轻量级密码MANTIS的唯密文故障分析

李 玮[1,2,3,4],张雨希[1],谷大武[2],张金煜[1],朱晓铭[1],刘 春[1],蔡天培[1],李嘉耀[1]
(1. 东华大学计算机科学与技术学院,上海 201620; 2. 上海交通大学计算机科学与工程系,上海 200240;
3. 上海市可扩展计算机与系统重点实验室(上海交通大学),上海 200240;
4. 上海市信息安全综合管理技术研究重点实验室(上海交通大学),上海 220240)

摘 要: MANTIS密码是于2016年美密会上提出的一种轻量级可调分组密码,它的设计采用FX结构和TWEAKEY框架,适用于物联网环境中具有低延迟、高实时安全需求的受限设备中. 本文基于半字节随机故障模型以及唯密文攻击,提出并讨论一种针对MANTIS密码的新型唯密文故障分析. 该分析结合公开调柄,利用故障注入后中间状态的不均匀性,可以破译MANTIS的全部版本. 实验结果表明,提出的新型双重区分器狄利克雷分布-汉明重量以及狄利克雷分布-极大似然最少分别需要392和396个故障,以99%及以上的成功率破译MANTIS各版本的128 bit原始密钥,不仅减少了故障注入数,而且提高了攻击效率,因此,MANTIS密码不能抵抗唯密文故障分析的攻击. 该结果为其他轻量级可调分组密码的安全性分析和防护提供了重要参考.

关键词: 故障分析; 轻量级密码; MANTIS; 唯密文分析; 物联网
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2022)04-0967-10
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20211026

Ciphertext-Only Fault Analysis on the MANTIS Lightweight Cipher

LI Wei[1,2,3,4], ZHANG Yu-xi[1], GU Da-wu[2], ZHANG Jin-yu[1], ZHU Xiao-ming[1], LIU Chun[1], CAI Tian-pei[1], LI Jia-yao[1]
(1. *School of Computer Science and Technology, Donghua University, Shanghai* 201620, *China*;
2. *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240, *China*;
3. *Department of Shanghai Key Laboratory of Scalable Computing and Systems (Shanghai Jiao Tong University), Shanghai* 200240, *China*;
4. *Shanghai Key Laboratory of Integrate Administration Technologies for Information Security (Shanghai Jiao Tong University), Shanghai* 200240, *China*)

Abstract: The lightweight tweakable block cipher MANTIS was published at the international Cryptology conference in 2016. It adopts the FX construction and the TWEAKEY framework, and can be applicable to the devices with the security requirements of low latency and high real time in the Internet of Things. The novel ciphertext-only fault analysis on MANTIS is proposed and discussed on the basis of the random nibble-oriented fault model and the assumption of ciphertext-only attack. On the public tweaks, the attackers can take advantage of the non-uniform property of the nibbles after fault injections, and recover the secret keys of all versions of MANTIS. The experimental results show that the new double distinguishers of Dirichlet distribution-Hamming weight and Dirichlet distribution-maximum likelihood can recover the 128-bit secret key with 392 and 396 faults, respectively. And the probability of success is no less than 99%. The proposed ciphertext-only fault analysis can not only decrease the faults, but improve the attacking efficiency. Thus, MANTIS cannot resist against the ciphertext-only fault analysis. It is vital for the security analysis and protection of other lightweight tweakable block ciphers.

Key words: fault analysis; lightweight cipher; MANTIS; ciphertext-only attack; Internet of Things

1 引言

近年来,随着5G技术对物联网普及的持续推动,智能家居、智能电网、智能交通等应用正给人们的工作、学习和生活带来极大的便利. 然而,如何保护网络

收稿日期:2021-08-01;修回日期:2022-01-17;责任编辑:孙瑶
基金项目:国家自然科学基金(No.61772129,No.61932014);国家密码发展基金(No.MMJJ20180101);上海市自然科学基金(No.19ZR14 02000);上海市可扩展计算与系统重点实验室开放课题;上海市信息安全综合管理技术研究重点实验室开放课题;中央高校基本科研业务费专项资金

中的数据免遭中断、截获、篡改和伪造等威胁，已成为物联网面临的重大安全挑战[1,2]. 由于智能卡、射频识别(Radio Frequency Identification，RFID)技术等存储、计算能力方面的限制，物联网中的数据难以直接采用传统密码兼顾安全性和高效性，因此，轻量级密码一经提出，便受到国内外工业界和学术界的广泛关注[3~9].

MANTIS密码是于2016年美密会上由Beierle等提出的一种轻量级可调分组密码，具有低延迟、高灵活性等特点，适用于保护物联网中的数据安全[9]. MANTIS密码采用FX结构和TWEAKEY框架的设计，分组长度、调柄长度均为64 bit，密钥长度为128 bit，用户可以根据实际需求选择不同的轮数及对应版本，其中轮数$r\geqslant 3$，对应版本记为MANTIS_r[9~12]. 密码设计者Beierle等[9]分析了该密码抵抗差分分析、线性分析、中间相遇分析、积分分析、滑动分析和不变子空间分析等的能力. 2016年，Dobraunig等[13]利用截断差分的多条高概率差分特征，实现了对MANTIS_5版本的截断差分分析. 2018年，Eichlseder等[14]提出寻找半截断差分特征族并计算其概率的通用方法，并对MANTIS_6版本进行了分析. 2019年，Chen等[15]提出聚类多个差分的通用自动搜索方法，给出了对MANTIS_6和MANTIS_7的分析结果. 同年，Ankele等[16]提出了针对使用线性扩展可调密钥的分组密码的零相关攻击，并将其应用于缩减轮的MANTIS_8的分析. 2020年，Beyne等[17]将积分分析方法应用在MANTIS_4版本密码的安全性分析中. 表1列举了针对MANTIS密码不同版本的多种密码分析结果.

表1 针对MANTIS密码的安全性分析汇总

分析类型	基本假设	MANTIS_r版本	文献
截断差分分析	选择明文	$r=5$	[13]
半截断差分分析	选择明文	$r=6$	[14]
多差分分析	选择明文	$r=6/7$	[15]
零相关分析	选择明文	$r=8$	[16]
积分分析	选择明文/文本	$r=4$	[17]
唯密文故障分析	唯密文	$r\geqslant 3$	本文

与上述传统密码分析方法不同，故障分析对物联网中密码的实现安全进行分析. 1997年，Boneh等[18]首次提出故障分析的概念，并将其应用于RSA公钥密码的破译. 攻击者通常可以物理上访问运行中的设备，并在执行算法加解密运算时，采用电压毛刺、激光脉冲和异常温度等方式向设备注入故障，干扰设备的工作状态，利用错误输出破译密钥信息. 在故障分析的发展历程中，逐渐衍生出差分故障分析、代数故障分析、线性故障分析、中间相遇故障分析以及唯密文故障分析等方法，对现代密码的安全实现提出了严峻的挑战[19~22].

在密码分析中，根据攻击者能力由弱到强将攻击假设分成唯密文、已知明文、选择明文和选择密文等攻击. 其中，唯密文攻击对攻击者控制使用算法设备的能力要求最弱、在实际中易实施，倘若在该假设下，攻击者能够成功破解密码，则该密码在其他攻击假设下必将遭受更大的安全威胁. 唯密文故障分析是一种基于唯密文攻击假设的故障分析方法，由Fuhr等[22]于2013年提出并应用于AES等密码的分析中，攻击者仅需获取随机故障密文，利用统计分析即可破译出密钥. 在AES密码的唯密文故障分析中，攻击者可通过错误输出来获取密码的中间状态值，利用平方欧氏距离、汉明重量和极大似然等区分器，结合中间状态的统计信息筛选出AES密码的原始密钥. 2016年，Dobraunig等[23]提出了认证加密算法的统计故障分析，并在智能卡、微控制器等硬件上利用激光和时钟毛刺实现了故障注入，成功破译了基于AES密码原语的认证加密算法. 近年来，李玮等[24~26]结合LED算法、LBlock和SIMON等算法提出了拟合优度、拟合优度-平方欧氏距离、拟合优度-极大似然和拟合优度-汉明重量等多种区分器，适用于代换置换网络(SPN)结构和Feistel结构密码的安全性分析.

目前，国内外未有公开发表的基于TWEAKEY框架的可调分组密码算法的唯密文故障分析研究. 与常见的分组密码相比，MANTIS密码的首尾轮具有白化密钥，再根据密码自身设计细节的分析，攻击者只能通过密钥之间的异或关系来确定密钥的值，此外结合可调分组密码中的调柄设计，无疑增加了密码破译的难度. 本文针对MANTIS密码抵抗唯密文故障分析的安全性进行了分析，并构造了狄利克雷分布-汉明重量和狄利克雷分布-极大似然等新型区分器. 表2总结了攻击者使用不同区分器分析AES密码、LED密码、LBlock密码、SIMON密码以及MANTIS密码并恢复完整密钥所需的故障数，可以看出狄利克雷分布-汉明重量和狄利克雷分布-极大似然等新型区分器，不仅能以99%及以上的成功率破译MANTIS密码所有版本的完整密钥，而且降低了密钥恢复所需注入的故障数，有效地提升了攻击效率. 该结果为轻量级可调分组密码的实现安全提供了有价值的参考.

2 MANTIS密码简介

2.1 符号说明

记X为明文，Y为密文，Y^*为故障密文.

记K为原始密钥，k_0和k_0'为白化密钥，k_1和$\bar{k}_1$为轮密钥，其中，$\bar{k}_1=k_1\oplus\alpha$，$\alpha$为常数.

表2　AES密码、LED密码、LBlock密码、SIMON密码及MANTIS密码的唯密文故障分析结果比较

故障数 / 区分器 \ 算法	AES-128[22]	LED-128[24]	LBlock-80[25]	SIMON-64/128[26]	MANTIS-128
平方欧氏距离(SEI)	320	560	124	∞	∞
汉明重量(HW)	288	312	-	-	440
极大似然(ML)	224	320	92	264	424
拟合优度(GF)	-	480	114	408	736
拟合优度-平方欧式距离(GF-SEI)	-	424	70	376	528
拟合优度-极大似然(GF-ML)	-	-	90	288	436
拟合优度-汉明重量(GF-HW)	-	-	-	248	428
狄利克雷分布-极大似然(DD-ML)	-	-	-	-	396
狄利克雷分布-汉明重量(DD-HW)	-	-	-	-	392

记r为轮数,$2r$为算法总轮数,其中,$r\in[3,\infty)$.

记T为原始调柄值,t_i为第i轮调柄值,$\mathrm{TK}_i=t_i\oplus k_1$,$\bar{T}_i=t_i\oplus\alpha$,且$\mathrm{TK}_{2r+1-i}=\mathrm{TK}_i$,$\bar{T}_{2r+1-i}=\bar{T}_i$,其中,$r\in[3,\infty)$,$i\in[1,2r]$.

记RC_i为第i轮轮常数,且$\mathrm{RC}_{2r+1-i}=\mathrm{RC}_i$,其中,$r\in[3,\infty)$,$i\in[1,2r]$.

记R_i为前向轮函数,R_i^{-1}为后向轮函数,R_i^{-1}是R_i的逆变换.

记SC, AC, ART, PC, MC, PC^{-1}分别为信元代替、轮常数加、可调密钥加、信元置换、列混合和逆信元置换操作.

记h为调柄的更新函数,h^{-1}为h的逆运算.

记$k_1[j]$, $\bar{T}[j]$, RC[j], $\mathrm{IS}_i[j]$分别为k_1, $\bar{T}$,轮常数和第i轮ART输出的第j个半字节,其中,$i\in[1,2r]$,$j\in[0,15]$.

记⊕为异或操作,//为连接操作,>>、>>>和<<<分别为右移、循环右移和循环左移操作.

2.2　算法描述

轻量级可调分组密码MANTIS算法由Beierle等学者在2016年美密会上提出,采用FX结构和TWEAKEY框架设计,分组长度和调柄长度均为64 bit,密钥长度为128 bit. 根据轮数不同,该密码分为不同版本,记为MANTIS_r,总轮数为$2r$轮,包括r轮前向轮和r轮后向轮,由一不带密钥的中间层连接,有首尾白化密钥,如图1所示. MANTIS_r的不同版本均使用相同的轮函数,64 bit数据结构采用4×4矩阵,其中,每个单元格为4 bit.

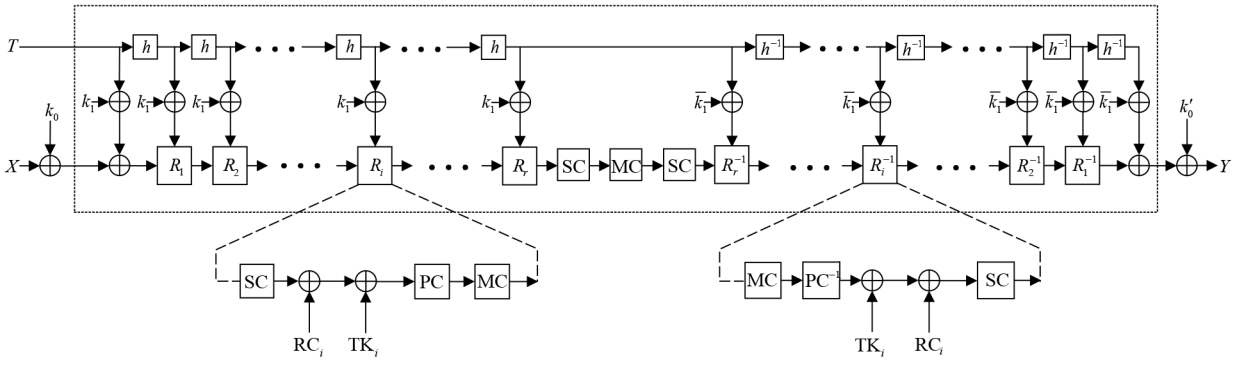


图1　MANTIS密码结构和轮函数

前向轮函数R_i包含如下5种基本运算.

(1)信元代替(SubCells,SC):使用以4 bit为单位的S盒进行替换,如表3所示.

(2)轮常数加(AddConstant,AC):与轮常数进行异或操作.

(3)可调密钥加(AddRoundTweakey,ART):与可调密钥进行异或操作.

(4)信元置换(PermuteCells,PC):对16个单元格进行移位.

(5)列混合(MixColumns,MC):与矩阵$\boldsymbol{M}$相乘实

表3　信元代替表

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
SC(x)	12	10	13	3	14	11	15	7	8	9	1	5	0	2	4	6

现，其中，$\boldsymbol{M}=\begin{pmatrix}0&1&1&1\\1&0&1&1\\1&1&0&1\\1&1&1&0\end{pmatrix}$.

后向轮函数 R_i^{-1} 中包含 5 种运算：MC，PC^{-1}，ART，AC 和 SC. 其中，逆信元置换表如表 4 所示，MANTIS_r 的加密算法如算法 1 所示.

表 4 逆信元置换表

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
SC(x)	0	5	15	10	13	8	2	7	11	14	4	1	6	3	9	12

算法 1 MANTIS_r **加密算法**

输入： X, k_0, k_0', TK, α, r

输出： Y

1: $S=X\oplus k_0$;
2: $S=S\oplus \mathrm{TK}_0$;
3: FOR $i=1$ TO r DO
4: SubCells(S);
5: AddConstant(S, i);
6: AddRoundTweakey(S, TK_i);
7: PermuteCells(S);
8: MixColumns(S);
9: END FOR
10: SubCells(S);
11: MixColumns(S);
12: SubCells(S);
13: FOR $i=r$ TO 1 DO
14: MixColumns(S);
15: InvPermuteCells(S);
16: AddRoundTweakey(S, TK_i, α);
17: AddConstant(S, i);
18: SubCells(S);
19: END FOR
20: $S=S\oplus \mathrm{TK}_0\oplus\alpha$;
21: $Y=S\oplus k_0'$.

2.3 密钥编排方案

128 bit 原始密钥 K 与 64 bit 子密钥 k_0，k_1 和 k_0' 的关系如下：

$$K=k_0 /\!/ k_1$$
$$k_0'=(k_0 \ggg 1)\oplus(k_0 \gg 63)$$

其中，k_0 和 k_0' 为白化密钥，k_1 为轮密钥.

3 唯密文故障分析

3.1 故障模型和基本假设

本文采用半字节随机故障模型，基本假设如下：

（1）攻击者可在加密过程中注入随机半字节故障，以“与”运算方式对原半字节进行注入；

（2）攻击者能够获得由同一密钥加密得到的故障密文.

图 2 统计了半字节经随机故障注入后的分布规律. 由于比特之间的“与”运算会出现不均匀性，因此注入半字节故障后，结果会出现不均匀分布.

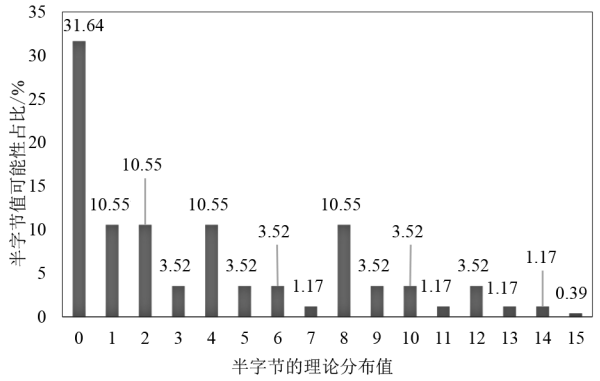


图 2 半字节经故障注入后的分布律

3.2 攻击过程

在可调分组密码算法的设计中，调柄通常公开且已知，分为固定和不固定，分别表示每次加密时使用相同或不同的调柄值. 考虑普遍性，本文在调柄不固定时检测 MANTIS 密码各版本抵御唯密文故障分析的能力，该攻击方法同样适用于调柄固定时的所有情况. 攻击过程主要包含如下 3 个步骤.

步骤 1 恢复 k_1 的 16 bit 相关值和 $k_1\oplus k_0'$ 的 48 bit.

攻击者在倒数第二轮导入随机半字节故障，并获得故障密文. 重复上述操作，攻击者能够收集到一组故障密文用于分析. 攻击者通过分析轮密钥、白化密钥、调柄和故障密文之间的关系，利用调柄、故障密文和猜测的子密钥做解密运算，将故障密文恢复至导入故障时的中间状态. 对于候选密钥比特，攻击者逆推故障密文得到对应的中间状态值，再利用区分器获得最佳区分值，筛选出正确候选密钥比特. 以注入位置在 $\mathrm{IS}_{2r-1}[0]$ 为例，故障扩散路径如图 3 示，攻击者利用部分候选子密钥 $(k_1\oplus k_0')[5]$，$(k_1\oplus k_0')[10]$，$(k_1\oplus k_0')[15]$ 和 $k_1[5]\oplus k_1[10]\oplus k_1[15]$，可用故障密文恢复出错误半字节 $\mathrm{IS}_{2r-1}[0]$，推导公式为

$$\begin{aligned}IS_{2r-1}[0]=&SC(Y^*[5]\oplus(k_1\oplus k_0')[5]\oplus\bar{T}_0[5])\oplus RC_1[5]\\&\oplus k_1[5]\oplus\bar{T}_1[5]\oplus SC(Y^*[10]\oplus(k_1\oplus k_0')[10]\\&\oplus\bar{T}_0[10])\oplus RC_1[10]\oplus k_1[10]\oplus\bar{T}_1[10]\\&\oplus SC(Y^*[15]\oplus(k_1\oplus k_0')[15]\oplus\bar{T}_0[15])\\&\oplus RC_1[15]\oplus k_1[15]\oplus\bar{T}_1[15]\end{aligned}$$

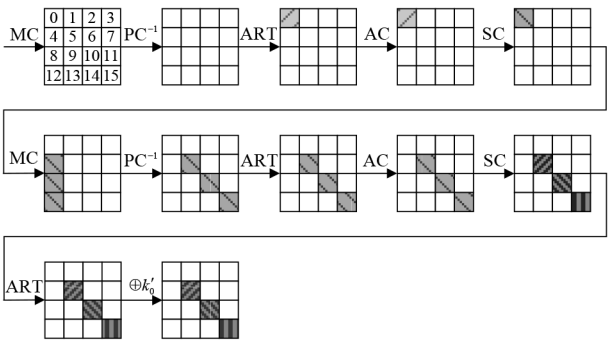


图3　故障导入在倒数第二轮后的扩散路径

通过遍历$IS_{2r-1}[0]$对应的2^{16}个密钥候选值,将每个密钥候选值对应的一组中间状态值分别输入到区分器中,获取2^{16}个区分值,再将区分值进行比较,即可得出符合理论分布的一组中间状态,所对应的密钥候选值即为正确密钥候选值. 攻击者通过改变故障注入位置,将故障注入在$IS_{2r-1}[1]$,$IS_{2r-1}[2]$和$IS_{2r-1}[3]$半字节,可得到$(k_1\oplus k_0')[1]$,$(k_1\oplus k_0')[2]$,$(k_1\oplus k_0')[3]$,$(k_1\oplus k_0')[4]$,$(k_1\oplus k_0')[7]$,$(k_1\oplus k_0')[8]$,$(k_1\oplus k_0')[9]$,$(k_1\oplus k_0')[12]$,$(k_1\oplus k_0')[14]$以及$k_1[1]\oplus k_1[4]\oplus k_1[14]$,$k_1[3]\oplus k_1[9]\oplus k_1[12]$和$k_1[2]\oplus k_1[7]\oplus k_1[8]$的值.

步骤2　恢复k_1的48 bit相关值和$k_1\oplus k_0'$的16 bit.

攻击者注入随机半字节故障至倒数第三轮,得到故障密文. 以$IS_{2r-2}[3]$作为注入位置为例,故障扩散路径如图4所示.

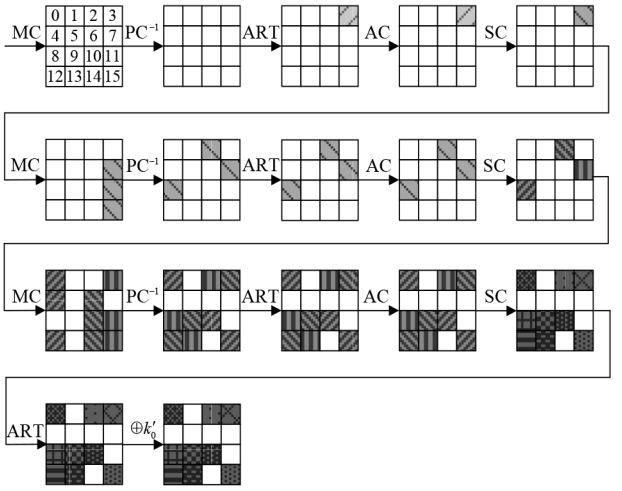


图4　故障导入在倒数第三轮后的扩散路径

利用已恢复的k_1的相关比特值以及部分$k_1\oplus k_0'$的值,攻击者可将故障密文恢复至IS_{2r-2}. 以$IS_{2r-2}[3]$为例,用对应的待猜测子密钥$(k_1\oplus k_0')[0]$,$(k_1\oplus k_0')[13]$,$k_1[2]\oplus k_1[8]\oplus k_1[13]$和$k_1[0]\oplus k_1[10]\oplus k_1[15]$,将故障密文恢复至$IS_{2r-2}[3]$,推导公式可表示为

$$\begin{aligned}IS_{2r-2}[3]=&SC\begin{pmatrix}SC\left(Y^*[3]\oplus(k_1\oplus k_0')[3]\oplus\bar{T}_0[3]\right)\oplus RC_1[3]\oplus k_1[3]\oplus\bar{T}_1[3]\\\oplus SC\left(Y^*[9]\oplus(k_1\oplus k_0')[9]\oplus\bar{T}_0[9]\right)\oplus RC_1[9]\oplus k_1[9]\oplus\bar{T}_1[9]\\\oplus SC\left(Y^*[12]\oplus(k_1\oplus k_0')[12]\oplus\bar{T}_0[12]\right)\oplus RC_1[12]\oplus k_1[12]\oplus\bar{T}_1[12]\end{pmatrix}\oplus RC_2[2]\oplus k_1[2]\oplus\bar{T}_2[2]\\&\oplus SC\begin{pmatrix}SC\left(Y^*[2]\oplus(k_1\oplus k_0')[2]\oplus\bar{T}_0[2]\right)\oplus RC_1[2]\oplus k_1[2]\oplus\bar{T}_1[2]\\\oplus SC\left(Y^*[8]\oplus(k_1\oplus k_0')[8]\oplus\bar{T}_0[8]\right)\oplus RC_1[8]\oplus k_1[8]\oplus\bar{T}_1[8]\\\oplus SC\left(Y^*[13]\oplus(k_1\oplus k_0')[13]\oplus\bar{T}_0[13]\right)\oplus RC_1[13]\oplus k_1[13]\oplus\bar{T}_1[13]\end{pmatrix}\oplus RC_2[7]\oplus k_1[7]\oplus\bar{T}_2[7]\\&\oplus SC\begin{pmatrix}SC\left(Y^*[0]\oplus(k_1\oplus k_0')[0]\oplus\bar{T}_0[0]\right)\oplus RC_1[0]\oplus k_1[0]\oplus\bar{T}_1[0]\\\oplus SC\left(Y^*[10]\oplus(k_1\oplus k_0')[10]\oplus\bar{T}_0[10]\right)\oplus RC_1[10]\oplus k_1[10]\oplus\bar{T}_1[10]\\\oplus SC\left(Y^*[15]\oplus(k_1\oplus k_0')[15]\oplus\bar{T}_0[15]\right)\oplus RC_1[15]\oplus k_1[15]\oplus\bar{T}_1[15]\end{pmatrix}\oplus RC_2[8]\oplus k_1[8]\oplus\bar{T}_2[8]\end{aligned}$$

攻击者依次对$IS_{2r-2}[3]$,$IS_{2r-2}[4]$,$IS_{2r-2}[13]$和$IS_{2r-2}[10]$半字节进行故障注入,每次注入恢复的部分子密钥用于后续的密钥恢复. 重复上述攻击步骤,攻击者可以得到$(k_1\oplus k_0')[6]$,$(k_1\oplus k_0')[11]$,$k_1[7]\oplus k_1[8]\oplus k_1[13]$,$k_1[0]\oplus k_1[5]\oplus k_1[15]$,$k_1[2]\oplus k_1[7]\oplus k_1[13]$,$k_1[3]\oplus k_1[6]\oplus k_1[12]$,$k_1[1]\oplus k_1[11]\oplus k_1[14]$,$k_1[3]\oplus k_1[6]\oplus k_1[9]$,$k_1[1]\oplus k_1[4]\oplus k_1[11]$,$k_1[0]\oplus k_1[5]\oplus k_1[10]$,$k_1[4]\oplus k_1[11]\oplus k_1[14]$和$k_1[6]\oplus k_1[9]\oplus k_1[12]$的值.

步骤3　恢复原始密钥K.

攻击者利用步骤1、步骤2可以恢复k_1的64 bit相关值以及$k_1\oplus k_0'$的16个半字节值,可得到关于k_1的16个半字节的方程组和$k_1\oplus k_0'$的值,具体如下:

$$\begin{cases} b_0 = k_1[5] \oplus k_1[10] \oplus k_1[15] \\ b_1 = k_1[1] \oplus k_1[4] \oplus k_1[14] \\ b_2 = k_1[3] \oplus k_1[9] \oplus k_1[12] \\ b_3 = k_1[2] \oplus k_1[7] \oplus k_1[8] \\ b_4 = k_1[2] \oplus k_1[8] \oplus k_1[13] \\ b_5 = k_1[0] \oplus k_1[10] \oplus k_1[15] \\ b_6 = k_1[4] \oplus k_1[11] \oplus k_1[14] \\ b_7 = k_1[7] \oplus k_1[8] \oplus k_1[13] \\ b_8 = k_1[0] \oplus k_1[5] \oplus k_1[15] \\ b_9 = k_1[2] \oplus k_1[7] \oplus k_1[13] \\ b_{10} = k_1[3] \oplus k_1[6] \oplus k_1[12] \\ b_{11} = k_1[1] \oplus k_1[11] \oplus k_1[14] \\ b_{12} = k_1[3] \oplus k_1[6] \oplus k_1[9] \\ b_{13} = k_1[1] \oplus k_1[4] \oplus k_1[11] \\ b_{14} = k_1[0] \oplus k_1[5] \oplus k_1[10] \\ b_{15} = k_1[6] \oplus k_1[9] \oplus k_1[12] \end{cases}$$

其中，b_u为已恢复的k_1的相关值，$u \in [0, 15]$. 攻击者解出方程组获得k_1后，再与$k_1 \oplus k_0'$的值进行异或操作，可得到k_0'的值，即$k_0' = k_1 \oplus (k_1 \oplus k_0')$.

最后，攻击者通过密钥编排方案恢复MANTIS各版本的原始密钥，即

$$K = (k_0' \oplus ((k_0' <<< 1) >> 63)) <<< 1 \;/\!/\; k_1$$

3.3 区分器

本节使用平方欧氏距离、汉明重量等7种现有区分器及2种新型区分器对MANTIS密码进行唯密文故障分析. 2013年，Fuhr等[22]首次提出平方欧式距离、汉明重量和极大似然区分器对AES密码进行唯密文故障分析. 近年来，李玮等[24,26]针对LED等密码提出了拟合优度、拟合优度-平方欧氏距离、拟合优度-极大似然和拟合优度-汉明重量等区分器，降低了故障注入数. 本节提出了狄利克雷分布-极大似然和狄利克雷分布-汉明重量新型区分器. 各区分器的原理及取值如表5所示. 新型区分器原理如下所述.

(1)狄利克雷分布-极大似然区分器

狄利克雷分布(Dirichlet Distribution，DD)区分器通过计算在理论分布下中间状态值得到的概率筛选出一组最符合理论分布的状态，概率值DD越越大，候选密钥为真实密钥的可能性越大. DD值可表示为

$$\mathrm{DD} = \frac{\Gamma\left(\sum_{m=0}^{15} 1 + O[m]\right)}{\prod_{m=0}^{15} \Gamma\left(1 + O[m]\right)} \cdot \prod_{m=0}^{15} D[m]^{O[m]} = (n+15)! \cdot \prod_{m=0}^{15} \frac{D[m]^{O[m]}}{(O[m])!}$$

狄利克雷分布-极大似然(Dirichlet Distribution-Maximum Likelihood，DD-ML)区分器是结合DD区分器和ML区分器的双重区分器，攻击者依次计算DD值和ML值，从DD区分值较佳结果中取ML的最大值，即为最可能的候选密钥，ML计算式为

$$\mathrm{ML} = \prod_{v=0}^{n-1} D[\mathrm{IS}^v] = \prod_{m=0}^{15} D[m]^{O[m]}$$

其中，n为导入故障数，IS^v为第v个中间状态值，$O[m]$表示中间状态值中值为m的个数，$D[m]$表示中间状态值为m的理论概率.

(2) 狄利克雷分布-汉明重量区分器

狄利克雷分布-汉明重量(Dirichlet Distribution-Hamming Weight，DD-HW)区分器首先计算在理论分布下中间状态值得到的概率，得到较大概率对应的一组中间状态，然后在这一组中间状态中进行进一步的筛选，以减少所需故障数. 攻击者首先利用DD区分器筛选出一组高概率值的候选值，计算式为

$$\mathrm{DD} = \frac{\Gamma\left(\sum_{m=0}^{15} 1 + O[m]\right)}{\prod_{m=0}^{15} \Gamma\left(1 + O[m]\right)} \cdot \prod_{m=0}^{15} D[m]^{O[m]} = (n+15)! \cdot \prod_{m=0}^{15} \frac{D[m]^{O[m]}}{(O[m])!}$$

然后利用HW区分器筛选出最小值，计算式为

$$\mathrm{HW} = \frac{1}{n} \sum_{v=0}^{n-1} \mathrm{hw}(\mathrm{IS}^v) = \frac{1}{n} \sum_{m=0}^{15} \mathrm{hw}(m) \cdot O[m]$$

其中，n为导入故障数，IS^v为第v个中间状态值，hw为汉明重量值的计算函数，$O[m]$表示中间状态值中值为m的个数，$D[m]$表示中间状态值为m的理论概率.

4 实验分析

本实验在Intel Core Processor (Broadwell, no TSX, IBRS)，Ubuntu 21.04，2.4GHz计算机服务器上运行，采用C++编程语言实现对MANTIS密码的唯密文故障分析. 攻击者采用计算机软件生成半字节随机故障并模拟故障注入，使用“与”运算的方式对原中间状态的指定位置产生影响，再使用各区分器恢复原始密钥. 由于MANTIS_r的不同版本仅有加密轮数的区别，轮函数和密钥编排均相同，使得从故障密文倒推至注入故障的中间状态的过程也相同，因此相同区分器恢复MANTIS密码各版本原始密钥的效果相同.

本实验以MANTIS_8为例，利用SEI，HW，ML，GF，GF-SEI，GF-ML和GF-HW区分器以及DD-ML，DD-HW新型区分器进行统计分析. 在攻击过程中，每次统计分析可恢复16 bit子密钥的信息，在倒数第二轮和倒数第三轮先后分别注入半字节故障，用于恢复128 bit原始密钥. 图5、图6和表6展示了针对MANTIS_8

表5　各区分器对比

区分器	原理	取值	文献
平方欧式距离(SEI)	衡量总体分布与均匀分布的差距,筛选最不符合均匀分布的样本分布	SEI最大值	[22]
汉明重量(HW)	计算样本分布与零的距离,筛选汉明重量值与零距离最远的样本分布	HW最小值	[22]
极大似然(ML)	计算中间状态分布概率的乘积,筛选似然函数最大的样本分布	ML最大值	[22]
拟合优度(GF)	判断已知样本分布与理论分布的拟合程度,筛选拟合程度最大的样本分布	GF最小值	[24]
拟合优度-平方欧氏距离(GF-SEI)	先用GF筛选与理论分布拟合程度最优的一组样本分布,再用SEI筛选最不均匀的样本分布	GF最小值 SEI最大值	[24]
拟合优度-极大似然(GF-ML)	先用GF筛选与理论分布拟合程度最优的一组样本分布,再用ML筛选似然函数最大的样本分布	GF最小值 ML最大值	[25]
拟合优度-汉明重量(GF-HW)	先用GF筛选与理论分布拟合程度最优的一组样本分布,再用HW筛选汉明重量最小的样本分布	GF最小值 HW最小值	[26]
狄利克雷分布-极大似然(DD-ML)	先用DD筛选中间状态对应的概率最大的一组样本分布,再用ML筛选似然函数最大的样本分布	DD最大值 ML最大值	本文
狄利克雷分布-汉明重量(DD-HW)	先用DD筛选中间状态对应的概率最大的一组样本分布,再用HW筛选汉明重量最小的样本分布	DD最大值 HW最小值	本文

版本的攻击结果,所有结果均为1000次实验后的统计结果.

4.1　故障数

在故障攻击中,攻击算法需要注入的故障数越少,在实际硬件实现时越具有优势. 表6给出了恢复MANTIS_8完整密钥且成功率达到99%及以上时,各区分器所需的故障注入数. 本文提出的DD-HW和DD-ML双重区分器分别需要392个和396个故障数,与现有区分器相比,所需故障数较少. 其中,SEI区分器对每一个中间状态值统计所得的个数采用了相同的处理系数,故中间状态值与统计所得个数间映射关系的改变不会影响区分值大小,同时,异或操作会导致这个映射关系发生变化. 因此,如果待分析的中间状态值是通过故障密文与待猜测密钥候选值直接异或所得的,那么SEI区分器无法起到区分效果.

表6　各区分器恢复完整密钥所需故障数、时间复杂度和数据复杂度

区分器	故障数	时间复杂度	数据复杂度
平方欧氏距离(SEI)	∞	∞	∞
汉明重量(HW)	440	$2^{30.61}$	$2^{24.78}$
极大似然(ML)	424	$2^{30.51}$	$2^{24.75}$
拟合优度(GF)	736	$2^{31.99}$	$2^{25.52}$
拟合优度-平方欧氏距离(GF-SEI)	528	$2^{31.20}$	$2^{25.15}$
拟合优度-极大似然(GF-ML)	436	$2^{30.87}$	$2^{24.77}$
拟合优度-汉明重量(GF-HW)	428	$2^{30.78}$	$2^{24.74}$
狄利克雷分布-极大似然(DD-ML)	396	$2^{30.50}$	$2^{24.63}$
狄利克雷分布-汉明重量(DD-HW)	392	$2^{30.49}$	$2^{24.61}$

4.2　成功率

成功率指成功恢复密钥的次数占实验次数的比例. 在故障分析中,若候选密钥经区分器筛选后得到唯一候选密钥且该候选密钥与真实密钥值相同,那么该次密钥恢复实验成功. 恢复完整密钥需进行两阶段攻击,依次在加密的倒数第二轮和倒数第三轮分别注入故障,由于注入故障轮数不同,故障对加密过程的影响不同,导致区分器恢复密钥的成功率不同,因此图5(a)和(b)分别展示在倒数第二轮和倒数第三轮注入故障时不同区分器的攻击效果,即子密钥恢复成功率与导入故障个数的关系,其中横坐标为故障注入数,纵坐标为子密钥恢复成功率. 为了减少第一阶段攻击对第二阶段攻击的实验数据的影响,第二阶段攻击的实验数据在第一阶段攻击待恢复子密钥已知的基础上进行统计. 从数据可以看出,HW, ML, GF, GF-SEI, GF-ML, GF-HW, DD-ML和DD-HW区分器均可以99%及以上的成功率恢复MANTIS密码原始密钥. 鉴于SEI区分器成功率最高不超过20%,实际攻击时不建议采用SEI区分器.

4.3　复杂度

时间复杂度和数据复杂度是衡量密码破译的时间量和数据量的重要指标,其计算式分为

$$4\cdot\omega\cdot(f_1\cdot 2^{16}+f_2\cdot 2^{16})$$

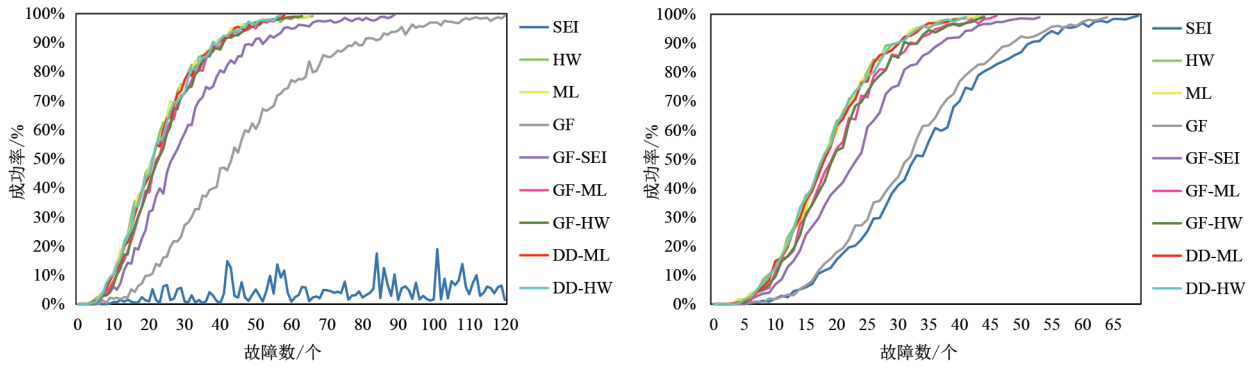
和

$$4\cdot(f_1\cdot 2^{16}+f_2\cdot 2^{16})$$

其中,f_1和f_2分别为两阶段攻击中注入的故障数,ω为不同区分器对应的复杂度系数. 表6给出了不同区分器以不小于99%的成功率恢复MANTIS_8完整密钥所需的时间复杂度和数据复杂度,新型双重区分器DD-ML和DD-HW的时间复杂度以及数据复杂度均小于已有区分器.

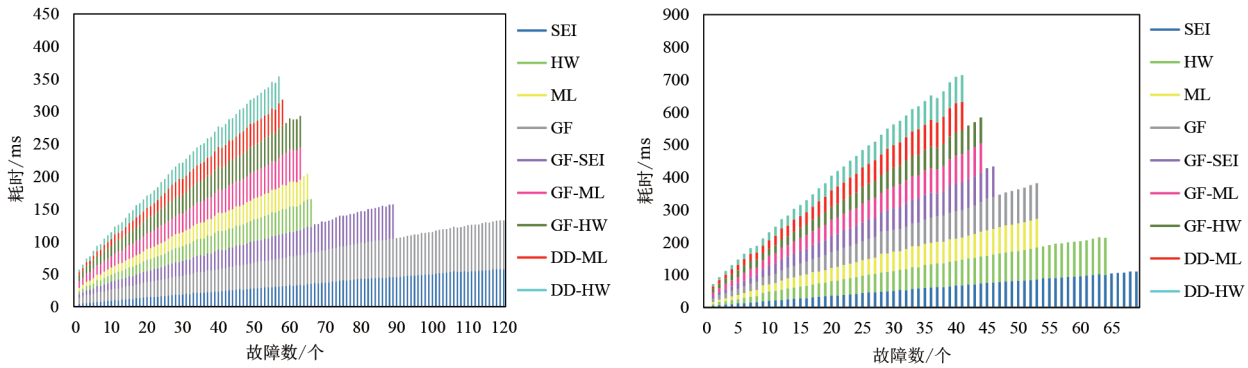
4.4　耗时

在密码算法的攻击中,耗时越少则攻击的时间成本越小. 图6(a)和(b)分别表示在不同区分器下,在两



(*a*) 在倒数第二轮注入故障 (*b*) 在倒数第三轮注入故障

图5 各区分器恢复16 bit密钥的成功率



(*a*) 在倒数第二轮注入故障 (*b*) 在倒数第三轮注入故障

图6 各区分器恢复16 bit密钥的耗时

阶段攻击中恢复子密钥的耗时与故障注入数的关系. 其中横坐标表示注入的故障个数;纵坐标表示耗时,具体为遍历候选密钥和故障密文、统计中间状态的分布律、计算区分值并筛选正确密钥的总时间. 实验结果表明,除SEI区分器外,使用HW, ML, GF, GF-SEI, GF-ML, GF-HW, DD-ML和DD-HW区分器以99%及以上的成功率恢复出完整密钥消耗的最少时间分别483.6 ms, 462.8 ms, 756.0 ms, 564.8 ms, 577.6 ms, 554.8 ms, 500.4 ms, 490.8 ms. 其中,DD-ML和DD-HW新型区分器恢复完整密钥的耗时次于HW和ML单区分器,但在所有双重区分器比较中,新型区分器耗时最少.

因此,结合图5、图6和表6的统计分析,新型区分器DD-ML和DD-HW恢复MANTIS完整密钥的成功率可达99%及以上,所需的故障数、时间复杂度、数据复杂度均达到最优,耗时低于现有双重区分器.

5 结束语

本文提出了针对MANTIS密码的唯密文故障分析方法,采用狄利克雷分布-汉明重量和狄利克雷分布—极大似然等新型区分器,不仅能以99%及以上的成功率破译密码,而且降低了故障注入数,提升了攻击效率. 研究表明,MANTIS密码易受到唯密文故障攻击的威胁,因此,在物联网中的智能卡、RFID等设备中使用该密码算法时,建议实施必要的举措对密码最后若干轮加以防护,以减少受到该类分析的威胁. 下一步工作将结合MANTIS密码的内部更深轮进行唯密文故障分析研究.

参考文献

[1] ZAINUDDIN N, DAUD M, AHMAD S, et al. A study on privacy issues in Internet of Things(IoT) [C]//Proceedings of the 5th International Conference on Cryptography, Security and Privacy. New York: IEEE, 2021: 96-100.

[2] SHAIKH E, MOHIUDDIN I, MANZOOR A. Internet of Things(IoT): Security and privacy threats[C]//Proceedings of the 2nd International Conference on Computer Applications & Information Security. New York: IEEE, 2019: 1-6.

[3] GUO J, PEYRIN T, POSCHMANN A, et al. The LED block cipher[C]// PRENEEL B, TAKAGI T. Proceedings of the 13th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2011: 326-341.

[4] WU W, ZHANG L. LBlock: a lightweight block cipher[C]// LOPEZ J, TSUDIK G. Proceedings of the 9th International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2011: 327-344.

[5] BORGHOFF J, CANTEAUT A, GÜNEYSU T, et al. PRINCE-a low-latency block cipher for pervasive comput-

ing applications[C]//WANG X, SAKO K. Proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2012: 208-225.

[6] BANIK S, BOGDANOV A, ISOBE T, et al. Midori: A block cipher for low energy[C]//IWATA T, CHEON J. Proceedings of the 21st International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2015: 411-436.

[7] BEIERLE C, LEANDER G, MORADI A, et al. CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks[J]. IACR Transactions on Symmetric Cryptology, 2019, 2019(1): 5-45.

[8] KIM H, JEON Y, KIM G, et al. PIPO: A lightweight block cipher with efficient higher-order masking software implementations[C]//HONG D. Proceedings of the 23rd Information Security and Cryptology. Berlin: Springer, 2020: 99-122.

[9] BEIERLE C, JEAN J, KÖLBL S, et al. The SKINNY family of block ciphers and its low-latency variant MANTIS [C]//ROBSHAW M, KATZ J. Proceedings of the 36th International Cryptology Conference. Berlin: Springer, 2016: 123-153.

[10] KILIAN J, ROGAWAY P. How to protect DES against exhaustive key search[J]. Lecture Notes in Computer Science, 1996, 1109: 252-267.

[11] LISKOV M, RIVEST R L, WAGNER D. Tweakable block ciphers[J]. Journal of Cryptology, 2002, 2442: 531-46.

[12] JEAN J, NIKOLIĆ I, PEYRIN T. Tweaks and keys for block ciphers: The TWEAKEY framework[C]//SARKAR P, IWATA T. Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2014: 274-288.

[13] DOBRAUNIG C, EICHLSEDER M, KALES D, et al. Practical key-recovery attack on MANTIS$_5$[J]. IACR Transactions on Symmetric Cryptology, 2016, 2016(2): 248-260.

[14] EICHLSEDER M, KALES D. Clustering related-tweak characteristics: application to MANTIS-6[J]. IACR Transactions on Symmetric Cryptology, 2018, 2018(2): 111-132.

[15] CHEN S Y, LIU R, CUI T T, et al. Automatic search method for multiple differentials and its application on MANTIS[J]. Science China Information Sciences, 2019, 62(3): 145-159.

[16] ANKELE R, DOBRAUNIG C, GUO J, et al. Zero-correlation attacks on tweakable block ciphers with linear tweakey expansion[J]. IACR Transactions on Symmetric Cryptology, 2019, 2019(1): 192-235.

[17] BEYNE T. Block cipher invariants as eigenvectors of correlation matrices[J]. Journal of Cryptology, 2020, 33(3): 1156-1183.

[18] BONEH D, DEMILLO R, LIPTON R. On the importance of checking cryptographic protocols for faults[C]//FUMY W. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1997: 37-51.

[19] BIHAM E, SHAMIR A. Differential fault analysis of secret key cryptosystems[C]//KALISKI B S. Proceedings of the 17th International Cryptology Conference. Berlin: Springer, 1997: 513-525.

[20] COURTOIS N T, WARE D, JACKSON K. Fault-algebraic attacks on inner rounds of DES[C]//Proceedings of the European Smart Card Security Conference. Montreuil: Computer Science, 2010: 22-24.

[21] DERBEZ P, FOUQUE P A, LERESTEUX D. Meet-in-the-middle and impossible differential fault analysis on AES[C]//PRENEEL B, TAKAGI T. Proceedings of the 13th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2011: 274-291.

[22] FUHR T, JAULMES E, LOMNÉ V, et al. Fault attacks on AES with faulty ciphertexts only[C]//Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography. New York: IEEE, 2013: 108-118.

[23] DOBRAUNIG C, EICHLSEDER M, KORAK T, et al. Statistical fault attacks on nonce-based authenticated encryption schemes[C]//CHEON J, TAKAGI T. Proceedings of the 22nd International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2016: 369-395.

[24] LI W, LIAO L F, GU D W, et al. Ciphertext-only fault analysis on the LED lightweight cryptosystem in the Internet of Things[J]. IEEE Transactions on Dependable and Secure Computing, 2019, 16(3): 454-461.

[25] 李玮, 吴益鑫, 谷大武, 等. LBlock轻量级密码算法的唯密文故障分析[J]. 计算机研究与发展, 2018, 55(10): 2174-2184.
LI W, WU Y X, GU D W, et al. Ciphertext-only fault analysis of the LBlock lightweight cipher[J]. Journal of Computer Research and Development, 2018, 55(10): 2174-2184. (in Chinese)

[26] 李玮, 吴益鑫, 谷大武, 等. SIMON轻量级密码算法的唯密文故障分析[J]. 通信学报, 2019, 40(11): 122-137.
LI W, WU Y X, GU D W, et al. Ciphertext-only fault

analysis of the SIMON lightweight cipher[J]. Journal on Communications, 2019, 40(11): 122-137. (in Chinese)

作者简介

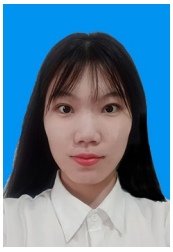
李 玮 女，1980 年 8 月出生，安徽寿县人. 现为东华大学教授，博士生导师. 主要研究方向为对称密码的设计与分析.
E-mail: liwei.cs.cn@gmail.com

张雨希 女，1998 年 8 月出生，黑龙江哈尔滨人. 现为东华大学硕士研究生. 主要研究方向为轻量级密码的安全分析.

谷大武 男，1970 年 10 月出生，河南漯河人. 现为上海交通大学教授，博士生导师. 主要研究方向为密码学和计算机安全.

张金煜 男，1998 年 2 月出生，浙江嘉兴人. 现为东华大学硕士研究生. 主要研究方向为轻量级密码的故障分析.

朱晓铭 男，1998 年 1 月出生，河北邯郸人. 现为东华大学硕士研究生. 主要研究方向为轻量级密码的安全分析.



刘 春 女，2000 年 3 月出生，江西萍乡人. 现为东华大学硕士研究生. 主要研究方向为轻量级密码的安全分析.

蔡天培 男，1996 年 12 月出生，浙江温州人. 现为东华大学硕士研究生. 主要研究方向为对称密码的安全性分析.

李嘉耀 男，1996 年 4 月出生，广东广州人. 现为东华大学博士研究生. 主要研究方向为对称密码的故障分析.