doi:10.3969/j.issn.1000-436x.2014.07.001

基于高阶差分的 type-1 广义 Feistel-SP 结构与 Feistel-SPSP 结构比较研究

董乐[1,3]，杜蛟[1,3]，吴文玲[2]

(1. 河南师范大学 数学与信息科学学院，河南 新乡 453007；
2. 中国科学院 软件研究所 可信计算与信息保障实验室，北京 100190；
3. 河南师范大学 数学与科学计算实验室，河南 新乡 453007)

摘 要：通过对代数次数增加情况的分析，研究了 type-1 广义 Feistel 结构下，单 SP(substitution-permutation)模型与双 SP 模型抵抗高阶差分分析的能力。结合高阶积分与高阶差分思想，开发了四路 type-1 广义 Feistel-SP 与 Feistel-SPSP 结构代数次数上界估计的新方法。利用这一方法，分别构造了这 2 种结构在 2 种常用参数下的区分器。结果显示，四路 type-1 广义 Feistel 结构下，双 SP 模型抵抗高阶差分攻击的能力不如单 SP 模型。

关键词：type-1 广义 Feistel 结构；单 SP 函数；双 SP 函数；高阶差分；伪随机性

中图分类号：TN918 **文献标识码**：A **文章编号**：1000-436X(2014)07-0001-09

Higher-order differences based research on comparison between type-1 generalized Feistel-SP network and Feistel-SPSP network

DONG Le[1,3], DU Jiao[1,3], WU Wen-ling[2]

(1. College of Mathematics and Information Science, Henan Normal University, Xinxiang 453007, China;
2. Trust Computing and Information Assurance Laboratory, Institute of Software Chinese Academy of Sciences, Beijing 100190, China;
3. Mathematics and Scientific Computing Laboratory, Henan Normal University, Xinxiang 453007, China)

Abstract: The powers against the higher-order differential cryptanalysis of the single-SP(substitution-permutation) model and the double-SP model are studied in the type-1 Feistel network by analyzing the growths of algebraic degrees. Combining the higher-order integral and the higher-order difference, a new method is exploited to estimate the upper bounds of algebraic degrees for the 4-line type-1 Feistel-SP scheme and the 4-line type-1 Feistel-SPSP scheme. Applying the new method, distinguishers of the two schemes are constructed with four common parameters. As a result, the double-SP model is weaker than the single-SP model against the higher-order differential attack under the 4-line type-1 Feistel structure.

Key words: type-1 Feistel structure; single SP-function; double SP-function; higher-order difference; pseudo- randomness

1 引言

自从 20 世纪 70 年代，分组密码先驱 Horst Feistel 提出 Feistel 结构以来，包括 DES[1] (data encryption standard)在内的许多分组密码算法选择了这一结构作为核心架构。随着计算能力的迅猛发展，很多分组密码算法的分组长度与密钥长度不能再提供给人们足够的安全信心。为了增加分组长度，并且保留原有分组密码算法的绝大部分特点，人们设计了各种各样的“广义 Feistel 结构”，其中比较著名的有郑玉良等人设计的 type-1、type-2 和 type-3 广义 Feistel 结构[2]。

另一方面，用 Feistel 结构设计分组密码算法时，它的轮函数设计经常采用所谓的 SP (substitu-

收稿日期：2014-06-01；**修回日期**：2014-07-04
基金项目：河南师范大学博士启动基金资助项目（01016500148）；国家自然科学基金资助项目（61272476, 61202422）
Foundation Items: The Scientific Research Foundation for High Level Talents of Henan Normal University (01016500148); The National Natural Science Foundation of China (61272476, 61202422)

tion-permutation) 结构，也就是说，此轮输入的一半进入轮函数，首先异或上这一轮的轮子密钥，而后进入由若干并置 S 盒组成的 S 层，最后进入一个线性扩散层 P，习惯上称此类密码算法为 Feistel-SP 类算法，采用这一结构的有 Camellia[3]和 LBlock[4]等分组密码算法。

在 2011 年的 ACISP (information security and privacy-australasian conference) 会议上，Andrey Bogdanov 等人提出了“四路”(4-line) type-1 和 type-2 结构下的“双 SP 函数”(double SP-function) 的理念[5]，并且证明了使用双 SP 函数的算法，活跃的差分(线性) S 盒所占比例，要高于使用单 SP 函数的算法。也就是说，双 SP 函数具有更好的抵抗差分 (线性) 攻击能力。

在 2012 年的印度密码年会 (Indocrypt 2012) 上 Yu Sasaki 指出，对于某些攻击来说，采用双 SP 函数的算法并不比采用单 SP 函数的算法有更强的抵御能力，有时反而更弱[6]。文章给出了采用双 SP 函数的 type-2 广义 Feistel 结构的 7 轮区分攻击 (包含 28 个 SP 层)，而对采用单 SP 函数的同一结构却只能攻击到 11 轮 (包含 22 个 SP 层)。这一与设计者相反的论调使得广义 Feistel 结构下的“单 SP 模型与双 SP 模型优劣性对比问题”更加有趣。2013 年的印度密码年会上，Donghoon Chang 等人甚至将 Yu Sasaki 的攻击扩展到了 8 轮 (包含 32 个 SP 层)[7]。需要说明的是，双 SP 函数的设计者在评估安全性的时候采用的攻击为一般意义下的差分与线性攻击，而 Yu Sasaki 等人采用的是由截断差分攻击衍生出来的“反弹攻击”。

本文以代数次数增长性质为依据，讨论四路 type-1 广义 Feistel 结构下单 SP 模型与双 SP 模型抵抗高阶差分攻击的能力，为这 2 种模型的比较提供新的视角与证据。首先通过对置换性质的检测给出其高阶积分性质，然后利用 SP 结构的特点开发出这类算法代数次数上界估计的新方法，最后将这一方法应用于 4 种常用参数下单 SP 模型 (四路 type-1 广义 Feistel-SP 结构) 与双 SP 模型(四路 type-1 广义 Feistel-SPSP 结构)抵抗高阶差分攻击能力的结果。

2 基础知识

2.1 单 SP 模型与双 SP 模型

Andrey Bogdanov 等人在 2011 年提出，在 type-1 和 type-2 广义 Feistel 结构下建议采用双 SP 函数，来代替常用的单 SP 函数[5]。这里的“双 SP 函数”为 2 个 SP 函数的串联。图 1 为这 2 种 SP 函数的具体流程。

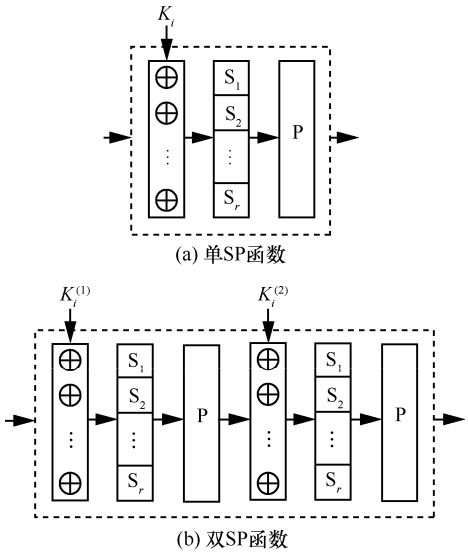


图 1 单 SP 函数与双 SP 函数

本文的研究对象为采用单 SP 函数与双 SP 函数的四路 type-1 广义 Feistel 结构，这里分别称它们为“单 SP 模型”与“双 SP 模型”，如图 2 所示。在下文中，每一路的数据称为一个“字”，从左至右分别为第一、二、三、四个字。

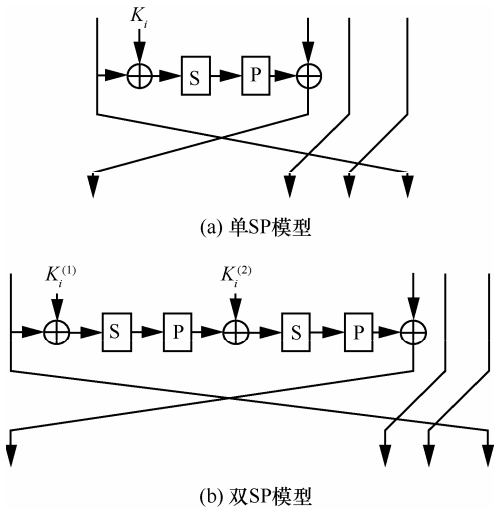


图 2 单 SP 模型与双 SP 模型

根据已有算法设计规律，这里所选的 S 盒层与线性扩散层 P 有如下具体要求。

1) S 盒层：由 r 个 c 比特大小的平衡 S 盒并置，每个 S 盒的代数次数都达到了 $c-1$。

2) 线性扩散层 P：代数次数为 1。

2.2　高阶差分与高阶差分区分器

1994 年，来学嘉给出了密码函数微分的定义[8]。

定义 1　设 P 为一个 F_2^n 上的置换。对于任意的 $a\in F_2^n$，P 在点 a 处的微分为函数

$$D_aP(x)=P(x\oplus a)\oplus P(x)$$

这里 $x=(x_1,x_2,\cdots,x_n)$ 为 F_2 上的 n 维变量。而 P 在点 $a_1,\cdots,a_i$ 处的 i 阶微分定义为

$$D_{a_1,\cdots,a_i}P(x)=D_{a_i}(D_{a_{i-1}}(\cdots D_{a_1}P(x)))$$

$$=\bigoplus_{(k_1,\cdots,k_i)\in F_2^i}P\left(x\oplus\left(\bigoplus_{j=1}^{i}k_ja_j\right)\right)$$

函数微分的代数次数与原函数的代数次数有关系：$\deg(D_aP(x))\leqslant\deg P(x)-1$。所以，对于任意的 $(\deg P+1)$ 个点 $a_1,\cdots,a_{\deg P+1}$，置换 P 的 $(\deg P+1)$ 阶微分为 0。

利用上述性质可以构造高阶差分区分器。首先，将函数某些输出比特 $y_1,\cdots,y_i$ 的代数正规型写出，如果它们的代数次数都小于等于某一个常数 k，则可以遍历输入的某 k 个比特所有可能的值，其他比特的值固定，则对应的 2^k 个密文的异或和在 $y_1,\cdots,y_i$ 处一定为零。

如果函数是一个分组密码算法，则按此方法可以得到其高阶差分区分器，进而恢复密钥。如果函数是一个杂凑函数的内部置换，或者是一个已知密钥的分组密码算法，则还可以同时进行逆向构造，得到中间起始的已知密钥高阶差分区分器。

本文将同时讨论单向的高阶差分区分器与中间起始的双向高阶差分区分器。

2.3　高阶积分

积分攻击[9,10]自问世以来，一直是分组密码的重要分析工具。后来经过发展，还提出了高阶积分的思想[11,12]。在高阶积分攻击中，输入含有多个活跃单元，这些活跃单元相互独立，有时它们在通过某些 S 盒层与线性扩散层之后仍然是活跃且独立的。所以有时可以用若干运算之后的状态作为起始状态，进行下一步的攻击[13]。判断若干运算之后活跃单元是否活跃且独立，关键在于判断这些计算是否是一个置换。本文便基于这一性质开展攻击。

2.4　代数次数的估计方法

一般高阶差分攻击主要基于对函数代数次数上界的估计。对于常见的迭代分组密码算法来说，最初的估计方法是根据“乘法规则”。也就是说，如果一轮算法的代数次数为 a，则 i 轮算法的代数次数有上界 a^i。

2011 年，Christina Boura 等人针对 SP 类迭代置换，给出估算代数次数上界的新公式[14]。这里将其表述为 SP 类迭代分组密码的形式。

定理 1　设 E^i 为分组密码算法 E 的第 i 轮，其由轮密钥加、S 盒层与线性置换层 P 组成，其中 S 盒层为 m 个平衡 S 盒的并置，并且这些 S 盒的大小相同，记为 n_0。如果此分组密码算法的前 $i-1$ 轮有代数次数上界 d，则 i 轮之后的代数次数

$$d'\leqslant n-\frac{n-d}{n_0-1}$$

其中，n 为分组密码算法 E 的分组长度。

3　单 SP 模型与双 SP 模型代数次数上界估计的新方法

3.1　置换检测

当密钥固定时，一般的 F_2^n 上的分组密码算法都可以看作是 F_2^n 上的一个双射，这里也称此双射是 F_2^n 上的一个“置换”。有的时候，需要固定输入的一部分比特为常数，考察“局部输入”到“局部输出”所构造的新映射是否为置换。此时需要引入一个置换检测的方法。这种检测通常可以用引入输入差分，检测输出差分的方式来解决。

命题 1　设 P 为一个 F_2^n 到 F_2^n 的置换。

1) 固定其输入的某 i 个比特为常数，$i<n$，其他比特仍为变量。如果所有对应输出的某 i 个比特也为常数，则此时置换 P 诱导了一个 F_2^{n-i} 到 F_2^{n-i} 的映射 P'。

2) 在满足条件①的情况下，在 P' 输入的任意处引入一个差分，如果输出一定含有差分，则可以断定函数 P' 是一个置换。

证明　① 不失一般性，记 P 的输入为

$$(x_1,\cdots,x_{n-i},c_1,\cdots,c_i)\text{，}$$

这里 $x_1,\cdots,x_{n-i}\in F_2$，$c_1,\cdots,c_i$ 为常数。由于 P 是一个置换，则对于 $x_1,\cdots,x_{n-i}$ 的每一个取值，都有一个像与其对应，这个像是一个 F_2 上 n 维向量。根据已知条件，无论 $x_1,\cdots,x_{n-i}$ 如何取值，对应的像中有 i 个比特不会发生变化，不妨假设为后 i 个比特，则输出可以记为

$$(y_1,\cdots,y_{n-i},c_1',\cdots,c_i')$$

其中，$y_1,\cdots,y_{n-i}\in F_2$，$c_1',\cdots,c_i'$为常数。

这样实际上建立了一个F_2^{n-i}到F_2^{n-i}的对应

$$P':\ F_2^{n-i}\to F_2^{n-i},\ (x_1,\cdots,x_{n-i})\mapsto(y_1,\cdots,y_{n-i})$$

由P为置换容易得出，F_2^{n-i}中的每一个元素在P诱导的P'下都有且仅有一个F_2^{n-i}中的像与其对应，所以P'是一个映射。

② 由已知，在P'输入的任意处引入一个差分，如果输出一定含有差分，则说明F_2^{n-i}中2个不相同的元素的像一定不同，即映射P'是一个单射。

这样就说明了，F_2^{n-i}的2^{n-i}个元素对应了2^{n-i}个不同的像，所以得出F_2^{n-i}中的每一个元素都有原像，即P'是一个满射。

所以P'是一个双射，即置换。证毕。

下面利用命题1，构造四路type-1广义Feistel结构的2轮高阶积分路径，这里假设其轮函数为置换。

命题2 设输入输出长度为N=4n的四路type-1广义Feistel结构中(每个字的长度为n)，输入的2个字具有高阶积分模式(A,A,A,A^*)，其中A表示全活跃且相互独立的字，A^*表示一部分比特活跃且独立，剩余比特为常数的字，则2轮之后的输出模式为(A,A^*,A,A)。

证明 将此2轮迭代看作一个F_2^N到F_2^N的置换P。设模式为A^*的字中有i个比特为常数，剩余的$n-i$个比特活跃。显然2轮之后的第二个字对应地有i个比特为常数，则由命题1第一部分可得，此时P诱导了一个F_2^{N-i}到F_2^{N-i}的映射P'。下面证明这个映射是一个置换，引入输入差分，检测输出差分的方式来证明，如图3所示。

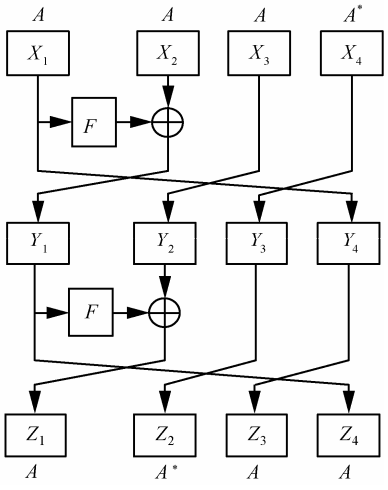


图3 四路type-1广义Feistel结构的2轮高阶积分路径

记输入的2个字为(X_1,X_2,X_3,X_4)，一轮之后状态的4个字为(Y_1,Y_2,Y_3,Y_4)，2轮之后状态的2个字为(Z_1,Z_2,Z_3,Z_4)。

若在输入的第一个字X_1中引入一个差分，因为$Z_3=X_1$，故无论输入的后3个字X_2,X_3,X_4中有无差分，输出的第三个字Z_3中一定含有差分，即输出中必有差分。

设输入的第一个字X_1中不含差分。若在第二个字X_2中引入差分，因X_1中不含差分，则Y_1中一定含有差分，又由于$Z_4=Y_1$，故无论输入的后2个字X_3,X_4中有无差分，输出的第四个字Z_4中一定含有差分，即输出中必有差分。

设X_1,X_2中均无差分，则Y_1中不含差分。若X_3中引入差分，则无论X_4有无差分，Z_1中必有差分，即输出中必有差分。

设X_1,X_2,X_3中均无差分，只有X_4的活跃比特中有差分，由于$Z_2=X_4$，则Z_2的对应比特中一定含有差分，此时输出中必有差分。

由命题1第二部分得，P'是一个F_2^{N-i}到F_2^{N-i}的置换，所以Z_1,Z_3,Z_4中的所有比特与Z_2中的活跃比特，活跃且独立，即2轮之后的输出模式为(A,A^*,A,A)。证毕。

3.2 等价结构

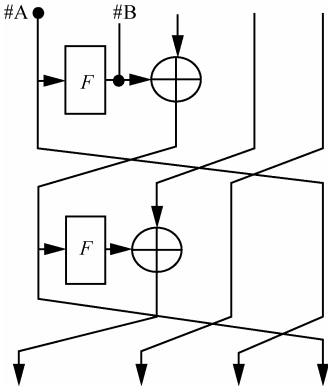
将轮函数为置换的type-1广义Feistel结构，转化为另外一个在估计代数次数时等价的结构。具体如图4所示。

在构造高阶差分区分器时，通常在起始状态选取一些活跃且独立的比特作为活跃比特。由3.1节可以看到，适当选取明文中的活跃比特，可以使若干轮之后的比特同样活跃且独立。将此时的状态作为高阶差分攻击的起始状态，便可以以一种组合的方式构造区分器。具体步骤可以参看文献[13]。

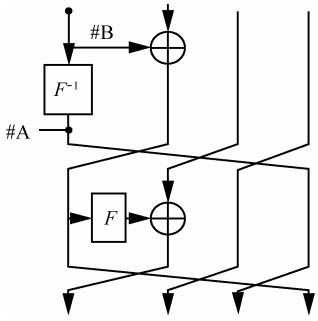
针对轮函数为置换的四路type-1广义Feistel结构，记初始状态为(U_1,U_2,U_3,U_4)。如果其第一个字U_1(也就是图4(a)中的#A处)的全部比特活跃且与U_2,U_3,U_4中活跃比特互相独立。由于轮函数F为置换，所以图4(a)中的#B处的全部比特也全活跃，且与U_2,U_3,U_4中活跃比特互相独立，所以，起始状态可以选择#B处的字与U_2,U_3,U_4，即$(F(U_1),U_2,U_3,U_4)$。

这样，可以将四路type-1广义Feistel结构变为图4(b)的形式，即输入为$(F(U_1),U_2,U_3,U_4)$，#B处

的字经过 F^1 变为#A 处的 U_1。需要说明的是，这一等价结构与前面轮连接之后，在计算上与原始结构并不等价，只是在某些条件下，估计其代数次数上界时，才和原始结构等价。



(a) 四路 type-1 广义 Feistel 结构



(b) 四路 type-1 广义 Feistel 结构在估计代数次数时的等价结构

图 4　估计代数次数时四路 type-1 广义 Feistel 结构的等价变换

设轮函数 F 和它的逆 F^1 的代数次数均为 m，在 U_1 全活跃的情况下，针对这 2 种结构估计每一轮的 4 个字的代数次数上界，然后加以比较。具体如表 1 所示。

表 1　2 种结构下估计的代数次数上界结果比较

轮次	状态中 4 个字的代数次数上界							
	原始结构				等价结构			
0	1	1	1	1	1	1	1	1
1	m	1	1	1	1	1	1	m
2	m^2	1	1	m	m	1	m	1
3	m^3	1	m	m^2	m^2	m	1	m
4	m^4	m	m^2	m^3	m^3	1	m	m^2
5	m^5	m^2	m^3	m^4	m^4	m	m^2	m^3
6					m^5	m^2	m^3	m^4

在原始结构中，输入的 4 个字中每个比特的代数次数都为 1。每一轮只有第一个字进入 F 函数，再异或上第二个字，所以此后的每一轮都只有第二个字更新，经过换位变成下一轮的第一个字，其代数次数上界随之增加，这里的上界估计只简单地采用乘法规则；而其他的 3 个字只有换位，所以代数次数不变。故一轮之后 4 个字的代数次数上界为 $(m,1,1,1)$，后面几轮照此办理。

而在等价结构中，虽然开始时输入的 4 个字中每个比特的代数次数也都为 1，但是由于第一轮结构的变化，第二个字只是异或上第一个字，然后换位，虽然值发生了变换，但是代数次数仍然是 1；同时第一个字通过 F^{-1} 运算后换到了第四个位置，由于 F^{-1} 的代数次数也为 m，所以第二轮第四个字的代数次数上界为 m。故一轮之后 4 个字的代数次数上界为 $(1,1,1,m)$。后面的轮结构与原始结构相同，按照原方法估计即可。

由表 1 可以看出，按原始结构估计，5 轮之后 4 个字的代数次数上界为 (m^5,m^2,m^3,m^4)，而利用等价结构估计的代数次数上界更紧，6 轮之后代数次数才会达到 (m^5,m^2,m^3,m^4)。基于此结果构造的高阶差分区分器将比基于原来方法构造的高阶差分区分器多出一轮。

4　4 种常用参数下单、双 SP 模型高阶差分区分器的构造

本节应用第 3 节介绍的新方法对单 SP 模型与双 SP 模型构造高阶差分区分器。具体构造时以 4 种常用参数为例，其他参数的情况可以类似处理。

研究对象是带单 SP 函数的轮函数与双 SP 函数的轮函数的四路 type-1 广义 Feistel 结构。此结构的输入输出长度记为 N bit，S 盒层共有 r 个大小为 c bit 的 S 盒并置，则有关系 $N=4rc$。后面用 (N,c) 表示所采用的参数，本节的攻击选取的 4 种参数分别为 (64,4)、(128,4)、(128,8) 和 (256,8)。根据定理 1 中公式，这 4 种参数在通过 SP 层时代数次数上界增长情况如表 2 所示，表中第一行的数字表示的是第几层。

表 2　4 种常用参数下通过 SP 层的代数次数增长情况

参数	0	1	2	3	4	5	6	7	8
(64,4)	1	3	9	27	51	59	**62**	63	
(128,4)	1	3	9	27	81	112	122	**126**	127
(128,8)	1	7	49	116	**126**	127			
(256,8)	1	7	49	226	**251**	255			

观察表 2 发现，4 种参数下非平凡结果的最高层数 (代数次数上界达到 N-1 时为平凡结果) 分别为 6 层、7 层、4 层和 4 层，在表 2 中用粗体表示。

首先以参数(128,8) 为例，构造高阶差分区分器。

4.1 参数为(128,8)时高阶差分区分器的构造

参数为(128,8)时，每一个字的大小为 32 bit，S 层含有 4 个 8 bit S 盒。在输入部分选取前三个字的所有比特与第四个字中的 31 个比特为活跃比特。由 3.1 节的命题 2，2 轮之后的第一、三、四个字仍然全活跃，第二个字中有 31 个比特活跃，并且它们都是互相独立的，记为 (A, A^*, A, A)。后面便从这一状态开始，分别对单 SP 模型和双 SP 模型进行攻击。

首先讨论单 SP 模型的情况。

利用本文 3.2 节中的等价结构，对其代数次数上界的增长情况进行估计，由于每个 F 函数中只有一个 SP 层，所以得出一轮之后的 4 个字的代数次数上界为 (1,1,1,7)，后面轮数具体代数次数增长情况如表 3 所示。

表 3 参数为(128,8)的单 SP 模型代数次数增长情况

轮次	4 个状态字的代数次数增长情况			
0	1	1	1	1
1	1	1	1	7
2	7	1	7	1
3	49	7	1	7
4	116	1	7	49
5	126	7	49	116
6	127	49	116	126
7	127	116	126	127
8	127	**126**	127	127

由于当密钥取定的情况下，分组密码算法可以看作是一个置换，所以输出的代数次数最多可以达到 N-1，N 是分组长度，也是输入中变量个数的最大值。所以表中的代数次数上界最大为 127，称其为平凡上界，所以非平凡上界的最大值为 126。由表 3 可以看出，8 轮之后第二个字的代数次数上界是不平凡的，这样就得到了一个 8 轮的高阶差分区分器。

将此区分器与上面的 2 轮高阶积分路径相连接，就可以得到一个 10 轮的高阶差分区分器。由选取的活跃比特个数得出，此区分器的数据复杂度为 2^{127}。

下面按照同样的方法讨论双 SP 模型的情况。

双 SP 模型与单 SP 模型的区别为，第一个字进入 F 函数的时候，要进行两次 SP 层运算，然后异或上第二个字，而后第二个字再换为下一轮的第一个字。这样第一个字每次更新的时候，要在表 2 中向右跳一格选取代数次数上界，这样攻击的轮数就会缩短。双 SP 模型的代数次数增长情况如表 4 所示。

表 4 参数为(128,8)的双 SP 模型代数次数增长情况

轮次	4 个状态字的代数次数增长情况			
0	1	1	1	1
1	1	1	1	49
2	49	1	49	1
3	126	49	1	49
4	127	1	49	126
5	127	49	126	127
6	127	**126**	127	127

由表 4 可以看出，此时高阶差分区分器的轮数为 6 轮，比单 SP 模型少了 2 轮。加上 2 轮高阶积分路径，此时的高阶差分区分器共有 8 轮，数据复杂度为 2^{127}。

由于双 SP 模型代数次数增长为“跳格选取”，所以简单分析可得，区分器轮数大概应为单 SP 模型区分器轮数的一半。但是事实并非如此，原因为：根据 type-1 广义 Feistel 结构的特点，第一个字将毫无变化地向下保留 3 轮，直到移动至 3 轮之后的第二个字，这一特点与轮函数结构无关。如果去掉这 3 轮与开始的 2 轮高阶积分路径，单 SP 模型下的区分器剩下 5 轮，双 SP 模型下的区分器剩下 3 轮，两者呈近似半数的关系。

基于上述事实，将高阶差分区分器分为 2 个部分：首字代数次数增长部分与首字无更新换位部分。加上前面的 2 轮高阶积分路径，区分器总共由 3 部分组成。按照这一分法，参数为(128,8)的单 SP 模型的区分器有 10 =(2+5+3)轮，双 SP 模型的区分器有 8= (2+3+3)轮。

将区分器分成这样 3 个部分的好处在于，如果用此方法构造其他参数下的同类区分器，可以很容易得到区分器能够达到的轮数。这是因为，最初的 2 轮最后的 3 轮是源于四路 type-1 广义 Feistel 结构的固有特征，与参数没有关系；当分组长度与 S 盒大小等参数发生变化时，只会影响到中间部分的

轮数，由参数为(128,8)时的单、双 SP 模型区分器实例很容易验证这一点。

4.2　其他 3 种参数下高阶差分区分器的情况分析

由 4.1 节参数为(128,8)时的区分器情况，得出所构造的区分器可以分为 3 个部分，3 个部分合在一起组成了一个(2+X+3)轮的高阶差分区分器。将表 3 和表 4 的代数次数增长情况与表 2 对比容易得出，中间部分的轮数 X 与非平凡结果的最高层数相关。记非平凡结果的最高层数为 x，则单 SP 模型的中间部分的轮数 X 与 x 有关系

$$X = x + 1$$

双 SP 模型的中间部分的轮数 X 与 x 有关系

$$X = \lceil x/2 \rceil + 1$$

由于 $x/2$ 未必是一个整数 (参数为(128,4)的情况)，这里我们用 $\lceil x/2 \rceil$ 表示 $x/2$ 的上取整。这样可以推出单 SP 模型区分器的总轮数为 $x+6$，双 SP 模型区分器的总轮数为 $\lceil x/2 \rceil + 6$。

参数为(64,4)、(128,4)和(256,8)时，非平凡结果的最高层数 x 分别为 6、7 和 4，所以在单 SP 模型下，分别可以构造 12 轮、13 轮和 10 轮的高阶差分区分器，数据复杂度分别为 2^{63}、2^{127} 和 2^{252}；在双 SP 模型下，分别可以构造 9 轮、10 轮和 8 轮的高阶差分区分器。

最后对比一下单 SP 模型与双 SP 模型抵抗这种高阶差分攻击的强度。对于 4 种常见参数：(64,4)、(128,4)、(128,8)和(256,8)，单 SP 模型的区分器可以达到 12 轮、13 轮、10 轮和 10 轮，分别含有 12 个、13 个、10 个和 10 个 SP 层；双 SP 模型的区分器可以达到 9 轮、10 轮、8 轮和 8 轮，分别含有 18 个、20 个、16 个和 16 个 SP 层。

所以，综合来看，单 SP 模型具有更强的抵御高阶差分攻击的能力。

5　4 种常用参数下单、双 SP 模型已知密钥区分器的构造

为了考察一个分组密码算法的伪随机性，或者考察一个杂凑函数算法内部置换的伪随机性，有时会对分组密码算法的已知密钥区分器模型进行研究。高阶差分的已知密钥区分器是从中间起始，进行正向与逆向的计算，最后在明文与密文处得到平衡或局部平衡的状态，这里平衡的意思是所有数据的异或和为零。

事实上，在第 4 节中已经构造了已知密钥区分器的正向部分，本节来对 4 种参数下的模型构造逆向部分，最后将正向与逆向部分连接，得到整个高阶差分区分器。

首先对参数为(128,8)时的情况进行研究，然后推广至其他 3 种参数的情况。

5.1　参数为(128,8)时已知密钥区分器的构造

如前文所述，这里主要构造逆向的高阶差分区分器。构造正向区分器的时候，总的起始状态模式为 (A, A, A, A^*)，其中包含 127 个活跃比特。因为最后需要将正向区分器与逆向区分器相连接，所以逆向区分器的起始状态也应该是 (A, A, A, A^*)，并且活跃比特相同。

四路 type-1 广义 Feistel 结构逆向的扩散特点与正向不同：状态的第四个字换位至第一个位置进入 F 函数，而第一个字逆向换位至第二个字异或上其输出，所得字在之后的逆向 2 轮中没有更新；而正向计算时，更新的字会在下一轮直接进入 F 函数。所以可以说，这一结构的逆向扩散比正向慢。

在估计逆向函数代数次数上界的时候，不对函数做任何的等价变化。

首先讨论单 SP 模型的情况。

令起始状态 4 个字代数次数都为 1，则逆向的代数次数上界增加情况如表 5 所示。

表 5　参数为(128,8)的单 SP 模型逆向代数次数增长情况

逆向轮次	逆向 4 个状态字的代数次数增长情况			
15	**126**	127	127	127
14	126	127	127	126
13	126	127	126	126
12	116	126	126	126
11	116	126	126	116
10	116	126	116	116
9	49	116	116	116
8	49	116	116	49
7	49	116	49	49
6	7	49	49	49
5	7	49	49	7
4	7	49	7	7
3	1	7	7	7
2	1	7	7	1
1	1	7	1	1
0	1	1	1	1

从表 5 可以看出，逆向 15 轮之后的第一个字的代数次数不超过 126，如果在起始状态中选择 2^{127} 个数据，逆向 15 轮之后的第一个字将是平衡的。所以逆向区分器可以达到 15 轮。

将正向区分器与逆向区分器相连接，可以得到 $10+15=25$ 轮的已知密钥区分器，数据复杂度为 2^{127}。

通过观察表 5 可以看出，逆向第 3、6、9、12 和 15 轮之后的 4 个状态字的代数次数上界分别为 (1,7,7,7)、(7,49,49,49)、(49,116,116,116)、(116,126,126,126) 和 (126,127,127,127)，也就是说每 3 轮 4 个状态字的代数次数上界更新“升级”一遍，这里的“升级”指的是按照表 2 次序从左到右逐次升格。如果只关注其中的第一个字，升级情况为 $1\to 7\to 49\to 116\to 126$，刚好与表 2 中参数为 (128,8)时的前 5 列对应。

根据这一对应和 3 轮更新一遍的特点可以得出，单 SP 模型逆向区分器轮数为 $3(x+1)$，这里 x 的意义与 4.2 节中的相同。

现在讨论一下双 SP 模型的情况。

根据上面的“升级”特点，在双 SP 模型下，每 3 轮 4 个状态字将会“跳格升级”，也就是说每 3 轮代数次数上界更新时，会隔过一格选取。这样，逆向第 3、6 和 9 轮之后的 4 个状态字的代数次数上界分别为 (1,49,49,49)、(49,126,126,126) 和 (126,127,127,127)。所以，逆向区分器可达 9 轮。

将正向区分器与逆向区分器相连接，可以得到 $8+9=17$ 轮的已知密钥区分器，数据复杂度为 2^{127}。

由上述分析可得，双 SP 模型逆向区分器的轮数为 $3(\lfloor x/2\rfloor+1)$。

5.2 其他 3 种参数下已知密钥区分器的情况分析

由于单 SP 模型的逆向区分器轮数为 $3(x+1)$，双 SP 模型的逆向区分器轮数为 $3(\lfloor x/2\rfloor+1)$，其中 x 表示非平凡结果的最高层数。又由于参数为(64,4)、(128,4)和(256,8)时，非平凡结果的最高层数 x 分别为 6、7 和 4，所以在单 SP 模型下，分别可以构造 21 轮、24 轮和 15 轮的逆向区分器，数据复杂度分别为 2^{63}、2^{127} 和 2^{252}；在双 SP 模型下，分别可以构造 12 轮、12 轮和 9 轮的逆向区分器。

将正向区分器与逆向区分器连接，单 SP 模型下，分别可以构造 33 轮、37 轮和 25 轮的中间起始已知密钥区分器，数据复杂度分别为 2^{63}、2^{127} 和 2^{252}；在双 SP 模型下，分别可以构造 21 轮、22 轮和 17 轮的中间起始已知密钥区分器。

最后对比一下单 SP 模型与双 SP 模型抵抗这种高阶差分攻击的强度。对于 4 种常见参数：(64,4)、(128,4)、(128,8)和(256,8)，单 SP 模型的已知密钥区分器可以达到 33 轮、37 轮、25 轮和 25 轮，分别含有 33 个、37 个、25 个和 25 个 SP 层；双 SP 模型的已知密钥区分器可以达到 21 轮、22 轮、17 轮和 17 轮，分别含有 42 个、44 个、34 个和 34 个 SP 层。

所以从已知密钥模型来看，单 SP 模型仍然具有更强的抵御高阶差分攻击的能力。

6 结束语

本文对轮函数为 SP 函数的 type-1 广义 Feistel 结构进行分析，站在高阶差分攻击的视角上对四路 type-1 广义 Feistel-SP 结构与四路 type-1 广义 Feistel-SPSP 结构进行比较，本文将这 2 种结构称为“单 SP 模型”和“双 SP 模型”。首先，根据轮函数为置换的四路 type-1 广义 Feistel 结构特点，开发了一个估计其代数次数上界的新方法，根据这一方法可以将这一结构的高阶差分区分器扩展一轮。之后将此方法用于 4 种常用参数下的单 SP 模型与双 SP 模型，分别构造了它们的高阶差分区分器；此外，还讨论了已知密钥的区分器模型，构造了 4 种参数下的已知密钥区分器。具体结果如表 6 所示。

通过研究可得，在四路 type-1 广义 Feistel 结构

表 6 本文结果小结

参数(N,c)	高阶差分区分器				逆向高阶差分区分器				已知密钥高阶差分区分器			
	单 SP 模型		双 SP 模型		单 SP 模型		双 SP 模型		单 SP 模型		双 SP 模型	
	轮数	SP 层数	轮数	SP 层数	轮数	SP 层数	轮数	SP 层数	轮数	SP 层数	轮数	SP 层数
(64,4)	12	12	9	18	21	21	12	24	33	33	21	42
(128,4)	13	13	10	20	24	24	12	24	37	37	22	44
(128,8)	10	10	8	16	15	15	9	18	25	25	17	34
(256,8)	10	10	8	16	15	15	9	18	25	25	17	34

下，双 SP 模型的代数次数增长速度不如单 SP 模型，所以抵抗一些基于代数次数的攻击（例如高阶差分攻击、差值攻击和代数攻击等）的能力较弱。这一结果给未来分组密码的设计提供了参考依据。

参考文献：

[1] PUB N F. 46-3. Data Encryption Standard[EB/OL]. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, 1999.

[2] ZHENG Y, MATSUMOTO T, IMAI H. On the construction of block ciphers provably secure and not relying on any unproved hypotheses[A]. Proceedings of the Advances in Cryptology(CRYPTO 1989)[C]. Santa Barbara, California, USA, 1989. 461-480.

[3] AOKI K, ICHIKAWA T, KANDA M, *et al*. Camellia: a 128-bit block cipher suitable for multiple platforms—design and analysis[A]. Proceedings of the Selected Areas in Cryptography(SAC 2000)[C]. Waterloo, Ontario, Canada, 2001. 39-56.

[4] WU W, ZHANG L. LBlock: a lightweight block cipher[A]. Proceedings of the Applied Cryptography and Network Security(ACNS 2011) [C]. Nerja, Spain, 2011. 327-344.

[5] BOGDANOV A, SHIBUTANI K. Double SP-functions: enhanced generalized Feistel networks[A]. Proceedings of the Information Security and Privacy(ACISP 2011) [C]. Melbourne, Australia, 2011. 106-119.

[6] SASAKI Y. Double-SP is weaker than Single-SP: rebound attacks on Feistel ciphers with several rounds[A]. Proceedings of the International Conference on Cryptology in India (INDOCRYPT 2012)[C]. Kolkata, India, 2012. 265-282.

[7] CHANG D, KUMAR A, SANADHYA S. Security analysis of GFN: 8-round distinguisher for 4-branch type-2 GFN[A]. Proceedings of the International Conference on Cryptology in India (INDOCRYPT 2013)[C]. Mumbai, India, 2013. 136-148.

[8] LAI X J. Higher order derivatives and differential cryptanalysis[A]. Proceeding of the Symposium on Communication, Coding and Cryptography [C]. Monte-Verita, Ascona, Switzerland, 1994. 10-13.

[9] KNUDSEN L R, WAGNER D. Integral cryptanalysis[A]. Proceedings of the Fast Software Encryption(FSE 2002)[C]. Leuven, Belgium, 2002. 112-127.

[10] DAEMEN J, KNUDSEN L, RIJMEN V. The block cipher square[A]. Proceedings of the Fast Software Encryption(FSE 1997)[C]. Haifa, Israel, 1997. 149-165.

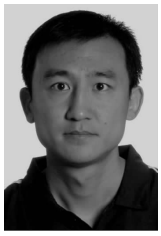
[11] FERGUSON N, KELSEY J, LUCKS S, *et al*. Improved cryptanalysis of Rijndael[A]. Proceedings of the Fast Software Encryption(FSE 2000)[C]. New York, NY, USA, 2001. 213-230.

[12] GALICE S, MINIER M. Improving integral attacks against Rijndael-256 up to 9 rounds[A]. Proceedings of the Progress in Cryptology(AFRICACRYPT 2008)[C]. Casablanca, Morocco, 2008. 1-15.

[13] 董乐, 吴文玲, 吴双等. 构造零和区分器的新方法[J]. 通信学报, 2012, 33(11): 91-99.
DONG L, WU W L, WU S, *et al*.Novel method of constructing the zero-sum distinguishers[J]. Journal on Communications, 2012, 33(11): 91-99.

[14] BOURA C, CANTEAUT A, CANNIERE C. Higher-order differential properties of Keccak and Luffa[A]. Proceedings of the Fast Software Encryption(FSE 2011)[C]. Lyngby, Denmark, 2011. 252-269.

作者简介：



董乐（1980-），男，河南新乡人，博士，河南师范大学副教授、硕士生导师，主要研究方向为杂凑函数和分组密码的分析。

杜蛟（1978-），男，湖北英山人，博士，河南师范大学副教授、硕士生导师，主要研究方向为布尔函数的设计与分析。

吴文玲（1966-），女，陕西蒲城人，博士，中国科学院研究员、博士生导师，主要研究方向为私钥密码体制的设计与分析。