轻量级密码 Pyjamask 和 SUNDAE-GIFT 的不可能统计故障分析

李 玮[1),2),3),4)] 高建宁[1)] 谷大武[2)] 秦梦洋[1)] 刘 源[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)](上海交通大学上海市可扩展计算与系统重点实验室 上海 200240)

[4)](上海交通大学上海市信息安全综合管理技术研究重点实验室 上海 200240)

摘 要 Pyjamask 密码是 2020 年由 Goudarzi 等学者在国际对称密码学期刊中提出的密码算法,同时也是国际轻量级密码竞赛第二轮候选算法,旨在保护物联网中传感器、智能芯片和嵌入式设备的数据安全.本文结合 Pyjamask 密码的设计结构和实现特点,基于不可能关系策略和统计分析,提出适用于在唯密文环境下的不可能统计故障分析方法,并设计了 Wasserstein 距离-汉明重量和 Wasserstein 距离-极大似然估计区分器.该分析方法分别仅需 1024 和 1120 个随机故障密文,即可在 59.84 ms 和 140.16 ms 内破译 Pyjamask 密码全部版本的 128 比特主密钥.并且,该方法和区分器均可用于认证加密算法 SUNDAE-GIFT 的分析中.不可能统计故障分析的攻击速度快,并且实现代价低,为轻量级密码的实现安全研究提供了有价值的参考.

关键词 轻量级密码;Pyjamask;SUNDAE-GIFT;故障分析;不可能关系;密码分析

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2024.01010

Impossible Statistical Fault Analysis of the Pyjamask and SUNDAE-GIFT Lightweight Cryptosystems

LI Wei[1),2),3),4)] GAO Jian-Ning[1)] GU Da-Wu[2)] QIN Meng-Yang[1)] LIU Yuan[1)]

[1)](*School of Computer Science and Technology, Donghua University, Shanghai* 201620)

[2)](*Department of Computer and Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240)

[3)](*Shanghai Key Laboratory of Scalable Computing and System, Shanghai Jiao Tong University, Shanghai* 200240)

[4)](*Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai Jiao Tong University, Shanghai* 200240)

Abstract The lightweight cryptosystems Pyjamask and SUNDAE-GIFT, proposed in the IACR Transactions on Symmetric Cryptology, are candidates for the second round of Lightweight Cryptography Standardization. They aim to protect the data of sensors, smart chips, and embedded devices on the Internet of Things. The Pyjamask block cipher adopts a substitution-permutation network and consists of two versions: Pyjamask-96 and Pyjamask-128, whose block sizes are 96 and 128 bits, respectively. Its key size is 128 bits, with 14 rounds of encryption or decryption. It has perfect diffusion and compatibility and can resist many types of attacks, such as side-channel analysis, differential analysis, linear analysis, impossible differential analysis, Boomerang analysis,

收稿日期:2023-06-05;在线发布日期:2024-02-06.本课题得到国家重点研发计划(2020YFA0712300)、国家自然科学基金项目(62072307)和上海市扬帆计划(21YF1401200,23YF1401000)资助.**李 玮**(通信作者),博士,教授,博士生导师,中国计算机学会(CCF)会员,主要研究领域为对称密码算法的设计与分析.E-mail:liwei.cs.cn@gmail.com.**高建宁**,硕士研究生,主要研究方向为分组密码的故障分析.**谷大武**,博士,教授,博士生导师,主要研究领域为密码学与计算机安全.**秦梦洋**,硕士研究生,主要研究方向为分组密码的故障分析.**刘 源**,硕士研究生,主要研究方向为分组密码的故障分析.

integral analysis, algebraic higher-order differential analysis, etc. The SUNDAE-GIFT authenticated encryption lies on a GIFT block cipher with a 128-bit secret key, 128-bit blocks, and 40 rounds of encryption or decryption. It provides confidentiality and authentication, and its security analysis includes typical fault analysis and traditional cryptanalysis. This study presents the Pyjamask and SUNDAE-GIFT lightweight cryptosystems against a new impossible statistical fault analysis. It is based on the basic assumption of a ciphertext-only attack and combines an impossible relationship with statistical analysis. In addition, this study constructs novel distinguishers of Wasserstein Distance-Hamming Weight (WD-HW) and Wasserstein Distance-Maximum Likelihood Estimation (WD-MLE) based on the Wasserstein distance. The attackers can inject random nibble faults to filter out some bits of the round keys through the impossible and statistical relationships. They can obtain all round keys to recover the secret key through successive fault injections and the key schedule. The experiments consider the number of faults, accuracy, reliability, latency, and complexity to study the performance of the new fault analysis and distinguishers. The number of faults is the minimum required for retrieving the secret key with the maximum probability. The smaller the faults, the better the attacking performance and the distinguisher. Accuracy is measured using root mean square error. The smaller the value of RMSE, the closer the prediction results are to the accurate results. Reliability refers to the probability of recovering the secret key. When the reliability reaches no less than 99%, the attacker can recover the secret key in most cases. Latency is the time required to retrieve the secret key using different distinguishers. The complexity serves as metrics to assess the computational time and total data processed required for recovery the key. In practice, latency and complexity are important indicators for measuring the performance of fault analysis and distinguishers. In this paper, the experimental results show that neither Pyjamask nor SUNDAE-GIFT can resist the proposed impossible statistical fault analysis. The analysis requires only 1024 and 1120 random fault ciphertexts to recover the secret keys of Pyjamask-96 and Pyjamask-128 in 59.84 and 140.16 milliseconds, respectively. In addition, the analysis requires only 400 faults to recover the 128-bit secret key of SUNDAE-GIFT in 5.78 seconds. Compared with the classical statistical fault analysis, the impossible statistical fault analysis performs better. It can reduce the attacking cost and improve the attacking effectiveness of lightweight cryptosystems. As a result, the impossible statistical fault analysis threatens the security of the Pyjamask and SUNDAE-GIFT lightweight cryptosystems. This study provides a valuable reference for securing lightweight cryptosystems in the Internet of Things.

Keywords　lightweight cryptosystem; Pyjamask; SUNDAE-GIFT; fault analysis; impossible relationship; cryptanalysis

1　引　言

近年来，随着物联网技术在各种小型设备的深入应用，它对人们生活和社会经济的影响日益显著.然而，随之而来的安全问题同样引发了工业界和学术界的广泛关注.传统的密码算法由于受到小型设备的资源限制，难以在安全、实现和效率之间取得平衡.因此，在确保高效性能的同时，如何保障数据的高安全性以适应不断发展的物联网领域变得尤为重要[1-2].轻量级密码算法应运而生，它能够在资源受限的设备上快速运行，并具有良好的安全性能和实现效率.目前，轻量级密码算法的设计与分析已成为保护物联网数据的有效安全解决方案，同时也是密码学领域的研究热点[3-9].

轻量级密码 Pyjamask 和 SUNDAE-GIFT 都是在国际对称密码学期刊(ToSC/FSE)中提出的算法，同时也作为美国国家技术标准研究院(NIST)征选的国际轻量级密码算法标准的候选算法[10-11].轻量级分组密码 Pyjamask 采用了 128 比特的密钥长度，具

有两个分组长度版本:Pyjamask-96 和 Pyjamask-128,具有良好的扩散性和兼容性,能够抵御侧信道攻击、差分分析、线性分析、不可能差分分析、Boomerang 分析、积分分析和代数高阶差分分析等多种不同类型的攻击[12-16].基于 GIFT 分组密码设计的轻量级认证加密算法 SUNDAE-GIFT,采用 128 比特的分组和密钥长度,兼具保密性和认证性,安全性研究包括故障分析及传统密码分析[17-22].这两个算法目前都是国际上受到广泛关注的轻量级密码.

故障分析作为一种常见的侧信道攻击,是指攻击者试图通过人为制造硬件或软件的故障来破解密码中的密钥,利用的是密码实现的物理泄露.攻击者可以通过对目标设备注入电磁波、控制供电电压或温度等手段来实现故障的注入,进而改变密码运行的内部状态,并利用这些信息来推导出密钥[23-24].Boneh 等学者[25]于 1996 年提出故障分析,在 RSA 密码运算过程中对模数进行随机扰动,导致密文发生错误,利用故障密文信息快速地破解了 RSA 密码;1997 年,Biham 等学者[26]利用故障分析成功地分析了典型分组密码标准 DES 算法.自此,故障分析作为密码学研究领域中一种新兴的分析方法,相继扩展出现了差分故障分析、不可能差分故障分析以及统计故障分析等多个种类,分析范围已覆盖分组密码和流密码[27-29].

根据攻击者能力要求不同,密码分析方法的基本假设可以分为:选择密文攻击、选择明文攻击、已知明文攻击和唯密文攻击.其中,差分故障分析、不可能差分故障分析等常见的故障分析均以选择明文攻击为基本假设,统计故障分析适用于唯密文攻击,即攻击者仅需具备截获密文的能力,无需获得明文或其他信息.因此,统计故障分析(Statistical Fault Analysis,SFA)对攻击者监听加密通讯信息的能力要求最弱,易在现实环境中实现.2013 年,Fuhr 等学者[30]首次提出了针对 AES 密码的统计故障分析.攻击者仅需在唯密文前提下,收集受故障影响的随机故障密文并计算部分解密过程,就可以使用统计分析的方法来恢复出正确的密钥,速度快且成功率高.近年来,LED 和 PRESENT 等密码均不能防范统计故障分析[31-32].因此,统计故障分析作为一种相对快速且易实现的攻击方式,适用于对物联网等现实环境中轻量级密码算法的安全性进行评估,用于及时发现和解决其中的安全漏洞,并采取相应的安全措施来保护密码及系统的实现安全.

目前,国内外尚未有轻量级密码算法 Pyjamask 和 SUNDAE-GIFT 抵御新型统计故障分析的公开成果.本文基于唯密文攻击基本假设,结合统计分析和不可能分析,提出了针对 Pyjamask 和 SUNDAE-GIFT 密码算法的不可能统计故障分析(Impossible Statistical Fault Analysis,ISFA)方法.在减少恢复密钥所需故障数的同时,降低了攻击时间,攻击效果佳.另外,本文通过构建基于 Wasserstein 距离算法的新型区分器 Wasserstein 距离-汉明重量(WD-HW)和 Wasserstein 距离-极大似然估计(WD-MLE),进一步提升了攻击效率,降低了攻击代价.这一结果为评估轻量级密码在防范唯密文分析方面的安全性提供了重要的参考.

2 相关工作

自 Pyjamask 算法提出以来,它的设计和安全性分析引起国内外学者的广泛关注.2020 年,Dobraunig 等学者[12]针对 Pyjamask-96 版本提出代数高阶差分密码分析方法,通过结合高阶差分和构造的 2.5 轮方程组,提供了 14 轮的攻击.同年,许泽雨等学者[13]利用简单定理证明约束求解器,构建了差分路线以及线性路线的自动化搜索模型,提出了针对 Pyjamask-128 版本的 4 轮线性分析、5 轮差分分析和 6 轮 Boomerang 分析.次年,Liu 等学者[15]结合行混淆运算扩散性,构造不可能差分攻击路径,并分析了 4 轮缩减轮 Pyjamask 算法.2022 年,Cui 等学者[16]使用积分攻击方法,用于分析 14 轮的 Pyjamask-96 版本和 11 轮缩减版 Pyjamask-128 版本.以上研究表明,Pyjamask 算法在抗差分、线性等经典密码分析方法具有良好的安全性,基本假设仅限于已知以及选择明文攻击的前提下.目前国内外未有公开发表的对 Pyjamask 算法抵御唯密文攻击下的相关分析成果,总结如表 1 所示.

表 1 针对 Pyjamask 算法的安全性分析对比

分析类型	基本假设	攻击版本	攻击轮数	文献
线性分析	已知明文攻击	—/128	—/4	[13]
不可能差分分析	选择明文攻击	96/128	4/4	[15]
差分分析	选择明文攻击	—/128	—/5	[13]
Boomerang 分析	选择明文攻击	—/128	—/6	[13]
代数高阶差分分析	选择明文攻击	96/—	14/—	[12]
积分分析	选择明文攻击	96/128	14/11	[16]
统计故障分析	唯密文攻击	96/128	14/14	本文
不可能统计故障分析	唯密文攻击	96/128	14/14	本文

统计故障分析作为常见的唯密文故障分析方法之一，于 2013 年由 Fuhr 等学者[30]提出并用于 AES 密码的分析. 该方法利用随机故障注入到加密过程中产生的大量随机错误密文，通过统计关系，可以计算出部分解密过程的中间状态值，再利用中间状态的统计分布规律，最终恢复出密钥. 在 AES 算法的分析过程中，攻击者将故障注入在倒数第二轮，使用汉明重量、极大似然估计等区分器，可以成功破译出 128 比特主密钥. 2016 年，Dobraunig 等学者[33]在硬件上实现了统计故障分析针对 AES 密码构造的认证加密算法. 近年来，Li 等学者[31,34-35]针对 LED、Piccolo 和 PRESENT 等轻量级密码算法应用统计故障分析方法进行了安全性研究，研究结果为分析不同结构的轻量级密码安全性提供了重要的参考. 此外，机器学习和深度学习在轻量级密码分析领域也取得了快速发展. 2019 年，Anubhab 等学者[36]提出了基于深度学习的 SPECK 密码的分析方法，使用残差网络，在 8 轮 SPECK-32/64 上训练了基于神经网络的区分器，降低了寻找区分器的复杂性. 2021 年，Wang 等学者[37]将机器学习技术拓展到相关密钥差分区分器，破译了缩减轮 SPECK-32/64 和 PRESENT-64/80. 2023 年，Yusuke 等学者[38]提出了一种针对 PRESENT 密码的基于深度学习的侧信道分析，成功破解了所有轮密钥.

本文针对 Pyjamask 密码的结构设计及实现特性，充分结合不可能关系以及统计故障分析的特点，提出不可能统计故障分析方法，进一步扩展了唯密文攻击的故障分析种类. 表 2 总结了统计故障分析和不可能统计故障分析破译 Pyjamask-96/128 密码的对比结果. 不可能统计故障分析进一步被应用到 SUNDAE-GIFT 认证加密算法上. 并且，本文还设计并构建了新型区分器 Wasserstein 距离-汉明重量和 Wasserstein 距离-极大似然估计，与已有矩估计-汉明重量-极大似然估计、汉明重量和极大似然估计区分器相比，在准确度、故障数和耗时方面均具有优势，性能得到较大提升[39].

表 2　统计故障分析和不可能统计故障分析方法破译 Pyjamask-96/128 主密钥结果对比

区分器	统计故障分析(SFA)			不可能统计故障分析(ISFA)		
	故障数/个	耗时/ms	成功率/%	故障数/个	耗时/ms	成功率/%
汉明重量(HW)	2176/2208	126.08/325.12	99/99	1120/1440	64.96/150.08	99/99
极大似然估计(MLE)	2176/2144	120.00/329.92	99/99	1280/1376	70.08/164.80	99/99
矩估计-汉明重量-极大似然估计(MME-HW-MLE)	1824/1888	118.36/324.80	99/99	1248/1344	66.78/154.88	99/99
Wasserstein 距离-极大似然估计(WD-MLE)	1696/1344	100.16/240.00	99/87	1152/1184	69.44/150.80	99/99
Wasserstein 距离-汉明重量(WD-HW)	1600/1728	95.04/299.84	99/99	1024/1120	59.84/140.16	99/99

3　Pyjamask 密码

3.1　符号说明

设 Z_2^e 为 e 比特的二进制向量集；

记 $X\in(Z_2^{32})^u$ 和 $Y\in(Z_2^{32})^u$ 分别为 96、128 比特的明文和密文，且 $u\in[3,4]$；

记 $K\in(Z_2^{32})^4$ 为主密钥；$RK_i\in(Z_2^{32})^4$ 为第 $i+1$ 轮的轮密钥，其中 $i\in[0,13]$，RK_{14} 为白化密钥；

记 ARK 为轮密钥加，AC 为常数加，SB 为 S 盒替换，MR 为行变换，MC 为列变换；ARK^{-1}、AC^{-1}、SB^{-1}、MR^{-1} 和 MC^{-1} 分别为 ARK、AC、SB、MR 和 MC 的逆运算；

记 $A_i\in(Z_2^{32})^u$、$B_i\in(Z_2^{32})^u$ 和 $C_i\in(Z_2^{32})^u$ 分别为第 $i+1$ 轮 ARK、SB 和 MR 运算后 96、128 比特的状态值，其中 $i\in[0,13]$，$u\in[3,4]$；

记 $\|$ 和 $\oplus$ 分别为级联和按位异或运算，Σ 和 Π 分别表示连加和连乘，inf 表示取下界；

记～为元素受故障影响后的符号；

记 0b 表示二进制比特，0^z 表示长度为 z 的全零二进制串.

3.2　Pyjamask 算法描述

Pyjamask 密码采用代换置换网络结构，包含两个版本：Pyjamask-96 和 Pyjamask-128，分组长度分别为 96 比特和 128 比特，使用的 S 盒分别为 s_3 和 s_4，密钥长度均为 128 比特，迭代 14 轮，如表 3 所示. 两个版本的中间状态分别表示为 3×32 和 4×32 的二维阵列. Pyjamask 密码由加密、解密和密钥扩展三部分组成，其中解密是加密的逆运算，如图 1 所示. 算法 1 和 2 分别给出了加密算法以及密钥扩展算法. Pyjamask 算法的设计旨在减少密码部件中的非线性门数量，以及高阶掩码的软件实现，提高侧信道攻击防御能力.

表 3　各版本 Pyjamask 算法简介

版本	分组长度/比特	密钥长度/比特	迭代轮数/轮
Pyjamask-96	96	128	14
Pyjamask-128	128	128	14

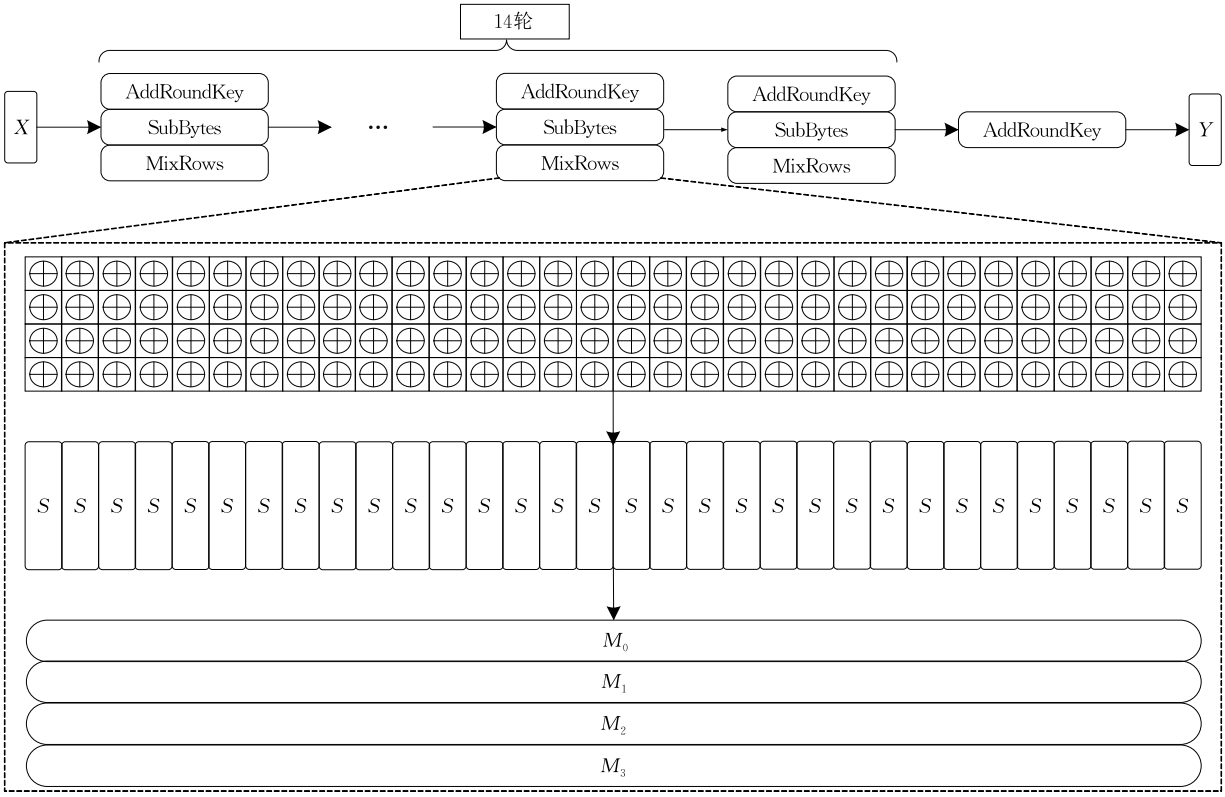

图 1 Pyjamask 算法结构

加密算法中的轮变换由三部分组成,具体为

(1)轮密钥加(ARK). 轮密钥逐比特异或到中间状态.

(2)S 盒替换(SB). 对中间状态每一列做替换,Pyjamask-96 和 Pyjamask-128 分别使用 s_3 和 s_4,如表 4 所示.

表 4 Pyjamask-96/128 的 S 盒

输入	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$s_3(x)$	1	3	6	5	2	4	7	0	—	—	—	—	—	—	—	—
$s_4(x)$	2	d	3	9	7	b	a	6	e	0	f	4	8	5	1	c

(3)行变换(MR). 对于状态值的每行左乘 32 阶方阵,4 个 32 阶方阵定义如下:

$$M_0=cir([1,1,0,1,0,0,0,0,1,0,0,0,0,1,0,0,0,0,1,1,0,0,0,0,1,1,1,0,0,0,1,0])$$

$$M_1=cir([0,1,0,0,0,0,1,0,0,0,0,0,0,1,1,1,0,1,0,0,0,0,0,1,0,1,1,0,0,0,1,1])$$

$$M_2=cir([0,0,0,0,0,0,0,0,1,0,1,0,0,1,1,1,1,0,0,1,1,0,1,0,0,1,0,0,1,0,1,1])$$

$$M_3=cir([0,1,1,0,0,1,0,0,0,0,0,0,1,0,0,1,0,1,0,1,0,0,1,0,1,0,0,0,1,0,0,1])$$

其中,对于向量 $\boldsymbol{V}\in\{0,1\}^{32}$,$cir(\boldsymbol{V})$表示由 $\boldsymbol{V}$ 定义的 32×32 的矩阵,矩阵第 j 行由向量 $\boldsymbol{V}$ 循环右移 j 位得到,其中 $j\in[0,31]$.

算法 1. Pyjamask 密码的加密算法.

输入:明文 X,轮密钥 $RK_0,RK_1,\cdots,RK_{13},RK_{14}$

输出:密文 Y

1. $L=X$;
2. FOR $i=0$ To 13 DO
3. $\quad L=MR(SB(L\oplus RK_i))$;
4. END FOR
5. $Y=L\oplus RK_{14}$;
6. RETURN Y.

算法 2. Pyjamask 的密钥扩展算法.

输入:主密钥 K

输出:轮密钥 $RK_0,RK_1,\cdots,RK_{13},RK_{14}$

1. $L=K$;
2. $RK_0=L$;
3. FOR $i=0$ To 13 DO
4. $\quad L=AC(MR(MC(L)))$;
5. $\quad RK_{i+1}=L$;
6. END FOR
7. RETURN $RK_0,RK_1,\cdots,RK_{13},RK_{14}$.

4 Pyjamask 的不可能统计故障分析

4.1 基本假设和故障模型

本文采用唯密文攻击的基本假设,即攻击者只需要截获随机密文,在实际攻击场景中,通过激光、

时钟毛刺和高强度电磁波等手段使密码芯片发生故障，从而达到篡改设备并使其执行一些错误操作以泄露秘密信息，攻击者无需关注和区分导入的故障是否有效，只需正常导入故障即可. 以 Pyjamask-128 版本为例，具体过程为，攻击者使用同一密钥加密一组随机明文，在加密过程中破坏半字节值使其产生随机错误，以“与”运算与中间状态相结合，从而产生错误密文.

通常情况下，半字节中间状态满足均匀分布，每个可能值出现的概率均为 6.25%. 在故障注入之后，中间状态各比特位为“0”和“1”的概率由原来的 50%和 50%变为 75%和 25%，半字节中间状态概率满足：

$$\left(\frac{3}{4}\right)^{n-\mathrm{HW}(l)}\cdot\left(\frac{1}{4}\right)^{\mathrm{HW}(l)}=\frac{3^{n-\mathrm{HW}(l)}}{4^n},$$

其中，n 表示注入故障的比特数，l 为中间状态所有可能取值，HW(·)为汉明重量. 本文采用半字节故障模型，$l\in[0,15]$，$\mathrm{HW}(l)\in[0,4]$，$n=4$. 根据“与”运算特点，当且仅当两个比特输入均为 1，比特输出为 1，否则结果为 0. 所以，任何中间状态和 $0b1111$ 做按位“与”运算，不改变原始中间状态值. 此时，中间状态值没有发生错误，相当于无效故障注入，因此，每种中间状态的数量和半字节中间状态总数量分别减少 1 和 2^n，半字节中间状态概率满足：

$$P_l=\frac{3^{n-\mathrm{HW}(l)}-1}{4^n-2^n},$$

其中，P_l 为中间状态值 l 出现的理论概率，受故障影响后的半字节分布律如图 2 所示.

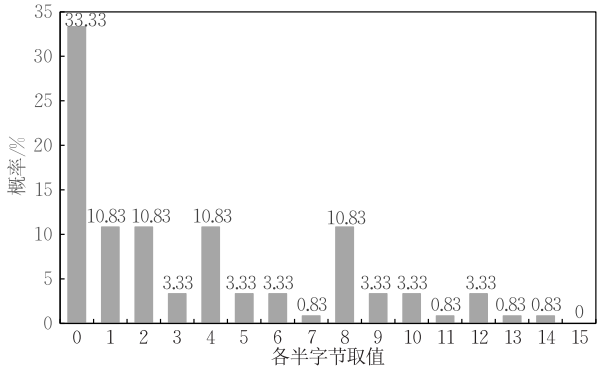

图 2　受故障影响后的半字节分布律

4.2　不可能关系分析

自 1999 年以来，国内外密码学者利用不可能关系设计了不可能差分分析、不可能差分故障分析等多种方法评测对称密码的安全性. Biham 等学者于 1999 年首次提出了不可能差分分析，并应用于 Skipjack 和 IDEA 等密码的分析中[40-41]. 2005 年，Biham 等学者[42]提出了不可能差分故障分析方法，并且破译了流密码 RC4 算法，降低了攻击复杂度. 2008 年，吴文玲等学者[43]系统地研究了不可能分析关系、不可能差分分析的原理和常用技巧方法. 2011 年，Derbez 等学者[44]提出针对 AES 密码的不可能差分故障分析，并成功恢复出全部密钥. 2019 年，Sadeghi 等学者[45]提出了相关密钥不可能差分分析，并利用中间相错策略破译了 SIMECK 算法. 2022 年，Du 等学者[46]通过构建 6 轮的不可能差分区分器，提出了一种针对 QARMA 算法的相关调柄不可能差分攻击，成功实现了 10 轮密钥以及白化密钥的恢复. 2023 年，Pal 等学者[47]提出了一种基于集群的不可能差分密码分析方法，破译了 5 轮缩减 AES 算法.

在经典的不可能差分故障分析中，攻击者仅能实现选择明文攻击的基本假设. 在传统的统计故障分析中，故障数较多，且分析密码所需的时空开销显著增加，在现实环境中易受到物联网环境中硬件设施的限制. 为了有效解决上述问题，本节结合不可能关系策略和统计故障分析的优势，降低对攻击者的能力要求，采用唯密文攻击的基本假设，同时设计了新型区分器，进一步降低了故障数、耗时和时空开销.

不可能统计故障分析的攻击原理可以概括为利用概率为 0 的不可能关系以及导入故障后的不均匀分布，排除错误的候选密钥值，从而恢复正确密钥. 实现不可能统计故障分析主要包括构造不可能关系和密钥筛选. 基于不可能关系，密钥候选空间被进一步筛选缩小，结合不均匀分布性质，即可恢复出正确

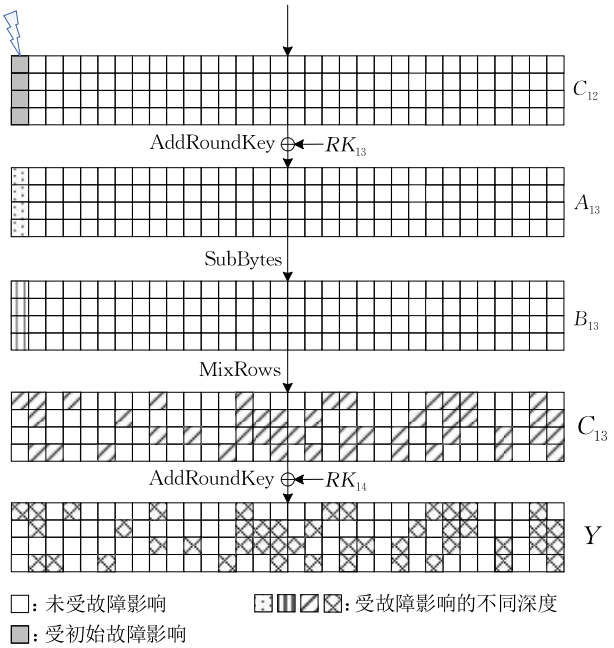

图 3　Pyjamask 算法故障传播路径图

密钥. 以图 3 所示的故障传播路径为例,攻击者通过受故障影响的错误密文倒推出中间状态值 $\tilde{C}_{12}$,存在以下不可能关系:

$$(\tilde{c}_{12,0+j}\tilde{c}_{12,32+j}\tilde{c}_{12,64+j}\tilde{c}_{12,96+j}) \nrightarrow (0b1111),$$

其中,$\tilde{c}_{i,\varepsilon}$ 表示第 $i+1$ 轮 MR 运算后状态值中的第 ε 比特,$i\in[0,13]$,$j\in[0,31]$,$\varepsilon\in[0,127]$. 攻击者利用不可能关系缩小密钥搜索空间,加速破译密钥.

4.3 攻击步骤

第 4.3 节提出的不可能统计故障分析,主要包括以下 4 个步骤:

步骤 1. 故障注入. 在 Pyjamask 算法运行加密过程中,攻击者在倒数第二轮随机注入故障破坏半字节值,生成受故障影响的随机错误密文. 以图 3 故障传播路径为例,每格代表一个比特位,不同的花纹表示受故障影响的不同轮数深度. 攻击者已知故障密文 $\tilde{Y}$,通过枚举中间状态 $MR^{-1}(RK_{14})$ 中的 4 比特以及轮密钥 RK_{13} 中的 4 比特来逆向推导出导入故障位置的中间状态值,即

$$\begin{aligned}\tilde{C}_{12}&=RK_{13}\oplus(SB^{-1}(MR^{-1}(RK_{14}\oplus\tilde{Y})))\\&=RK_{13}\oplus(SB^{-1}(MR^{-1}(RK_{14})\oplus MR^{-1}(\tilde{Y})))\\&=(rk_{13,0}\|0^{31}\|rk_{13,32}\|0^{31}\|rk_{13,64}\|0^{31}\|rk_{13,96}\|0^{31})\oplus\\&\quad(SB^{-1}(MR^{-1}(rk_{14,0}\|0^{31}\|rk_{14,32}\|0^{31}\|rk_{14,64}\|0^{31}\|\\&\quad rk_{14,96}\|0^{31})\oplus MR^{-1}(\tilde{Y}))),\end{aligned}$$

其中,$rk_{i,\varepsilon}$ 表示第 $i+1$ 轮轮密钥中的第 ε 比特值,$rk_{14,\varepsilon}$ 表示白化密钥中的第 ε 比特值,$i\in[0,13]$,$\varepsilon\in[0,127]$.

步骤 2. 不可能关系分析. 攻击者在倒数第二轮中任意位置多次导入故障,利用错误密文推导出故障注入所在的中间状态值,即

$$\begin{aligned}\tilde{C}_{12}&=RK_{13}\oplus(SB^{-1}(MR^{-1}(RK_{14}\oplus\tilde{Y})))\\&=RK_{13}\oplus(SB^{-1}(MR^{-1}(RK_{14})\oplus MR^{-1}(\tilde{Y})))\\&=(rk_{13,0+j}\|0^{31}\|rk_{13,32+j}\|0^{31}\|rk_{13,64+j}\|0^{31}\|rk_{13,96+j}\|\\&\quad 0^{31})\oplus(SB^{-1}(MR^{-1}(rk_{14,0+j}\|0^{31}\|rk_{14,32+j}\|0^{31}\|\\&\quad rk_{14,64+j}\|0^{31}\|rk_{14,96+j}\|0^{31})\oplus MR^{-1}(\tilde{Y}))),\end{aligned}$$

其中,$j\in[0,31]$. 结合按位“与”运算的特性,注入故障位置的半字节中间状态值不可能为 $0b1111$,从而产生了一条不可能分析路径:

$$(\tilde{c}_{12,0+j}\tilde{c}_{12,32+j}\tilde{c}_{12,64+j}\tilde{c}_{12,96+j})\oplus(0b1111)\neq 0.$$

利用概率为 0 的不可能分析路径,提前排除部分错误的候选密钥,从而有效缩减密钥搜索空间,加快分析效率,其中,$\tilde{c}_{i,\varepsilon}$ 表示第 $i+1$ 轮 MR 运算后状态值中的第 ε 比特,$i\in[0,13]$,$\varepsilon\in[0,127]$.

步骤 3. 区分器筛选. 根据步骤 1 和 2 所获取的每一组 $\tilde{C}_{12}$ 中的 4 比特,即 $\tilde{c}_{12}^{0+j}$、$\tilde{c}_{12}^{32+j}$、$\tilde{c}_{12}^{64+j}$ 和 $\tilde{c}_{12}^{96+j}$,攻击者选取第 4.4 节中的区分器,计算出区分器值,并选取其最大值或最小值所对应的密钥候选值,即为正确密钥. 通过重复前三个步骤,便可获取 RK_{14} 和 RK_{13} 的全部比特.

步骤 4. 主密钥恢复. 攻击者根据步骤三获取的轮密钥 RK_{14},可以依次推导 RK_i,其中 $i\in[0,13]$,根据 Pyjamask 密钥编排算法可得主密钥为

$$K=RK_0.$$

具体求解过程如算法 3 所示.

算法 3. Pyjamask 主密钥恢复算法.

输入:白化密钥 RK_{14}

输出:主密钥 K

1. $L=RK_{14}$;
2. FOR $i=13$ To 0 DO
3. $\quad L=MC^{-1}(MR^{-1}(AC^{-1}(L)))$;
4. $\quad RK_i=L$;
5. END FOR
6. $K=RK_0$;
7. RETURN K

4.4 区分器

统计故障分析常常利用汉明重量、极大似然估计等区分器来计算区分候选密钥的真假[30]. 本节基于 Wasserstein 距离,设计了两种新型区分器 Wasserstein 距离-汉明重量和 Wasserstein 距离-极大似然估计.

4.4.1 经典区分器

(1)汉明重量(Hamming Weight,HW)

汉明重量是由 Reed[48] 在 1954 年提出的数学分析方法. 后被广泛使用在密码分析中,由于按位与运算的特点,导入故障之后“0”的数量增多,“1”的数量减少,所以可以通过计算二进制串中“1”的个数来区分不同的轮密钥,其中最小值对应于正确的轮密钥. 表达式为

$$\mathrm{HW}=\frac{1}{f}\sum_{\alpha=0}^{f-1}\mathrm{HW}(l_\alpha)=\frac{1}{f}\sum_{\alpha=0}^{f-1}\sum_{\beta=0}^{n-1}l_{\alpha\beta}.$$

其中,n 表示注入故障的比特数,l_α 表示注入第 α 个故障后的中间状态值,$l_{\alpha\beta}$ 表示中间状态值 l_α 的第 β 位,f 为故障数,半字节故障模型下 $n=4$,且 $\alpha\in[0,f-1]$,$\beta\in[0,4]$.

(2)极大似然估计(Maximum Likelihood Estimation,MLE)

Wilks[49] 于 1938 年提出了极大似然估计方法用于估计概率模型的参数,广泛应用于统计学、机器学习等众多领域中. 在密码学领域,Fuhr 等学者[30] 提出了一种极大似然估计区分器,获得概率模型中观测数据出现概率最大的参数值,从而提高破译密钥的可能率,表达式为

$$\mathrm{MLE}=\prod_{l=0}^{15}(P_l)^{Q_l\cdot f}.$$

其中，f 代表故障数，P_l 为中间状态值 l 出现的理论概率，Q_l 为中间状态值 l 出现的实际概率，且 $l\in[0,15]$.

(3) 矩估计-汉明重量-极大似然估计(Method of Moment Estimation-Hamming Weight-Maximum Likelihood Estimation，MME-HW-MLE)

矩估计的概念最早是由英国统计学家卡尔·皮尔逊(Karl Pearson)于 1894 年提出的，是一种统计参数估计方法，它基于样本矩来估计总体参数. Li 等学者[34]于 2021 年提出了 MME-HW-MLE 区分器，以更高的效率破译了 Piccolo 密码算法. 该区分器结合了 MME、HW 和 MLE 区分器的优点，MME 区分器以参数估计中的矩估计作为基础. 攻击者首先计算出每组中间状态的一阶矩，表达式为

$$\mathrm{MME}=\frac{1}{f}\sum_{l=0}^{f-1}(l\cdot Q_l\cdot f),$$

其中，f 为故障数，l 为注入故障后中间状态所有可能取值，Q_l 为中间状态值 l 出现的实际概率，筛选出一阶矩值较小的部分候选密钥，接着用汉明重量进一步缩小密钥空间，最后再利用极大似然估计挑选出最大值所对应的候选密钥.

4.4.2　新型区分器

Wasserstein 距离是一种被广泛用于图像处理、自然语言处理和机器学习等领域的指标，用于衡量两个概率分布之间的距离[39]. 因此，该距离可以看作是将一个分布变换成另一个分布所需的最小代价，表达式为

$$\mathrm{WD}=\inf_{\gamma\in\Gamma(\eta,\theta)}E_{(P_l\cdot f,Q_l\cdot f)\in\gamma}(\|P_l\cdot f-Q_l\cdot f\|),$$

其中，f 为故障数，l 为注入故障后中间状态所有可能取值，η 表示中间状态值的理论分布，θ 表示导入故障后中间状态值的实际分布，$\Gamma(\eta,\theta)$ 是 η 和 θ 之间的所有联合分布集合，γ 是属于 $\Gamma(\eta,\theta)$ 的联合分布，P_l 为中间状态值 l 出现的理论概率，Q_l 为中间状态值 l 出现的实际概率，$E(\cdot)$ 表示数学期望，$\|\cdot\|$ 表示距离. 通过使用 Wasserstein 距离，可以计算每个候选密钥所对应的概率分布与目标概率分布之间的距离. 距离值越小表示两个概率分布越相似，因此可以通过筛选出距离最小的候选密钥来确定正确的密钥.

(1) Wasserstein 距离-汉明重量(Wasserstein Distance-Hamming Weight，WD-HW)

WD-HW 区分器结合了 Wasserstein 距离和极大似然估计二者的优点，先利用 Wasserstein 距离筛选出较小值所对应的部分密钥候选值，缩减候选密钥空间，再利用汉明重量区分器计算出最小值，其对应的密钥候选值为正确密钥，汉明重量表达式见第 4.4.1 节.

(2) Wasserstein 距离-极大似然估计(Wasserstein Distance-Maximum Likelihood Estimation，WD-MLE)

WD-MLE 区分器结合了 Wasserstein 距离和极大似然估计二者的优点，首先计算出各组状态的 Wasserstein 距离，排除较大值所对应的候选密钥，缩减密钥搜索空间，在此基础上利用极大似然估计在剩余的候选密钥中计算出最大值，其对应的候选密钥值一般为正确密钥，极大似然估计表达式见第 4.4.1 节.

表 5 给出了本文所使用区分器取值情况以及筛选过程说明.

表 5　各区分器的取值和筛选过程说明

区分器	取值范围	筛选过程
HW	最小值	评估中间状态的汉明重量，选取最小值对应的候选密钥
MLE	最大值	评估中间状态的极大似然估计值，选取最大值对应的候选密钥
MME-HW-MLE	MME 最小值 HW 最小值 MLE 最大值	先选出 MME 最小值对应的部分候选密钥，接着选择 HW 最小值对应的候选密钥，最后选择 MLE 最大值对应的候选密钥
WD-HW	WD 最小值 HW 最小值	先选出 WD 最小值对应的部分候选密钥，再选择 HW 最小值对应的候选密钥
WD-MLE	WD 最小值 MLE 最大值	先选出 WD 最小值对应的部分候选密钥，再选择 MLE 最大值对应的候选密钥

5　Pyjamask 算法的实验分析

本实验在 PC 端(CPU 为 Intel Core i7-8550U，1.80 GHz，内存为 8 GB)上，使用 C++编程语言来模拟加密、随机故障导入以及分析密钥过程. 选取轮密钥的 4 比特为实验数据单元，使用故障数、耗时、准确度、成功率以及复杂度来衡量不同故障分析方法以及不同区分器的攻击效果. 数据基于 10 000 次实验的平均值. 实验数据见附录表 A1、A2 和 A3.

5.1　故障数

故障数是指分析密钥达到最大概率时所需的最小导入故障数量. 具体地，本文中指统计故障分析和不可能统计故障分析利用不同区分器以最大概率破译 Pyjamask 算法的最小故障数. 表 2 统计了统计故障分析和不可能统计故障分析方法破译 Pyjamask 两个版本完整主密钥所需要的总故障数. 图 4 统计了两种分析方法破译 Pyjamask-128 版本的主密钥

所需要的故障数，对于经典的统计故障分析，HW、MLE、MME-HW-MLE、WD-MLE 和 WD-HW 区分器分别需要 2208、2144、1888、1344 和 1728 个故障以最大概率分析 128 比特主密钥；对于不可能统计故障分析，HW、MLE、MME-HW-MLE、WD-MLE 和 WD-HW 区分器则分别只需要 1440、1376、1344、1184 和 1120 个故障. 由此可见，不可能统计故障分析相比统计故障分析，在故障数上具有优势，并且新型区分器 WD-HW 和 WD-MLE 相比已有区分器 HW、MLE 和 MME-HW-MLE，故障数进一步被降低.

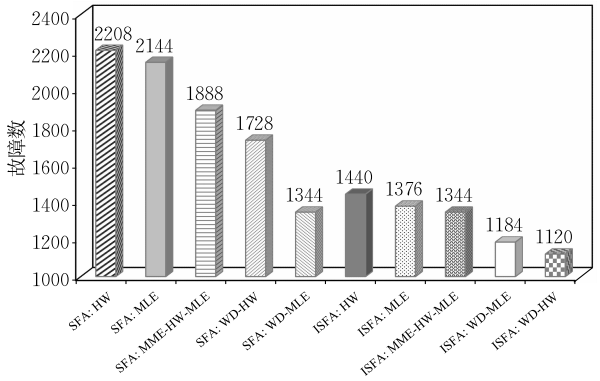

图 4 统计故障分析和不可能统计故障分析方法破译 Pyjamask-128 版本主密钥的故障数

5.2 准确度

均方根误差(Root Mean Square Error，RMSE)是一种统计量，用于衡量预测值与真实值之间的偏差程度. RMSE 可以用来评估不同故障分析方法以及不同区分器的性能，它的值越小，说明预测结果与真实结果越接近，RMSE 的表达式为

$$\mathrm{RMSE}=\sqrt{\frac{1}{\theta}\sum_{\varphi=0}^{\theta-1}(\Phi(\varphi)-1)^2},$$

其中，θ 表示实验次数，$\Phi(\varphi)$ 表示第 φ 次实验获取轮密钥候选值的实验个数. 理论上，正确密钥个数为 1. 以 Pyjamask-128 为例，图 5 展示了不同故障分析方法、不同区分器以及不同故障数破译部分轮密钥时的 RMSE，其值越小，表示效果越好. 横轴代表故障数，纵轴表示故障分析方法，竖轴表示 RMSE 值. 与统计故障分析相比，不可能统计故障分析准确度值趋向零的速度更快，说明该方法恢复密钥的准确度更高. 并且新型区分器 WD-HW 和 WD-MLE 相比已有的 HW、MLE 和 MME-HW-MLE 区分器，趋于零的速率更快，准确度有明显的优化.

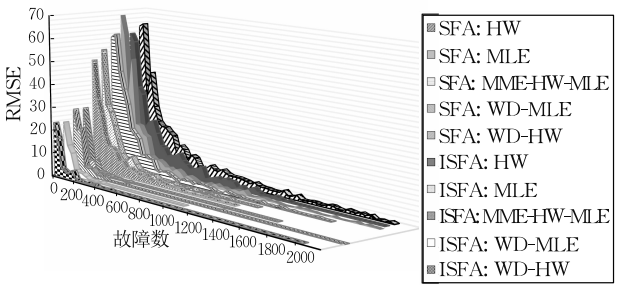

图 5 统计故障分析和不可能统计故障分析方法恢复 Pyjamask-128 版本主密钥的准确度

在不可能统计故障分析方法中，利用不可能关系排除候选密钥是一项关键任务. 以 Pyjamask-128 版本为例，表 6 给出了不可能统计故障分析利用不可能关系在不同故障数下排除候选密钥的比例. 数据变化趋势表明，排除候选密钥的比例随着故障数的增加而不断增长.

表 6 不同故障数下不可能关系排除密钥比例

故障数	比例/%
200	16.13
600	50.25
1000	62.35
1400	67.75
1800	73.31
2200	76.44

图 6 呈现了统计故障分析和统计不可能故障分析在经过不同的区分器筛选之后，剩余的密钥数量随故障数的变化趋势. 横轴表示故障数，纵轴表示 10000 次实验中剩余密钥数量的总和. 以不可能统计故障分析使用 HW 和 WD-HW 区分器为例，根据图 6 中的数据，当故障数为 300、600 和 900 时，HW 剩余候选密钥的比例分别为 2.03%、0.52%和 0.45%；WD-HW 剩余密钥的比例分别为 1.20%、0.40%和 0.39%，由此可见，基于 Wasserstein 距离的新型区分器相比经典区分器剩余候选密钥数量更少，即过滤数量更多，破译准确度更高.

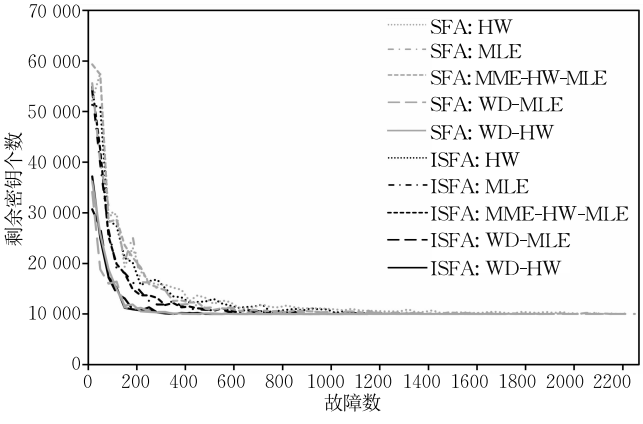

图 6 统计故障分析和不可能统计故障分析方法经不同区分器筛选后的剩余密钥数量

5.3　成功率

成功率是指在尝试一定次数或时间内，成功分析出密钥的概率或比例. 具体地，本文中指两种不同的故障分析方法成功恢复 Pyjamask 算法 128 比特主密钥的概率，以 Pyjamask-128 为例，图 7 给出了统计故障分析和不可能统计故障分析在不同区分器和不同故障数下所对应的成功率. 其中，纵轴表示破译密钥成功率，横轴代表导入的故障数量，不同折线代表不同分析方法利用不同区分器成功率的变化趋势. 对于统计故障分析，HW、MLE、MME-HW-MLE 和 WD-HW 四种区分器破译密钥成功率可达到 99% 以上，WD-MLE 区分器成功率最高为 87%；对于不可能统计故障分析，以上五种区分器破译密钥成功率均可达到 99%以上，并且速度相比统计故障分析更快，即所需故障数更少；新型 WD-MLE 和 WD-HW 区分器在成功率方面也优于区分器 HW、MLE 和 MME-HW-MLE.

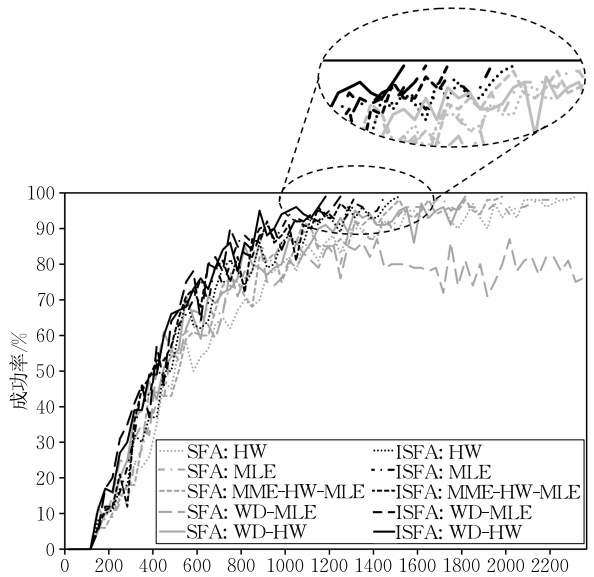

图 7　统计故障分析和不可能统计故障分析方法恢复 Pyjamask-128 版本主密钥的成功率

5.4　耗　时

耗时是指不同故障分析方法使用不同区分器破译密钥所需要的时间，主要包括故障导入、收集密文、逆推中间状态值、不可能关系分析和区分器筛选. 表 2 总结了统计故障分析和不可能统计故障分析使用不同区分器破译 Pyjamask-96/128 算法主密钥所需要的总时间. 图 8 给出了破译 Pyjamask-128 版本 128 比特主密钥所需时间伴随导入故障数变化的关系，横轴代表导入的故障数，纵轴代表在某一故障数下各方法的时间堆积. 不可能统计故障分析利用 HW、MLE、MME-HW-MLE、WD-MLE 和 WD-HW 区分器破译主密钥所需的时间分别为 150.08、164.80、154.88、150.80 和 140.16 ms，而统计故障分析利用以上五个区分器破译主密钥分别需要 325.12、329.92、334.80、334.72 和 299.84 ms. 由此可见，不可能统计故障分析在耗时方面优于统计故障分析，新型 WD-HW、WD-MLE 区分器也优于 HW、MLE 和 MME-HW-MLE 区分器.

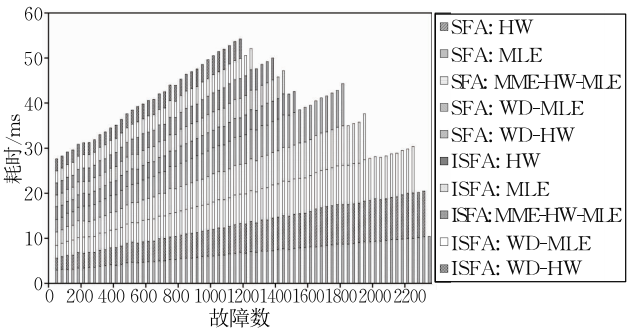

图 8　统计故障分析和不可能统计故障分析方法恢复 Pyjamask-128 版本主密钥时间堆积

5.5　复杂度

时间复杂度、数据复杂度和存储复杂度可用破译 Pyjamask 密码算法处理数据所需要的时间、数据总量和占用的存储空间来衡量. 记故障数为 f，候选密钥个数为 v，区分器复杂度系数为 w，则数据复杂度可以计算为

$$f \cdot v,$$

时间复杂度可以计算为

$$f \cdot v \cdot w.$$

以经典统计故障分析方法利用汉明重量区分器破译 Pyjamask-128 版本主密钥为例，时间、数据和存储复杂度分别为

$$2208 \cdot 2^8 \cdot (2^4+1) = 2^{23.21},$$

$$2208 \cdot 2^8 = 2^{19.11},$$

$$2208 \cdot (2^7+2^3+2^{12}) = 2^{23.16}.$$

表 7 和表 8 分别给出了不可能统计故障分析和统计故障分析方法在破译 Pyjamask-96 和 Pyjamask-128 主密钥成功率达到最大时的各项复杂度. 相比统计故障分析，不可能统计故障分析在时间、数据和存储复杂度上都具有优势，并且新型区分器 WD-MLE

表 7　统计故障分析和不可能统计故障分析方法恢复 Pyjamask-96 版本 128 比特主密钥复杂度对比

区分器	统计故障分析			不可能统计故障分析		
	时间	数据	存储	时间	数据	存储
HW	$2^{21.17}$	$2^{17.09}$	$2^{20.42}$	$2^{20.22}$	$2^{16.13}$	$2^{19.46}$
MLE	$2^{21.17}$	$2^{17.09}$	$2^{20.42}$	$2^{20.41}$	$2^{16.32}$	$2^{19.66}$
MME-HW-MLE	$2^{24.50}$	$2^{18.83}$	$2^{22.87}$	$2^{23.96}$	$2^{18.29}$	$2^{22.32}$
WD-MLE	$2^{20.82}$	$2^{16.73}$	$2^{20.06}$	$2^{20.26}$	$2^{16.17}$	$2^{19.51}$
WD-HW	$2^{20.73}$	$2^{16.64}$	$2^{19.98}$	$2^{20.09}$	$2^{16.00}$	$2^{19.34}$

表 8 统计故障分析和不可能统计故障分析方法恢复 Pyjamask-128 版本 128 比特主密钥复杂度对比

区分器	统计故障分析			不可能统计故障分析		
	时间	数据	存储	时间	数据	存储
HW	$2^{23.21}$	$2^{19.11}$	$2^{23.16}$	$2^{22.58}$	$2^{18.49}$	$2^{22.54}$
MLE	$2^{23.11}$	$2^{19.02}$	$2^{23.07}$	$2^{22.51}$	$2^{18.43}$	$2^{22.47}$
MME-HW-MLE	$2^{24.56}$	$2^{18.88}$	$2^{22.92}$	$2^{24.06}$	$2^{18.39}$	$2^{22.43}$
WD-MLE	$2^{22.48}$	$2^{18.39}$	$2^{22.44}$	$2^{22.38}$	$2^{18.21}$	$2^{22.26}$
WD-HW	$2^{22.92}$	$2^{18.75}$	$2^{22.80}$	$2^{22.30}$	$2^{18.13}$	$2^{22.18}$

和 WD-HW 相比于已有 MLE、HW 和 MME-HW-MLE 区分器，时间、数据和存储复杂度均有降低.

综合以上各项指标，针对 Pyjamask 密码，不可能统计故障分析相较于已有的统计故障分析方法在准确度、成功率、故障数、耗时和复杂度等指标方面均具有优势；新型区分器 WD-HW 和 WD-MLE 表现较优秀.

6 SUNDAE-GIFT 的不可能统计故障分析

在本节中，我们将提出的不可能统计故障分析和新型区分器应用于 SUNDAE-GIFT 算法中[11].

6.1 SUNDAE-GIFT 算法描述

SUNDAE 认证加密模式是由 Banik 等学者[11]于 2018 年对称密码学期刊中提出的. 该算法由初始化、处理关联数据、加解密和生成验证标签组成. 记初始向量为 $\boldsymbol{IV}$、关联数据为 AD、明文消息为 X，密文为 Y 和标签为 tag. SUNDAE-GIFT 核心算法 E_K 选用了密钥长度为 128 比特的 GIFT 轻量级分组密码，分组长度也为 128 比特，整体结构参见图 9[11]. 图中 Pad 为填充函数，⊙为常数乘运算，常数为 m，且 $m\in\{2,4\}$. GIFT 密码采用代换置换网络结构，共 40 轮. 每轮轮函数由 S 盒替代、P 置换和轮密钥加运算组成. 当前，除了传统的密码分析之外，还有对 SUNDAE-GIFT 算法的碰撞故障分析和统计故障分析[17-22]. 总结如表 9 所示.

表 9 SUNDAE-GIFT 算法的安全性分析总结

分析类型	基本假设	攻击轮数	文献
碰撞故障分析	选择明文攻击	40	[21]
统计故障分析	唯密文攻击	40	[22]
不可能统计故障分析	唯密文攻击	40	本文

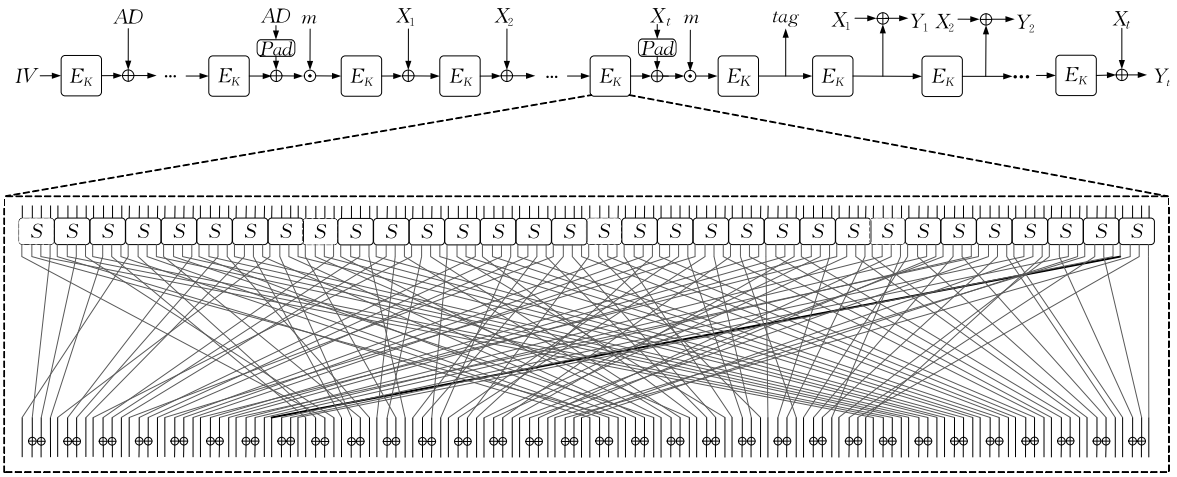

图 9 SUNDAE-GIFT 算法结构

6.2 SUNDAE-GIFT 的不可能统计故障分析

针对 SUNDAE-GIFT 的分析采用与 Pyjamask 算法相同的基本假设和故障模型. 攻击者在倒数第二轮注入半字节随机故障，通过不可能关系和区分器筛选出倒数第二轮密钥中的 2 比特以及最后一轮密钥中的 8 比特. 然后，他们通过连续的故障注入，可以获取最后两轮密钥的所有比特值，并结合密钥编排算法，恢复全部 128 比特主密钥.

图 10 展示了统计故障分析和不可能统计故障分析方法破译 SUNDAE-GIFT 算法主密钥所需要的故障数. 统计故障分析中的 HW、MLE、MME-HW-MLE、WD-MLE 和 WD-HW 区分器分别需要 576、608、592、560 和 544 个故障，能以最大成功率分析 128 比特主密钥；不可能统计故障分析分别仅需要 480、448、464、416 和 400 个故障，WD-MLE 和 WD-HW 区分器所需故障数较少.

图 11 和图 12 给出了统计故障分析和不可能统计故障分析在不同区分器和故障数下所对应的成功率和时间对比. 不可能统计故障分析达到 99%成功率的速度相比统计故障分析更快，HW、MLE、

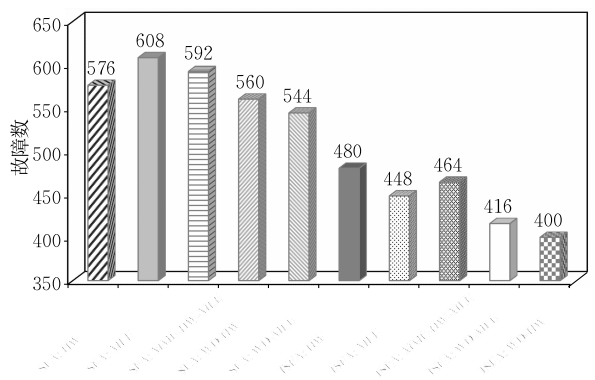

图 10　统计故障分析和不可能统计故障分析方法恢复 *SUNDAE-GIFT* 主密钥的故障数

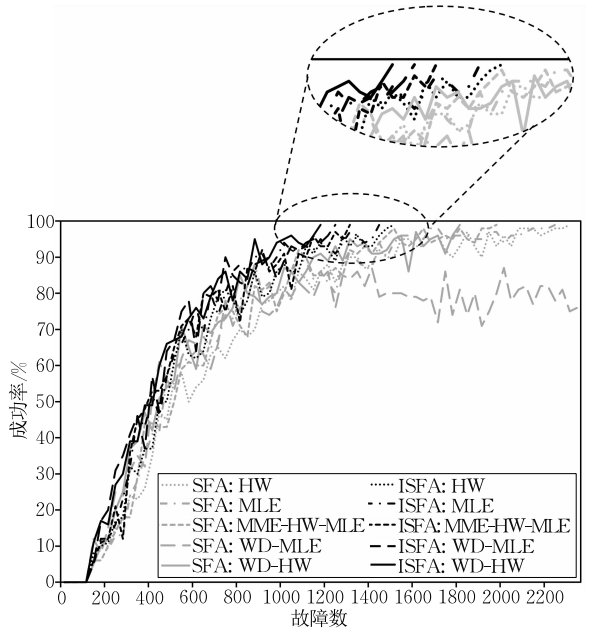

图 11　统计故障分析和不可能统计故障分析方法恢复 *SUNDAE-GIFT* 主密钥的成功率

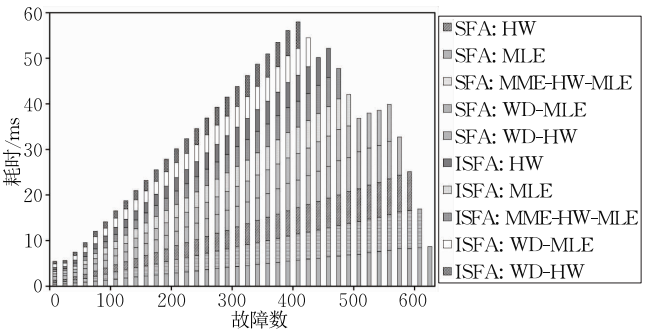

图 12　统计故障分析和不可能统计故障分析方法恢复 *SUNDAE-GIFT* 主密钥的时间堆积

MME-HW-MLE、WD-MLE 和 WD-HW 区分器的时间分别为 6.38、6.89、6.63、6.38 和 5.78 s，WD-MLE 和 WD-HW 区分器时间更少，完整实验数据如附录表 A4 和 A5 所示.

表 10 给出了破译主密钥成功率达到 99%时的时间、数据和存储复杂度的对比，可以看出不可能统计故障分析方法和新型区分器 WD-MLE 与 WD-HW 在 SUNDAE-GIFT 算法的分析上均具有优势.

表 10　统计故障分析和不可能统计故障分析方法恢复 SUNDAE-GIFT 算法 128 比特主密钥的复杂度对比

区分器	统计故障分析[22]			不可能统计故障分析		
	时间	数据	存储	时间	数据	存储
HW	$2^{23.26}$	$2^{19.17}$	$2^{21.30}$	$2^{22.99}$	$2^{18.91}$	$2^{20.95}$
MLE	$2^{23.19}$	$2^{19.25}$	$2^{21.26}$	$2^{22.89}$	$2^{18.81}$	$2^{20.86}$
MME-HW-MLE	$2^{24.88}$	$2^{19.21}$	$2^{21.26}$	$2^{24.53}$	$2^{18.86}$	$2^{20.94}$
WD-MLE	$2^{23.22}$	$2^{19.13}$	$2^{21.18}$	$2^{22.79}$	$2^{18.70}$	$2^{20.75}$
WD-HW	$2^{23.17}$	$2^{19.09}$	$2^{21.14}$	$2^{22.73}$	$2^{18.64}$	$2^{20.69}$

综合以上各项指标，针对 SUNDAE-GIFT 算法，不可能统计故障分析方法相比已有统计故障分析方法表现较佳；新型区分器 WD-HW 和 WD-MLE 相比已有区分器也具有优势.

7　结束语

本文针对轻量级分组密码 Pyjamask 和认证加密算法 SUNDAE-GIFT，在结合统计分析和不可能关系分析的基础上，提出了不可能统计故障分析方法，并构建了新型区分器 WD-HW 和 WD-MLE. 与经典的统计故障分析方法相比，该方法在故障数、成功率和时间消耗方面均有优化，不仅降低了密码算法的攻击代价而且提高了攻击效果. 由此可见，不可能统计故障分析同样对轻量级密码 Pyjamask 和 SUNDAE-GIFT 的安全性构成了威胁. 在使用 Pyjamask 和 SUNDAE-GIFT 算法时，需要考虑采取更多的安全措施. 该研究结果为轻量级密码算法的安全性提供了有价值的参考. 未来的研究方向将借鉴流密码等其他类型密码的分析方法，对新算法做更多的分析型故障分析.

参　考　文　献

[1] Chehab M, Mourad A. LP-SBA-XACML: Lightweight semantics based scheme enabling intelligent behavior-aware privacy for IoT. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 161-175

[2] Pant S, Sharma M, Sharma D K, et al. Enforcing intelligent learning-based security in Internet of Everything. IEEE Internet of Things Journal, 2023, 10(4): 3071-3078

[3] Naito Y, Sasaki Y, Sugawara T. Lightweight authenticated encryption mode suitable for threshold implementation//

Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques. Zagreb, Croatia, 2020: 705-735

[4] Choo K-K R. Internet of Things (IoT) security and forensics: Challenges and opportunities//Proceedings of the Workshop on CPS&-IoT Security and Privacy. Korea, 2021: 27-28

[5] Aryavalli S N G, Kumar H. Top 12 layer-wise security challenges and a secure architectural solution for Internet of Things. Computers and Electrical Engineering, 2023, 105: 108487

[6] Natarajan D, Dai W. SEAL-Embedded: A homomorphic encryption library for the Internet of Things. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2021, 2021(3): 756-779

[7] Guo Yi-Min, Zhang Zhen-Feng, Xiong Ping, et al. PUF-Based lightweight authentication protocols for fog assisted IoT. Chinese Journal of Computers, 2022, 45(7): 1412-1430(in Chinese)
(郭奕旻, 张振峰, 熊平等. 基于 PUF 的轻量级雾辅助物联网认证协议. 计算机学报, 2022, 45(7): 1412-1430)

[8] Jiao L, Feng D, Hao Y, et al. FAN: A lightweight authenticated cryptographic algorithm//Proceedings of the Cryptographers' Track at the RSA Conference. San Francisco, USA, 2021: 299-325

[9] Wu Wen-Ling, Sui Han, Zhang Bin. Lightweight Cryptography. Beijing: Tsinghua University Press, 2022(in Chinese)
(吴文玲, 眭晗, 张斌. 轻量级密码学. 北京: 清华大学出版社, 2022)

[10] Goudarzi D, Jean J, Kölbl S, et al. Pyjamask: Block cipher and authenticated encryption with highly efficient masked implementation. IACR Transactions on Symmetric Cryptology, 2020, 2020(S1): 31-59

[11] Banik S, Bogdanov A, Luykx A, et al. SUNDAE: Small universal deter-ministic authenticated encryption for the Internet of Things. IACR Transactions on Symmetric Cryptology, 2018, 2018(3): 1-35

[12] Dobraunig C, Rotella Y, Schoone J. Algebraic and higher-order differential cryptanalysis of Pyjamask-96. IACR Transactions on Symmetric Cryptology, 2020, 2020(1): 289-312

[13] Xu Ze-Yu. Automated Analysis of the Grouped Cryptographic Algorithm Pyjamask[M. S. dissertation]. Shandong University, Jinan, 2020(in Chinese)
(许泽雨. 分组密码算法 Pyjamask 的自动化分析[硕士学位论文]. 山东大学, 济南, 2020)

[14] Zhang X, Wei Y, Li L. New countermeasures against differential fault attacks//Proceedings of the International Conference on Internet of Things and Intelligent Applications. Zhenjiang, China, 2020: 1-5

[15] Liu Ya, Tang Wei-Ming, Shen Zhi-Yuan, et al. Impossible differential cryptanalysis of lightweight block cipher Pyjamask. Application Research of Computers, 2021, 38(10): 3428-3432(in Chinese)
(刘亚, 唐伟明, 沈致远等. 轻量级分组密码 Pyjamask 的不可能差分分析. 计算机应用研究, 2021, 38(10): 3428-3432)

[16] Cui J, Hu K, Wang Q, et al. Integral attacks on Pyjamask-96 and round-reduced Pyjamask-128//Proceedings of the Cryptographers' Track at the RSA Conference. San Francisco, USA, 2022: 223-246

[17] Zong R, Dong X, Chen H, et al. Towards key-recovery-attack friendly distinguishers: Application to GIFT-128. IACR Transactions on Symmetric Cryptology, 2021, 2021(1): 156-184

[18] Sun L, Wang W, Wang M. Linear cryptanalyses of three AEADs with GIFT-128 as underlying primitives. IACR Transactions on Symmetric Cryptology, 2021, 2021(2): 199-221

[19] Luo H, Chen W, Ming X, et al. General differential fault attack on PRESENT and GIFT cipher with nibble. IEEE Access, 2021, 9: 37697-37706

[20] Sasaki Y. Integer linear programming for three-subset meet-in-the-middle attacks: Application to GIFT//Proceedings of the International Workshop on Security. Sendai, Japan, 2018: 227-243

[21] Liu S, Guan J, Hu B. Fault attacks on authenticated encryption modes for GIFT. IET Information Security, 2022, 16(1): 51-63

[22] Zhu Xiao-Ming. Fault analysis of the authenticated encryption algorithm SUNDAE-GIFT. Intelligent Computer and Applications, 2023, 13(1): 72-76(in Chinese)
(朱晓铭. 认证加密算法 SUNDAE-GIFT 的故障分析. 智能计算机与应用, 2023, 13(1): 72-76)

[23] Feng J, Chen H, Li Y, et al. A framework for evaluation and analysis on infection countermeasures against fault attacks. IEEE Transactions on Information Forensics and Security, 2020, 15(2): 391-406

[24] Wang Yong-Juan, Fan Hao-Peng, Dai Zheng-Yi, et al. Advances in side channel attacks and countermeasures. Chinese Journal of Computers, 2023, 46(1): 202-228(in Chinese)
(王永娟, 樊昊鹏, 代政一等. 侧信道攻击与防御技术研究进展. 计算机学报, 2023, 46(1): 202-228)

[25] Boneh D, DeMillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Konstanz, Germany, 1997: 37-51

[26] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA, 1997: 513-525

[27] Zhang Lei, Wu Wen-Ling. Differential fault analysis on SMS4. Chinese Journal of Computers, 2006, 29(9): 1596-1602(in Chinese)

(张蕾，吴文玲. SMS4 密码算法的差分故障攻击. 计算机学报，2006，29(9)：1596-1602)

[28] Zhao Xin-Jie，Wang Tao，Guo Shi-Ze. An improved differential fault analysis on Camellia. Chinese Journal of Computers，2011，34(4)：613-627(in Chinese)
(赵新杰，王韬，郭世泽. 一种针对 Camellia 的改进差分故障分析. 计算机学报，2011，34(4)：613-627)

[29] Du S，Zhang B，Li Z，et al. Fault attacks on stream cipher scream//Proceedings of the International Conference on Information Security Practice and Experience. Beijing，China，2015：50-64

[30] Fuhr T，Jaulmes E，Lomne V，et al. Fault attacks on AES with faulty ciphertexts only//Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography. Los Alamitos，USA，2013：108-118

[31] Li W，Liao L，Gu D，et al. Ciphertext-only fault analysis on the LED lightweight cryptosystem in the Internet of Things. IEEE Transactions on Dependable and Secure Computing，2019，16(3)：454-461

[32] De Santis F，Guillen O M，Sakic E，et al. Ciphertext-only fault attacks on PRESENT//Proceedings of the International Workshop on Lightweight Cryptography for Security and Privacy. Istanbul，Turkey，2014：85-108

[33] Dobraunig C，Eichlseder M，Korak T，et al. Statistical fault attacks on nonce-based authenticated encryption schemes//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Hanoi，Vietnam，2016：369-395

[34] Li Wei，Li Jia-Yao，Gu Da-Wu，et al. Statistical fault analysis of the Piccolo lightweight cryptosystem. Chinese Journal of Computers，2021，44(10)：2104-2121(in Chinese)
(李玮，李嘉耀，谷大武等. 轻量级密码算法 Piccolo 的统计故障分析. 计算机学报，2021，44(10)：2104-2121)

[35] Li Wei，Zhu Xiao-Ming，Gu Da-Wu，et al. Meet-in-the-middle statistical fault analysis of the PRESENT lightweight cryptosystem. Chinese Journal of Computers，2023，46(2)：353-370(in Chinese)
(李玮，朱晓铭，谷大武等. PRESENT 轻量级密码的中间相遇统计故障分析. 计算机学报，2023，46(2)：353-370)

[36] Anubhab B. Classical and physical security of symmetric key cryptographic algorithms//Proceedings of the International Conference on Very Large Scale Integration. Singapore，2022：1-2

[37] Wang G，Wang G，He Y. Improved machine learning assisted (related-key) differential distinguishers for lightweight ciphers //Proceedings of the International Conference on Trust，Security and Privacy in Computing and Communications. Shenyang，China，2021：164-171

[38] Yusuke N，Shu T，Yoshiya I，et al. Deep learning based side-channel analysis for lightweight cipher PRESENT//Proceedings of the International Conference on Computer and Automation Engineering. Sydney，Australia，2023：570-574

[39] Panaretos V M，Zemel Y. Statistical aspects of wasserstein distances. Annual Review of Statistics and Its Application，2019，6(1)：405-431

[40] Biham E，Biryukov A，Shamir A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials//Proceedings of the International Conference on the Theory and Applications of Crypto-graphic Techniques. Prague，Czech Republic，1999：12-23

[41] Biham E，Biryukov A，Shamir A. Miss in the middle attacks on IDEA and Khufu//Proceedings of the International Workshop on Fast Software Encryption. Rome，Italy，1999：124-138

[42] Biham E，Granboulan L，Nguyễn P Q. Impossible fault analysis of RC4 and differential fault analysis of RC4//Proceedings of the International Workshop on Fast Software Encryption. Paris，France，2005：359-367

[43] Wu Wen-Ling，Zhang Lei. Research progress of impossible differential cryptanalysis. Journal of Systems Science and Mathematical Sciences，2008，28(8)：971-983(in Chinese)
(吴文玲，张蕾. 不可能差分密码分析研究进展. 系统科学与数学，2008，28(8)：971-983)

[44] Derbez P，Fouque P-A，Leresteux D. Meet-in-the-middle and impossible differential fault analysis on AES//Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems. Nara，Japan，2011：274-291

[45] Sadeghi S，Bagheri N. Security analysis of SIMECK block cipher against related-key impossible differential. Information Processing Letters，2019，147：14-21

[46] Du J，Wang W，Li M，et al. Related-tweakey impossible differential attack on QARMA-128. Science China Information Sciences，2022，65(2)：129102

[47] Pal D，Ali M，Das A，et al. A cluster-based practical key recovery attack on reduced-round AES using impossible-differential cryptanalysis. The Journal of Supercomputing，2023，79(6)：6252-6289

[48] Reed I. A class of multiple-error-correcting codes and the decoding scheme. Transactions of the IRE Professional Group on Information Theory，1954，4(4)：38-49

[49] Wilks S S. The large-sample distribution of the likelihood ratio for testing composite hypotheses. The Annals of Mathematical Statistics，1938，9(1)：60-62

附录 A. 实验数据.

明文：随机生成

主密钥：0x0123456789abcedf

表 A1 统计故障分析和不可能统计故障分析方法恢复 Pyjamask-96/128 算法部分轮密钥的成功率

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
2	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
3	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
4	0.04/0.06	0.03/0.06	0.06/0.06	0.04/0.05	0.13/0.12	0.08/0.08	0.11/0.05	0.05/0.06	0.12/0.11	0.03/0.05
5	0.09/0.11	0.07/0.12	0.11/0.06	0.16/0.10	0.18/0.08	0.11/0.10	0.14/0.12	0.10/0.11	0.18/0.17	0.17/0.17
6	0.14/0.10	0.13/0.09	0.12/0.10	0.17/0.12	0.24/0.15	0.10/0.11	0.19/0.12	0.10/0.12	0.21/0.16	0.16/0.20
7	0.14/0.15	0.20/0.13	0.26/0.14	0.31/0.20	0.21/0.25	0.31/0.17	0.26/0.16	0.22/0.21	0.38/0.27	0.21/0.31
8	0.12/0.17	0.24/0.13	0.25/0.18	0.29/0.25	0.31/0.24	0.24/0.18	0.31/0.23	0.18/0.12	0.42/0.30	0.41/0.35
9	0.24/0.24	0.30/0.24	0.31/0.18	0.32/0.37	0.36/0.31	0.28/0.32	0.37/0.32	0.41/0.36	0.44/0.39	0.38/0.41
10	0.25/0.23	0.32/0.28	0.33/0.29	0.34/0.39	0.43/0.35	0.44/0.30	0.49/0.46	0.48/0.45	0.55/0.39	0.41/0.46
11	0.36/0.26	0.43/0.35	0.48/0.44	0.50/0.47	0.48/0.32	0.46/0.37	0.43/0.43	0.53/0.48	0.61/0.49	0.46/0.37
12	0.38/0.35	0.44/0.41	0.42/0.44	0.45/0.42	0.41/0.51	0.43/0.37	0.54/0.52	0.55/0.53	0.56/0.49	0.45/0.57
13	0.31/0.47	0.52/0.42	0.48/0.43	0.45/0.51	0.50/0.61	0.57/0.50	0.60/0.46	0.62/0.53	0.66/0.60	0.56/0.47
14	0.34/0.45	0.52/0.56	0.51/0.43	0.53/0.54	0.59/0.56	0.62/0.50	0.69/0.57	0.71/0.57	0.75/0.66	0.64/0.64
15	0.41/0.56	0.56/0.59	0.54/0.50	0.56/0.56	0.56/0.53	0.61/0.61	0.66/0.63	0.64/0.65	0.65/0.67	0.66/0.67
16	0.56/0.58	0.60/0.61	0.52/0.59	0.55/0.71	0.60/0.62	0.60/0.70	0.70/0.66	0.73/0.71	0.77/0.68	0.64/0.75
17	0.47/0.50	0.53/0.62	0.54/0.61	0.54/0.65	0.61/0.67	0.77/0.63	0.76/0.70	0.78/0.73	0.83/0.73	0.68/0.78
18	0.61/0.54	0.64/0.64	0.58/0.60	0.57/0.59	0.65/0.66	0.78/0.62	0.75/0.76	0.75/0.68	0.75/0.76	0.78/0.64
19	0.58/0.56	0.63/0.68	0.59/0.60	0.60/0.71	0.73/0.63	0.79/0.64	0.79/0.69	0.80/0.80	0.80/0.73	0.78/0.80
20	0.69/0.63	0.62/0.65	0.65/0.67	0.69/0.69	0.76/0.59	0.81/0.73	0.88/0.80	0.79/0.79	0.83/0.79	0.85/0.82
21	0.68/0.65	0.55/0.67	0.68/0.74	0.70/0.72	0.70/0.66	0.81/0.79	0.87/0.74	0.85/0.81	0.90/0.84	0.82/0.78
22	0.69/0.62	0.72/0.74	0.73/0.76	0.74/0.73	0.70/0.78	0.82/0.81	0.80/0.80	0.86/0.75	0.87/0.86	0.87/0.90
23	0.66/0.67	0.75/0.73	0.71/0.75	0.69/0.76	0.70/0.71	0.80/0.78	0.81/0.86	0.85/0.82	0.87/0.78	0.79/0.85
24	0.67/0.70	0.73/0.78	0.74/0.71	0.81/0.85	0.72/0.76	0.82/0.74	0.91/0.88	0.89/0.72	0.90/0.86	0.83/0.83
25	0.73/0.68	0.73/0.82	0.72/0.68	0.72/0.80	0.82/0.78	0.87/0.78	0.94/0.86	0.82/0.87	0.86/0.84	0.91/0.82
26	0.58/0.70	0.77/0.88	0.75/0.82	0.76/0.79	0.76/0.86	0.91/0.86	0.89/0.90	0.90/0.86	0.94/0.95	0.90/0.88
27	0.72/0.77	0.78/0.80	0.82/0.81	0.83/0.77	0.76/0.75	0.92/0.79	0.90/0.91	0.92/0.92	0.87/0.88	0.93/0.89
28	0.80/0.78	0.78/0.82	0.79/0.83	0.81/0.79	0.85/0.74	0.92/0.80	0.95/0.87	0.93/0.86	0.96/0.90	0.93/0.90
29	0.69/0.80	0.83/0.86	0.83/0.75	0.85/0.80	0.76/0.76	0.93/0.86	0.93/0.90	0.91/0.88	0.94/0.94	0.95/0.84
30	0.80/0.82	0.83/0.88	0.85/0.80	0.83/0.87	0.83/0.81	0.96/0.88	0.97/0.94	0.90/0.91	0.93/0.95	0.92/0.89
31	0.78/0.78	0.77/0.86	0.86/0.86	0.87/0.86	0.79/0.79	0.97/0.86	0.93/0.92	0.95/0.81	0.96/0.96	0.91/0.93
32	0.85/0.86	0.83/0.89	0.83/0.92	0.83/0.83	0.82/0.83	0.93/0.86	0.97/0.92	0.92/0.91	1.00/0.94	0.95/0.92
33	0.80/0.84	0.86/0.89	0.88/0.90	0.92/0.86	0.87/0.81	0.94/0.93	0.95/0.93	0.94/0.90	−/0.93	0.98/0.94
34	0.81/0.81	0.94/0.84	0.92/0.85	0.90/0.90	0.82/0.79	0.97/0.91	0.98/0.92	0.95/0.96	−/0.96	0.95/0.95
35	0.78/0.86	0.88/0.86	0.90/0.85	0.92/0.91	0.90/0.84	0.99/0.94	0.94/0.95	0.95/0.93	−/0.99	0.95/0.94
36	0.80/0.88	0.94/0.83	0.91/0.85	0.92/0.89	0.83/0.86	−/0.92	0.95/0.93	0.93/0.93	−/−	0.99/0.96
37	0.91/0.83	0.85/0.80	0.85/0.87	0.87/0.93	0.91/0.76	−/0.89	0.96/0.91	0.97/0.93	−/−	−/0.99
38	0.86/0.88	0.91/0.88	0.87/0.85	0.89/0.89	0.92/0.85	−/0.96	0.94/0.94	0.97/0.95	−/−	−/−
39	0.83/0.90	0.82/0.92	0.88/0.92	0.92/0.95	0.89/0.84	−/0.93	0.98/0.97	0.99/0.94	−/−	−/−
40	0.89/0.90	0.92/0.89	0.90/0.91	0.91/0.93	0.86/0.86	−/0.96	0.99/0.96	−/0.95	−/−	−/−
41	0.83/0.87	0.90/0.87	0.90/0.93	0.92/0.94	0.88/0.82	−/0.93	−/0.94	−/0.97	−/−	−/−
42	0.92/0.88	0.90/0.87	0.89/0.91	0.90/0.91	0.95/0.87	−/0.93	−/0.95	−/0.99	−/−	−/−
43	0.87/0.92	0.92/0.94	0.92/0.94	0.91/0.91	0.89/0.79	−/0.96	−/0.99	−/−	−/−	−/−
44	0.80/0.90	0.90/0.90	0.91/0.96	0.96/0.92	0.92/0.80	−/0.98	−/−	−/−	−/−	−/−
45	0.94/0.90	0.92/0.94	0.95/0.98	0.88/0.95	0.95/0.80	−/0.99	−/−	−/−	−/−	−/−
46	0.91/0.95	0.95/0.96	0.89/0.94	0.91/0.96	0.91/0.80	−/−	−/−	−/−	−/−	−/−
47	0.94/0.95	0.96/0.96	0.93/0.93	0.94/0.86	0.86/0.79	−/−	−/−	−/−	−/−	−/−
48	0.93/0.93	0.92/0.96	0.92/0.95	0.94/0.97	0.91/0.79	−/−	−/−	−/−	−/−	−/−
49	0.91/0.93	0.94/0.95	0.95/0.98	0.92/0.93	0.96/0.78	−/−	−/−	−/−	−/−	−/−
50	0.94/0.95	0.91/0.98	0.93/0.94	0.99/0.95	0.91/0.79	−/−	−/−	−/−	−/−	−/−
51	0.92/0.96	0.94/0.98	0.90/0.95	−/0.96	0.97/0.72	−/−	−/−	−/−	−/−	−/−
52	0.94/0.92	0.96/0.95	0.96/0.96	−/0.91	0.94/0.86	−/−	−/−	−/−	−/−	−/−
53	0.91/0.90	0.94/0.96	0.95/0.95	−/0.96	0.99/0.74	−/−	−/−	−/−	−/−	−/−

（续表 A1）

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
54	0.95/0.93	0.95/0.96	0.97/0.98	−/0.99	−/0.81	−/−	−/−	−/−	−/−	−/−
55	0.92/0.97	0.90/0.96	0.93/0.95	−/−	−/0.74	−/−	−/−	−/−	−/−	−/−
56	0.93/0.93	0.95/0.95	0.98/0.94	−/−	−/0.80	−/−	−/−	−/−	−/−	−/−
57	0.96/0.90	0.97/0.95	0.99/0.98	−/−	−/0.71	−/−	−/−	−/−	−/−	−/−
58	0.96/0.97	0.98/0.97	−/0.98	−/−	−/0.75	−/−	−/−	−/−	−/−	−/−
59	0.94/0.93	0.98/0.97	−/0.99	−/−	−/0.80	−/−	−/−	−/−	−/−	−/−
60	0.97/0.96	0.94/0.94	−/−	−/−	−/0.87	−/−	−/−	−/−	−/−	−/−
61	0.94/0.93	0.96/0.96	−/−	−/−	−/0.78	−/−	−/−	−/−	−/−	−/−
62	0.94/0.98	0.95/0.96	−/−	−/−	−/0.81	−/−	−/−	−/−	−/−	−/−
63	0.98/0.98	0.96/0.97	−/−	−/−	−/0.82	−/−	−/−	−/−	−/−	−/−
64	0.97/0.98	0.98/0.98	−/−	−/−	−/0.77	−/−	−/−	−/−	−/−	−/−
65	0.96/0.96	0.98/0.98	−/−	−/−	−/0.82	−/−	−/−	−/−	−/−	−/−
66	0.93/0.97	0.97/0.98	−/−	−/−	−/0.82	−/−	−/−	−/−	−/−	−/−
67	0.97/0.98	0.96/0.99	−/−	−/−	−/0.78	−/−	−/−	−/−	−/−	−/−
68	0.99/0.98	1.00/−	−/−	−/−	−/0.81	−/−	−/−	−/−	−/−	−/−
69	−/0.99	−/−	−/−	−/−	−/0.75	−/−	−/−	−/−	−/−	−/−
70	−/−	−/−	−/−	−/−	−/0.76	−/−	−/−	−/−	−/−	−/−

表 A2　统计故障分析和不可能统计故障分析方法恢复 Pyjamask-96/128 算法部分轮密钥的准确度

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
1	7.00/15.00	7.00/15.00	7.00/15.00	7.00/15.00	7.00/15.00	7.00/15.00	7.00/15.00	7.00/15.00	7.00/15.00	7.00/15.00
2	6.56/14.36	5.96/15.40	5.52/14.96	4.88/7.76	4.60/8.64	6.88/13.32	6.72/11.60	4.96/11.52	4.80/8.52	6.16/8.20
3	3.00/4.22	2.88/4.56	2.49/4.93	2.10/2.62	1.72/2.41	3.48/4.13	3.32/4.41	2.93/4.49	1.94/2.72	3.12/2.07
4	3.92/4.76	3.34/2.99	2.24/4.73	2.03/1.58	1.65/0.88	3.35/4.08	2.76/2.96	2.03/3.24	1.56/1.50	3.18/1.71
5	1.83/1.94	1.58/2.13	1.53/1.82	0.80/0.88	0.70/0.60	2.02/1.85	1.76/1.66	1.31/1.53	0.97/0.73	1.55/0.72
6	2.29/1.98	1.53/1.86	0.90/1.87	0.60/0.49	0.56/0.64	1.57/1.74	1.15/0.90	1.17/0.99	0.57/0.52	1.20/0.41
7	1.24/0.93	1.01/1.04	0.86/1.36	0.20/0.17	0.25/0.13	1.10/1.11	1.02/0.81	0.96/0.80	0.32/0.12	1.20/0.31
8	2.15/1.31	1.08/1.53	0.63/1.12	0.22/0.19	0.20/0.10	1.28/1.02	0.83/0.63	0.72/0.49	0.22/0.09	0.71/0.09
9	1.06/0.84	0.59/0.63	0.46/0.92	0.16/0.05	0.17/0.12	1.02/0.57	0.70/0.44	0.62/0.37	0.19/0.07	0.67/0.07
10	0.85/0.64	0.52/0.62	0.47/0.59	0.18/0.04	0.07/0.06	0.79/0.65	0.47/0.26	0.39/0.37	0.06/0.13	0.61/0.07
11	0.80/0.58	0.30/0.51	0.22/0.53	0.08/0.03	0.04/0.04	0.61/0.68	0.46/0.19	0.33/0.32	0.07/0.03	0.49/0.04
12	0.82/0.58	0.22/0.48	0.18/0.47	0.07/0.03	0.02/0.04	0.58/0.51	0.38/0.19	0.30/0.18	0.17/0.01	0.51/0.01
13	0.70/0.52	0.29/0.23	0.22/0.26	0.10/0.01	0.01/0	0.39/0.35	0.30/0.26	0.20/0.22	0.10/0	0.30/0.01
14	0.68/0.48	0.25/0.19	0.13/0.27	0.03/0.01	0.03/0	0.31/0.33	0.22/0.16	0.17/0.13	0.02/0.02	0.29/0
15	0.46/0.26	0.20/0.20	0.15/0.23	0.02/0	0.05/0	0.29/0.23	0.21/0.10	0.15/0.15	0.05/0.01	0.23/0.02
16	0.55/0.37	0.23/0.17	0.11/0.23	0.03/0	0.08/0	0.37/0.24	0.28/0.09	0.13/0.11	0.02/0.02	0.22/0
17	0.47/0.32	0.18/0.12	0.10/0.10	0.03/0.01	0.02/0.01	0.27/0.25	0.15/0.08	0.10/0.10	0/0	0.25/0
18	0.38/0.20	0.13/0.13	0.06/0.08	0.03/0	0.04/0.01	0.15/0.30	0.20/0.08	0.09/0.06	0/0	0.18/0
19	0.38/0.27	0.09/0.09	0.11/0.11	0/0	0.01/0	0.15/0.21	0.15/0.08	0.10/0.11	0/0	0.13/0
20	0.25/0.24	0.24/0.13	0.07/0.10	0.01/0	0/0	0.14/0.17	0.12/0.04	0.08/0.07	0/0.01	0.10/0
21	0.22/0.13	0.17/0.10	0.03/0.07	0/0	0/0	0.12/0.12	0.03/0.04	0.02/0.03	0/0	0.08/0
22	0.23/0.10	0.12/0.04	0.08/0.04	0.01/0	0.01/0	0.12/0.14	0.09/0.04	0.01/0.08	0/0	0.05/0
23	0.18/0.14	0.09/0.08	0.06/0.00	0.01/0	0.01/0	0.14/0.15	0.09/0.03	0.10/0.06	0/0	0.07/0
24	0.27/0.19	0.10/0.06	0.05/0.07	0.02/0	0.01/0	0.09/0.19	0.05/0.04	0.03/0.05	0.01/0	0.12/0
25	0.17/0.14	0.09/0.03	0.03/0.05	0/0	0/0	0.09/0.04	0.04/0.01	0.05/0.03	0.01/0	0.04/0
26	0.36/0.13	0.07/0.02	0.03/0.06	0.01/0	0/0	0.06/0.06	0.03/0.01	0.02/0.03	0/0	0.06/0
27	0.22/0.17	0.08/0.02	0.03/0.03	0/0	0/0	0.06/0.08	0.04/0.02	0.01/0.03	0/0	0.07/0
28	0.21/0.13	0.12/0.05	0.04/0.07	0/0	0/0	0.05/0.10	0.04/0.01	0.01/0.04	0.01/0	0.02/0
29	0.20/0.11	0.06/0.03	0.00/0.06	0/0	0/0	0.05/0.07	0.05/0.03	0/0	0/0	0.04/0
30	0.10/0.11	0.09/0.06	0.00/0.05	0/0	0.01/0	0.05/0.11	0.03/0	0.03/0	0/0	0.01/0
31	0.10/0.11	0.06/0.03	0.01/0.04	0/0	0.01/0	0.02/0.09	0.01/0.02	0.01/0.01	0/0	0.05/0
32	0.09/0.10	0.06/0.04	0.00/0.01	0/0	0/0	0.04/0.09	0.01/0.01	0.01/0.00	0/0	0.02/0
33	0.12/0.09	0.03/0.02	0.01/0.00	0/0	0/0	0.04/0.02	0.02/0.02	0.00/0.01	−/0	0.02/0
34	0.10/0.07	0/0.04	0.01/0.01	0.01/0	0/0	0.07/0.06	0/0.02	0.01/0.01	−/0	0.02/0
35	0.17/0.10	0.08/0.05	0.02/0.05	0/0	0/0	0.01/0.01	0.02/0	0/0.02	−/0	0.01/0
36	0.14/0.07	0.02/0.04	0.01/0.03	0/0	0/0	−/0.05	0.01/0	0.03/0.01	−/−	0.01/0
37	0.06/0.06	0.05/0.07	0.01/0.02	0/0	0/0	−/0.08	0.02/0	0.02/0.01	−/−	−/0
38	0.08/0.06	0.03/0.01	0.00/0.03	0/0	0/0	−/0.03	0.03/0	0.03/0.00	−/−	−/−
39	0.07/0.05	0.06/0.01	0.01/0.01	0/0	0/0	−/0.01	0/0	0/0.01	−/−	−/−

（续表 A2）

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
40	0.09/0.05	0.02/0.02	0.00/0.01	0/0	0/0	−/0.01	0/0	−/0	−/−	−/−
41	0.08/0.05	0.01/0.03	0.01/0.01	0/0	0/0	−/0.01	−/0	−/0.01	−/−	−/−
42	0.04/0.09	0.01/0.03	0.00/0.01	0/0	0/0.01	−/0.04	−/0	−/0	−/−	−/−
43	0.15/0.03	0.04/0.01	0.03/0.03	0/0	0/0	−/0.02	−/0	−/−	−/−	−/−
44	0.13/0.04	0.01/0.02	0.03/0	0/0	0/0	−/0	−/−	−/−	−/−	−/−
45	0.02/0.07	0.02/0.01	0.01/0.01	0/0	0/0	−/0.02	−/−	−/−	−/−	−/−
46	0.04/0.02	0/0	0/0	0/0	0/0	−/−	−/−	−/−	−/−	−/−
47	0.04/0.02	0.01/0	0.01/0.03	0/0	0/0	−/−	−/−	−/−	−/−	−/−
48	0.06/0.03	0.05/0	0.02/0.02	0/0	0/0	−/−	−/−	−/−	−/−	−/−
49	0.05/0.03	0/0.02	0.01/0	0/0	0/0	−/−	−/−	−/−	−/−	−/−
50	0.03/0.02	0.02/0.01	0.02/0.01	0/0	0/0	−/−	−/−	−/−	−/−	−/−
51	0.06/0.02	0.01/0.02	0/0	−/0	0/0	−/−	−/−	−/−	−/−	−/−
52	0.06/0.04	0.01/0.01	0.02/0	−/0	0/0	−/−	−/−	−/−	−/−	−/−
53	0.07/0.04	0.02/0.01	0.01/0	−/0	0/0	−/−	−/−	−/−	−/−	−/−
54	0.01/0.02	0/0	0/0	−/0	−/0	−/−	−/−	−/−	−/−	−/−
55	0.04/0.01	0.01/0	0.01/0.01	−/−	−/0	−/−	−/−	−/−	−/−	−/−
56	0.05/0.04	0.03/0	0.01/0.01	−/−	−/0	−/−	−/−	−/−	−/−	−/−
57	0.04/0.03	0.01/0.02	0/0	−/−	−/0	−/−	−/−	−/−	−/−	−/−
58	0/0.02	0/0	−/0	−/−	−/0	−/−	−/−	−/−	−/−	−/−
59	0.05/0.04	0.01/0	−/0	−/−	−/0	−/−	−/−	−/−	−/−	−/−
60	0.04/0.02	0.03/0	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
61	0.04/0.04	0/0.01	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
62	0.02/0	0.02/0.02	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
63	0.02/0.01	0.01/0	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
64	0.01/0	0/0.02	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
65	0.03/0.02	0/0.01	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
66	0.03/0	0/0.01	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
67	0.03/0.01	0/0	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
68	0/0	0/−	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
69	−/0.01	−/−	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−
70	−/−	−/−	−/−	−/−	−/0	−/−	−/−	−/−	−/−	−/−

表 A3 统计故障分析和不可能统计故障分析方法恢复 Pyjamask-96/128 算法部分轮密钥的耗时 （单位：ms）

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
1	1.09/2.66	1.10/2.81	1.09/2.97	1.09/2.81	1.09/2.97	0.94/2.81	1.09/2.61	0.94/2.81	0.94/2.65	1.09/2.68
2	0.94/2.82	1.10/2.97	1.09/2.97	1.09/2.81	1.09/3.13	0.94/2.66	0.94/2.66	0.94/2.66	0.94/2.66	1.10/2.77
3	1.25/3.10	1.09/3.12	1.10/2.97	1.25/2.97	1.10/3.12	1.09/2.65	0.94/2.66	1.07/2.81	1.10/2.81	1.10/2.81
4	1.10/3.12	1.25/3.38	1.25/3.28	1.10/2.97	1.10/3.13	1.25/2.66	1.09/2.81	1.08/2.66	0.94/2.81	1.09/2.81
5	1.10/3.44	1.88/3.28	1.25/3.28	1.25/2.97	1.25/3.44	1.10/2.81	1.09/2.82	1.08/2.65	1.09/2.66	1.25/2.90
6	1.25/3.28	1.25/3.59	1.56/3.75	1.25/3.28	1.10/3.43	1.25/2.82	1.25/2.65	1.20/2.81	1.10/2.66	1.25/2.97
7	1.25/3.28	1.25/3.44	1.25/3.59	1.41/3.43	1.25/3.60	1.09/2.65	1.09/2.83	1.15/2.97	1.25/2.66	1.09/2.97
8	2.82/3.33	1.56/3.56	1.41/3.44	1.14/3.44	1.25/3.59	1.09/2.97	1.25/2.97	1.15/2.97	1.25/2.81	1.25/2.81
9	1.25/3.59	1.41/3.80	1.41/3.59	1.41/3.44	1.41/3.75	1.25/2.81	1.25/2.97	1.25/2.81	1.09/2.83	1.41/2.97
10	2.82/3.60	1.56/3.75	1.41/3.59	1.56/3.75	1.41/3.91	1.10/2.96	1.25/2.97	1.25/3.28	1.09/2.81	1.25/3.12
11	1.40/3.80	1.41/3.91	1.56/3.75	1.40/3.76	1.56/4.12	1.25/2.97	1.25/3.09	1.25/2.97	1.25/2.81	1.41/3.19
12	1.40/3.90	1.87/4.06	1.56/3.91	1.57/3.75	1.41/4.06	1.25/3.13	1.25/3.12	1.25/2.97	1.25/2.97	1.25/3.13
13	1.41/4.06	2.66/4.12	1.56/3.90	1.56/4.07	1.40/4.22	1.25/3.28	1.41/3.13	1.46/3.12	1.41/3.04	1.40/3.12
14	1.40/4.36	1.56/4.28	1.72/4.22	1.56/4.17	1.56/4.53	1.56/3.34	1.25/3.12	1.50/3.13	1.40/3.12	1.41/3.22
15	1.57/4.48	1.56/4.38	1.56/4.22	1.72/4.06	1.72/4.69	1.41/3.44	1.41/3.20	1.42/3.28	1.41/3.13	1.56/3.28
16	1.56/4.42	1.56/4.53	1.56/4.37	1.56/4.22	1.72/4.53	1.25/3.12	1.40/3.28	1.37/3.44	1.41/3.43	1.41/3.43
17	1.57/4.52	1.56/4.77	1.72/4.53	1.72/4.43	1.88/4.69	1.41/3.28	1.41/3.28	1.43/3.75	1.40/3.29	1.41/3.29
18	1.87/4.53	1.72/4.84	1.72/4.53	1.72/4.53	1.72/4.84	1.40/3.44	1.40/3.29	1.43/3.75	1.41/3.43	1.41/3.59
19	1.72/4.53	1.72/4.96	1.72/4.68	1.72/4.53	1.87/4.85	1.57/3.28	1.57/3.39	1.58/3.43	1.56/3.44	1.40/3.43
20	1.72/4.95	1.88/5.00	1.87/4.85	1.87/4.62	1.72/4.98	1.40/3.44	1.40/3.44	1.40/3.60	1.41/3.44	1.41/3.44
21	1.87/5.00	2.81/5.00	1.87/5.00	1.72/4.84	1.87/5.00	1.88/3.46	1.57/3.44	1.59/3.75	1.56/3.59	1.56/3.59
22	1.88/5.00	1.87/5.16	1.72/5.00	1.71/4.84	1.88/5.31	1.40/3.43	1.56/3.59	1.56/3.59	1.59/3.44	1.56/3.69
23	1.87/5.15	1.88/5.21	1.72/5.62	1.88/5.00	1.87/5.31	1.57/3.44	1.56/3.63	1.56/3.91	1.57/3.59	1.72/3.59

（续表 A3）

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
24	2.04/5.24	1.87/5.38	1.87/5.31	2.03/5.16	2.03/5.47	2.65/3.75	1.72/3.75	1.56/3.75	1.56/3.59	1.56/3.75
25	1.87/5.38	1.87/5.47	1.87/5.47	2.03/5.20	2.03/5.62	1.72/3.89	1.56/3.75	1.72/3.75	1.72/3.75	1.56/3.86
26	2.03/5.47	2.66/5.63	2.03/5.47	2.03/5.32	2.19/5.63	1.56/3.91	1.87/3.81	1.72/4.06	1.56/3.75	1.72/3.91
27	1.87/5.52	2.81/5.78	2.03/5.63	2.19/5.47	2.19/5.78	2.03/3.75	1.57/3.75	1.56/3.91	1.56/3.91	1.72/3.92
28	2.03/5.62	2.03/5.78	2.03/5.81	2.03/5.62	2.03/5.94	1.57/4.06	1.56/3.90	1.56/3.91	1.87/3.91	1.56/3.91
29	2.19/5.74	2.19/5.80	2.19/5.78	2.19/5.71	2.19/6.05	1.57/4.07	1.72/4.00	1.72/4.06	1.72/4.21	2.18/3.90
30	2.03/5.88	2.19/6.09	2.19/6.09	2.18/5.78	2.18/6.09	1.72/3.90	1.72/4.06	1.72/4.06	1.72/4.22	3.75/4.03
31	2.19/6.05	2.19/6.25	2.34/6.25	2.35/5.78	2.19/6.25	1.88/4.15	1.87/3.91	1.72/4.22	1.72/4.53	1.72/4.06
32	2.34/6.05	2.19/6.25	2.34/6.25	2.35/5.93	2.35/6.25	2.03/4.06	1.72/4.07	1.87/4.22	1.87/4.54	1.88/4.06
33	2.34/6.10	3.13/6.37	2.34/6.25	2.19/6.10	2.34/6.56	1.87/4.22	2.03/4.18	1.87/4.53	−/4.06	1.87/4.38
34	2.34/6.40	2.34/6.57	2.50/6.41	2.34/6.22	2.34/6.64	1.88/4.23	1.88/4.22	1.87/4.38	−/4.22	2.03/4.22
35	2.50/6.41	2.50/6.56	2.34/6.56	2.81/6.25	2.35/6.87	2.03/4.06	1.87/4.37	2.03/4.37	−/4.38	1.88/4.41
36	2.50/6.44	2.34/6.72	2.50/6.56	2.50/6.40	2.50/6.72	−/4.38	1.87/4.32	2.03/4.38	−/−	2.17/4.52
37	2.50/6.71	2.50/6.83	2.81/6.72	2.50/6.57	2.50/7.03	−/4.35	1.88/4.37	2.50/4.38	−/−	−/4.69
38	2.66/6.57	3.75/6.87	2.50/7.03	2.50/6.86	2.50/6.87	−/4.38	2.03/4.53	2.50/4.53	−/−	−/−
39	2.66/6.87	2.50/7.02	2.65/6.87	2.66/6.88	2.50/7.19	−/4.38	2.03/4.53	2.66/4.69	−/−	−/−
40	2.50/6.87	2.50/7.18	2.66/7.04	2.65/6.72	2.50/7.19	−/4.84	2.19/4.54	−/4.71	−/−	−/−
41	2.50/7.28	2.50/7.35	2.81/7.18	2.66/6.88	2.66/7.22	−/4.53	−/4.71	−/4.69	−/−	−/−
42	2.65/7.24	2.66/7.34	2.81/7.19	2.81/7.03	2.66/7.50	−/4.53	−/4.85	−/4.84	−/−	−/−
43	2.97/7.38	2.96/7.66	2.81/7.34	2.81/7.18	2.66/7.66	−/4.69	−/5.15	−/−	−/−	−/−
44	2.81/7.42	2.82/7.70	2.66/7.50	2.66/7.19	2.81/7.50	−/4.68	−/−	−/−	−/−	−/−
45	2.97/7.53	2.82/7.86	2.97/7.53	2.81/7.19	2.81/7.81	−/4.69	−/−	−/−	−/−	−/−
46	2.81/7.60	3.12/7.86	2.81/7.50	2.81/7.34	2.82/7.88	−/−	−/−	−/−	−/−	−/−
47	2.97/7.65	2.81/7.81	2.97/7.84	2.97/7.66	2.96/7.97	−/−	−/−	−/−	−/−	−/−
48	2.81/7.82	2.81/7.97	2.97/7.97	2.97/7.65	2.97/8.13	−/−	−/−	−/−	−/−	−/−
49	2.97/8.43	2.97/8.13	2.81/7.97	2.97/7.74	2.82/8.06	−/−	−/−	−/−	−/−	−/−
50	2.97/8.51	2.81/8.28	2.81/8.16	2.97/7.81	2.96/8.28	−/−	−/−	−/−	−/−	−/−
51	2.97/8.59	3.12/8.28	2.97/8.28	−/7.97	3.13/8.44	−/−	−/−	−/−	−/−	−/−
52	2.97/8.64	2.97/8.44	3.12/8.29	−/8.12	3.12/8.59	−/−	−/−	−/−	−/−	−/−
53	3.12/8.75	3.12/8.59	3.12/8.44	−/8.13	3.13/8.75	−/−	−/−	−/−	−/−	−/−
54	3.13/8.79	3.13/8.66	3.59/8.59	−/9.37	−/8.75	−/−	−/−	−/−	−/−	−/−
55	3.12/8.75	3.12/8.75	3.12/8.76	−/−	−/8.75	−/−	−/−	−/−	−/−	−/−
56	3.59/8.83	3.29/8.91	3.28/8.75	−/−	−/8.82	−/−	−/−	−/−	−/−	−/−
57	3.28/8.75	3.28/8.91	3.28/8.90	−/−	−/9.06	−/−	−/−	−/−	−/−	−/−
58	3.28/9.06	3.28/9.21	−/9.07	−/−	−/9.22	−/−	−/−	−/−	−/−	−/−
59	3.44/9.19	3.28/9.34	−/10.15	−/−	−/9.22	−/−	−/−	−/−	−/−	−/−
60	4.22/9.38	3.59/9.37	−/−	−/−	−/9.37	−/−	−/−	−/−	−/−	−/−
61	3.44/9.21	3.75/9.38	−/−	−/−	−/9.38	−/−	−/−	−/−	−/−	−/−
62	3.44/9.28	3.44/9.53	−/−	−/−	−/9.50	−/−	−/−	−/−	−/−	−/−
63	3.43/9.39	3.43/9.69	−/−	−/−	−/9.69	−/−	−/−	−/−	−/−	−/−
64	3.60/9.53	3.44/9.69	−/−	−/−	−/9.68	−/−	−/−	−/−	−/−	−/−
65	3.59/9.85	3.59/9.85	−/−	−/−	−/9.84	−/−	−/−	−/−	−/−	−/−
66	3.59/9.98	3.75/9.84	−/−	−/−	−/10.00	−/−	−/−	−/−	−/−	−/−
67	3.75/10.05	3.75/10.31	−/−	−/−	−/10.03	−/−	−/−	−/−	−/−	−/−
68	3.94/10.04	3.75/−	−/−	−/−	−/10.15	−/−	−/−	−/−	−/−	−/−
69	−/10.16	−/−	−/−	−/−	−/10.32	−/−	−/−	−/−	−/−	−/−
70	−/−	−/−	−/−	−/−	−/10.46	−/−	−/−	−/−	−/−	−/−

表 A4　统计故障分析和不可能统计故障分析方法恢复 SUNDAE-GIFT 算法部分轮密钥的成功率

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0.01	0.01	0	0	0	0.01	0.01	0
3	0.01	0.02	0.01	0.02	0	0.01	0.02	0.02	0.02	0
4	0.05	0.03	0.08	0.03	0.05	0.04	0.06	0.06	0.11	0.03
5	0.08	0.10	0.14	0.06	0.07	0.15	0.08	0.09	0.19	0.15
6	0.11	0.12	0.27	0.14	0.16	0.20	0.20	0.16	0.26	0.20
7	0.22	0.20	0.19	0.23	0.26	0.28	0.24	0.27	0.36	0.28

（续表 A4）

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
8	0.24	0.22	0.21	0.27	0.32	0.27	0.32	0.35	0.41	0.36
9	0.33	0.26	0.40	0.29	0.33	0.40	0.42	0.35	0.41	0.44
10	0.38	0.39	0.35	0.37	0.46	0.44	0.53	0.56	0.59	0.56
11	0.41	0.40	0.52	0.49	0.47	0.58	0.55	0.59	0.68	0.59
12	0.49	0.54	0.53	0.62	0.52	0.62	0.62	0.62	0.60	0.68
13	0.53	0.50	0.57	0.52	0.65	0.71	0.56	0.64	0.76	0.70
14	0.56	0.55	0.64	0.58	0.69	0.69	0.68	0.73	0.80	0.76
15	0.60	0.59	0.74	0.73	0.79	0.75	0.70	0.71	0.88	0.82
16	0.67	0.64	0.77	0.84	0.76	0.83	0.76	0.88	0.82	0.88
17	0.72	0.76	0.75	0.79	0.80	0.83	0.86	0.88	0.96	0.94
18	0.76	0.70	0.79	0.78	0.81	0.88	0.82	0.85	0.90	0.92
19	0.78	0.76	0.77	0.90	0.73	0.91	0.74	0.85	0.94	0.95
20	0.80	0.80	0.79	0.80	0.85	0.92	0.92	0.94	0.93	0.91
21	0.85	0.83	0.88	0.90	0.83	0.90	0.88	0.87	0.98	0.93
22	0.87	0.87	0.92	0.92	0.86	0.91	0.92	0.94	0.96	0.96
23	0.89	0.82	0.92	0.89	0.84	0.93	0.91	0.96	0.98	0.98
24	0.90	0.86	0.91	0.86	0.92	0.92	0.97	0.96	0.97	0.94
25	0.93	0.82	0.93	0.87	0.88	0.95	0.95	0.94	0.99	0.96
26	0.90	0.89	0.90	0.94	0.91	0.97	0.98	0.97	—	0.99
27	0.89	0.90	0.95	0.93	0.95	0.98	0.97	0.96	—	—
28	0.91	0.86	0.94	0.94	0.88	0.99	0.97	0.95	—	—
29	0.94	0.90	0.90	0.94	0.93	—	0.98	0.99	—	—
30	0.93	0.92	0.95	0.98	0.96	—	0.99	—	—	—
31	0.92	0.95	0.96	0.98	0.94	—	—	—	—	—
32	0.90	0.93	0.93	0.98	0.96	—	—	—	—	—
33	0.94	0.89	0.98	0.98	0.92	—	—	—	—	—
34	0.93	0.92	0.97	0.99	0.98	—	—	—	—	—
35	0.96	0.95	0.98	—	0.99	—	—	—	—	—
36	0.99	0.96	0.97	—	—	—	—	—	—	—
37	—	0.97	0.99	—	—	—	—	—	—	—
38	—	0.99	—	—	—	—	—	—	—	—

表 A5 统计故障分析和不可能统计故障分析方法恢复 SUNDAE-GIFT 算法部分轮密钥的耗时 （单位：s）

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
1	0.42	0.47	0.44	0.55	0.83	0.46	0.50	0.44	0.54	0.80
2	0.52	0.52	0.48	0.55	0.80	0.49	0.50	0.45	0.55	0.76
3	0.66	0.72	0.68	0.70	0.96	0.67	0.70	0.64	0.74	0.99
4	0.88	0.84	0.88	0.93	1.25	0.88	0.88	0.83	0.95	1.25
5	1.14	1.12	1.09	1.14	1.53	1.08	1.13	1.06	1.16	1.60
6	1.33	1.32	1.33	1.39	1.68	1.29	1.38	1.29	1.39	1.74
7	1.56	1.54	1.58	1.58	1.98	1.55	1.56	1.54	1.62	2.05
8	1.81	1.78	1.80	1.84	2.13	1.80	1.82	1.74	1.80	2.22
9	2.01	2.04	2.00	2.07	2.43	2.00	2.04	1.95	2.04	2.40
10	2.28	2.22	2.24	2.32	2.61	2.21	2.23	2.21	2.31	2.58
11	2.48	2.45	2.41	2.56	2.82	2.44	2.56	2.46	2.53	2.83
12	2.73	2.72	2.72	2.79	2.97	2.67	2.70	2.64	2.75	3.18
13	3.00	2.93	2.96	2.94	3.20	2.92	2.93	2.92	3.00	3.33
14	3.23	3.14	3.19	3.22	3.43	3.13	3.14	3.10	3.23	3.53
15	3.44	3.36	3.40	3.43	3.64	3.35	3.40	3.33	3.51	3.69
16	3.66	3.64	3.61	3.66	3.86	3.57	3.66	3.61	3.68	3.93
17	3.90	3.86	3.87	3.87	4.09	3.83	3.88	3.77	3.93	4.26
18	4.11	4.11	4.05	4.11	4.39	4.05	4.10	4.07	4.14	4.32
19	4.37	4.31	4.34	4.36	4.53	4.28	4.39	4.32	4.34	4.54
20	4.60	4.54	4.58	4.60	4.76	4.55	4.59	4.54	4.62	4.84
21	4.83	4.79	4.81	5.03	4.94	4.76	4.84	4.74	4.87	5.08
22	5.12	5.00	5.02	5.25	5.15	4.99	5.05	5.00	5.11	5.26
23	5.32	5.24	5.25	5.45	5.54	5.20	5.32	5.27	5.34	5.55
24	5.53	5.49	5.54	5.63	5.97	5.50	5.54	5.44	5.55	5.89
25	5.79	5.72	5.77	5.83	6.00	5.64	5.76	5.72	5.79	5.94
26	6.05	5.94	5.96	6.04	6.32	5.88	6.01	5.93	—	6.39
27	6.25	6.17	6.17	6.39	6.67	6.12	6.21	6.18	—	—

（续表 A5）

故障数	统计故障分析					不可能统计故障分析				
	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE	HW	MLE	MME-HW-MLE	WD-HW	WD-MLE
28	6.42	6.44	6.45	6.64	6.96	6.39	6.47	6.39	—	—
29	6.76	6.61	6.65	6.88	7.50	—	6.72	6.63	—	—
30	6.95	6.84	6.95	6.96	7.43	—	6.90	—	—	—
31	7.17	7.04	7.14	7.31	8.15	—	—	—	—	—
32	7.44	7.34	7.39	7.66	8.13	—	—	—	—	—
33	7.56	7.58	7.58	7.72	8.13	—	—	—	—	—
34	7.88	7.86	7.80	8.12	8.22	—	—	—	—	—
35	8.07	8.27	8.02	—	8.35	—	—	—	—	—
36	8.53	8.26	8.34	—	—	—	—	—	—	—
37	—	8.44	8.51	—	—	—	—	—	—	—
38	—	8.70	—	—	—	—	—	—	—	—

LI Wei, Ph. D., professor, Ph. D. supervisor. Her main research interests include the design and analysis of symmetric ciphers.

GAO Jian-Ning, M. S. candidate. His main research interests focus on fault analysis of block ciphers.

GU Da-Wu, Ph. D., professor, Ph. D. supervisor. His main research interests include cryptology and computer security.

QIN Meng-Yang, M. S. candidate. His main research interests focus on fault analysis of block ciphers.

LIU Yuan, M. S. candidate. Her main research interests focus on fault analysis of block ciphers.

Background

Our work has been supported by the National Key Research and Development Program of China (Grant No. 2020YFA-0712300), the National Natural Science Foundation of China (Grant No. 62072307), and the Shanghai Sailing Program (Grant Nos. 21YF1401200 and 23YF1401000).

Pyjamask and SUNDAE-GIFT, both proposed at ToSC/FSE, are the candidates for the Lightweight Cryptography Standardization. These two lightweight cryptosystems are suitable for the Internet of Things (IoT). They can offer low storage and power consumption with flexibility in area, throughput, and power. Their security has been rigorously analyzed by a series of classical analysis or side channel analysis, such as differential analysis, linear analysis, impossible differential analysis, integral analysis, forgery analysis, algebraic analysis, and fault analysis, etc.

Fault analysis has been a competitive threat to cryptographic systems since 1996. It allows the attackers to exploit secret keys through fault injections. Boneh et al. successfully used fault analysis to break the RSA cryptosystem by exploiting the Chinese Remainder Theorem. Since then, more types of fault analysis have emerged, such as differential fault analysis, algebraic fault analysis, impossible differential fault analysis, and statistical fault analysis. Most classical cryptanalysis and fault analysis are based on the assumptions of the known plaintext attack or the chosen plaintext attack.

However, these assumptions do not hold for applications in the IoT, where the attackers may require more capabilities to obtain the corresponding ciphertexts. In the practical situations, the attackers may possess only minimal capabilities for a ciphertext-only attack (COA). Fuhr et al. introduced statistical fault analysis (SFA) specifically for the software implementation of AES. Following this, Dobraunig et al. successfully applied SFA to distinct authenticated encryption modes. Later, Li et al. extended SFA to Present and other lightweight cryptosystems.

Previous research has been limited in the known plaintext and chosen plaintext attacks, which prompt us to investigate new types and novel distinguishers of fault analysis. Our study proposes impossible statistical fault analysis (ISFA) for Pyjamask and SUNDAE-GIFT to combine the advantages of the impossible relationship and statistical fault analysis in software implementation. The results also demonstrate that the novel distinguishers of WD-HW and WD-MLE can reliably recover the secret keys of Pyjamask and SUNDAE-GIFT with no less than 99%. The presented ISFA not only decreases the faults, but also reduces the time and complexities. It offers a crucial reference for assessing the security of lightweight cryptosystems in the IoT.