ 上服从均匀分布的假设下，$p_{(k_1,\cdots,k_t)}$ 的数学期望为

$$\begin{aligned}E\left(p_{(k_1,\cdots,k_t)}\right)&=\frac{1}{2^{mt}}\sum_{k_1,\cdots,k_t\in\{0,1\}^m}p_{(k_1,\cdots,k_t)}\\&=\frac{1}{2^{mt}}\sum_{k_1,\cdots,k_t\in\{0,1\}^m}\prod_{i=1}^{t}p_{S_{k_i}}(\alpha_i\to\beta_i)\\&=\prod_{i=1}^{t}\frac{1}{2^m}\sum_{k_i\in\{0,1\}^m}p_{S_{k_i}}(\alpha_i\to\beta_i)\\&=\prod_{i=1}^{t}E\left(p_{S_{k_i}}(\alpha_i\to\beta_i)\right)\end{aligned}\tag{2}$$

据此，下面给出动态 S 盒差分对应 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 差分概率的定义。

定义 2　设 $S_i:\{0,1\}^n\to\{0,1\}^n, i\in\{0,1\}^m, \boldsymbol{\alpha},\boldsymbol{\beta}\in\{0,1\}^n$，则称

$$\begin{aligned}p_{S_i}(\boldsymbol{\alpha}\to\boldsymbol{\beta})&=E\left(p_{S_i}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\right)\\&=\frac{1}{2^m}\sum_{i\in\{0,1\}^m}p_{S_i}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\end{aligned}\tag{3}$$

为动态 S 盒 $\{S_i\}_{i=0}^{2^m-1}$ 的差分对应 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 的差分概率。

下面针对诸 S 盒 $S_0,S_2,\cdots,S_{2^m-1}$ 都是有限域 $\mathrm{GF}(2^n)$ 上的乘法逆变换与仿射函数的复合这一情形，研究动态 S 盒 $\{S_i\}_{i=0}^{2^m-1}$ 的设计及其差分分布问题。动态 S 盒 $\{S_i\}_{i=0}^{2^m-1}$ 的一般结构如图 1 所示，图 2 和图 3 是其两个特例。

显然，从差分分布和线性分布的角度来看，特例 3 是特例 2 的逆变换。由于特例 2 和特例 3 只涉及 1 层密钥且结构比较简单，既容易分析也容易实现，因而以下仅对特例 2 进行分析而不再分析特例 3 和一般结构。本文考察的密码指标主要是其最大差分概率和不可能差分对应的个数，本文将以使最大差分概率和不可能差分对应的个数极小化为目标，研究此类动态 S 盒的设计问题。

在以下的分析中，本文均假设控制参数 i 在 $\{0,1\}^m$ 上服从均匀分布。首先给出此类动态 S 盒差分概率的刻画形式。

引理 1　设 $\boldsymbol{A}$ 是二元域上的 $n\times n$ 可逆矩阵，$\boldsymbol{\alpha},\boldsymbol{\beta}\in\{0,1\}^n$，S 盒由 $\mathrm{GF}(2^n)$ 上的乘法逆变换 x^{-1} 及 $[\mathrm{GF}(2)]^n$ 上的仿射双射 $L(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}\oplus\boldsymbol{\alpha}$ 的复合构成，即 $S(\boldsymbol{x})=\boldsymbol{A}\boldsymbol{x}^{-1}\oplus\boldsymbol{b}$，则有 $p_s(\boldsymbol{\alpha}\to\boldsymbol{\beta})=p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}^{-1}\boldsymbol{\beta})$。

证明

$$\begin{aligned}p_S(\boldsymbol{\alpha}\to\boldsymbol{\beta})&=\frac{1}{2^n}\#\left\{\boldsymbol{x}\in Z_2^n:\left[\boldsymbol{A}(\boldsymbol{x}\oplus\boldsymbol{\alpha})^{-1}\oplus\boldsymbol{b}\right]\right.\\&\qquad\left.\oplus\left[\boldsymbol{A}\boldsymbol{x}^{-1}\oplus\boldsymbol{b}\right]=\boldsymbol{\beta}\right\}\\&=\frac{1}{2^n}\#\left\{\boldsymbol{x}\in Z_2^n:(\boldsymbol{x}\oplus\boldsymbol{\alpha})^{-1}\right.\\&\qquad\left.\oplus\,\boldsymbol{x}^{-1}=\boldsymbol{A}^{-1}\boldsymbol{\beta}\right\}\\&=p_{x^{-1}}\left(\boldsymbol{\alpha}\to\boldsymbol{A}^{-1}\boldsymbol{\beta}\right)\end{aligned}\tag{4}$$

证毕

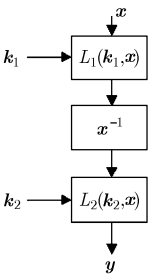

图 1 动态 S 盒的一般结构

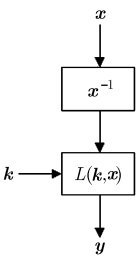

图 2 动态 S 盒的特例 1

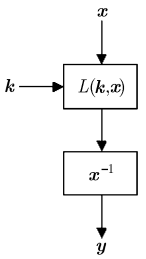

图 3 动态 S 盒的特例 2

推论 1 设 $\boldsymbol{A}_i$ 是二元域上的 $n\times n$ 可逆矩阵，$\boldsymbol{\alpha},\boldsymbol{\beta},\boldsymbol{\alpha}_i,\boldsymbol{b}_i\in\{0,1\}^n$，动态 S 盒 $\{S_i\}_{i=1}^m$ 是 $\mathrm{GF}(2^n)$ 上的乘法逆变换 x^{-1} 及二元域上的 m 个 n 维仿射双射 $L_i(\boldsymbol{x})=\boldsymbol{A}_i\boldsymbol{x}\oplus\boldsymbol{a}_i$ 的复合，即 $S_i(\boldsymbol{x})=\boldsymbol{A}_i\boldsymbol{x}^{-1}\oplus\boldsymbol{b}_i$，则动态 S 盒的差分对应 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 的差分概率为

$$\frac{1}{m}\sum_{i=1}^{m}p_{x^{-1}}\left(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta}\right)$$

推论 1 说明，针对由 $\mathrm{GF}(2^n)$ 上的乘法逆变换 x^{-1} 及二元域上的 m 个 n 维仿射双射 $L_i(\boldsymbol{x})=\boldsymbol{A}_i\boldsymbol{x}\oplus\boldsymbol{a}_i$ 的复合构造的动态 S 盒，其差分概率的分析可以归结为对乘法逆变换 x^{-1} 在输入差固定且输出差变动时的平均差分概率的分析。因此，可以借助于乘法逆变换 x^{-1} 的差分分布，确定动态 S 盒的差分分布。下面先给出动态 S 盒的设计准则与构造方法。

3 动态 S 盒的设计准则与不可能差分对应个数

不可能差分对应就是差分概率为 0 的差分对应。下面首先讨论动态 S 盒中不可能差分对应的个数问题，并由此刻画动态 S 盒的差分均匀性。显然，不可能差分对应的个数越少，则意味着差分分布可能越均匀。

引理 2[24] 设 n 为偶数，S 变换为 $\mathrm{GF}(2^n)$ 上的乘法求逆变换，则任意的 $\boldsymbol{\alpha}\in\mathrm{GF}(2^n)\setminus\{0\}$，有：

(1) $p(\boldsymbol{\alpha}\to\boldsymbol{\beta})=2^{2-n}$ 的充分必要条件为 $\boldsymbol{\beta}=\boldsymbol{\alpha}^{-1}$。

(2) 任意的 $\boldsymbol{\beta}\in\mathrm{GF}(2^n)\setminus\{\boldsymbol{\alpha}^{-1},0\}$，$p(\boldsymbol{\alpha}\to\boldsymbol{\beta})=p(\boldsymbol{\alpha}\times\boldsymbol{\beta}\to1)=2^{1-n}$ 且 $p(\boldsymbol{\alpha}\to\boldsymbol{\beta})=2^{1-n}$ 的充分必要条件是 $\mathrm{Tr}_{\mathrm{GF}(2^n)}((\boldsymbol{\alpha}\times\boldsymbol{\beta})^{-1})=0$。

(3) 使 $p(\boldsymbol{\alpha}\to\boldsymbol{\beta})=2^{2-n}$ 的 $\boldsymbol{\beta}$ 只有 1 个，使 $p(\boldsymbol{\alpha}\to\boldsymbol{\beta})=2^{1-n}$ 的 $\boldsymbol{\beta}$ 共有 $2^{n-1}-2$ 个。

推论 2[24] 设 $\boldsymbol{a},\boldsymbol{b}\in\mathrm{GF}(2^n)\setminus\{0\}$，S 变换为 $\mathrm{GF}(2^n)$ 上的乘法求逆变换，则 $p_S(\boldsymbol{a}\to\boldsymbol{b})\neq0$ 的充分必要条件是 $\mathrm{Tr}_{\mathrm{GF}(2^n)}(\boldsymbol{a}^{-1}\times\boldsymbol{b}^{-1})=0$。

定理 1 设 n 为偶数，$\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathrm{GF}(2^n)\setminus\{0\}$，动态 S 盒由 $\mathrm{GF}(2^n)$ 上的乘法逆变换 x^{-1} 及二元域上的 m 个 n 维仿射双射 $L_i(\boldsymbol{x})=\boldsymbol{A}_i\boldsymbol{x}\oplus\boldsymbol{a}_i$ 的复合构成，则 $\sum_{i=1}^m p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$ 的充分必要条件为

$$\left.\begin{aligned}\mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\left(\boldsymbol{A}_1^{-1}\boldsymbol{\beta}\right)^{-1}\times\boldsymbol{\alpha}^{-1}\right)=1\\ \mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\left(\boldsymbol{A}_2^{-1}\boldsymbol{\beta}\right)^{-1}\times\boldsymbol{\alpha}^{-1}\right)=1\\ \vdots\\ \mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\left(\boldsymbol{A}_m^{-1}\boldsymbol{\beta}\right)^{-1}\times\boldsymbol{\alpha}^{-1}\right)=1\end{aligned}\right\}\tag{5}$$

成立。

证明 由推论 2 知，$p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$ 等价于 $\mathrm{Tr}_{\mathrm{GF}(2^n)}((\boldsymbol{A}_i^{-1}\boldsymbol{\beta})^{-1}\times\boldsymbol{\alpha}^{-1})=1$，故 $\sum_{i=1}^m p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$ 等价于对满足 $1\le i\le m$ 的 i，都有 $\mathrm{Tr}_{\mathrm{GF}(2^n)}((\boldsymbol{A}_i^{-1}\boldsymbol{\beta})^{-1}\times\boldsymbol{\alpha}^{-1})=1$。 证毕

定理 2 设 n 为偶数，$\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathrm{GF}(2^n)\setminus\{0\}$，动态 S 盒由 $\mathrm{GF}(2^n)$ 上的乘法逆变换 x^{-1} 及二元域上的 m 个 n 维仿射双射 $L_i(\boldsymbol{x})=\boldsymbol{A}_i\boldsymbol{x}\oplus\boldsymbol{a}_i$ 的复合构成，则：

(1)对于给定的输出差 $\boldsymbol{\beta}\neq0$，使得 $\sum_{i=1}^m p_{x^{-1}}\cdot(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$ 的输入差 $\boldsymbol{\alpha}$ 的个数要么是 1，要么是 $2^{n-R}+1$，其中 R 为 $(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1},(\boldsymbol{A}_2^{-1}\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 的秩。

(2)对于给定的输入差 $\boldsymbol{\alpha}\neq0$，使得 $\sum_{i=1}^m p_{x^{-1}}\cdot(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$ 的输出差 $\boldsymbol{\beta}$ 的个数为 $\left|\bigcap_{i=1}^m\cdot\boldsymbol{A}_i f_{\boldsymbol{\alpha}}^{-1}(1)\right|+1$，其中 $f_{\boldsymbol{\alpha}}(\boldsymbol{y})=\mathrm{Tr}_{\mathrm{GF}(2^n)}(\boldsymbol{y}^{-1}\boldsymbol{\alpha}^{-1})$。

证明 (1)首先考查对于给定的输出差 $\boldsymbol{\beta}\neq0$，使得 $\sum_{i=1}^m p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$ 的输入差 $\boldsymbol{\alpha}$ 的个数。由于 $\boldsymbol{\alpha}\neq0$，记 $\boldsymbol{x}=\boldsymbol{\alpha}^{-1}$，则有 $\boldsymbol{x}\neq0$，且方程组(5)等价于

$$\left.\begin{aligned}\mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\left(\boldsymbol{A}_1^{-1}\boldsymbol{\beta}\right)^{-1}\times\boldsymbol{x}\right)=1\\ \mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\left(\boldsymbol{A}_2^{-1}\boldsymbol{\beta}\right)^{-1}\times\boldsymbol{x}\right)=1\\ \vdots\\ \mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\left(\boldsymbol{A}_m^{-1}\boldsymbol{\beta}\right)^{-1}\times\boldsymbol{x}\right)=1\end{aligned}\right\}\tag{6}$$

故在 $\boldsymbol{\beta}$ 给定且 $\boldsymbol{\beta}\neq0$ 时，使 $\sum_{i=1}^m p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$ 的输入差分 $\boldsymbol{\alpha}$ 的个数为方程组(6)的解数加 1，其个数要么是 1(方程组无解的情形)，要么是 $2^{n-R}+1\ge2^{n-m}+1$(方程组解数为 2^{n-R} 的情形)，这里 R 为 $(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1},(\boldsymbol{A}_2^{-1}\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 的秩。

(2) 对于给定的输入差 $\boldsymbol{\alpha}\neq0$，考查使 $\sum_{i=1}^m p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$ 的输出差 $\boldsymbol{\beta}$ 的个数。使 $\sum_{i=1}^m p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$ 的输出差 $\boldsymbol{\beta}$ 的个数就是方程组

$$\left.\begin{aligned}\mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\left(\boldsymbol{A}_1^{-1}\boldsymbol{x}\right)^{-1}\times\boldsymbol{\alpha}^{-1}\right)=1\\ \mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\left(\boldsymbol{A}_2^{-1}\boldsymbol{x}\right)^{-1}\times\boldsymbol{\alpha}^{-1}\right)=1\\ \vdots\\ \mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\left(\boldsymbol{A}_m^{-1}\boldsymbol{x}\right)^{-1}\times\boldsymbol{\alpha}^{-1}\right)=1\end{aligned}\right\}\tag{7}$$

的解 $\boldsymbol{x}$ 的个数。设布尔函数 $f_{\boldsymbol{\alpha}}(\boldsymbol{y})=\mathrm{Tr}_{\mathrm{GF}(2^n)}(\boldsymbol{y}^{-1}\boldsymbol{\alpha}^{-1})$，则式(7)的解 $\boldsymbol{x}$ 的个数为 $\left|\bigcap_{i=1}^m\boldsymbol{A}_i f_{\boldsymbol{\alpha}}^{-1}(1)\right|$，又由于 $\boldsymbol{\beta}=0$，一定使 $\sum_{i=1}^m p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=0$，故输出差 $\boldsymbol{\beta}$ 的个数为 $\left|\bigcap_{i=1}^m\boldsymbol{A}_i f_{\boldsymbol{\alpha}}^{-1}(1)\right|+1$。 证毕

定理 2 之(1)说明在给定输出差 $\boldsymbol{\beta}\neq 0$ 时，随着向量组 $(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1},(\boldsymbol{A}_2^{-1}\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 秩的增大，对应的差分概率为 0 的输入差 $\boldsymbol{\alpha}$ 的个数成倍地降低。因此，在输出差给定时，为使对应的差分概率为 0 的输入差 $\boldsymbol{\alpha}$ 的个数尽量的少，应当使 $(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1}$, $(\boldsymbol{A}_2^{-1}\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 的秩极大化。定理 2 之(2)说明要使 $\left|\bigcap_{i=1}^{m}\boldsymbol{A}_i f_{\alpha}^{-1}(1)\right|+1$ 越小越好。设 $t<m$，显然，对于给定的 $\boldsymbol{\beta}\neq 0$，当 $(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1},(\boldsymbol{A}_2^{-1}\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 只有 t 个不同元时，其秩 $\leq t$，因而达不到最大值 m。故设计者希望所设计的动态 S 盒 $\{S_i\}_{i=1}^{m}$ 能够对于任意的 $\boldsymbol{\beta}\neq 0$，$(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1},(\boldsymbol{A}_2^{-1}\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 都是不同元，以使其秩可以达到最大值 m。反过来，对于给定的 $\boldsymbol{\alpha}\neq 0$，如果将 $f_{\boldsymbol{\alpha}}^{-1}(1)$ 看作一个随机选取的集合，由于

$$\bigcap_{i=1}^{m}\boldsymbol{A}_i f_{\boldsymbol{\alpha}}^{-1}(1)=\Big\{\boldsymbol{y}\in \mathrm{GF}(2^n):\exists \boldsymbol{x}_1,\cdots,\boldsymbol{x}_m\in f_{\boldsymbol{\alpha}}^{-1}(1),\ \text{s.t. } \boldsymbol{A}_1\boldsymbol{x}_1=\cdots=\boldsymbol{A}_m\boldsymbol{x}_m=\boldsymbol{y}\Big\} \tag{8}$$

故对任意的 $\boldsymbol{x}\in f_{\boldsymbol{\alpha}}^{-1}(1)$，若 $i\neq j$ 时，均有 $\boldsymbol{A}_i\boldsymbol{x}\neq\boldsymbol{A}_j\boldsymbol{x}$，由此减少了当从 $f_{\boldsymbol{\alpha}}^{-1}(1)$ 中随机选取 $\boldsymbol{x}_1,\cdots,\boldsymbol{x}_m$ 使 $\boldsymbol{A}_1\boldsymbol{x}_1=\cdots=\boldsymbol{A}_m\boldsymbol{x}_m$ 成立的可能性，从而有助于减少集合 $\bigcap_{i=1}^{m}\boldsymbol{A}_i f_{\boldsymbol{\alpha}}^{-1}(1)$ 中点的个数。

综上，可得到仿射双射簇 $L_i(\boldsymbol{x})=\boldsymbol{A}_i\boldsymbol{x}\oplus\boldsymbol{\alpha}_i$, $1\leq i\leq m$ 的设计标准：对任意 $\boldsymbol{\beta}\neq 0$ 及任意 $1\leq i,j\leq m$，均有 $\boldsymbol{A}_i^{-1}\boldsymbol{\beta}\neq\boldsymbol{A}_j^{-1}\boldsymbol{\beta}$。

下面给出在动态 S 盒满足仿射双射簇的设计标准时，其不可能差分对应的个数。首先讨论给定输出差 $\boldsymbol{\beta}\neq 0$ 时，动态 S 盒的不可能差分对应的个数问题。由仿射双射簇的设计标准知 $\boldsymbol{A}_1^{-1}\boldsymbol{\beta},\boldsymbol{A}_2^{-1}\boldsymbol{\beta},\cdots,\boldsymbol{A}_m^{-1}\boldsymbol{\beta}$ 互不相同，由于有限域上的逆变换 $f(\boldsymbol{x})=\boldsymbol{x}^{-1}$ 具有高度的非线性性，故即使 $\boldsymbol{A}_1^{-1}\boldsymbol{\beta},\boldsymbol{A}_2^{-1}\boldsymbol{\beta},\cdots,\boldsymbol{A}_m^{-1}\boldsymbol{\beta}$ 具有线性制约性(例如线性相关)，$(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1},(\boldsymbol{A}_2^{-1}\cdot\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 也一般不再具有线性制约性。因而可将 $(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1},(\boldsymbol{A}_2^{-1}\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 近似看作是从 $\mathrm{GF}(2^n)\setminus\{0\}$ 中随机选取的 m 个互不相同的向量。

本文利用模拟实验方法，给出有序向量组 $(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1},(\boldsymbol{A}_2^{-1}\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 的秩的数学期望的分布情况。针对 $m=3,4,\cdots,8$，分别从 $\mathrm{GF}(2^8)\setminus\{0\}$ 中随机选取 m 个互不相同的向量，计算出向量组 $(\boldsymbol{A}_1^{-1}\boldsymbol{\beta})^{-1},(\boldsymbol{A}_2^{-1}\boldsymbol{\beta})^{-1},\cdots,(\boldsymbol{A}_m^{-1}\boldsymbol{\beta})^{-1}$ 秩的期望值。对于每个 m，分别进行 35000 组实验，具体实验结果见表 1 所示。

从表 1 可以看出，当 $3\leq m\leq 8$ 时，随机选取的 m 个互不相同的向量的秩的期望值十分接近 m，这也使得不可能差分对应个数的期望值十分接近 $2^{n-m}+1$，只是比 $2^{n-m}+1$ 略大。通过实验可知，大多数情况下向量组的秩都是 m，这说明大多数情况下不可能差分对应个数就是 $2^{n-m}+1$。此外，还可看出，随着 m 的增大，其不可能差分对应的个数的期望值成倍递减。例如，当有限域为 $\mathrm{GF}(2^8)$ 且 $m=8$ 时，动态 S 盒不可能差分对应个数的期望值仅为 2.32。但是，使用单个 S 盒时，其不可能差分对应的个数为 129。这说明增大 m 将显著降低不可能差分对应的个数。

下面对给定输入差 $\boldsymbol{\alpha}\neq 0$ 时，动态 S 盒中不可能差分对应的个数问题进行粗略的分析。由于对 $\forall\boldsymbol{x}\in f_{\boldsymbol{\alpha}}^{-1}(1)$，当 $i\neq j$ 时均有 $\boldsymbol{A}_i^{-1}\boldsymbol{x}\neq\boldsymbol{A}_j^{-1}\boldsymbol{x}$，因而集合 $\boldsymbol{A}_i^{-1}f_{\boldsymbol{\alpha}}^{-1}(1)$ 与集合 $\boldsymbol{A}_j^{-1}f_{\boldsymbol{\alpha}}^{-1}(1)$ 可近似认为是两个独立的随机选取的集合。由于线性函数 $f_{\boldsymbol{\alpha}}(\boldsymbol{y})=\mathrm{Tr}_{\mathrm{GF}(2^n)}(\boldsymbol{y}^{-1}\times\boldsymbol{\alpha}^{-1})$ 是平衡函数，因而 $|f_{\boldsymbol{\alpha}}^{-1}(1)|=2^{n-1}$，故 $|\boldsymbol{A}_i f_{\boldsymbol{\alpha}}^{-1}(1)|=2^{n-1}$，因此，在上述假设下 $\left|\bigcap_{i=1}^{m}\boldsymbol{A}_i f_{\boldsymbol{\alpha}}^{-1}(1)\right|$ 的期望值为 2^{n-m}。这说明对于固定的非 0 输入差，随着 m 的增大，其不可能差分对应个数的期望将成倍减小。

综上，在固定输出差或输入差时，动态 S 盒中概率为 0 的差分对应的个数都将随着 m 的增大而成倍地减小，而单个 S 盒中差分概率为 0 的差分对应的个数的最小值只能取到 2^{n-1}。不可能差分对应越少，意味着在固定输入差时，可能差分对应的输出差可以在更大的范围内选择，因而差分概率有可能更小。这表明从不可能差分对应的个数分布来看，动态 S 盒的差分分布要显著优于单个 S 盒的差分分布。

表 1 $\mathrm{GF}(2^8)\setminus\{0\}$ 上 m 个互不相同向量构成的向量组的秩与不可能差分对应个数的期望值

m 取值	秩的期望值	不可能差分对应的期望值	m 取值	秩的期望值	不可能差分对应的期望值
3	2.99	33.22	6	5.94	5.17
4	3.99	17.11	7	6.86	3.20
5	4.97	9.17	8	7.60	2.32

4 动态 S 盒不可能差分对应的个数

下面借助于特征多项式为不可约多项式的二元方阵，给出满足设计标准的仿射双射簇的一种构造方法。

定义 3[25] 设 $\boldsymbol{A}$ 为有限域上一个 $n\times n$ 可逆矩阵，称 $p(\boldsymbol{A})=\min\{t\ge 1:\boldsymbol{A}^t=\boldsymbol{E}\}$ 为矩阵 $\boldsymbol{A}$ 的周期。

定义 4[25] 设 $\boldsymbol{A}$ 是域 F 上的 $n\times n$ 矩阵，$\boldsymbol{x}$ 是一个未定元，则称域 F 上的 n 次多项式 $f(\boldsymbol{x})=|\boldsymbol{xE}-\boldsymbol{A}|$ 是 $\boldsymbol{A}$ 的特征多项式。

定义 5[26] 设群 G 作用在非空集合 X 上，$x,y\in X$，如果存在 $g\in G$ 使得 $y=g(x)$，则称 x 等价于 y。在该等价关系下，集合 X 的元素被分成若干等价类，其中每个等价类称为一个轨道，包含元素 x 的轨道就是集合 $O_x=\{g(x):g\in G\}$，$|O_x|$ 称为轨道 O_x 的阶。

对于二元域上的 $n\times n$ 可逆矩阵 $\boldsymbol{A}$，集合 $\{\boldsymbol{A},\boldsymbol{A}^2,\cdots,\boldsymbol{A}^{p(\boldsymbol{A})}\}$ 关于矩阵乘法构成一个群 G，如果群 G 在 $\mathrm{GF}(2^n)$ 上的作用定义为 $\forall\boldsymbol{x}\in\mathrm{GF}(2^n)$，$\boldsymbol{A}^i(\boldsymbol{x})=\boldsymbol{A}^i\boldsymbol{x}$，$\boldsymbol{A}^i\boldsymbol{x}$ 表示矩阵 $\boldsymbol{A}^i$ 与列向量 $\boldsymbol{x}$ 作矩阵乘法，$\boldsymbol{x}\in\mathrm{GF}(2^n)$ 的轨道为 $O_{\boldsymbol{x}}=\{\boldsymbol{A}^i\boldsymbol{x}:1\le i\le p(\boldsymbol{A})\}$。

引理 3[25] 设 $\boldsymbol{a}=(a_0,a_1,a_2,\cdots)$ 是适合以 $\boldsymbol{T}$ 为状态转移矩阵的 n 级线性移位寄存器序列，如果 $\boldsymbol{a}$ 是周期为 $p(\boldsymbol{a})$ 的周期序列，那么一定有 $\boldsymbol{s}_0\boldsymbol{T}^{p(\boldsymbol{a})}=\boldsymbol{s}_0$，而且下面这 $p(\boldsymbol{a})$ 个状态 $\boldsymbol{s}_0,\boldsymbol{s}_0\boldsymbol{T},\cdots,\boldsymbol{s}_0\boldsymbol{T}^{p(\boldsymbol{a})-1}$ 两两不同。

引理 4 设 $\boldsymbol{A}$ 为 $\mathrm{GF}(2)$ 上 n 级可逆方阵且周期为 $p(\boldsymbol{A})$，G 是 $\boldsymbol{A},\boldsymbol{A}^2,\cdots,\boldsymbol{A}^{p(\boldsymbol{A})}$ 关于矩阵乘法构成的群，G 在 $\mathrm{GF}(2^n)$ 上的作用定义为群 G 中元素 $\boldsymbol{A}^i$ 与列向量 $\boldsymbol{x}\in\mathrm{GF}(2^n)$ 作矩阵乘法，则当矩阵 $\boldsymbol{A}$ 的特征多项式是二元域上的不可约多项式时，$\mathrm{GF}(2^n)$ 中任意非零元的轨道的阶均为 $p(\boldsymbol{A})$。

证明 设矩阵 $\boldsymbol{A}$ 的特征多项式为 $f(x)=x^n+c_1x^{n-1}+c_2x^{n-2}+\cdots+c_n,c_i\in\mathrm{GF}(2)$，根据文献[25]的定理 3 可知，矩阵 $\boldsymbol{A}$ 与它的有理标准形 $\boldsymbol{T}$ 相似。

$$\boldsymbol{T}=\begin{pmatrix}0&0&\cdots&0&c_n\\1&0&\cdots&0&c_{n-1}\\\vdots&\vdots&\ddots&\vdots&\vdots\\0&0&\cdots&0&c_2\\0&0&\cdots&1&c_1\end{pmatrix}\tag{9}$$

即存在 $\mathrm{GF}(2)$ 上的 n 级可逆方阵 $\boldsymbol{P}$，使得 $\boldsymbol{T}=\boldsymbol{PAP}^{-1}$。矩阵 $\boldsymbol{T}$ 可看作是 $f(x)$ 对应的除法电路 LFSR 的状态转移矩阵，$\boldsymbol{a}=(a_0,a_1,a_2,\cdots)$ 为该 n 级线性移位寄存器的序列，$\boldsymbol{x}\in\mathrm{GF}(2^n)\setminus\{0\}$ 为该 n 级线性移位寄存器的任意一个非 0 状态，则由引理 3 可知，$\boldsymbol{Tx},\boldsymbol{T}^2\boldsymbol{x},\cdots,\boldsymbol{T}^{p(\boldsymbol{a})}\boldsymbol{x}$ 两两不同，即 $(\boldsymbol{PAP}^{-1})\boldsymbol{x},(\boldsymbol{PA}^2\boldsymbol{P}^{-1})\boldsymbol{x},\cdots,(\boldsymbol{PA}^{p(\boldsymbol{a})}\boldsymbol{P}^{-1})\boldsymbol{x}$ 两两不同。当 $f(x)$ 为二元域上的不可约多项式时，有 $p(\boldsymbol{a})=p(f)=p(\boldsymbol{T})$，又由于 $\boldsymbol{T}=\boldsymbol{PAP}^{-1}$，故 $p(\boldsymbol{T})=p(\boldsymbol{A})$。综上，$(\boldsymbol{PAP}^{-1})\boldsymbol{x},(\boldsymbol{PA}^2\boldsymbol{P}^{-1})\boldsymbol{x},\cdots,(\boldsymbol{PA}^{p(\boldsymbol{a})}\boldsymbol{P}^{-1})\boldsymbol{x}$ 两两不同等价于 $(\boldsymbol{PAP}^{-1})\boldsymbol{x},(\boldsymbol{PA}^2\boldsymbol{P}^{-1})\boldsymbol{x},\cdots,(\boldsymbol{PA}^{p(\boldsymbol{A})}\boldsymbol{P}^{-1})\boldsymbol{x}$ 两两不同，再由 $\boldsymbol{P}$ 可逆可知，$\boldsymbol{Ax},\boldsymbol{A}^2\boldsymbol{x},\cdots,\boldsymbol{A}^{p(\boldsymbol{A})}\boldsymbol{x}$ 两两不同，故 $\mathrm{GF}(2^n)$ 中任意非零元的轨道的阶均为 $p(\boldsymbol{A})$。证毕

定理 3 设 $\boldsymbol{x}\in\mathrm{GF}(2^n)\setminus\{0\}$，$\boldsymbol{A}$ 为 $\mathrm{GF}(2)$ 上 $n\times n$ 可逆矩阵且矩阵 $\boldsymbol{A}$ 的周期 $p(\boldsymbol{A})$，$k_1,k_2,\cdots,k_{p(\boldsymbol{A})}$ 为 $1,2,\cdots,p(\boldsymbol{A})$ 的任意一个全排列，则当矩阵 $\boldsymbol{A}$ 的特征多项式为二元域上的不可约多项式时，对任意的 $1\le i\ne j\le p(\boldsymbol{A})$，均有 $\boldsymbol{A}^{k_i}\boldsymbol{x}\ne\boldsymbol{A}^{k_j}\boldsymbol{x}$。

证明 如果存在 $1\le i<j\le p(\boldsymbol{A})$，使得 $\boldsymbol{A}^{k_i}\boldsymbol{x}=\boldsymbol{A}^{k_j}\boldsymbol{x}$，不妨设 $k_i>k_j$，则 $\boldsymbol{A}^{k_i-k_j}\boldsymbol{x}=\boldsymbol{x}$，这说明 $\boldsymbol{x}$ 的轨道的阶 $\le k_i-k_j<k_i\le p(\boldsymbol{A})$，矛盾。该矛盾说明对任意的 $1\le i\ne j\le p(\boldsymbol{A})$，均有 $\boldsymbol{A}^{k_i}\boldsymbol{x}\ne\boldsymbol{A}^{k_j}\boldsymbol{x}$。证毕

由定理 3 可知，只需选取 $\mathrm{GF}(2)$ 上周期 $\ge m$ 且特征多项式是二元域上不可约多项式的 $n\times n$ 矩阵 $\boldsymbol{A}$，再令 $\boldsymbol{A}_i=\boldsymbol{A}^{k_i}$，$1\le i\le m$，这样构造出的仿射函数簇 $L_i(\boldsymbol{x})=\boldsymbol{A}_i\boldsymbol{x}\oplus\boldsymbol{a}_i$，$1\le i\le m$ 就满足仿射函数簇的设计标准。

定理 4 设二元域上的 $n\times n$ 可逆矩阵 $\boldsymbol{A}$ 的特征多项式是不可约多项式，则任意的 $\boldsymbol{x}\in\mathrm{GF}(2^n)\setminus\{0\}$，轨道 $O_{\boldsymbol{x}}=\{\boldsymbol{A}^i\boldsymbol{x}:1\le i\le p(\boldsymbol{A})\}$ 的阶 $\ge n$。

证明 由引理 4 知，任意的 $\boldsymbol{x}\in\mathrm{GF}(2^n)\setminus\{0\}$，轨道 $O_{\boldsymbol{x}}=\{\boldsymbol{A}^i\boldsymbol{x}:1\le i\le p(\boldsymbol{A})\}$ 的阶是 2^n-1 的因子且都相等。设轨道的阶为 t，则任意的 $\boldsymbol{x}\in\mathrm{GF}(2^n)\setminus\{0\}$，都有 $\boldsymbol{A}^t\boldsymbol{x}=\boldsymbol{x}$，取 $\boldsymbol{e}_i$ 是第 i 分量为 1 其它分量为 0 的 n 维列向量，则有

$$\begin{aligned}\boldsymbol{A}^t&=\boldsymbol{A}^t\boldsymbol{E}=\boldsymbol{A}^t(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_n)\\&=(\boldsymbol{A}^t\boldsymbol{e}_1,\boldsymbol{A}^t\boldsymbol{e}_2,\cdots,\boldsymbol{A}^t\boldsymbol{e}_n)\\&=(\boldsymbol{e}_1,\boldsymbol{e}_2,\cdots,\boldsymbol{e}_n)=\boldsymbol{E}\end{aligned}\tag{10}$$

即 $\boldsymbol{A}^t=\boldsymbol{E}$，这说明 $x^t\oplus 1$ 是矩阵 $\boldsymbol{A}$ 的零化多项式，即 $\boldsymbol{A}^t\oplus\boldsymbol{E}=0$。设 $f(x)$ 是 $\boldsymbol{A}$ 的特征多项式，则由凯莱-哈密顿定理[25]知 $f(\boldsymbol{A})=0$，再由 $f(x)$ 不可约多项式知 $x^t\oplus 1$ 是 $f(x)$ 的倍式，即 $f(x)\,|\,(x^t\oplus 1)$，这说明 $t\ge\partial f=n$。证毕

设动态 S 盒由 8 个 8×8 的 S 盒构成，由定理 4 知二元域上特征多项式为不可约多项式的 8×8 矩阵中的周期均大于等于动态 S 盒中 S 盒的个数 8，故二元域上特征多项式为不可约多项式的 8×8 矩阵 $\boldsymbol{A}$ 都可用来构造仿射变换 $L_i(\boldsymbol{x})=\boldsymbol{A}_i\boldsymbol{x}\oplus\boldsymbol{a}_i$ 中的

8×8 矩阵 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_8$，这里 $\boldsymbol{A}_t=\boldsymbol{A}^{i_t}$，$0\le i_1<i_2<\cdots<i_8\le 7$。这说明满足设计标准的仿射函数簇的选择非常丰富。

5　动态 S 盒差分概率的上界及可达性

下面先给出动态 S 盒的最大差分概率的上界，仅针对 n 为偶数时进行讨论。此时，由有限域 $\mathrm{GF}(2^n)$ 的乘法逆变换构成的单 S 盒的最大差分概率是 2^{2-n}。

定理 5　设 n 为偶数，动态 S 盒由 $\mathrm{GF}(2^n)$ 上的乘法逆变换及 $[\mathrm{GF}(2)]^n$ 上的 m 个仿射变换 $L_i(\boldsymbol{x})=\boldsymbol{A}_i\boldsymbol{x}\oplus\boldsymbol{a}_i$ 的复合构成，且任意的 $\boldsymbol{\beta}\in\mathrm{GF}(2^n)\setminus\{0\}$，$\boldsymbol{A}_i^{-1}\boldsymbol{\beta}\ne\boldsymbol{A}_j^{-1}\boldsymbol{\beta}$ 对 $1\le i\ne j\le m$ 均成立，则动态 S 盒的最大差分概率 $\le 2^{1-n}(m+1)/m$。

证明　设 $\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathrm{GF}(2^n)\setminus\{0\}$，则由引理 2 知

$$p_{x^{-1}}\left(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta}\right)=\begin{cases}2^{2-n}, & \boldsymbol{\alpha}^{-1}=\boldsymbol{A}_i^{-1}\boldsymbol{\beta}\\ 2^{1-n}, & \boldsymbol{\alpha}^{-1}\ne\boldsymbol{A}_i^{-1}\boldsymbol{\beta},\\ & \mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\boldsymbol{\alpha}^{-1}\times\left(\boldsymbol{A}_i^{-1}\boldsymbol{\beta}\right)^{-1}\right)=0\\ 0, & \mathrm{Tr}_{\mathrm{GF}(2^n)}\left(\boldsymbol{\alpha}^{-1}\times\left(\boldsymbol{A}_i^{-1}\boldsymbol{\beta}\right)^{-1}\right)=1\end{cases}\tag{11}$$

如果对 $1\le i\le m$ 均有 $p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})\le 2^{1-n}$，则由引理 1 可知，此时动态 S 盒 S_k 的差分概率为

$$p_{S_k}(\boldsymbol{\alpha}\to\boldsymbol{\beta})=\frac{1}{m}\sum_{i=1}^{m}p_{x^{-1}}\left(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta}\right)\le\frac{1}{m}\sum_{i=1}^{m}2^{1-n}=2^{1-n}\Big/m\tag{12}$$

如果存在 $1\le i\le m$，使得 $p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta})=2^{2-n}$，则有 $\boldsymbol{\alpha}=(\boldsymbol{A}_i^{-1}\boldsymbol{\beta})^{-1}$。再由本定理的假设知，对任意的 $j\ne i$，均有 $\boldsymbol{A}_j^{-1}\boldsymbol{\beta}\ne\boldsymbol{A}_i^{-1}\boldsymbol{\beta}=\boldsymbol{\alpha}$，因而 $p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{A}_j^{-1}\boldsymbol{\beta})\le 2^{1-n}$，故此时动态 S 盒 S_k 的差分概率为

$$\begin{aligned}p_{S_k}(\boldsymbol{\alpha}\to\boldsymbol{\beta})&=\frac{1}{m}\sum_{j=1}^{m}p_{x^{-1}}\left(\boldsymbol{\alpha}\to\boldsymbol{A}_j^{-1}\boldsymbol{\beta}\right)\\&=\frac{1}{m}p_{x^{-1}}\left(\boldsymbol{\alpha}\to\boldsymbol{A}_i^{-1}\boldsymbol{\beta}\right)+\frac{1}{m}\sum_{j=1,j\ne i}^{m}p_{x^{-1}}\left(\boldsymbol{\alpha}\to\boldsymbol{A}_j^{-1}\boldsymbol{\beta}\right)\\&\le\frac{1}{m}\times 2^{2-n}+\sum_{j=1,j\ne i}^{m}2^{1-n}\\&=2^{1-n}(m+1)\Big/m\end{aligned}\tag{13}$$

这说明 $\max\limits_{\boldsymbol{\alpha},\boldsymbol{\beta}\ne 0}p_{S_k}(\boldsymbol{\alpha}\to\boldsymbol{\beta})\le 2^{1-n}(m+1)/m$　　证毕

由定理 5 的证明可知，由于仿射函数簇设计标准的限制，使得动态 S 盒中 m 个 S 盒在相同输入差下差分概率取最大值 2^{2-n} 的 S 盒至多只有一个，从而保证了动态 S 盒的最大差分概率的上界极小化，这也表明了本文给出的仿射函数簇的设计标准的合理性。

下面给出当仿射函数都是有限域 $\mathrm{GF}(2^n)$ 上的一次函数 $L_i(\boldsymbol{x})=\boldsymbol{a}_i\boldsymbol{x}\oplus\boldsymbol{b}_i$ 时，动态 S 盒的最大差分概率达到其上界的充分必要条件。

定理 6　设 n 为偶数，$m<n$，动态 S 盒由 $\mathrm{GF}(2^n)$ 上的乘法逆变换 x^{-1} 及 $\mathrm{GF}(2^n)$ 上的 m 个一次可逆函数 $L_i(\boldsymbol{x})=\boldsymbol{a}_i\boldsymbol{x}\oplus\boldsymbol{b}_i$ 构成且 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_m$ 互不相同，$\boldsymbol{\alpha},\boldsymbol{\beta}\in\mathrm{GF}(2^n)\setminus\{0\}$。则动态 S 盒的差分对应 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 的差分概率为 $2^{1-n}(m+1)/m$，当且仅当存在 $1\le i\le m$ 使得 $\boldsymbol{\alpha}\times\boldsymbol{\beta}=\boldsymbol{a}_i$，且对 $1\le j\le m$ 均有 $Tr_{\mathrm{GF}(2^n)}(\boldsymbol{a}_i^{-1}\times\boldsymbol{a}_j)=0$。

证明　记 $\boldsymbol{x}=\boldsymbol{\beta}^{-1}\times\boldsymbol{\alpha}^{-1}$，由于 $\boldsymbol{a}_1,\boldsymbol{a}_2,\cdots,\boldsymbol{a}_m$ 互不相同，故当 $\boldsymbol{\alpha}^{-1}=\boldsymbol{a}_i^{-1}\times\boldsymbol{\beta}$ 时，对 $\forall j\ne i$，均有 $\boldsymbol{\alpha}^{-1}=\boldsymbol{a}_i^{-1}\times\boldsymbol{\beta}\ne\boldsymbol{a}_j^{-1}\times\boldsymbol{\beta}$。这说明动态 S 盒的差分对应 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 的差分概率是 $2^{1-n}(m+1)/m$，等价于 $p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{a}_j^{-1}\times\boldsymbol{\beta})\ge 2^{1-n}$，对 $1\le j\le m$ 均成立且存在 $1\le i\le m$，使得 $p_{x^{-1}}(\boldsymbol{\alpha}\to\boldsymbol{a}_i^{-1}\times\boldsymbol{\beta})=2^{2-n}$。由引理 2 知，前者等价于 $\mathrm{Tr}_{\mathrm{GF}(2^n)}(\boldsymbol{a}_j\times\boldsymbol{x})=0$，对 $1\le j\le m$ 均成立，后者 $\boldsymbol{\alpha}^{-1}=\boldsymbol{a}_i^{-1}\times\boldsymbol{\beta}$ 即 $\boldsymbol{\alpha}\times\boldsymbol{\beta}=\boldsymbol{a}_i$，故由 $\boldsymbol{x}=\boldsymbol{\beta}^{-1}\times\boldsymbol{\alpha}^{-1}$ 知，动态 S 盒的差分对应 $\boldsymbol{\alpha}\to\boldsymbol{\beta}$ 的差分概率是 $2^{1-n}(m+1)/m$，等价于存在 $1\le i\le m$，使得 $\boldsymbol{\alpha}\times\boldsymbol{\beta}=\boldsymbol{a}_i$ 且 $\mathrm{Tr}_{\mathrm{GF}(2^n)}(\boldsymbol{a}_i^{-1}\times\boldsymbol{a}_j)=0$ 对 $1\le j\le m$ 均成立。　　证毕

本文利用模拟实验，针对 $1\le m\le 8$ 这 8 种情形，且在有限域为 $\mathrm{GF}(2^8)$ 时，给出动态 S 盒中的矩阵 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_m$ 由 $p(\boldsymbol{x})$ 对应的 n 级除法电路 LFSR 的状态转移矩阵 $\boldsymbol{A}$ 构造时的最大差分概率达到上界的分布情况。本文对每个 m 的取值随机选取了 2^{16} 组 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_m$ 进行测试，具体结果见表 2 所示。

从表 2 中可以看出，随着 m 的增大，动态 S 盒的最大差分概率达到上界 $2^{1-n}(m+1)/m$ 的概率逐渐变小，当 $m=8$ 时，最大差分概率达到上界 2.25×2^{-8} 仅占样本的 0.25%，这说明由 $\boldsymbol{A}$ 随机构造的 $\boldsymbol{A}_1,\boldsymbol{A}_2,\cdots,\boldsymbol{A}_8$ 绝大部分都达不到上界。但随着 m 的增大，构造动态 S 盒的代价也随之增大，故可以根据密码算法实际的需求来选择合适的 m 来构造动态 S 盒。

当 n 为偶数时，动态 S 盒中最大差分概率的上界都小于单个 S 盒的最大差分概率的上界 2^{2-n}，随着 m 取值的增大，动态 S 盒中最大差分概率的上界会逐渐变小，并逐渐趋近于 2^{1-n}，故动态 S 盒的最大差分概率要优于单个 S 盒的最大差分概率。

表 2 8×8 维状态转移矩阵构造动态 S 盒的最大差分概率的分布情况

m 取值	最大差分概率 ($\times 2^{-7}$)	概率分布(%)
1	0/1	0.00
	1/1	0.00
	2/1	100.00
2	1/2	0.00
	2/2	47.91
	3/2	52.09
3	2/3	0.00
	7/7	66.56
	8/7	33.44
4	6/7	0.00
	4/4	84.28
	5/4	15.72
5	4/5	0.00
	5/5	99.22
	6/5	6.46
6	5/6	0.00
	6/6	97.66
	7/6	2.34
7	5/6	0.00
	6/6	97.66
	7/6	0.78
8	7/8	37.24
	8/8	62.51
	9/8	0.25

6 随机 S 盒构造动态 S 盒的差分概率

前面几节分析了各 S 盒均为有限域 GF(2^n) 上的乘法逆与仿射变换复合的动态 S 盒的差分性质，本节将研究由随机 S 盒来构造的动态 S 盒的差分性质。下面利用模拟实验方法，给出此类动态 S 盒的差分性质。当 $m=2,4,8$ 时，对于 8 进 8 出的随机 S 盒，本文通过大量模拟实验考查了动态 S 盒的最大差分概率及输入差给定时不可能差分个数的平均值。本文随机生成了 700 个满足最大差分概率为 8/256 且最大 Walsh 谱的绝对值为 60/256 的 S 盒，并在 $m=2,4,8$ 时任取其中 8 个分别作为 SPS 模型中的 8 个 S 盒，共进行 2^{16} 组实验。实验给出的最大差分概率及不可能差分个数见表 3 所示，2^{16} 组实验的最大差分概率分布情况见表 4 所示。

表 3 随机 S 盒构造的动态 S 盒的最大差分概率及不可能差分个数

m	最大差分概率平均值($\times 2^{-8}$)	不可能差分个数平均值
2	7.01	92.35
4	5.03	33.37
8	3.68	4.35

由表 3 可知，对于利用随机 S 盒来构造的动态 S 盒，最大差分概率随着 m 的增大而减小，不可能差分对应的个数随着 m 的增大而大幅度减小，其差分性质要远好于单个 S 盒的差分性质。

由表 4 可知，对于测试的 2^{16} 组随机样本，当 $m=2,4,8$ 时，动态 S 盒中最大差分概率的最小值分别为 6.00×2^{-8}，4.00×2^{-8}，3.25×2^{-8}。事实上，可以在构造随机 S 盒时，通过适当的调整，使得动态 S 盒中的各个 S 盒的最大或次大差分概率尽量不同时出现，从而降低动态 S 盒的最大差分概率。

表 4 随机 S 盒构造的动态 S 盒的最大差分概率分布情况

	最大差分概率($\times 2^{-8}$)	占样本比例(%)
m=2	6.00	10.4
	7.00	78.0
	8.00	11.6
m=4	4.00	0.1
	4.50	17.9
	5.00	61.4
	5.50	18.1
	6.00	2.3
	6.50	0.2
m=8	3.25	2.9
	3.50	40.7
	3.75	39.7
	4.00	13.3
	4.25	2.8
	4.50	0.5
	4.75	0.1

7 结束语

S 盒是许多分组密码中唯一的非线性模块，它的密码强度直接影响整个分组密码的安全强度。动态 S 盒技术可以显著提高 S 盒的密码学性质，目前已经在一些密码算法的设计中得到了应用。本文基于有限域 GF(2^n)上的乘法逆与仿射变换的复合变换，给出了动态 S 盒一种新的构造方法，并对其不可能差分、最大差分概率的上界及可达性等安全指标进行了研究。理论分析和实验分析都表明，此类

动态 S 盒变换具有良好的差分特性，且远好于单个 S 盒的差分特性。本文仅对这类动态 S 盒的差分性质进行了讨论，对其线性性质的分析，有待进一步深入研究。

参 考 文 献

[1] 吴文玲, 冯登国, 张文涛. 分组密码的设计与分析[M]. 北京: 清华大学出版社, 2009: 229–234.
Wu Wen-ling, Feng Deng-guo, and Zhang Wen-tao. Design and Analysis of Block Cipher[M]. Beijing: Tsinghua University Press, 2009: 229–234.

[2] Daemen J and Rijmen V. The cipher SHARK[J]. LNCS, 1997, 1039: 99–111.

[3] Daemen J, Kundsen L, and Rijmen V. The block cipher SQUARE[J]. *LNCS*, 1997, 1039: 149–165.

[4] Daemen J and Rijmen V 著, 谷大武, 徐胜波译, 高级加密标准(AES)算法-Rijndael 的设计[M]. 北京: 清华大学出版社, 2003: 34–41.

[5] Specification of SMS4, Block cipher for WLAN products-SMS4[OL]. http: //www.oscca.gov.cn/UpFile/2006 21016423197990.pdf, 2006.

[6] 殷新春, 杨洁, 谢立. 密钥控制的多 S 盒 Rijndeal 算法[J]. 通信学报, 2007, 28(9): 125–132.
Yin Xin-chun, Yang Jie, and Xie Li. Key-controlled Rijndael algorithm with multiple S-boxes[J]. *Journal on Communications,* 2007, 28(9): 125–132.

[7] Szaban M and Seredynski F. Dynamic cellular automata-based S-boxes[J]. *LNCS*, 2012, 6927: 184–191.

[8] Stoianov N. One approach of using key-dependent S-boxes in AES[C]. Proceedings of 4th Multimedia Communications, Services and Security, Krakow, 2011: 317–323.

[9] 王文华, 郑志明. 基于可变 S 盒的随机加密方案[J]. 北京航空航天大学学报, 2011, 37(7): 811–816.
Wang Wen-hua and Zheng Zhi-ming. Random encryption scheme based on variable S-boxes[J]. *Journal of Beijing University of Aeronautics and Astronautics*, 2011, 37(7): 811–816.

[10] Peng J and Jin S Z. Designing key-dependent S-boxes using hyperchaotic Chen system[J]. *Lecture Notes in Electrical Engineering*, 2013, 216: 733–740.

[11] 郭现峰. 基于混沌动态 S 盒的密码算法及其应用研究[D]. [博士论文], 西南交通大学, 2011.
Guo Xian-feng. Research on chaotic dynamic S-box based cryptography and its applications[D]. [Ph.D. dissertation], Southwest Jiaotong University, 2011.

[12] Merkle R. Fast software encryption functions[J]. *LNCS*, 1991, 537: 477–501.

[13] Schneier B. Description of a new variable-length key, 64-bit block cipher (blowfish)[J]. *LNCS*, 1994, 809: 191–204.

[14] Biryukov A and Shamir A. Structural cryptanalysis of SASAS[J]. *LNCS*, 2001, 2045: 394–405.

[15] C2 block cipher specification[OL]. http://edipermadi.files.wordpress.com/2008/08/cryptomeria-c2-spec.pdf, 2008.

[16] Knudsen L R, Leander G, Poschmann A, *et al.*. PRINTcipher: a block cipher for ICPrinting[J]. *LNCS*, 2010, 6225: 16–32.

[17] Borghoff J, Knudsen L R, Leander G, *et al.*. Slender-set differential cryptanalysis[J]. *In Journal of Cryptology*, 2013, 26: 11–38.

[18] Webster A F and Tavares S E. On the design of S-boxes[J]. *LNCS*, 1986, 218: 523–534.

[19] Millan W, Burnett L, Carter G, *et al.*. Evolutionary heuristics for finding cryptographically strong S-boxes[J]. *LNCS*, 1999, 1726: 263–274.

[20] Clark J A, Jacob J L, and Stepney S. The design of S-boxes by simulated annealing[J]. *New Generation Computing*, 2005, 23(3): 219–231.

[21] Nedjah N and Mourelle L. Designing substitution boxes for secure ciphers[J]. *International Journal Innovative Computing and Application*, 2007, 1(1): 86–91.

[22] Tu C X. Design of an improved method of Rijndael S-box[C]. Proceedings of the International Conference on Computing, Information and Control, Wuhan, 2011, 231: 46–51.

[23] 崔杰. Rijndael 中若干关键问题的研究[D]. [博士论文], 中国科学技术大学, 2012.
Cui Jie. Study on several key problems in Rijndael[D]. [PhD. dissertation], University of Science and Technology of China, 2012.

[24] Daemen J and Rijmen V. Two-round AES differentials[J]. *LNCS*, 2006, 4116: 78–94.

[25] 万哲先. 代数与编码 [M]. (第 3 版), 北京: 高等教育出版社, 2007, 6: 201, 163, 179–180.
Wan Zhe-xian. Algebraic and Coding[M]. Beijing: Higher Education Press, 2007, 6: 201, 163, 179–180

[26] 聂灵沼, 丁石孙. 代数学引论 [M]. (第 2 版), 北京: 高等教育出版社, 2000, 9: 73–75.
Nie Ling-zhao and Ding Shi-sun. Introduction to Algebraic[M]. Beijing: Higher Education Press, 2000, 9: 73–75.

刘国强：　男，1986 年生，博士生，研究方向为分组密码设计与分析.

金晨辉：　男，1965 年生，博士，教授，博士生导师，研究方向为密码学和信息安全.