doi:10.11959/j.issn.1000-436x.2016256

轻量级分组密码 Klein 的差分故障攻击

王永娟[1]，任泉宇[2]，张诗怡[1]
（1. 洛阳外国语学院语言工程系，河南 洛阳 471003；2. 解放军 78007 部队，四川 成都 610041）

摘 要：Klein 算法是一个基于 SP 型结构的轻量级分组密码算法，具有执行效率高、能耗低等特点。通过分析算法 S 盒差分传播途径，发现在相同输入、不同差分条件下，输出差分对应中间状态集合交集元素唯一，提出差分故障攻击方案。通过在算法最后一轮注入 2 次不同故障，可恢复出 Klein 算法的全部密钥，复杂度可忽略不计。此方法可推广到基于 SP 结构和 Feistel 结构分组密码算法。

关键词：分组密码；S 盒；差分传播；差分故障
中图分类号：TN918.1 **文献标识码**：A

Differential fault attack on lightweight block cipher Klein

WANG Yong-juan[1], REN Quan-yu[2], ZHANG Shi-yi[1]
(1. Department of Language Engineering, Luoyang Foreign Language College, Luoyang 471003, China;
2. PLA 78007 Troops, Chengdu 610041, China)

Abstract: As a lightweight block cipher algorithm based on SP structure, Klien has the characteristics of high efficiency and low energy consumption. By analyzing the S-boxes differential propagation path, it was found that under the condition of same input and different difference, the intersection elements were unique, which fall in the intermediate state set corresponds to output difference, and a differential fault attack scheme was proposed. By injecting two different faults in the last round of the algorithm, all the keys of the Klein algorithm can be recovered, and the complexity is negligible. This method can be promoted to other block cipher algorithms based on SP structure and Feistel structure.

Key words: block cipher, S-box, differential transmission, differential fault

1 引言

随着物联网技术的日趋成熟，RFID 芯片和无线传感网络等越来越深入到人们的日常生活中，随之而来的安全问题也成为信息安全领域重要的研究课题。而诸如银行卡、门禁卡、公交卡等便携式密码设备计算能力有限。基于此背景，密码学者提出轻量级分组密码算法，它为便携式密码设备的安全技术开辟了新的途径。鉴于轻量级分组密码算法使用在资源受限的环境，这类算法力求寻找安全性和执行效率的最佳平衡点，Klein 算法就是轻量级密码算法中的佼佼者，它是一个基于 SP 型结构的轻量级分组密码算法，借鉴 AES 的设计思想，实现效率和能耗方面做了诸多改进，且其面向软件的设计思想使其更便于维护，应用范围更广。

密码故障分析是在 1996 年由 Boneh 等[1]提出的，并对基于 CRT 算法实现的 RSA 签名密钥进行了相关分析。1997 年，Biham 和 Shamir 结合该方法和差分分析方法分析了 DES 算法[2]，提出差分故障分析方法，差分故障攻击源于差分密码分析方法，本质上是将秘密方案看做一个数学函数，通过人工导入的故障差分，得到输出密文与加密密钥之间的联系，重复进行故障导入，最终得到密钥信息，实现对密码的破译。随着故障注入技术的不断提高，故障差分攻击被视作对分组密码算法最有效的现实威胁之一。2008 年，李琳等[3]用差分故障分析方法对 KeeLoq 算法和 SHACAL-1 算法进行攻击，结果显示对 KeeLoq 算法，平均诱导 11 个错误即可恢复 1 bit 的密钥；对 SHACAL-1 算法，平均诱导 6 个错误可恢复 32 bit 的密钥。2009 年，李卷孺等[4]采用

收稿日期：2016-08-31

面向字节的随机故障模型，在 PRESENT 算法的加密过程中任意位置导入故障，通过差分故障特性识别需要的故障密文，平均 175~300 次导入故障可恢复 PRESENT 算法的 80 bit 原始密钥。2011 年，文献[5]在 AES-256 算法执行过程中注入 2 对错误字节，通过差分分析，以 $O(2^{32})$ 的时间复杂度恢复密钥，并将密钥穷举空间降为 2^{16}。2012 年，范伟杰等[6]采用单字节级的未知故障值的差分故障模型，在 HIGHT 算法倒数第 3 轮和倒数第 4 轮注入故障，模拟实验结果显示采用 32 次故障诱导便可恢复 HIGHT 算法密钥，计算复杂度约为 2^{56}。Zhao 等[7]在 Lblock 算法第 25 轮和 31 轮之间注入比特错误，通过差分故障分析可以恢复最后 3 轮轮密钥，然后通过密钥扩展算法恢复主密钥。Jeong 等[8]在 LED-64 算法第 30 轮寄存器中随机注入 4 bit 故障，通过差分故障分析可把密钥穷举量降为 2^8。

本文对 Klein 算法进行差分故障分析，以 Klein-64 为目标，利用算法 S 盒在不同故障条件下输出差分不均匀性，发现在输入已定的情况下，对于 2 个特定的输入差分，输入值集合的交集唯一。因此，仅在算法最后一轮注入 2 次不同故障，即可成功实施差分故障攻击，攻击复杂度极低。并且该方法对基于 Feistel 结构的分组密码算法同样有效。

2 预备知识

2.1 Klein 算法

Klein 算法[9]是中国学者龚征在 RFIDSEC 2011 会议上提出的轻型分组密码。其具有执行效率更高、计算资源消耗更少、更适合计算资源受限环境（如物联网）的优点。算法采用 64 bit 分组，支持 64/80/90 bit 3 种密钥长度，分别对应 12/16/20 轮加密，算法整体采用 SP 结构，微观结构上每轮由轮密钥加、S 盒代换、行移位、列混淆顺序组成，末轮进行了白化操作。算法流程如下。

$KEY\rightarrow sk^1$, $Plaintext\rightarrow state$

for i=1 to N:

$AddroundKey(state,sk^i)$;

$SubNibbles(state)$;

$RotateNibbles(state)$;

$MixNibbles(state)$;

$Sk^{i+1}=KeySchedule(sk^i,i)$;

end for

$AddroundKey(state,sk^N+1)\rightarrow ciphertext$

吴文玲等[10]构造出一个 6 轮的截断差分区分器，对 8 轮 Klein 算法进行截断差分攻击，攻击时间复杂度为 $2^{46.8}$，数据复杂度为 2^{32}。文献[11]对 Klein 算法进行代数旁路分析，首先应用代数方法构建 Klein 算法等价布尔方程组，然后经功耗分析获取 Klein 加密操作的汉明重量并表示为布尔方程，最后使用 CryptMinisat 解析器进行密钥求解，在已知明文条件下，1 轮泄露分析即可恢复完整 Klein 密钥；在未知明密文条件下，2 轮泄露分析可成功实施攻击。本文通过分析 S 盒的差分传播特性，发现在输入已定的情况下，对于 2 个特定的输入差分，输入值集合的交集唯一。仅在算法最后一轮注入 2 次不同故障，即可成功实施差分故障攻击，攻击复杂度极低。

2.2 差分故障攻击原理与改进

目前，分组密码算法普遍采用查找 S 盒来提高算法非线性度。基于 SP 结构的分组密码算法大都在密文输出前加上一次白化密钥；显然只要能准确找到 S 盒的输入值，对于 SP 结构算法，将此输入值通过一次正确算法过程，结果与密文异或可得到轮密钥。

差分故障分析主要原理是通过在 S 盒输入处注入故障，利用 S 盒差分分布不均匀性，结合差分方程 $S(a)\oplus S(a\oplus\Delta a)=\Delta S$ 获得 S 盒输入值 a，通过故障差分快速准确地确定 S 盒输入值 a 是差分故障攻击成功的关键因素。李卷儒等[12]提出一种针对特定结构的 SPN 结构分组密码算法的差分故障攻击方法。其基于单字节故障模型，对于具有特定置换层设计的 SPN 结构分组密码算法，仅需要少量的错误密文即可还原其所使用的密钥。

本文在文献[12]基础上，继续分析分组密码算法 S 盒差分传播特性，发现当 S 盒输入差分 Δa 一定的情况下，对于每一个可能的输出差分 ΔS，其对应的输入 a 可看成一个集合 $\{a_1,a_2,\cdots,a_n\}$。每一个二元组<输入差分, 输出差分>确定的输入值集合相互之间交集为空。在输入 a 一定的情况下，对于 2 个特定不同的输入差分，a 一定属于输入差分和某个输出差分二元组确定的输入值集合，且这 2 个输入值集合的交集有且只有一个元素，该元素即为输入 a。以 Klein 算法 S 盒 16 进制表示为例。

由表 1~表 3 可知，当 Klein 算法的 S 盒输入差分为 01 时，其输出差分只有 7 个值，分别为 3、4、

6、8、b、e、f。每个差分值对应 2 或 4 个输入。当 S 盒输入差分为 0f 时，其输出差分只有 8 个值，分别为 1、2、4、7、8、9、c、d，每个差分值对应 2 个输入。每一个二元组<输入差分，输出差分>对应了一个输入集合。可简写为

$$<01,03>=\{0,1,2,3\}$$

$$<01,04>=\{a,b\}\cdots<0f,01>=\{3,c\}$$

$$<0f,02>=\{0,f\}\cdots$$

表 1　Klein 算法 S 盒

a	$S(a)$
0	7
1	4
2	a
3	9
4	1
5	f
6	b
7	0
8	c
9	3
a	2
b	6
c	8
d	e
e	d
f	5

表 2　当输入差分为 01 时输入与输出差分对应关系

输出差分 ΔS	输入 a
3	0,1,2,3
4	a,b
6	c,d
8	e,f
b	6,7
e	4,5
f	8,9

表 3　当输入差分为 0f 时输入与输出差分对应关系

输出差分 ΔS	输入 a
1	3,c
2	0,f
4	2,d
7	4,b
8	6,9
9	1,e
c	7,8
d	5,a

当明文确定以后，在故障注入前，S 盒的输入值都是一定的。2 次注入不同故障，故障差分值不同，但两者对应的输入集合有且只有一个交集，由此可确定出输入。如表 2 和表 3 所示，算法 S 盒输入值为 03，当注入故障为 01 时，输出差分为 03，其对应的候选输入值有 0,1,2,3 这 4 个值；再重新注入故障 0f，输出差分为 01，其对应的候选输入值有 3,c 这 2 个值，将候选输入值取交集以后只有唯一值 3，即为正确输入值，同理可确定其他输入值。同时对于任意 2 个输入差分，其对应的输出差分不完全相同，这样通过观察输出差分可以很大概率确定输入差分的值。改进的差分故障攻击流程如图 1 所示。

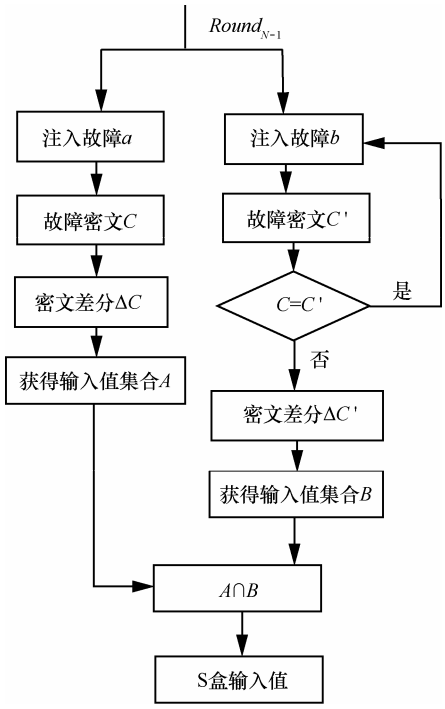

图 1　改进的差分故障攻击流程

由上例可知，在理想情况下，只需在算法最后一轮注入 2 次不同故障，即可快速获得 S 盒输入 a，从而高效准确地恢复出轮密钥，最后通过密钥扩展算法恢复主密钥。将此方法扩展到不同 SP 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。

3 对 Klein 算法的差分故障攻击

通过分析 Klein 算法 S 盒发现：在输入差分为 0x01、0x0f 时，输入 a 与输出差分 ΔS 有对应关系，（如表 2 和表 3 所示）。据此，本文确定了 Klein 算法的差分故障攻击策略如下。

1) 选定一组明文，进行一次正确的加密过程，得到相应的密文 C。

2) 使用相同的明文进行加密，并在加密过程最后一轮引入随机故障，得到一组故障密文 C^*。

3) 把密文差分经逆列混淆运算、逆行移位运算后得到 S 盒输出差分。观察输出差分，确定输入差分。

4) 对应<输入差分，输出差分>二元组确定的输入获得 S 盒输入 a 的一组候选值集合 A。

5) 再次使用相同的明文进行加密，并在加密过程最后一轮引入故障。得到一组故障密文 C^{**}。

6) 把密文差分经逆列混淆运算、逆行移位运算后得到 S 盒输出差分。观察输出差分的值，若与 3)一样，返回 5)；若不一样，继续。

7) 对应<输入差分，输出差分>二元组确定的输入获得 S 盒输入 a 的另一组候选值 B。

8) 取 $A \cap B$ 可以唯一确定 S 盒的输入 a。

9) 得到 a 后经算法 S 盒、行移位、列混淆运算得到 C'，那么最后一轮加密子密钥 key 即为 $C \oplus C'$。

10) 得到 key 后，经密钥扩展算法的逆运算可得到初始密钥。

实验结果为任意选择明文和加密密钥：明文为 01 23 45 67 89 ab cd ef；密钥为 01 23 45 67 89 ab cd ef。

1) 首先进行一次正确加密，得到密文为 6d 6c a6 e8 12 69 cd b5。

2) 在最后一轮引入差分故障 01，得到故障密文为 50 e9 41 da fc b1 a1 8e。

3) 将密文差分通过逆列混淆、逆行移位运算后得到 S 盒的输出差分为 b8 6f 3b 83 3b ee f8 4e。

4) 将差分故障改为 0f，重复 2)和 3)，得到另一组输出差分为 82 4c 2c 24 2c 7d 89 7d。

5) 结合表 1 和表 2 确定出 S 盒未加故障时的输入：每一个位置的输入候选值均只有一个交集，这样就唯一确定出 S 盒的输入为 6f d8 07 f2 07 45 9e b5。

6) 得到中间状态后，进行一轮 S 盒运算、行移位、列混淆。将结果与前文的密文异或后得到最后一轮轮密钥。最后通过逆密钥扩展算法可获得初始加密密钥。

经测试，对基于 SP 结构的算法，如 LED、PRESENT、AES 运用此方法等都取得了良好效果，说明对于 SP 结构的分组密码算法，只要故障注入条件可以达到，该方法将是一种普适高效的攻击方法。

4 结束语

本文通过分析轻量级分组密码 Klein 算法 S 盒差分传播特性，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，提出差分故障分析改进方案。利用本文提出的改进方案，只需在 Klein 算法运行最后一轮注入 2 次不同故障，即可快速准确地恢复了算法全部密钥，并由此可将方法扩展到其他基于 SP 结构的分组密码算法中。

参考文献：

[1] DAN D, DEMILLO R A, LIPTON R J. On the importance of checking cryptographic protocols for faults[C]//Advances in Cryptology –EUROCRYPT 1997, LNCS 1233. 1997: 37-51.

[2] BIHAM E, SHAMIR A. Differential fault analysis of secret key cryptosystems[C]//CRYPTO 1997. Santa Barbara, California, USA, 1997: 513-525.

[3] 李琳, 李瑞林, 谢端强, 等. KeeLoq 和 SHACAL-1 算法的差分故障攻击[J]. 武汉大学学报（理学报）, 2008, 54(5): 507-512.
LI L, LI R L, XIE D Q, et al. Differential fault analysis on keeloq and SHACAL-1[J]. Journal of Wuhan University (Natural Science Edition), 2008, 54(5): 507-512.

[4] 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. 2009: 3-13.
LI J R, GU D W. Differential fault attack on PRESENT block cipher[C]//China Crypt 2009, 2009: 3-13.

[5] ALI S S, MUKHOPADHYAY D. An improved differential fault analysis on AES-256[C]//4th International Conference on Cryptology in Africa. 2011: 332-347.

[6] 范伟杰, 吴文玲, 张蕾. HIGHT 算法的差分故障攻击[J]. 中国科学院研究生院学报, 2012, 29(2): 271-276.
FAN W J, WU W L, ZHANG L. Differential fault analysis on HIGHT[J]. Journal of the Graduate School of the Chinese Academy of Sciences, 2012,29(2): 271-276.

[7] ZHAO L, NISHIDE T, SAKURAI K. Differential fault analysis of full LBlock[C]//Third International Workshop. 2012: 135-150.

[8] JEONG K, LEE C H. Differential fault analysis on block cipher LED-64[C]//FutureTech. 2012: 747-755.

[9] ZHENG G, NIKOVA S, LAW Y W.KLEIN: a new family of light-weight block ciphers[C]//Proc of RFID Security and Privacy. Berlin:Springer-Verlag, 2012: 1-18.

[10] YU X L, WU W L, LI Y J, et al. Cryptanalysis of reduced-round klein blockcipher[C]//Information Security and Cryptology. 2012: 237-250.

[11] AUMASSON J P, MARÍA N P. Practical attack on 8 rounds of the lightweight block cipher KLEIN[C]//Progress in Cryptology- INDOCRYPT. 2011: 134-145.

[12] 李卷孺, 谷大武, 张媛媛. 一种针对特定结构 SPN 密码算法的差分故障攻击[J]. 信息网络安全, 2009(4): 48-51.
LI J R, GU D W, ZHANG Y Y. A fault injection attack against certain types of SPN structures[J]. Net info Security, 2009(4): 48-51.

作者简介：

王永娟（1982-），女，河南开封人，博士，洛阳外国语学院副教授、硕士生导师，主要研究方向为密码学理论和对称密码算法的设计与分析。

任泉宇（1988-），男，四川成都人，解放军 78007 部队研究实习员，主要研究方向为密码分析。

张诗怡（1993-），女，四川乐山人，解放军外国语学院硕士生，主要研究方向为密码学中的逻辑函数。