轻量级分组密码PUFFIN的差分故障攻击

袁庆军[①②] 张勋成*[①] 高 杨[①] 王永娟[①②]
[①](战略支援部队信息工程大学 郑州 450001)
[②](河南省网络密码技术重点实验室 郑州 450001)

摘 要：基于代换–置换网络结构的轻量级分组密码算法PUFFIN在资源受限的硬件环境中使用较广泛，差分故障攻击是针对硬件密码算法较为有效的攻击手段。该文针对PUFFIN算法，改进多比特故障模型，通过构建输出差分和可能输入值之间的关系，注入5次故障即可确定单个S盒唯一输入值；在最后一轮加密过程中注入10次故障，成功恢复轮密钥的概率为78.64%，进而可恢复初始密钥。

关键词：差分故障攻击；代换–置换网络结构；PUFFIN算法
中图分类号：TN918.4; TP309.7 **文献标识码**：A **文章编号**：1009-5896(2020)06-1519-07
DOI: 10.11999/JEIT190506

Differential Fault Attack on the Lightweight Block Cipher PUFFIN

YUAN Qingjun[①②] ZHANG Xuncheng[①] GAO Yang[①] WANG Yongjuan[①②]
[①](*PLA Strategic Support Force Information Engineering University*, *Zhengzhou* 450001, *China*)
[②](*Henan Key Laboratory of Network Cryptography Technology*, *Zhengzhou* 450001, *China*)

Abstract: The lightweight block cipher algorithm PUFFIN based on substitution-permutation network structure is widely used in resource-constrained hardware environments. Differential fault attack is a more effective attack method for hardware cryptographic algorithms. The multi-bit fault model for PUFFIN algorithm is improved. By constructing the relationship between the output difference and the possible input values, the single input value of a single S-box can be determined by injecting 5 faults. The probability of successfully recovering the round key is 78.64%, and the initial key can be recovered.

Key words: Differential fault attack; Substitution-permutation network structure; PUFFIN algorithm

1 引言

近年来物联网技术飞速发展，为保证信息传输的安全性，嵌入在物联网上的密码芯片中运行的轻量级分组密码越来越受到研究人员的关注。PUFFIN算法在2008年由文献[1]提出，是一种轻量级分组密码，采用代换–置换网络(Substitution-Permutation Network, SPN)结构，其分组长度为64 bit，密钥长度为128 bit，迭代32轮。非线性层由16个相同的4×4的S盒并置而成，线性层则为64 bit置换，硬件实现时占用芯片面积较小，适用于微型计算设备。目前对PUFFIN的分析方法主要有差分分析[2]、线性分析[3]和积分攻击[4]。文献[1]中，设计者针对PUFFIN算法抵抗差分分析、线性分析和相关密钥攻击[5]的能力进行了研究，并且分析了算法的弱密钥。文献[6]主要介绍了PUFFIN算法的线性特征，并对其进行了线性攻击；文献[7]首次对PUFFIN类的SPN密码算法抵抗积分攻击的能力进行了研究。

差分故障攻击是将差分分析和故障攻击相结合提出的一种基于硬件的密码攻击技术。攻击原理是在密码算法加密过程某一轮注入故障，制造明文差分，利用得到的故障密文和故障动作，结合差分方程得到轮密钥可能值，通过多次注入故障可以快速缩小密钥空间，实现密钥破解[8]。故障攻击是算法层面上的攻击方法，其实施基础是算法的特殊结构[9]，利用故障注入点之后的故障局部数据流与正常局部数据流之间的差异进行密钥恢复。差分故障攻击对PRESENT[10], MIBS[11], KLEIN[12], SIMON[13], LBlock[14]等算法具有较好的攻击结果。在差分故障攻击中，设立合适的故障模型发挥着至关重要的作用。为了实施故障攻击，攻击者需要考虑许多因素，比如故障时机、故障位置、故障动作

收稿日期：2019-07-05；改回日期：2020-01-23；网络出版：2020-02-25
*通信作者： 张勋成 zhangxunc1122@gmail.com
基金项目：国家自然科学基金(61602512)，河南省网络密码技术重点实验室开放基金(LNCT2019-S02)
Foundation Items: The National Natural Science Foundation of China(61602512), Henan Key Laboratory of Network Cryptography Technology(LNCT2019-S02)

和故障效果等，通常故障注入轮数越高，攻击效率越高，但同时占用资源较大。因此，综合资源和效率两方面考虑，研究者们更多地着眼于通过优化故障注入位置或者选取更合理的故障时机，从而尽可能地减少故障注入次数，以提高攻击的效率和成功率。

本文针对PUFFIN算法，采用改进的多比特故障模型，通过构建输出差分和可能输入值之间的关系，理论上只需注入5次故障即可确定单个S盒唯一输入值；在最后一轮加密过程中注入10次故障，能够以78.64%的概率成功恢复轮密钥信息，从而进行初始密钥恢复。

2 PUFFIN算法简介

PUFFIN算法是一种SPN型结构的轻量级分组密码算法，为充分保证算法的安全性，PUFFIN算法的密钥长度固定为128 bit。在加密和解密时，由密钥扩展方案通过查表进行置换和设定的位置反转，生成33个子密钥。其分组长度为64 bit，迭代轮数为32轮。

非线性层由16个相同的4×4的S盒并置而成，线性层则为64 bit置换。64 bit明文(中间状态，轮密钥及密文)$p_0, p_1, \cdots, p_{63}$排列成一个4行16列的2维数组形式。

轮函数由以下3个部分复合而成，分别是非线性层(substitution)、密钥加变换层(add round key)和置换层(permutation)。

(1) 非线性层γ由16个相同的4×4的S盒并置而成，S盒映射见表1；

(2) 密钥加变换层σ：将64 bit的轮密钥K_i与64 bit状态进行异或运算；

(3) 置换层P64：进行64 bit的一个置换，记作P64，该置换以表2的置换规则进行，以保证同一个S盒的输出所有bit在下一轮中进入不同的S盒。此外，该置换是可逆的；因此，算法一轮加密过程可用$\mathrm{P64}\circ\sigma_{k_r}\circ\gamma$来表示。在PUFFIN算法的加密之前，首先进行密钥白化和一个P64置换，然后进行32轮的轮函数迭代。因此PUFFIN函数的加密过程可表示为：$\prod_{r=1}^{32}(\mathrm{P64}\circ\sigma_{k_r}\circ\gamma)\circ\mathrm{P64}\circ\sigma_{k_0}$；

(4) PUFFIN的密钥扩展方案：PUFFIN算法的密钥扩展方案是基于线性置换的，128 bit的主密钥通过密钥扩展算法生成33个轮密钥，如表3所示。

表 1 S盒映射(16进制表示)

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	D	7	3	2	9	A	C	1	F	4	5	E	6	0	B	8

表 2 P64置换

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	13	2	60	50	51	27	10	36
1	25	7	32	61	1	49	47	19
2	34	53	16	22	57	20	48	41
3	9	52	6	31	62	30	28	11
4	37	17	58	8	33	44	46	59
5	24	55	63	38	56	39	15	23
6	14	4	5	26	18	54	42	45
7	21	35	40	3	12	29	43	64

3 PUFFIN算法的差分故障攻击

3.1 攻击模型

通常对于轻量级分组密码，其基本单元均为半字节，因此前人采用的一般是半字节故障模型，但PUFFIN算法采用SPN结构，运算过程中每个半字节均通过S盒，且在S盒操作之后进行全轮置换操作，因此前人根据算法结构求出故障值的方法，在实际场景中存在许多局限性，现实应用价值较低。因此，本文建立多比特故障模型对PUFFIN算法进行分析。

比特级故障注入比半字节级故障更精确。它需要微电子工程提供大量技术支持，许多研究人员已经分析并证明了比特级故障注入的可行性。2010年，Agoyan等人[15]使用8 bit, 0.35 m微控制器进行了实际实验，该控制器可通过激光产生随机单比特中间值翻转；Ayatolahi等人[16]从寄存器的灵敏度问题，对比了生成单比特故障注入和多比特故障注入之间区别；Sangchoolie等人[17]的研究表明，在大多数情况下，单比特故障产生的静默数据损坏的百分比高于多比特故障。也就是说，多比特故障在一定程度上比单位故障更容易实现。

近年来，侧信道分析与测评实验室普遍采用波长为1100 nm以下的二极管激光，光斑直径可精确

表 3 PUFFIN密钥扩展算法

输入：初始密钥K。

输出：轮密钥$\mathrm{RK}_i, i \in 1, 2, \cdots, 33$。

(1) 依据轮密钥选择表，从K提取64 bit的第1轮轮密钥RK_1, 轮密钥选择表见文献[1]；

(2) for i in range(2～33), do

(3) 依据密钥状态置换表，更新主密钥K，密钥状态置换表见文献[1]；

(4) if $i \neq (2, 5, 6, 8)$, do

(5) 翻转主密钥K第0, 1, 2, 4个比特；

(6) end

(7) 依据轮密钥选择表，从K提取64 bit的第i轮轮密钥RK_i；

(8) end

(9) return RK_i.

控制为μm级，极大地提升了故障注入的精度。激光照射芯片，使之产生数据位翻转是一个概率性事件，此外，芯片设计中采用的故障防护措施，也降低了故障发生的概率。在故障攻击实验中，攻击者往往在短时间内攻击目标芯片成千上万次，并从输出的错误密文中筛选适合的错误密文进行下一步分析。因此，即使攻击者使用μm级激光发射器攻击主流的nm级芯片，仍然可以得到一定数量的符合条件的密文。以本文所提攻击方法为例，仅需筛选出10组满足条件的密文，就能以78.64%概率恢复轮密钥。此外，业界普遍采用多源激光进行故障生成，即采用多个激光光源同时诱发算法故障，因此本文分析所需的多比特故障的实现难度较小。

随着故障注入设备精度的提高，符合多比特的故障模型的错误密文生成概率也在提高。相比于基于字节、基于半字节的差分故障分析方法，基于比特模型和多比特模型的差分故障方法可以在故障注入次数较少、差分表规模较低的情况下恢复密钥。在现实攻击过程中，仅需基于原有基于字节的差分故障攻击系统，在错误密文筛选时以比特级故障为目标进行筛选，并建立基于多比特模型的故障分析模型，即可实现本文提出的故障分析方法。

在此给出攻击条件以及具体假设：

(1) 攻击者完全掌握密码设备，可以在加密过程中任意时刻任意位置注入多比特的随机故障，故障具体值未知；

(2) 攻击者可以反复多次在同一位置重复导入随机故障；

(3) 攻击者可以反复重启密码设备，加密相同的明文和初始密钥。

3.2 攻击步骤

(1) 算法加密：任意选择明文P，用初始密钥K加密，获取正确密文C。

(2) 故障注入：由算法结构以及密钥扩展方案确定故障注入位置。使用相同的明文以及密钥进行加密运算，在最后一轮运算至S盒时，在每个半字节位置分别同时导入1 bit随机故障，并记录错误密文C^*。

(3) 计算S盒输出差分：由正确密文C和错误密文C^*，通过逆P置换得到16个S盒输出差分$\{\beta_1,\beta_2,\cdots,\beta_{16}\}$。

(4) 筛选S盒输入值：

(a) 对步骤(3)中得到的每个输出差分，在输出差分表中查找所有可能的S盒输入值，将其记为密钥候选值集合$A_i,1\le i\le 16$；

(b) 返回步骤(2)，重新注入故障并计算输出差分，得到密钥候选值集合$B_i,1\le i\le 16$，取A_i与B_i的交集。若存在i，使得$A_i\cap B_i$不唯一，令$A_i=A_i\cap B_i$，再次执行(b)。最终得到的唯一$A_i\cap B_i$即为S盒第i个半字节输入值$m_i,1\le i\le 16$。

(5) 恢复轮密钥：由步骤(4)得到的S盒输入值，结合SPN结构的特点可以将最后一轮轮密钥表示为$\mathrm{RK}=P^{-}\mathrm{Layer}(S(m))\oplus C$。

(6) 恢复初始主密钥K：将已经求出的轮密钥代入密钥扩展逆推，经过线性置换最终可得到初始密钥K。

3.3 S盒差分特性

PUFFIN算法非线性变换的复杂度取决于S盒，因此研究S盒的差分分布情况是极为关键的。在进行S盒代换时，若S盒输入值a未知，导入随机的故障值(输入差分)f，得到故障差分(输出差分)f'。它们之间满足差分关系$S[a]\oplus S[a\oplus f]=f'$。差分故障攻击的核心步骤之一就是该差分方程的求解，之前研究者们采用的方法是对S盒输入值a进行遍历穷举。为了缩减穷举量以提高攻击效率，考虑针对算法S盒列出其差分分布表，将穷举输入值转化为查表操作，能快速高效求取S盒输入值a。下面给出PUFFIN算法的S盒差分分布表，如表4所示。

观察表4可知，当S盒输入差分f一定的情况下，对于每一个可能的输出差分f'，其对应的输入a可看成一个集合$\{a_1,a_2,\cdots,a_n\}$。记为$\{f,f'\}=\{a|\,S[a]\oplus S[a\oplus f]=f',a\in F_2^n\}$。

因此，本文可以得到$\{f,f'\}$如下性质：

性质1　对算法S盒注入故障值f，对于不同的输出差分f'_1,f'_2，对应输入值可能不交，即$\{f,f'_1\}\cap\{f,f'_2\}=\phi$。

性质2　在输入a一定的情况下，对于两个待定不同的输入差分f_1,f_2，一定存在f'_1,f'_2，使得$a\in\{f,f'_1\}\cap\{f,f'_2\}$。

因此，通过建立$<a,f,f'>$的对应关系，可以快速直观地缩小输入值取值空间，通过查表，对可能输入值集合取交集即可快速确定唯一可能输入值，进而恢复轮密钥信息和初始主密钥。

4　差分故障攻击的改进

在上一节中，针对PUFFIN算法采取多比特故障模型，建立输入差分、输出差分和可能输入值的3元关系，通过S盒差分分布表的查找，可以快速确定S盒唯一输入值，从而进行密钥恢复。但由于需要同时在16个S盒注入故障，S盒差分分布表规模较大，筛选交集效率较低，需要故障注入次数较多，因此本文需要减小故障值f的取值范围，以便求解

表 4 PUFFIN算法S盒差分分布表

f		输入差分固定情况下输出差分与输入值的对应关系							
1	f'	1	3	6	A	B	D		
	a	2,3	4,5,E,F	C,D	0,1	8,9,A,B	6,7		
2	f'	5	8	A	B	D	E		
	a	1,3,4,6	D,F	8,9,A,B	5,7	C,E	0,2		
3	f'	1	4	6	8	B	E	F	
	a	8,9,A,B	1,2	5,6	4,7	D,E	C,F	0,3	
4	f'	3	4	6	9	D	E	F	
	a	3,7	0,4,9,D	B,F	8,C	1,5	A,E	2,6	
5	f'	2	5	7	D	E	F		
	a	2,7,9,C	B,E	0,5	A,F	1,3,4,6	8,D		
6	f'	1	3	4	6	8	A	C	E
	a	0,6	A,C	8,E	1,7	3,5	2,4	9,F	B,D
7	f'	5	7	8	9	B	C	F	
	a	A,D	8,F	B,C	2,5	1,3,4,6	0,7	9,E	
8	f'	2	3	6	7	9	A	C	F
	a	0,8	1,9	2,A	6,E	7,F	5,D	3,B	4,C
9	f'	4	7	8	9	A	C	D	
	a	6,F	3,A	1,8	0,4,9,D	7,E	5,C	2,B	
A	f'	1	2	6	8	9	A	C	
	a	7,D	4,5,E,F	3,9	0,A	1,B	6,C	2,8	
B	f'	1	2	3	7	C	D		
	a	4,5,E,F	1,A	0,B	2,7,9,C	6,D	3,8		
C	f'	6	7	8	9	A	B	E	F
	a	4,8	1,D	2,E	6,A	3,F	0,C	5,9	7,B
D	f'	1	2	4	5	9	B	D	
	a	1,C	6,B	7,A	5,8	3,E	2,F	0,4,9,D	
E	f'	2	3	4	5	6	C	F	
	a	3,D	6,8	5,B	2,7,9,C	0,E	4,A	1,F	
F	f'	3	4	5	7	8	C	E	F
	a	2,D	3,C	0,F	4,B	6,9	1,E	7,8	5,A

差分方程。在多比特故障模型的基础上，将注入故障值限定在某一个范围内，从而减小S盒差分分布表规模，能够更加快速地求解差分方程。

进行攻击实践时，在PUFFIN算法运算的最后一轮的16个S盒处同时注入单比特故障，这些故障仅导致S盒输入半字节中的单个比特翻转。将注入故障值的范围限定在集合{0×1, 0×2, 0×4, 0×8}中，大大缩减了查表的复杂度。进一步列出PUFFIN算法S盒的局部差分分布表，如表5所示。

观察表5可知，在多比特故障注入模型假设下，得到输出差分f'后可以将输入值缩小到较小的范围。另一方面，由于前后两次在同一个半字节处注入故障，而该位置S盒输入值保持不变，因此连续注入两次故障后得到两个输出差分$\{f'_1, f'_2\}$所对应的输入值相同。将攻击模型简化为$\{f', a\}$的2元筛选模型。为了便于筛选S盒输入值，将表5转化为表6的形式。

若注入两次故障后，得到的输出差分分别为6和D，通过查找输出差分表，取两个集合{2, A, B, C, D, F}和{1, 5, 6, 7, C, E}的交集{C}，那么可以得到该S盒的唯一输入值为C。原本需要更多次注入故障值才能确定的唯一交集，现在只要两次故障注入就可以实现。不仅减少了故障注入次数，同时降低了筛选S盒输入值的复杂度，攻击效率得到了明显提升。经过大量实验证明，经过5次故障注入即可确定唯一的S盒输入值。

表 5　PUFFIN算法S盒局部差分分布表

f		输入差分固定情况下输出差分与输入值的对应关系							
1	f'	1	3	6	A	B	D		
	a	2,3	4,5,E,F	C,D	0,1	8,9,A,B	6,7		
2	f'	5	8	A	B	D	E		
	a	1,3,4,6	D,F	8,9,A,B	5,7	C,E	0,2		
4	f'	3	4	6	9	D	E	F	
	a	3,7	0,4,9,D	B,F	8,C	1,5	A,E	2,6	
8	f'	2	3	6	7	9	A	C	F
	a	0,8	1,9	2,A	6,E	7,F	5,D	3,B	4,C

表 6　PUFFIN输出差分表

输出差分f'	可能的输入值集合
1	2, 3
2	0, 8
3	1, 3, 4, 5, 7, 9, E, F
4	0,4,9,D
5	1, 3, 4, 6
6	2, A, B, C, D, F
7	6,E
8	D, F
9	7, 8, C, F
A	0, 1, 5, 8, 9, A, B, D
B	5, 7, 8, 9, A, B
C	3, B
D	1, 5, 6, 7, C, E
E	0, 2, A, E
F	2, 4, 6, C

重复上述操作，通过尽量少的故障注入次数得到一轮16个S盒的唯一输入值，即可与逆置换的密文进行异或操作得到轮密钥信息。接着仿照上述做法恢复上一轮密钥，再由密钥扩展方案恢复出初始密钥。将此方法扩展到不同SPN结构分组密码算法和部分Feistel结构的轻量级分组密码算法，均取得了良好的攻击效果。

5　差分故障攻击复杂度分析

单轮故障注入次数是衡量差分故障攻击效果的关键指标，故用不同故障注入次数下的轮密钥恢复概率刻画差分故障攻击复杂度。

由上文的PUFFIN算法的改进差分故障攻击方案可知，当注入一次故障后，存在交集不是唯一值的情况。由表4知，当输出差分为3时，相应的S盒输入值集合为$\{1,3,4,5,7,9,\mathrm{E},\mathrm{F}\}$；当输出差分为A时，S盒输入值集合为$\{0,1,5,8,9,\mathrm{A},\mathrm{B},\mathrm{D}\}$。上述两集合的交集为$\{1,5,9\}$，即S盒的半字节输入值是这4个值之一。因此，必须注入更多次故障继续筛选出唯一的S盒输入值。记注入L次故障后可筛选出唯一输入值的输出差分组数目为N_L，无法筛选出唯一输入值的输出差分组数目为N'_L，成功筛选出唯一输入值的概率为P。通过软件模拟实验分析，PUFFIN算法注入10次以内单个S盒输入值恢复情况如表7所示。

由于PUFFIN算法中单轮16个半字节相互独立且应用于同一个S盒，因此由乘法原理知，轮密钥恢复概率可以通过单个半字节密钥恢复概率计算得出，易知注入L次故障后轮密钥恢复概率为：$P_L=\left(\dfrac{N_L}{N_L+N'_L}\right)^{16}$。

进一步，可以得到定理。

定理　在多比特故障注入模型下，注入L次故障后轮密钥恢复概率为$P_L=\left(\dfrac{N_L}{N_L+N'_L}\right)^{M}$。

其中M为单次故障比特注入数(一般为单轮参与运算S盒数量)。

对于SPN结构的分组密码而言，参与一轮运算的轮密钥为16个半字节，故一般情况下M=16；而Feistel结构中一轮运算有8个nibble参与运算，即M=8。由上式可以看出Feistel结构的轮密钥恢复概率明显高于SPN结构，因此在多比特故障模型

表 7　PUFFIN算法10次故障注入以内单个S盒输入值恢复情况

L	2	3	4	5	6	7	8	9	10
N_L	76	564	2932	13380	57556	240324	987412	4019460	20389796
N'_L	63	183	493	1335	3663	10263	29295	84855	308491
P	0.55	0.76	0.86	0.91	0.94	0.96	0.97	0.98	0.99

下，Feistel结构密码算法整体上较SPN结构而言更易遭受差分故障攻击。因此，越来越多的密码芯片更倾向于选择SPN结构的轻量级分组密码算法，从侧面也说明了本文针对典型SPN结构的PUFFIN算法差分故障攻击研究的重要性。

本文以基于多比特模型的故障分析方法与文献[18]采用的半字节故障模型，对PUFFIN算法进行了差分故障分析，在注入10次故障内，其轮密钥恢复概率如图1所示。

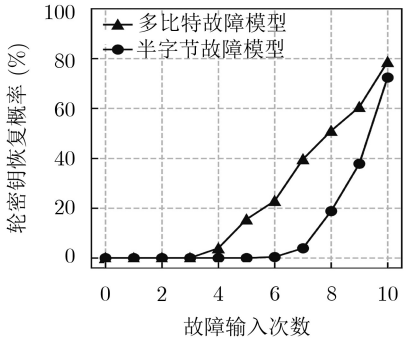

图 1 PUFFIN算法轮密钥恢复概率

由图1可知，在多比特故障模型下，获取的故障注入次数较少时，相比于半字节故障模型，具有较高的恢复效率。针对PUFFIN算法，注入10次故障即可以78.64%的概率恢复最后一轮轮密钥信息，进而恢复主密钥。

6 仿真实验下的攻击过程

6.1 实验环境

硬件配置为一台PC机(CPU为Intel Core i7-6700HQ 2.60 GHz，操作系统为64位，内存为12 GB)，编程环境为Microsoft Visual Studio 2015平台下的Visual C++语言。

6.2 攻击过程

本节选取明文：01 23 45 67 89 ab cd ef，密钥：01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10。

(1) 首先进行1次正确加密，得密文：3d b0 0f 3e e3 51 03 cf。

(2) 在最后一轮每个S盒变换之前注入故障：88 41 22 41 81 81 44 42，得到第1组输出差分：2c 43 a5 93 aa 2b 49 65。

(3) 重复步骤(2)，再次注入故障，得到另外几组输出差分。

故障值：21 21 18 28 82 12 84 21，对应输出差分：eb a3 bf af a5 aa 39 83。

故障值：41 44 84 81 88 41 22 41，对应输出差分：4b 4e c4 23 63 4b aa 63。

故障值：24 82 12 81 42 44 14 18，对应输出差分：e6 3d b5 23 45 44 b9 3f。

(4) 结合表6确定出S盒未加故障时的输入：每一个未知的输入候选值只有一个交集，这样就唯一确定出S盒的输入为：0b 9e b4 84 d1 09 98 f4。

(5) 将S盒输入与密文逆置换后的结果进行异或运算，得到最后一轮轮密钥RK^{32}：87 58 67 c4 e6 ae 25 a5。

(6) 将故障注入位置提高到上一轮，重复上述步骤(2)—步骤(5)，得到第31轮轮密钥RK^{31}：9c ca b6 3f 87 58 67 c4。同样地，得到第30轮轮密钥RK^{30}：73 0e 6a 51 9c ca b6 3f。

(7) 结合PUFFIN算法的密钥扩展方案和已知的轮密钥信息，推出初始密钥K：01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10。

通过以上计算机仿真实验具体攻击过程可以看出，在算法的最后一轮注入4次故障即可确定S盒唯一输入值，验证了第5节的结论。

7 结束语

本文分析轻量级分组密码PUFFIN算法的S盒差分传播特性，通过建立<输出差分、可能输入值>的2元对应关系表，利用不同故障条件下故障差分对应的输入值集合交集唯一的特性，针对PUFFIN算法的最后一轮运算，进行故障注入，理论上至多进行5次故障注入即可唯一确定S盒输入值，注入10次故障能够以78.64%的概率恢复最后一轮轮密钥信息。最后结合密钥扩展方案，推导出主密钥。该方法对其他SPN结构密码算法同样适用。下一步的研究将力求减小故障注入次数，提升攻击效率和可行性，同时关注PUFFIN算法抗差分故障攻击的研究。

参 考 文 献

[1] CHENG Huiju, HEYS H M, and WANG Cheng. Puffin: A novel compact block cipher targeted to embedded digital systems[C]. The 11th EUROMICRO Conference on Digital System Design Architectures, Methods and Tools, Parma, 2008: 383–390. doi: 10.1109/DSD.2008.34.

[2] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. *Journal of Cryptology*, 1991, 4(1): 3–72. doi: 10.1007/bf00630563.

[3] MATSUI M. Linear Cryptanalysis Method for DES Cipher[M]. HELLESETH T. Advances in Cryptology - EUROCRYPT '93. Berlin: Springer, 1994: 386-397. doi: 10.1007/3-540-48285-7_33.

[4] BIHAM E. New types of cryptanalytic attacks using related

keys[C]. The Workshop on the Theory and Application of Cryptographic Techniques, Berlin, Germany, 1994: 398–409.

[5] MOORE J H and SIMMONS G J. Cycle structure of the DES for keys having palindromic (or Antipalindromic) sequences of round keys[J]. *IEEE Transactions on Software Engineering*, 1987, 13(2): 262–273. doi: 10.1109/TSE.1987.233150.

[6] LEANDER G. On linear hulls, statistical saturation attacks, PRESENT and a cryptanalysis of PUFFIN[C]. The 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, ESTOnia, 2011: 303–322. doi: 10.1007/978-3-642-20465-4_18.

[7] 魏悦川, 孙兵, 李超. 一种PUFFIN类SPN型分组密码的积分攻击[J]. 国防科技大学学报, 2010, 32(3): 139–143, 148. doi: 10.3969/j.issn.1001-2486.2010.03.026.

WEI Yuechuan, SUN Bing, and LI Chao. An integral attack on PUFFIN and PUFFIN-like SPN Cipher[J]. *Journal of National University of Defense Technology*, 2010, 32(3): 139–143, 148. doi: 10.3969/j.issn.1001-2486.2010.03.026.

[8] 王永娟, 张诗怡, 王涛, 等. 对MIBS分组密码的差分故障攻击[J]. 电子科技大学学报, 2018, 47(4): 601–605. doi: 10.3969/j.issn.1001-0548.2018.04.020.

WANG Yongjuan, ZHANG Shiyi, WANG Tao, *et al*. Differential fault attack on block cipher MIBS[J]. *Journal of University of Electronic Science and Technology of China*, 2018, 47(4): 601–605. doi: 10.3969/j.issn.1001-0548.2018.04.020.

[9] 欧庆于, 罗芳, 叶伟伟, 等. 分组密码算法抗故障攻击能力度量方法研究[J]. 电子与信息学报, 2017, 39(5): 1266–1270. doi: 10.11999/JEIT160548.

OU Qingyu, LUO Fang, YE Weiwei, *et al*. Metric for Defences against fault attacks of block ciphers[J]. *Journal of Electronics & Information Technology*, 2017, 39(5): 1266–1270. doi: 10.11999/JEIT160548.

[10] 李卷孺, 谷大武. PRESENT算法的差分故障攻击[C]. 中国密码学会2009年会论文集, 广州, 2009: 1–13.

LI Juanru and GU Dawu. Differential fault attack on PRESENT[C]. inaCrypt2009, Guangzhou, China, 2009: 1–13.

[11] GAO Yang, WANG Yongjuan, YUAN Qingjun, *et al*. Probabilistic analysis of differential fault attack on MIBS[J]. *IEICE Transactions on Information and Systems*, 2019, 102(2): 299–306. doi: 10.1587/transinf.2018EDP7168.

[12] GRUBER M and SELMKE B. Differential fault attacks on KLEIN[C]. The 10th International Workshop on Constructive Side-Channel Analysis and Secure Design, Darmstadt, Germany, 2019: 80–95. doi: 10.1007/978-3-030-16350-1_6.

[13] ANAND R, SIDDHANTI A, MAITRA S, *et al*. Differential fault attack on SIMON with very few faults[C]. Progress in Cryptology-INDOCRYPT 2018: The 19th International Conference on Cryptology in India, New Delhi, India, 2018: 107–119. doi: 10.1007/978-3-030-05378-9_6.

[14] GAO Yang, WANG Yongjuan, YUAN Qingjun, *et al*. Methods of differential fault attack on LBlock with analysis of probability[C]. The 3rd IEEE Advanced Information Technology, Electronic and Automation Control Conference, Chongqing, China, 2018: 474–479. doi: 10.1109/IAEAC.2018.8577744.

[15] AGOYAN M, DUTERTRE J M, MIRBAHA A P, *et al*. Single-bit DFA using multiple-byte laser fault injection[C]. 2010 IEEE International Conference on Technologies for Homeland Security, Waltham, USA, 2010: 113–119. doi: 10.1109/THS.2010.5655079.

[16] AYATOLAHI F, SANGCHOOLIE B, JOHANSSON R, *et al*. A Study of the Impact of Single Bit-flip and Double Bit-flip Errors on Program Execution[M]. BITSCH F, GUIOCHET J, and KAÂNICHE M. Computer Safety, Reliability, and Security. Berlin: Springer, 2013: 265–276. doi: 10.1007/978-3-642-40793-2_24.

[17] SANGCHOOLIE B, PATTABIRAMAN K, and KARLSSON J. One bit is (not) enough: An empirical study of the impact of single and multiple bit-flip errors[C]. The 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Denver, USA, 2017: 97–108.

[18] 高杨, 王永娟, 王磊, 等. 轻量级分组密码算法TWINE差分故障攻击的改进[J]. 通信学报, 2017, 38(S2): 178–184. doi: 10.11959/j.issn.1000-436x.2017274.

GAO Yang, WANG Yongjuan, WANG Lei, *et al*. Improvement Differential fault attack on TWINE[J]. *Journal on Communications*, 2017, 38(S2): 178–184. doi: 10.11959/j.issn.1000-436x.2017274.

袁庆军：男，1993年生，讲师，研究方向为侧信道分析.

张勋成：男，1997年生，实习研究员，研究方向为侧信道分析.

高　杨：男，1994年生，研究方向为密码算法设计与分析.

王永娟：女，1982年生，研究员，研究方向为侧信道分析与密码系统安全.