计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.191200036

基于线性划分的陷门S盒的设计与分析

韩 羽 张文政 董新锋
保密通信重点实验室 成都 610041
(hanyu003@163.com)

摘 要 带陷门的分组密码算法是一种可以满足特定场景下特殊需求的密码算法,陷门函数被广泛地应用于非对称加密算法中,考虑将非对称加密中陷门函数的思想引入分组密码。分组密码算法的核心是S盒,是绝大多数分组算法中唯一的非线性部件,在加密过程中起到混淆的作用,因此在构造分组算法的陷门时主要就是研究在S盒中植入陷门。针对这个问题,文中主要研究了基于陪集对有限域进行线性划分的代数性质来构造陷门S盒的方法,这种陷门S盒的陷门信息就是线性划分的方法。文中首先介绍了线性划分设计陷门算法和陷门S盒的原理,构造了一种映射在线性划分上的8×8陷门S盒,给出了具体的构造方法,并分析了这种S盒的线性性质和差分性质。为了说明这种S盒的安全性和实用性,采用Bannier等提出的陷门分组算法作为模型,简要地验证分析了陷门的有效性,证明了陷门S盒和陷门算法对线性分析和差分分析的安全性。

关键词:陷门函数;陪集划分;陷门S盒;差分分析;线性分析
中图法分类号 TP309.7

Design and Analysis of Trapdoor S-Box Based on Linear Partition

HAN Yu,ZHANG Wen-zheng and DONG Xin-feng
Science and Technology on Communication Security Laboratory,Chengdu 610041,China

Abstract The block cipher algorithm with trapdoor is a kind of cipher algorithm that can meet the special needs in specific scenarios. The trapdoor function is widely used in asymmetric encryption algorithms. The idea of trapdoor function in asymmetric encryption is considered to be introduced into block cipher. the S-box isthe core of block cipher,which is the only non-linear component in mostly block cipher algorithm. It plays a role of confusion in the encryption process. Therefore,when constructing the trapdoor of the block cipher,the main research is to implant trapdoor into S-box. Aiming at this problem,this paper first studies the method of constructing trapdoor S-box based on the algebraic properties of linear partition of finite fields based on cosets. The trapdoor information is the linear partition method. This article first introduces the principle of trapdoor algorithm and trapdoor S-box based on linear partition. The 8×8 trapdoor S-box mapped on the linear partition is constructed,and the specific construction method is given. The linear and differential properties of this type of S-box are analyzed. In order to illustrate the safety and practicability of this type of S-box,the trapdoor block cipher proposed by Bannier et al is used as a model to briefly verify and analyze the effectiveness of the trapdoor,and prove the safety of trapdoor S-box and trapdoor algorithm to linear analysis and differential analysis.

Keywords Trapdoor function,Coset partition,Trapdoor S-box,Differential analysis,Linear analysis

1 引言

陷门函数被广泛地应用于非对称加密算法中,既可以用于信息加密,也可以用于示证者和验证者间的数字签名与验证。非对称加密中的陷门机制可以完全公开其设计细节,它的安全性仅依赖于对密钥信息的保护,换句话说,密钥就是陷门。我们把陷门函数的思想引入对称加密,关键问题就在于如何在对称加密算法中构造“陷门”,使知道这个“陷门”的人可以较容易地攻破密码算法,并且这个“陷门”应该与密钥信息相独立。

公开资料中最早的陷门对称密码算法是在1997年由Rijmen等提出的[1],他们构造了一种弱化线性攻击的S盒。虽然后来有学者提出了对这种S盒陷门的寻找方法[2],但是在实际应用中,对于一个带有陷门的算法,攻击者在不知道陷门信息具体设计方法的情况下是很难发现算法存在陷门或者成功寻找到陷门信息的。2016年Bannier等提出了一种分组密码的陷门构造方法[3],对明文空间和密文空间做某种划分——陪集划分,再基于这种划分来构造S盒和轮函数,使得轮函数加密都在线性划分上。这种陷门算法[4]在知道陪集划分方法的情况下能够使用较少的已知明密文对搜索到加密密钥。

本文研究了Bannier等的陷门设计方法,主要研究了基

本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。

基金项目:国家重点研发计划(2017YFB0802000)
This work was supported by the National Key R&D Program of China (2017YFB0802000).

通信作者:张文政(zwz85169038@sina.com)

于对加密空间的线性划分来构造陷门 S 盒的方法，使陷门 S 盒可以从一个线性划分映射到另一个线性划分。本文第 2 节从线性划分设计轮函数的角度引出这种陷门 S 盒的设计依据；第 3 节研究这种陷门 S 盒的设计原理；第 4 节构造一类 8×8 的陷门 S 盒实例，研究这种 S 盒的差分性质和线性性质；第 5 节基于 Bannier 等设计的陷门分组算法，简要分析使用这种陷门 S 盒构造的陷门算法；最后指出后续值得研究的问题。

2　线性划分构造陷门算法原理

线性划分实际上就是利用陪集进行划分，下面首先介绍陪集[5]的概念。

定义 1（陪集 Coset）　设 H 是群 G 的一个子群，群上的运算为“+”，对 $\forall a\in G$，称集合 $\{a+h\mid h\in H\}$ 为 H 的一个左陪集，记为 aH；同样地，定义右陪集为 $Ha=\{h+a\mid h\in H\}$。

若群 G 是一个交换群，H 是 G 的正规子群，用 G/H 来表示 H 的所有不同陪集组成的集合，不难验证，这个集合在陪集间的运算下仍是一个群，称这个群为 G 对 H 的商群，记作 G/H。

定义 2[3]（线性划分 Linear Partition）　$\mathscr{A}$ 是 F_2^n 上的一个划分，V 是一个含 0_n 的集合。称划分 $\mathscr{A}$ 是线性划分，若 V 是 F_2^n 上的子空间，并且 $\mathscr{A}$ 的每一部分都是 V 在 F_2^n 的一个陪集，即：

$$\mathscr{A}=\{x+V\mid x\in F_2^n\}=F_2^n/V$$

其中，F_2^n/V 表示 F_2^n 对 V 的商群，记这样的线性化分 $\mathscr{A}$ 为 $\mathscr{L}(V)$。

在设计陷门算法时，采用双射 S 盒构造 SPN 型的加密算法，轮函数设计与 AES 标准算法[6]类似。在此基础上，利用线性划分来设计对称加密陷门，这样的陷门不是依赖于密钥信息，而是 S 盒本身的“设计弱点”，即 S 盒映射的划分方法。

定义 3[3]（替代置换网络）　SPN 取整数 $s,n\geqslant 1,\sigma_1,\cdots,\sigma_s$ 是 $n\times n$ 的 S 盒，$\pi:F_2^{ns}\to F_2^{ns}$ 是一个线性置换，定义映射 σ：

$$\sigma:(F_2^n)^s\to(F_2^n)^s$$

$$(x_1,\cdots,x_s)\mapsto(\sigma_1(x_1),\cdots,\sigma_s(x_s))$$

对任意的轮密钥 $k\in F_2^{ns}$，定义函数 $\alpha_k:F_2^{ns}\to F_2^{ns}$ 为 $\alpha_k(x)=x+k$。映射 α_k，σ 和 π 分别称为加密钥层、替代层和扩散层。k 比特加密的轮函数 $F_k=\pi\sigma\alpha_k$，取整数 $r\geqslant 1$，则轮密钥为 $(k_1,\cdots,k_{r+1})$ 的 r 轮加密函数为：

$$E_{(k_1,\cdots,k_{r+1})}=\alpha_{k_{r+1}}F_{k_r}\cdots F$$

称这样的加密轮函数为 SPN 型的。

定理 1[3]　令 $\mathscr{A}$ 和 $\mathscr{B}$ 是 F_2^{ns} 上的两个划分，设任意轮密钥为 $(k_1,\cdots,k_{r+1})$ 的 $(k+1)$ 元组的 r 轮加密函数 $E_{(k_1,\cdots,k_{r+1})}$ 是 $\mathscr{A}$ 到 $\mathscr{B}$ 的映射，定义 $\mathscr{A}_1=\mathscr{A}$ 并对所有的 $2\leqslant i\leqslant r+1$，有 $\mathscr{A}_i=(\pi\sigma)^{i-1}\mathscr{A}$，则：

(1) $\mathscr{A}_{r+1}=\mathscr{B}$；

(2) 对任意 $1\leqslant i\leqslant r+1$ 和 $k_i\in F_2^{ns}$，有 $F_{k_i}(\mathscr{A}_i)=\mathscr{A}_{i+1}$；

(3) 对任意 $1\leqslant i\leqslant r+1$，$\mathscr{A}_i$ 是一个线性划分。

这个定理表明，对于线性划分上的 r 轮加密的 SPN 型算法，如果每一轮函数都可以将一个线性划分映射到另一个线性划分，加密过程最终就表现为将明文空间的线性划分映射到密文空间的线性划分，这样设计的算法就是陷门分组算法，如图 1 所示。

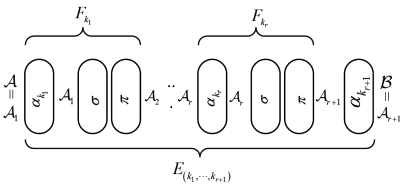

图 1　轮函数对线性划分的映射

Fig. 1　Round function map on linear partition

根据陷门算法的设计原理，要设计算法轮函数映射到线性划分上，其中的加密钥层和扩散层都是自同构映射，可以将一个线性划分映射到另一个线性划分；而替换层 S 盒作为轮函数中的唯一非线性部件，则需要进行特殊的构造使其将一个线性划分映射到另一个线性划分。下面将详细讨论这种陷门 S 盒的设计方法。

3　线性划分构造陷门 S 盒的原理

若陷门算法轮函数设计为定义 3 中的 SPN 结构，则替换层由 s 个 $n\times n$ 的 S 盒并列构成，若每个 S 盒都可以保持线性划分之间的映射，那么整个替换层可以将一个线性划分映射到另一个线性划分。

引理 1　设 V 和 M 为 F_2^n 上两个同构的子空间，则存在一个 F_2^n 上的自同构映射 L 使得 $L(V)=W$。且 L 可以将划分 $\mathscr{L}(V)$ 映射到划分 $\mathscr{L}(W)$。

证明：设 V 和 W 的基分别为 $(v_0,v_1,\cdots,v_s)$ 和 $(w_0,w_1,\cdots,w_s)$，其中 $0\leqslant s<n$。将这两组基：分别扩充为 F_2^n 的两组基：

$$\mathscr{B}_V=(v_i)_{i<n}=(v_0,\cdots,v_s,v_{s+1},\cdots,v_{n-1})$$

$$\mathscr{B}_W=(w_i)_{i<n}=(w_0,\cdots,w_s,w_{s+1},\cdots,w_{n-1})$$

则对 $\forall x\in F_2^n$，在基 $\mathscr{B}_V$ 下 $x=x_0v_0+x_1v_1+\cdots+x_{n-1}v_{n-1}$，其中 $x_i\in F_2$，$0\leqslant i<n$，L 定义为：

$$L:\mathscr{B}_V\to\mathscr{B}_W$$

$$L(x)=L(\sum_{i=0}^{n-1}x_iv_i)=\sum_{i=0}^{n-1}x_iw_i$$

显然，L 是一个 F_2^n 上的自同构映射，并且有 $L(V)=W$。所以就有 $L(\mathscr{L}(V))=\mathscr{L}(L(V))=\mathscr{L}(W)$，即，$L$ 可以将划分 $\mathscr{L}(V)$ 映射到划分 $\mathscr{L}(W)$。证毕。

设 S 盒 $\mathbb{S}$ 是 F_2^n 上的置换，将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(W)$，由引理 1 知存在一个 F_2^n 上的自同构映射 L 使得 $L(V)=W$，并且存在 $S=L^{-1}\circ\mathbb{S}$ 使得 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(V)$，易知 $\mathbb{S}$ 和 S 的差分性质和线性性质是等价的[7-8]。

由于在同一个划分上可以利用陪集的代数性质，便于对 S 盒的差分性质和线性性质进行分析。因此，在构造 S 盒时可以在同一个划分上进行设计，再使用自同构映射 L 将其映射到另一个划分。

考虑 F_2^n 上的 V 是一个 d 维非平凡子空间，U 是 V 的补空间，S 盒 S 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(V)$，则对 F_2^n 上任意元素 x 都可以表示成 $x=u+v$，其中 $u\in U,v\in V$，即 F_2^n 可以表示成 U 和 V 的直和形式，$F_2^n=U\oplus V$，这里的“$\oplus$”表示子空间的直和。那么 $\mathscr{L}(V)$ 中的每一部分都可以表示成 $[u]=u+V$，称 u 为陪集代表元，则有 $\mathscr{L}(V)=\{[u]\mid u\in U\}$。

定理 2[3]　对 F_2^n 上的置换 S，将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(V)$，则在 U 上存在唯一的置换 ρ，在 V 上存在唯一的一族置换 $(\tau_u)_{u\in U}$，对 F_2^n 上任意 $x=u+v$ 有：

$$S(u+v)=\rho(u)+\tau_u(v)$$

反过来，若在 U 上存在置换 ρ，且在 V 上存在一族置换 $(\tau_u)_{u\in U}$，那么就可以确定一个 F_2^n 上的置换 S 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(V)$。

定理 2 表明，在设计将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(V)$ 的 S 盒时，可以在线性划分 $\mathscr{L}(V)$ 的所有陪集代表元构成的子空间 U 上设计置换 ρ，然后对其相应的陪集中元素 $v\in V$ 设计一族置换 $(\tau_u)_{u\in U}$，并分别讨论其线性性质和差分性质，以此降低讨论的维度，降低了设计和分析的难度。下面将使用这种方法对陷门 S 盒进行实例构造。

4 线性划分陷门 S 盒的构造

本文以构造 8×8 的 S 盒为例，S 盒 $\mathbb{S}$ 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(W)$，陷门信息就是 $\mathscr{L}(V)$ 和 $\mathscr{L}(W)$ 的划分方式。

4.1 对有限域的线性划分

首先构造置换 S 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(V)$，取 F_2^8 上的三维子空间 $V(F_2^8$ 中元素均用 16 进制表示$)$，$V=span(03,48,66)=\{00,03,48,66,4b,65,2e,2d\}$，利用 V 对 F_2^8 进行陪集划分，划分 $\mathscr{L}(V)$，如图 2 所示。

00+V {00,03,48,66,4b,65,2e,2d}	**01+V** {01,02,49,67,4a,64,2f,2c}	**04+V** {04,07,4c,62,4f,61,2a,29}	**05+V** {05,06,4d,63,4e,60,2b,28}
08+V {08,0b,40,6e,43,6d,26,25}	**09+V** {09,0a,41,6f,42,6c,27,24}	**0c+V** {0c,0f,44,6a,47,69,22,21}	**0d+V** {0d,0e,45,6b,46,68,23,20}
10+V {10,13,58,76,5b,75,3e,3d}	**11+V** {11,12,59,77,5a,74,3f,3c}	**14+V** {14,17,5c,72,5f,71,3a,39}	**15+V** {15,16,5d,73,5e,70,3b,38}
18+V {18,1b,50,7e,53,7d,36,35}	**19+V** {19,1a,51,7f,52,7c,37,34}	**1c+V** {1c,1f,54,7a,57,79,32,31}	**1d+V** {1d,1e,55,7b,56,78,33,30}
80+V {80,83,c8,e6,cb,e5,ae,ad}	**81+V** {81,82,c9,e7,ca,e4,af,ac}	**84+V** {84,87,cc,e2,cf,e1,aa,a9}	**85+V** {85,86,cd,e3,ce,e0,ab,a8}
88+V {88,8b,c0,ee,c3,ed,a6,a5}	**89+V** {89,8a,c1,ef,c2,ec,a7,a4}	**8c+V** {8c,8f,c4,ea,c7,e9,a2,a1}	**8d+V** {8d,8e,c5,eb,c6,e8,a3,a0}
90+V {90,93,d8,f6,db,f5,be,bd}	**91+V** {91,92,d9,f7,da,f4,bf,bc}	**94+V** {94,97,dc,f2,df,f1,ba,b9}	**95+V** {95,96,dd,f3,de,f0,bb,b8}
98+V {98,9b,d0,fe,d3,fd,b6,b5}	**99+V** {99,9a,d1,ff,d2,fc,b7,b4}	**9c+V** {9c,9f,d4,fa,d7,f9,b2,b1}	**9d+V** {9d,9e,d5,fb,d6,f8,b3,b0}

图 2 对 F_2^8 进行 $\mathscr{L}(V)$ 的划分

Fig. 2 Division of F_2^8 by $\mathscr{L}(V)$

$$\begin{aligned}F_2^8 &= L(V)\\ &=\{00+V,01+V,04+V,05+V,08+V,09+V,0c+V,0d+V,10+V,11+V,14+V,15+V,18+V,19+V,1c+V,1d+V,80+V,81+V,84+V,85+V,88+V,89+V,8c+V,8d+V,90+V,91+V,94+V,95+V,98+V,99+V,9c+V,9d+V\}\end{aligned}$$

那么 V 的补空间 U 为：

$$\begin{aligned}U &= span(01,04,08,10,80)\\ &=\{00,01,04,05,08,09,0c,0d,10,11,14,15,18,19,1c,1d,80,81,84,85,88,89,8c,8d,90,91,94,95,98,99,9c,9d\}\end{aligned}$$

对 $\forall x\in F_2^8$，$x=u+v$，其中 $u\in U$，$v\in V$，由定理 2 知，S 可以表示为：

$$S(u+v)=\rho(u)+\tau_u(v)$$

其中，置换 $\rho(u)$ 定义在 U 上，对 $\forall u\in U$，其是一个划分的代表元，对其相应的 V 定义置换 $\tau_u(v)$，一共 32 个置换，S 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(V)$。

再取 F_2^8 上的三维子空间 $W=span(01,1a,52)$，W 的补空间为 $\overline{W}=span(02,04,08,20,80)$，对 F_2^8 的划分为 $\mathscr{L}(W)$。

4.2 陷门 S 盒的构造

S 盒的构造主要分为两步，首先在线性划分 $\mathscr{L}(V)$ 上构造映射 S，然后再复合上一个线性映射 L 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(W)$。

定义线性映射 L 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(W)$。

$$\mathscr{B}_V=(v_i)_{i<8}=(03,48,66,01,04,08,10,80)$$

$$\mathscr{B}_W=(w_i)_{i<8}=(01,1a,52,02,04,08,20,80)$$

对 $\forall x\in F_2^8$，在基 $\mathscr{B}_V$ 下 $x=x_0v_0+x_1v_1+\cdots+x_7v_7$，在基 $\mathscr{B}_W$ 下 $x=x_0w_0+x_1w_1+\cdots+x_7w_7$，其中 $x_i\in F_2$，$0\leqslant i<8$。

$$L:\mathscr{B}_V\rightarrow\mathscr{B}_W$$

$$L(x)=L(\sum_{i=0}^{7}x_iv_i)=\sum_{i=0}^{7}x_iw_i$$

那么 S 盒 $\mathbb{S}=L\circ S$ 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(W)$。

对 $\mathscr{L}(V)$ 上的置换 S：

$$S(u+v)=\rho(u)+\tau_u(v)$$

置换 $\rho(u)$ 定义在 U 上，对 $\forall u\in U$，对其相应的 V 设计置换 $\tau_u(v)$。S 要达到较好的密码学性质，$\rho(u)$ 和 $\tau_u(v)$ 就需要具备良好的密码学性质。

4.3 对 $\rho(u)$ 和 $\tau_u(v)$ 的构造

对 S 盒的密码学性质，主要考虑其差分性质和线性性质，因此 $\rho(u)$ 和 $\tau_u(v)$ 就需要具有良好的差分性质和线性性质。由于 $\rho(u)$ 和 $\tau_u(v)$ 都是 F_2^8 的子空间上的置换，为了讨论其差分和线性性质，引入自同构映射 L_U 和 L_V，将其映射到 F_2^5 和 F_2^3 上分别进行讨论。

$\mathscr{B}_u=(u_i)_{i<5}=(01,04,08,10,80)$ 和 $\mathscr{B}_v=(v_i)_{i<3}=(03,48,66)$ 分别是 U 和 V 的基，L_U 和 L_V 为：

$$L_U:F_2^5\rightarrow U$$

$$(x_4,\cdots,x_0)\mapsto\sum_{i=0}^{4}x_iu_i$$

$$L_V:F_2^3\rightarrow V$$

$$(y_4,\cdots,y_0)\mapsto\sum_{i=0}^{2}y_iv_i$$

L_U 和 L_V 如表 1 和表 2 所列。定义 F_2^5 上的置换 $\rho'(x)=L_U^{-1}\rho L_U$ 和 F_2^3 上的置换 $\tau_u'(y)=L_V^{-1}\tau_uL_V$，易知 $\rho'(x)$ 与 $\rho(u)$ 的差分性质和线性性质等价，$\tau_u'(y)$ 与 $\tau_u(v)$ 的差分和线性性质等价。

表 1 线性映射 L_U

Table 1 Linear map L_U

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$L_U(x)$	00	01	04	05	08	09	0c	0d	10	11	14	15	18	19	1c	1d
x	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
$L_U(x)$	80	81	84	85	88	89	8c	8d	90	91	94	95	98	99	9c	9d

表 2　线性映射 L_V

Table 2　Linear map L_V

y	0	1	2	3	4	5	6	7
$L_V(y)$	00	03	48	4b	66	65	2e	2d

接下来只需要设计性质良好的 $\rho'(x)$ 和 $\tau_u'(y)$。

根据文献[3]中的分析，S 的线性均匀度取决于 $\rho(u)$，$\rho(u)$ 的线性均匀度越低，S 的线性均匀度就越低，S 的差分均匀度取决于 $\rho(u)$ 和 $\tau_u(v)$ 的差分均匀度，$\rho(u)$ 和 $\tau_u(v)$ 的差分均匀度越低，S 的差分均匀度就越低。因此，需要分别选取差分特性和线性特性都好的 $\rho'(x)$，以及差分特性好的 $\tau_u'(y)$。

考虑如表 3 所列置换 $\rho'(x)$。其线性均匀度为 8，差分均匀度为 6。

对每一个 $u\in U$，设计置换 $\tau_u'(y)$，考虑如表 4 所列的 32 个置换。其差分均匀度都为 2。

利用 $\rho'(x)$ 和 $\tau_u'(y)$ 来构造置换 S，因为对 $\forall x\in F_2^8$，$x=u+v$，则：

$$S(u+v)=\rho(u)+\tau_u(v)$$
$$=L_U\rho' L_U^{-1}(u)+L_V\tau_u' L_V^{-1}(v)$$

将表 3 和表 4 中的 $\rho'(x)$ 和 $\tau_u'(y)$ 代入计算就得到如表 5 所列的置换 S。S 的差分均匀度为 42，线性均匀度为 64，容易验证，S 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(V)$。

由第 4 节知，对 S 复合上线性映射 L 就得到陷门 S 盒 $\mathbb{S}$，$\mathbb{S}=L\circ S$ 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(W)$，陷门信息就是 $\mathscr{L}(V)$ 和 $\mathscr{L}(W)$ 的划分方式。

表 3　置换 $\rho'(x)$

Table 3　Permutation $\rho'(x)$

x	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f
0.	19	14	03	0f	06	08	02	15	1e	05	09	13	1b	16	1f	10
1.	18	07	17	04	01	12	1d	0b	0a	00	1c	1a	0d	0c	11	0e

表 4　置换 $\tau'_u(y)$

Table 4　Permutation $\tau'_u(y)$

y	0	1	2	3	4	5	6	7	y	0	1	2	3	4	5	6	7
$\tau'_{00}(y)$	3	6	5	4	0	7	1	2	$\tau'_{01}(y)$	3	6	5	4	0	7	1	2
$\tau'_{04}(y)$	3	6	4	0	7	1	5	2	$\tau'_{05}(y)$	0	2	3	4	6	5	7	1
$\tau'_{08}(y)$	0	2	1	7	6	5	4	3	$\tau'_{09}(y)$	2	7	1	0	6	5	4	3
$\tau'_{0c}(y)$	0	6	1	4	5	7	2	3	$\tau'_{0d}(y)$	0	6	1	4	5	7	2	3
$\tau'_{40}(y)$	3	7	6	0	1	4	2	8	$\tau'_{41}(y)$	3	6	7	0	4	2	5	1
$\tau'_{44}(y)$	6	7	3	0	4	2	5	1	$\tau'_{45}(y)$	4	6	3	0	7	2	5	1
$\tau'_{48}(y)$	4	6	0	7	3	2	5	1	$\tau'_{49}(y)$	6	0	7	4	2	5	1	3
$\tau'_{4c}(y)$	6	0	7	4	5	1	2	3	$\tau'_{4d}(y)$	1	7	6	4	5	0	3	2
$\tau'_{80}(y)$	1	7	4	5	0	3	6	2	$\tau'_{81}(y)$	7	1	4	5	0	3	2	6
$\tau'_{84}(y)$	7	4	5	0	3	1	2	6	$\tau'_{85}(y)$	7	4	5	0	3	2	6	1
$\tau'_{88}(y)$	4	5	0	3	7	2	6	1	$\tau'_{89}(y)$	4	5	0	3	2	6	7	1
$\tau'_{8c}(y)$	5	4	0	3	2	6	1	7	$\tau'_{8d}(y)$	5	0	3	4	2	6	1	7
$\tau'_{c0}(y)$	5	0	3	4	6	2	7	1	$\tau'_{c1}(y)$	5	0	4	6	3	2	7	1
$\tau'_{c4}(y)$	3	5	4	6	0	7	1	2	$\tau'_{c5}(y)$	3	2	6	4	7	1	0	5
$\tau'_{c8}(y)$	2	7	5	6	4	0	1	3	$\tau'_{c9}(y)$	1	2	6	3	4	5	0	7
$\tau'_{cc}(y)$	1	2	5	3	6	4	0	7	$\tau'_{cd}(y)$	1	3	7	6	0	4	2	5

表 5　S 将 $\mathscr{L}(V)$ 映射到 $\mathscr{L}(V)$

Table 5　S maps $\mathscr{L}(V)$ to $\mathscr{L}(V)$

S	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	b4	ad	26	3f	20	1d	5e	ab	0c	53	d8	4f	21	89	27	cc
1	b9	2c	a7	54	bf	68	2b	d9	78	22	8c	3b	33	c2	48	9d
2	ac	47	8f	ca	35	29	e1	fd	5f	46	8e	d5	cb	d2	d3	ca
3	c3	b8	de	a5	a9	d7	1e	ce	c7	53	9a	0e	4b	17	df	82
4	4e	52	be	a2	46	cb	02	aa	1a	65	03	91	e8	38	b3	cd
5	95	44	cf	b0	55	2e	0b	16	32	c1	e4	de	34	a0	4d	fc
6	96	47	05	f0	40	59	7c	88	41	e9	04	64	9b	87	c4	10
7	c6	52	11	85	4a	71	9c	09	80	df	70	6d	07	d6	5d	61
8	d2	c5	4f	58	45	c0	e5	60	ec	69	0f	8a	12	9e	15	74
9	9f	8b	00	14	bd	b1	d7	13	5a	5a	5b	d1	c3	5e	39	c2
a	dd	51	db	57	c6	43	af	4c	4a	23	ce	a6	a3	d3	3e	4e
b	97	49	81	5f	d0	3c	5b	18	1f	db	da	94	42	56	dc	c8
c	01	84	c7	c9	99	30	56	da	7d	e0	0d	90	06	83	2d	a8
d	92	b6	f5	f4	0a	d4	1c	2f	31	ed	25	ba	75	3a	5c	98
e	4b	cf	8d	08	28	b5	1b	86	bb	37	bc	f8	2a	42	24	a1
f	d6	50	36	79	43	57	f9	ae	f1	6c	a4	b2	93	19	b7	3d

5　陷门 S 盒构造陷门算法的安全分析

本节采用文献[4]中 Bannier 等的陷门算法作为模型，利用陷门 S 盒设计加密算法来分析这种 S 盒的实用性和安全性。在本文的算法模型中使用 AES 的密钥扩展算法，密钥长度为 96 bit，使用 AES 的密钥扩展算法，轮函数输入为 64 bit，使用 16 轮 SPN 结构，分别为加密钥层 α_k，替换层 σ 和扩散层 π，k 比特加密的轮函数 $F_k=\pi\sigma\alpha_k$，轮函数及其对线性划分的映射如图 3 所示，在最后一轮将扩散层换为加密钥层。其中加密钥层每轮使用 64 bit 子密钥；替换层重复排列使用 4 个 8×8 的陷门 S 盒 $S_i(i=1,2,3,4)$；设计扩散层使其分支数为 5，达到最优。

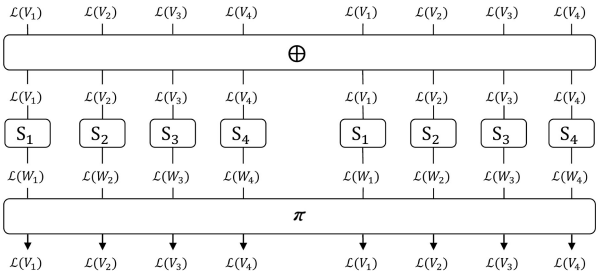

图 3 陷门算法轮函数

Fig. 3 Round function of trapdoor algorithm

由前文的讨论可知，加密钥层将 $\mathcal{L}(V_i)$ 映射到 $\mathcal{L}(V_i)$，替换层每个陷门 S 盒将 $\mathcal{L}(V_i)$ 映射到 $\mathcal{L}(W_i)$，扩散层将 $\mathcal{L}(W_i)$ 映射到 $\mathcal{L}(V_i)$，整个轮函数就将 $\mathcal{L}(V_i)$ 映射到 $\mathcal{L}(V_i)$，陷门信息就是 $\mathcal{L}(V_i)$ 和 $\mathcal{L}(W_i)$ 对 F_2^8 的划分方式。在已知陷门信息的情况下利用文献[3]中的密钥搜索算法，使用 $2^{14}\sim2^{16}$ 对已知明密文就可以完全恢复 96 bit 密钥。

在不知道陷门信息的情况下，对算法进行差分分析和线性分析，由第 4 节对陷门 S 盒的构造，S 盒差分均匀度为 42，线性均匀度为 64。因为分支数为 5，16 轮加密至少有 40 个活动 S 盒，对 16 轮加密使用差分分析恢复 64 bit 子密钥需要 $(42/256)^{40})^{-1}\approx2^{104}$ 对明密文，对 16 轮加密使用线性分析恢复 64 bit 子密钥需要 $((64/128)^{40})^{-2}\approx2^{80}$ 对明密文，而使用穷举算法只需要 2^{64} 对明密文，说明算法在陷门信息保密的情况下对差分分析和线性分析是安全的。

结束语 本文在 Bannier 等的研究基础上，基于线性划分的原理，提出了 8×8 的陷门 S 盒的设计方法，对这种 S 盒的差分性质和线性性质进行了研究，构造了一个 8×8 的陷门 S 盒的实例并加以分析；并研究了使用这种 S 盒的加密算法的安全性，在知道陷门信息的情况下可以很快恢复加密密钥，但在陷门信息保密的情况下，此类算法对差分分析和线性分析是安全的。

关于此类陷门设计方法，今后值得研究的方向有：1）使用 APN 函数等优化陷门 S 盒的差分性质和线性性质[9-11]；2）分析和优化陷门 S 盒的其他安全性质，如代数免疫性[12-13]、非线性性[14-15]等；3）研究基于线性划分构造陷门原理的序列密码，设计带陷门的序列加密算法[16]；4）在算法实现方面考虑更加高效快速的运算，如减少或简化算法扩散层异或运算数等[17-18]；5）基于陷门算法，实现公钥加密等功能；6）研究基于其他代数结构来构造陷门的方法。

参 考 文 献

[1] RIJMEN V, PRENEEL B. A family of trapdoor ciphers[M]// Fast Software Encryption. Springer-Verlag, 1997: 139-148.

[2] WU H J, BAO F, DENG R H, et al. Cryptanalysisof rijmenpreneel trapdoor ciphers[C]// Advances in Cryptology-Asiacrypt'98. Springer, 1998: 126-132.

[3] BANNIER A, BODIN N, FILIOL E. Partition-based trapdoor ciphers[OL]. http://dx. doi. org/10. 5772/intechopen. 70420.

[4] BANNIER A, FILIOL E. Mathematical backdoors in symmetric encryption systems: Proposal for a backdoored AES-like block cipher[C]// International Workshop on FORmal Methods in Security Engineering (ForSE). 2017: 622-631.

[5] 聂灵沼，丁石孙. 代数学引论[M]. 北京：高等教育出版社，2003.

[6] DAEMEN J, RIJMEN V. The design of Rijndael[M]. Heidelberg: Springer, 2002.

[7] BUDAGHYAN L, HELLESETH T. On isotopisms of commutative presemifields and CCZ-equivalence of functions. Int. [J]. Found. Comput. Sci., 2011, 22: 1243-1258.

[8] CHEN X, QU L J, LI C, et al. A New Method to Investigate the CCZ- Equivalence between Functions with Low Differential Uniformity[J]. Finite Fields and Their Applications, 2016, 42: 165-186.

[9] YOSHIARA S. Equivalences of power APN functions with power or quadratic APN functions[J]. Journal of Algebraic Combinatorics, 2016, 44(3): 561-585.

[10] QU T J, CHEN X, NIU T L, et al. Recent Progress in Low Differential Uniformity Functions over Finite Fields[J]. Journal of Computer Research and Development, 2018, 55(9): 1931-1945.

[11] CANTEAUT A, DUVAL S, PERRIN L. A generalisation of Dillon's APN permutation with the best knowndifferential and nonlinear properties for all fields of size 2^{4k+2}[J]. IEEE Transactions on Information Theory, 2017, 63(11): 7575-7591.

[12] WANG X C, CHEN K F, SHEN Z H, et al. Construction of a Family of Balanced Boolean Functions with Optimal Algebraic Immunity[J]. Computer Applications and Software, 2018, 35(1): 325-329.

[13] SUN L, FU F W. Constructions of even-variable RSBFs with optimal algebraic immunity and high nonlinearity[J]. Journal of Applied Mathematics & Computing, 2018, 56: 593-610.

[14] ZHANG F R, PASALIC E, WEI Y Z. Constructing bent functions outside the Maiorana-McFarland class using a general form of rothaus[J]. IEEE Transactions on Information Theory, 2017, 63(8): 5336-5349.

[15] ZHANG W G, PASALIC E. Generalized Maiorana-McFarland Construction of Resilient Boolean Functions with High Nonlinearity and Good Algebraic Properties[J]. IEEE Transactions on Information Theory, 2014, 60(10): 6681-6695.

[16] FILIOL E. BSEA-1-A Stream Cipher Backdooring Technique [J]. arXiv: 1903. 11063, 2019.

[17] CHEN S Z, ZHANG Y F, REN J J. Constructions of Maximal Distance Separable Matrices with Minimum XOR-counts[J]. Journal of Electronics and Information Technology, 2019, 41(10): 2416-2422.

[18] JEAN J, PEYRIN T, SIM S M, et al. Optimizingimplementations of lightweight building blocks[J]. IACRTransactions on Symmetric Cryptology, 2017, 2017(4): 130-168.

HAN Yu, born in 1995, postgraduate. His main research interests include cryptography and symmetric cryptography.

ZHANG Wen-zheng, born in 1966, researcher, chief expert of CETC. His main research interests include cryptography, design and analysis of cryptographic algorithms, and Boolean functions.