轻量级认证加密算法SAEAES的滑动差分统计故障分析

摘要：SAEAES是2018年于国际密码硬件和嵌入式系统会议提出的轻量级认证加密算法，适用于资源受限场景。本文基于唯密文基本假设，采取随机单字节故障，提出了一种新型唯密文故障分析方法，即滑动差分统计故障分析。该方法基于滑动攻击，结合差分关系和统计故障分析，通过随机注入单字节故障，获取故障密文和标签并进行统计学分析破译SAEAES算法。本文还设计了基于机器学习的新型随机森林区分器。实验结果表明，本文提出的滑动差分统计故障分析方法使故障注入轮数加深一轮，随机森林区分器最少仅需78个故障即可破译SAEAES算法的128比特原始密钥。该结果聚焦于新型唯密文分析，有助于推动轻量级密码算法的进一步研究。

关键词：SAEAES；轻量级认证加密算法；滑动攻击；差分关系；唯密文
文献标志码：A
doi：*

Slide differential statistical fault analysis of the lightweight authentication encryption SAEAES

Abstract: SAEAES is a lightweight authentication encryption proposed at the cryptographic hardware and embedded systems in 2018. It is suitable for resource constrained scenarios. Based on the ciphertext-only assumption, this study adopts random single-byte faults and proposes a new ciphertext-only fault analysis method called slide differential statistical fault analysis. This method is derived from slide analysis and combines differential relations with statistical fault analysis. By randomly injecting single-byte faults, it collects faulty ciphertexts and tags, and decrypts the SAEAES algorithm through statistical analysis. This paper also designs a novel Random Forest distinguisher based on machine learning. The sliding differential statistical fault analysis method proposed in this study increases the number of fault injection rounds by one. The Random Forest distinguisher only needs 78 faults at minimum to recover the 128-bit original key of SAEAES. Focusing on the new ciphertext-only analysis, the results are helpful for further research on lightweight cryptographic algorithms.

Key words: SAEAES, lightweight authentication encryption, slide analysis, differential relation, ciphertext-only

0 引言

近年来，随着低空传感、无线通信以及边缘计算技术的集成应用，低空智联网已形成空地一体的融合体系，如图1所示。该体系外层为终端节点，包括低轨卫星、侦察机、智能汽车、智能穿戴设备、机器人与无人机。中间层由感知设施构成，涵盖传感器、信号接收器、雷达和摄像头。内层则为以控制中心为核心的管控中枢。外层低空设备是关键终端与组网节点，负责采集空域环境参数、交通运行状态和应急救援信息等敏感数据。中间层感知设施执行多源数据的汇聚、预处理以及转发任务。内层控制中心聚焦于感知分析、决策调度与安全管控等核心任务。这类场景下，一旦数据被恶意截获、篡改或伪造，将直接引发空域管控失效和任务中断等一系列安全事故。低空设备自身的载荷能力、计算资源及存储资源存在固有局限，导致传统密码算法难以寻求安全强度与运行效率之间的最优平衡。而轻量级密码算法凭借其低功耗和高安全的设计优势，针对低空智联网这类资源受限的应用场景能够在较低的计算成本下提供可靠的加密保护，因此成为保障低空设备数据安全的核心技术方案[1-7]。

2018年，Naito等学者在国际密码硬件和嵌入式系统会议(Cryptographic Hardware And Embedded Systems, CHES)提出了本文所研究的轻量级认证加密算法SAEAES[8]。同时，该算法也是美国国家标

收稿日期：XXXX–XX–XX；修回日期：XXXX–XX–XX

图 1　低空智联网络示意图

表 1　SAEAES 算法的安全性分析对比

分析类型	基本假设	攻击轮	故障注入轮	文献
伪造分析	选择明文	2 轮	-	[10]
中间相遇分析	选择明文	7 轮	-	[8]
差分分析	选择明文	7 轮	-	[11]
差分功耗分析	选择明文	10 轮	-	[9]
统计故障分析	唯密文	10 轮	第 8 轮	本文
滑动差分统计故障分析	唯密文	10 轮	第 7 轮	本文

准与技术研究院举办的轻量级密码标准化竞赛二轮入选算法。SAEAES 算法用 AES 高级加密标准做底层算法，分组长度为 64 比特，密钥长度为 128、192 或 256 比特，支持 64 和 128 比特可变长度的认证标签，可同时保证数据的机密性与完整性。2018 年，Naito 等学者利用中间相遇分析分段边界处存在可枚举、可匹配、可达的多重集状态冗余依赖关系，优化攻击的分段划分与集合匹配策略，恢复 SAEAES 算法的原始密钥[8]。2020 年，Sugawara 等学者通过分析 SAEAES 算法中 S 盒与非线性密钥扩展的功耗泄漏特性，实现差分功耗分析[9]。2022 年，Datta 等学者从 SAEAES 算法完整性验证之前明文的结构特性出发，构造出复杂度为 2^{32} 的伪造分析[10]。2025 年，Dinur 等学者针对 SAEAES 算法轮密钥独立模型下的差分传播结构特性，通过谱分析与泛函分析方法将成对置换独立性的理论下界压缩至 40 轮[11]。表 1 汇总了针对该算法不同安全性分析方法的对比。

1997 年，Boneh 等人针对 DES 算法首次提出了故障分析技术[12]。目前，该技术已成为衡量密码算法实现安全性的重要手段之一。该技术通过在算法执行过程中主动注入可控故障，获取正确与故障密文对，并借助数学分析逆向还原原始密钥，有效破坏算法安全性。主流的故障分析技术涵盖多种类型，包括差分故障分析、不可能差分故障分析、统计故障分析、无效故障分析、代数故障分析、中间相遇故障分析以及持久故障分析等[13]。其中，统计故障分析通过构建随机故障密文与中间状态之间的概率统计关联来反推密钥。攻击者能够依据自身能力与可用资源，灵活选取适配的故障分析手段，从而对认证加密算法、分组密码、流密码以及公钥密码等多种密码体制实施有效攻击。

基本假设在密码分析中起着决定性作用，它直接划定了攻击者的能力边界，也决定了攻击实现的复杂度。根据攻击者对加解密系统所拥有的控制权限，可将攻击模型分为选择密文、选择明文、已知明文与唯密文四种攻击类型[14]。传统攻击手段如线性密码分析和差分密码分析，通常假设攻击者能够获得相应的明密文对，即建立在选择明文或已知明文模型之上。与之不同，统计故障分析所依据的是唯密文攻击假设，攻击者仅需截获随机密文便可开展分析，对攻击者的要求相对较低。因此，统计故障分析在低空智联网等实际场景中表现出更强的实用性和可实施性。

2018 年，Dobraunig 等学者在 CHES 会议上提出统计故障分析[15]。其核心在于向算法中注入故障，分析故障对中间状态的影响，再借助统计手段对中间状态理论分布及其演化规律进行推导，最终实现密码破解。该方法近年来已具备绕过部分故障检测机制的能力，并可将应用范围延伸至瞬态、持久、永久、无效和有效等多种故障类型，从而对密码算法的实际安全性构成实质性威胁[16]。

1999 年，Biryukov 等学者提出滑动攻击[17]。滑动攻击的核心思想在于利用轮函数的结构相似性构建滑动路径来破译密码算法[18]。理论分析表明，采用迭代轮函数结构的密码算法均可能被滑动攻击破译。针对 SAEAES 算法的结构分析发现，其轮函数具备上述相似性特征，因此，攻击者可以构建滑动路径对 SAEAES 算法实施滑动攻击，从而破译该

算法。

目前，国内外尚无针对SAEAES算法抵抗唯密文攻击的相关研究。SAEAES算法独特的设计结构增加了传统故障分析的难度，传统方法难以覆盖更多轮次，也无法精准追踪复杂路径下的故障传播。因此，本文提出一种新型滑动差分统计故障分析方法，该方法基于唯密文假设，利用滑动路径关系和差分关系对SAEAES算法进行安全性评估[19]。与传统统计故障分析相比，滑动差分统计故障分析可以将故障注入位置加深一轮。同时，本文引入机器学习思想，提出新型随机森林区分器，使用此区分器可显著提升攻击效率。

实验结果表明，滑动差分统计故障分析可对SAEAES算法的倒数第三轮注入故障，仅需78次故障注入即可恢复128比特原始密钥，攻击成功率为99.9%及以上。本文所提出的滑动差分统计故障分析与统计故障分析相比，在所需故障数量、攻击深度和攻击效率上均更具优势。表2展示了上述两种故障分析结合六种区分器破译SAEAES算法的结果，并与现有AES算法统计故障分析的结果进行对比。六种区分器分别是平方欧氏距离区分器(Square Euclidean Imbalance, SEI)、最大后验估计区分器(Maximum a posterior, MAP)、拟合优度区分器(Goodness of Fit, GF)、极大似然估计区分器(Maximum Likelihood Estimation, MLE)、汉明重量区分器(Hamming Weight, HW)和随机森林区分器(Random Forest, RF)。

后续章节将依次介绍SAEAES算法及其故障分析、区分器设计、仿真实验结果和总结。

1　SAEAES算法简介

1.1　符号说明

记$P \in \{0,1\}^{64}$和$C \in \{0,1\}^{128}$分别为明文和密文，$A \in \{0,1\}^{64}$为关联数据，$N \in \{0,1\}^{128}$为随机数，$T \in \{0,1\}^{128}$为认证标签，IV为初始化向量，1^{64}表示长度为64比特的全1比特串；

记$K \in \{0,1\}^{128}$、$k_v \in \{0,1\}^{32}$和$RK_r \in \{0,1\}^{128}$分别为算法的128比特原始密钥、第v个密钥子集k的值和由四个不同密钥子集组合成的轮密钥，其中，$K = k_0 \| k_1 \| k_2 \| k_3$，$0 \leqslant v \leqslant 43$，$1 \leqslant r \leqslant 10$；

记SC、SR、MC和ARK分别表示加密算法的S盒替换、行移位、列混淆和轮密钥加四种操作，SC^{-1}、SR^{-1}、MC^{-1}和ARK^{-1}分别表示四种逆操作，$STATE$表示加密算法的中间状态；

记SW、RW和ARC分别表示密钥编排算法的S盒替换、列混淆和轮常数加操作，$TEMP$表示密钥编排的中间状态；

记R表示算法的轮函数，MSB_{64}和MSB_{128}分别表示为取最高64比特位和128比特位，H_K表示以K为密钥的认证变换；

记A_r、B_r、C_r和D_r分别表示第r轮的S盒替换、行移位、列混淆和轮密钥加的输出状态值，其中，$1 \leqslant r \leqslant 10$；

记$\oplus$、mod、&和||分别表示按位异或、取模运算、按位与和级联操作，$\ll$和$\gg$分别表示比特串的循环左移和循环右移。

1.2　SAEAES算法

2018年，Naito等学者在CHES会议上提出SAEAES轻量级认证加密算法，其底层基于AES高级加密标准的轮函数运算构建[8]。该算法以明文和密钥为输入，密文和标签为输出，主要适用于低空

表2　AES统计故障分析、SAEAES统计故障分析与SAEAES滑动差分统计故障分析的结果对比

区分器	AES统计故障分析[20]			SAEAES统计故障分析			SAEAES滑动差分统计故障分析		
	故障注入轮	故障数/个	成功率/%	故障注入轮	故障数/个	成功率/%	故障注入轮	故障数/个	成功率/%
SEI[21]	第10轮	320	≥99.9	第9轮	340	≥99.9	第8轮	212	≥99.9
HW[22]	第10轮	288	≥99.9	第9轮	217	≥99.9	第8轮	139	≥99.9
MLE[23]	第10轮	224	≥99.9	第9轮	229	≥99.9	第8轮	143	≥99.9
MAP[24]	–	–	–	第9轮	277	≥99.9	第8轮	176	≥99.9
GF[25]	–	–	–	第9轮	258	≥99.9	第8轮	167	≥99.9
RF	–	–	–	第9轮	145	≥99.9	第8轮	78	≥99.9

智联网等资源受限场景。其算法结构包含 S 盒替换、行移位、列混淆和轮密钥加四种核心操作，底层密码沿用 AES 算法的 S 盒与线性变换逻辑，该算法的函数结构如图 2 所示。算法按照 128、192 和 256 比特密钥，分为 SAEAES-128、SAEAES-192 和 SAEAES-256 三个版本。

1.2.1　加解密过程

SAEAES 算法每轮变换包括四种核心操作：S 盒替换、行移位、列混淆和轮密钥加。算法 1 给出了密钥长度为 128 比特的 SAEAES-128 算法的加密过程。

算法 1.　SAEAES-128 算法加密过程.

输入：N, A, K, P;

输出：C, T.

1) $IV = H_K(N,A)$;

2) $(RK_1,RK_2,\cdots,RK_{10}) = KeySchedule(K)$;

3) FOR r = 1 TO 10 DO

4) $STATE = ARK(MC(SR(SC(IV,RK_r))))$;

5) END FOR

6) $C = MSB_{64}(STATE) \oplus P$;

7) FOR r = 1 TO 10 DO

8) $STATE = ARK(MC(SR(SC(STATE,RK_r))))$;

9) END FOR

10) $T = MSB_{128}(STATE)$;

11) RETURN (C,T).

1.2.2　密钥编排方案

SAEAES 算法的密钥编排方案包括 S 盒替换、列混淆和轮常数加三种操作。算法 2 给出了 SAEAES-128 算法的密钥编排方案。

算法 2.　SAEAES-128 算法密钥编排算法.

输入：K;

输出：$RK_1,RK_2,\cdots,RK_{10}$.

1) $k_0 \,//\, k_1 \,//\, k_2 \,//\, k_3 = K$;

2) FOR v = 4 TO 43 DO

3) $TEMP = k_{v-1}$;

4) IF $v \bmod 4 = 0$ THEN

5) $TEMP = SW(RW(TEMP)) \oplus ARC_{v/4}$;

6) $RK_{(v/4)-1} = k_{v-4} \| k_{v-3} \| k_{v-2} \| k_{v-1}$;

7) ELSE

8) $k_v = k_{v-4} \oplus TEMP$;

9) END IF

10) END FOR

11) $RK_{10} = k_{40} \| k_{41} \| k_{42} \| k_{43}$;

12) RETURN $RK_1,RK_2,\cdots,RK_{10}$.

2　SAEAES 密码的故障分析

2.1　故障模型

攻击者构建面向随机单字节的故障模型，通过监听加密信道并在特定位置注入故障实施攻击。定义单字节的汉明重量 $h(t)$ 为其内部值为 1 的比特数，则 8 - $h(t)$ 表示值为 0 的比特数。受按位与操作的传播特性约束，故障注入后中间状态的各比特

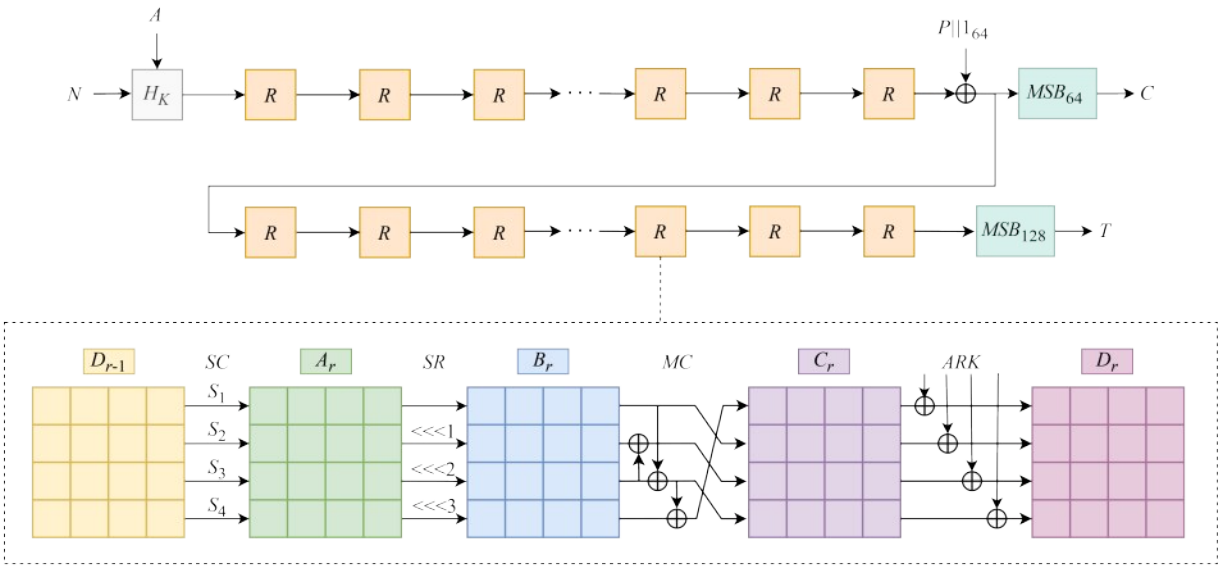

图 2　SAEAES-128 算法的结构图

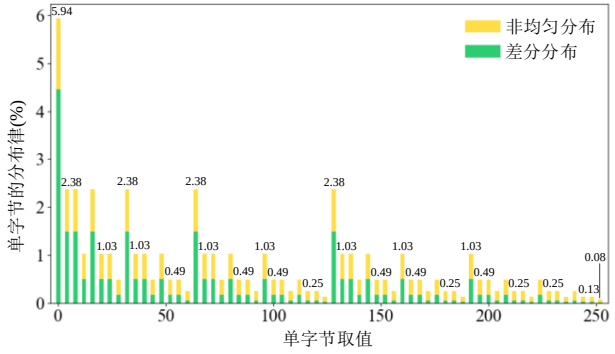

图3　受单字节故障影响的中间状态值分布

分布发生偏移。仅当原始比特与故障比特同时为1时，输出结果为1，否则恒为0。受此非线性变换影响，中间状态的统计分布如图3所示。据此，单字节取值的概率分布满足：

$$\left(\frac{3}{4}\right)^{8-h(t)}\cdot\left(\frac{1}{4}\right)^{h(t)}=\frac{3^{8-h(t)}}{4^{8}},\tag{1}$$

其中，t表示单字节中间状态所有可能取值，$h(t)$表示其汉明重量，$0\leqslant t\leqslant 255$，$0\leqslant h(t)\leqslant 8$。

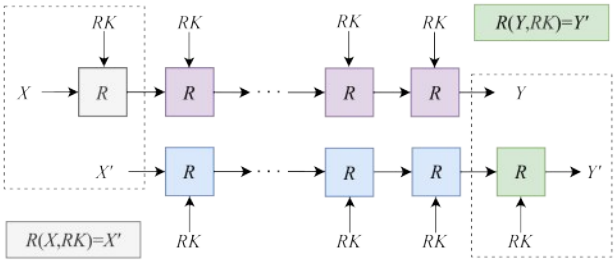

图4　滑动攻击的攻击模型

本节在统计故障分析中引入差分关系，通过对同一密钥推导出的中间状态两两差分运算，并依据差分值的统计分布实现密钥恢复。单字节差分值的取值分布满足：

$$\left(\frac{5}{8}\right)^{8-h(t)}\cdot\left(\frac{3}{8}\right)^{h(t)}=\frac{5^{8-h(t)}\cdot 3^{h(t)}}{8^{8}},\tag{2}$$

其中，t和$h(t)$的含义及范围同公式(1)。

2.2　滑动差分统计故障分析

2.2.1　滑动关系分析

1999年，Biryukov等学者提出滑动攻击，其利用密码算法每轮结构相似这一特点，通过构造滑动路径将多轮加密简化成单轮方程组，求解方程组即可恢复密钥[18]。具体而言，对于一个由相似轮函数加密构成的密码，已知两组明文密文对(X,Y)和(X',Y')，满足X'等于核心轮函数R通过轮密钥RK对X的加密结果，公式如下所示：

$$R(X,RK)=X'。\tag{3}$$

由于轮函数结构相似，Y通过相同轮函数R通过轮密钥RK加密后可得到Y'，公式如下所示：

$$R(Y,RK)=Y'。\tag{4}$$

此时，(X,Y)和(X',Y')构成滑动路径，如图4所示。找到滑动路径后，原本需分析多轮复杂变换的问题被简化为求解单轮方程组，公式如下所示：

$$\begin{cases}R(X,RK)=X'\\R(Y,RK)=Y'\end{cases}。\tag{5}$$

满足方程组成立的RK即可认为是正确轮密钥，再通过密钥扩展的逆过程，即可从轮密钥还原出主密钥。

在上述滑动攻击的基础上，本文提出了一种改进的滑动攻击方法，用于对SAEAES算法进行安全性分析。与传统滑动攻击不同，本文构造的滑动路径不再需要通过特定明文密文对主动构建，而是通过枚举所有可能的轮密钥和中间状态来构建。该设计削弱了经典滑动攻击中对轮密钥一致性的严格约束，同时将攻击能力从选择明文提升至唯密文场景，从而在轮密钥存在差异且无法主动构建明文密文对的实际环境中，仍然能够构建出滑动路径。

针对SAEAES算法，结合2.1节所述故障模型与滑动路径开展分析，将故障注入位置设定在倒数第三轮列混淆操作之后，此时对应中间状态为C_8，构建B_{10}映射到C_8的滑动路径，滑动路径的推导公式为：

$$\begin{aligned}C_8=&SC^{-1}(SR^{-1}(MC^{-1}(SC^{-1}(SR^{-1}(B_{10})))\\&\oplus RK_9))\oplus RK_8。\end{aligned}\tag{6}$$

穷举B_{10}的8比特、RK_8的8比特和RK_9的8比特，通过上述推导公式计算出倒推至C_8的映射结果，共$2^{24}(=2^8\cdot 2^8\cdot 2^8)$组映射结果，存储映射结果到映射矩阵。通过该映射矩阵，攻击过程中的推导过程无需再对C_8进行全量枚举，仅通过B_{10}的滑动映射即可完成状态推导，减少攻击过程中推导所需时间，降低攻击的计算复杂度。

2.2.2　差分关系分析

在2.1节所述故障模型中，推导出了受差分影响的故障发生的理论概率公式，并指出了故障值服从非均匀分布。图3展示了单字节差分值在实际攻击中统计分布情况，其非均匀特性与理论推导一

致，为后续差分关系分析提供了统计依据。

统计故障分析的加密过程采用同一密钥，因此对于采集的标签值而言，倒推中间状态过程中所使用的RK_8、RK_9和RK_{10}的值均相同。假设T_i和T_j为两个不同的标签值。由其逆向推导得到的差分值的公式为：

$$\begin{aligned} & C_8^i \oplus C_8^j \\ &= SC^{-1}(SR^{-1}(MC^{-1}(SC^{-1}(SR^{-1}(RK_{10}\oplus T_i)))\oplus RK_9 \\ &))\oplus RK_8 \oplus SC^{-1}(SR^{-1}(MC^{-1}(SC^{-1}(SR^{-1}(RK_{10}\oplus \\ &T_j)))\oplus RK_9))\oplus RK_8 \\ &= SC^{-1}(SR^{-1}(MC^{-1}(SC^{-1}(SR^{-1}(RK_{10}\oplus T_i)))\oplus RK_9 \\ &))\oplus SC^{-1}(SR^{-1}(MC^{-1}(SC^{-1}(SR^{-1}(RK_{10}\oplus T_j)))\oplus \\ &RK_9)), \end{aligned} \tag{7}$$

其中，$i \geqslant 1$,$j \geqslant 1$和$i \neq j$。由此可得，差分操作在统计故障分析中具有双重作用。其一，通过差分消去参数RK_8，可以有效压缩密钥的枚举空间，从而降低攻击实现的复杂度。其二，通过差分操作还能够有效扩充中间状态的样本数量。具体而言，假设收集到n个标签，将各标签逆向推导所得的中间状态进行两两异或，可以使样本量被扩充至$n(n-1)/2$倍，扩充后的样本集能够更充分地反映统计分布规律，从而提升正确密钥的识别效率，减少故障注入次数。其中，$n \geqslant 2$。同时，差分后滑动攻击的滑动路径不再需要枚举RK_8的8比特，只需枚举B_{10}和RK_9的8比特即可，消掉RK_8的滑动路径推导公式为：

$$\tilde{C}_8 = SC^{-1}(SR^{-1}(MC^{-1}(SC^{-1}(SR^{-1}(B_{10})))\oplus RK_9))。 \tag{8}$$

其中，$\tilde{C}_8$为原始中间状态C_8消掉RK_8后的中间状态。

本文创新地将滑动攻击所依赖的滑动路径、故障分析中的差分关系与统计故障分析相结合，提出滑动差分统计故障分析方法。该方法根据故障注入后得到的标签还原出倒数第一轮的中间状态，再借助滑动路径由该状态推导出倒数第三轮中间状态。此外，该方法借助差分操作对多组标签进行处理，在扩充有效样本数量的同时消除部分轮密钥，从而降低密钥枚举空间与计算复杂度。

2.2.3 *滑动差分统计故障分析*

本文结合滑动攻击和差分思想，提出了一种新型滑动差分统计故障分析方法。在该方法中，攻击者借助按位“与”操作，于加密流程的倒数第三轮引入单字节随机故障。该故障会修改中间状态对应比特位的数值，使其分布不再均匀。新方法基于唯密文攻击假设，只需获取随机标签，便可结合统计分析恢复密钥。攻击过程主要分为四个步骤:

步骤1：故障注入。攻击者在加密过程的倒数第三轮中通过按位“与”操作注入随机单字节故障。攻击者注入故障后会产生故障中间状态C_8^i和C_8^j，完成加密操作后，可以得到标签T^i和T^j。其中，$i \geqslant 1$,$j \geqslant 1$和$i \neq j$。故障注入后的扩散路径如图5所示。

步骤2：滑动差分关系分析。攻击者首先通过穷举中间状态B_{10}的8比特和RK_9的8比特，根据公式(8)构建中间状态B_{10}到$\tilde{C}_8$的完整映射路径，生成并存储共$2^{16}(=2^8 \cdot 2^8)$组映射结果。接着，攻击者通过得到的标签T^i结合最后一轮密钥RK_{10}的32比特，求得B_{10}^i，推导公式为：

$$B_{10}^i = ARK^{-1}(T^i) = RK_{10}\oplus T^i , \tag{9}$$

同理可通过T^j得到B_{10}^j。其中，i和j取值范围同步骤一所述。然后，攻击者通过预先储存的映射矩阵可以在得到B_{10}^i和B_{10}^j后快速得到$\tilde{C}_8^i$和$\tilde{C}_8^j$，二者异或即可得到$C_8^i \oplus C_8^j$。选取$C_8^i \oplus C_8^j$作为倒数第三轮的中间状态候选值，同时选取所对应的RK_9的8比特和RK_{10}的32比特作为候选密钥值。

步骤3：区分器筛选。攻击者选定合适的区分器，针对每个中间状态的差分值，计算出与之相对应的区分器的值，然后识别其中的极值，该极值对应的候选密钥即为真实密钥。攻击者在不同的单字节位置进行多次随机故障注入，并且在每次注入后，重复前述步骤一至三，从而获得RK_9的8比特和RK_{10}的32比特。图6展示了不同故障注入位置与密钥恢复位置的一一对应关系，通过覆盖全部4个位置的注入，即可拼接恢复出完整的128比特RK_{10}。同理，SAEAES算法其他版本的192比特和256比特密钥按照上述此步骤原理也可获取全部轮密钥信息。

步骤4：原始密钥恢复。攻击者通过故障分析成功获取轮密钥RK_{10}后，即可运用密钥编排算法完成对其余所有轮密钥以及原始密钥K的推导，具体密钥恢复算法推导过程如算法3所示。

算法3. SAEAES-128算法密钥恢复算法.

输入：RK_{10};

输出：K.

1) $k_{40} \,//\, k_{41} \,//\, k_{42} \,//\, k_{43} = RK_{10}$;

2) FOR v = 43 DOWN TO 4 DO

3) IF v mod 4 = 0 THEN

4) $TEMP = SW(RW(k_{v-1}))$;

5) $k_{v-4} = k_v \oplus TEMP \oplus ARC_{v/4}$;

6) ELSE

7) $k_{v-4} = k_{v-1} \oplus k_v$;

8) END IF

9) END FOR

10) $K = k_0 \| k_1 \| k_2 \| k_3$;

11) RETURN K.

2.3　区分器

利用故障注入后中间状态的分布偏差，可通过多种区分器对轮密钥候选集合进行评估。一旦满足特定分布条件，即可识别出轮密钥与原始密钥。攻击者可借助经典区分器在SAEAES的统计故障分析中实现密钥恢复，这与此前针对AES和LED等算法的统计故障分析思路类似。涉及的区分器包括：平方欧氏距离、汉明重量、极大似然估计和最大后验估计[27-28]。

2.3.1　经典区分器

(1)平方欧氏距离

距离是度量空间中点与点之间远近程度的基本指标，其中具有代表性的欧氏距离由古希腊学者Euclid提出。平方欧氏距离是在欧氏距离基础上进行平方运算得到的度量方式，可有效刻画向量之间的相似程度与差异程度，在密码分析、模式识别及机器学习等领域得到广泛应用。Fuhr等学者借助平方欧氏距离对中间状态的实际概率分布与理论概率分布进行对比，以距离的最大值为判别依据实现候选密钥的筛选，进而确定正确密钥[21]。平方欧氏距离区分器的数学表达式为：

$$\mathrm{SEI} = \sum_{u=0}^{255} \left(\frac{\Omega_u}{\Gamma} - \frac{1}{256} \right)^2, \tag{10}$$

其中，Ω_u代表中间状态u出现的理论概率，Γ为故障总数。由错误轮密钥产生的中间状态服从均匀分布，而由正确轮密钥产生的中间状态则不服从均匀分布。因此，预测轮密钥对应于使平方欧氏距离区分器取值最大化的密钥候选。

(2)最大后验估计

20世纪，最大后验估计作为贝叶斯推断的点估计策略被系统确立[22]。最大后验估计区分器的核心在于引入先验信息。该区分器需要预先完成先验假设计算，这与无需先验的极大似然估计形成鲜明对比。其底层采用贝叶斯统计模型对预测密钥进行区分，概率分布如图3所示。该方法提升了密钥筛选的可靠性与精度。最大后验估计区分器的表达式为：

$$\mathrm{MAP} = \frac{F(\tilde{\Omega}_u | \Phi_u) \cdot M(\Phi_u)}{\sum_{u=0}^{255} F(\tilde{\Omega}_u | \Phi_u) \cdot M(\Phi_u)}, \tag{11}$$

其中，$F(\tilde{\Omega}_u|\Phi_u)$表示由$\Phi_u$推导得到的$\tilde{\Omega}_u$的概率函数，$M(\Phi_u)$表示$\Phi_u$的先验函数，$\tilde{\Omega}_u$代表中间状态$u$出现的实际概率，$\Phi_u$为轮密钥候选值之一。预测轮密钥对应于使最大后验估计区分器取值最大化的密钥候选。

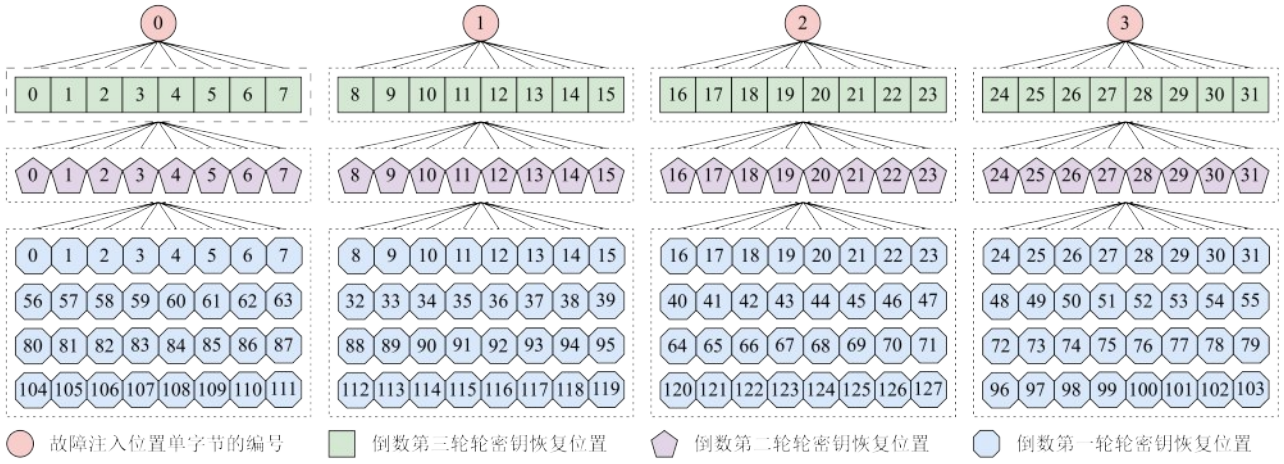

图6　注入故障位置与可恢复密钥位置对应关系

(3)拟合优度

拟合优度在密码分析中作为一种判别依据，用于评估以下两者之间的统计一致性，一是由错误密文逆向推导所得的中间状态值的实际分布，二是其理论分布[23]。使拟合优度取值最小的候选密钥，即判定为正确轮密钥。其表达式为：

$$\mathrm{GF}=\sum_{u=0}^{255}\frac{(\Omega_u-\Upsilon_u)^2}{\Upsilon_u}, \tag{12}$$

其中，Ω_u代表中间状态u出现的理论概率，Υ_u理论预期下中间状态值等于u的样本个数。

(4)极大似然估计

1922年，Fisher提出了基于概率模型的参数推断方法极大似然估计方法[24]。该方法是一种基于已知分布来对未知分布进行估计的统计方法，图3给出了极大似然估计方法按位与运算的概率分布。极大似然估计的表达式为：

$$\mathrm{MLE}=\prod_{u=0}^{255}\tilde{\Omega}_u^{\Omega_u}, \tag{13}$$

其中，$\tilde{\Omega}_u$为中间状态u的实际概率，Ω_u代表中间状态u的理论概率。此外，攻击者可利用图所示的概率分布。密钥即为使极大似然估计区分器取最大值的密钥候选。

(5)汉明重量

1954年，Reed提出了汉明重量的概念，用于表征二进制序列中非零比特的个数[25]。受按位“与”运算自身性质的影响，故障注入将破坏中间状态中比特0与比特1原有的均衡分布，导致比特0的出现频率显著高于比特1。基于这一现象，攻击者可基于按位与运算实施故障注入，统计得到比特0的数量，其通常会显著超过非零比特数量；其中，汉明重量取最小值时，对应的候选密钥即认为是正确轮密钥。汉明重量的表达式如下：

$$\mathrm{HW}=\frac{1}{256}\sum_{u=0}^{255}H(u)\cdot\Omega_u, \tag{14}$$

其中，$H(u)$用于计算u对应二进制串中非零比特的个数，Ω_u代表中间状态u出现的理论概率。

2.3.2　新型区分器

随机森林算法最早由Breiman等学者在20世纪90年代提出，旨在解决决策树模型的过拟合问题，并通过集成学习提高预测准确性[28-30]。其完整流程如图7所示，首先对原始数据集合进行有放回随机抽样得到子集1到子集m，其中$m\geqslant 2$；接着基于各子集分别训练独立的决策树，得到多个单树预测值；最终通过多数投票集成所有单树预测值，通过统计得票数量，选取获得票数最高的类别作为最终的决策输出。

本文在构建每一棵决策树时，随机选取原始数据中约2/3的样本作为训练集，剩余约1/3未被抽取的样本用于内部验证，以此方式生成多个差异化训练子集。

3　实验分析

本文基于搭载Intel(R) Core(TM) i7-9750H处理器的个人计算机平台，采用C++编程语言实现并完成了SAEAES-128算法仿真分析工作，覆盖随机故障注入与原始密钥恢复的全流程验证。为确保实验结果真实可靠，所有区分器恢复原始密钥所需故障数取1000次独立重复实验后成功率达到99%以上的最小故障数，实验耗时取该最小故障数下1000次独立重复实验的耗时平均值。

3.1　故障数

故障数对评估故障分析的效率至关重要，直接反映了攻击过程中所需注入的故障次数，是衡量不同故障分析方法性能优劣的核心量化指标。在采用统计故障分析方法恢复128比特原始密钥时，SEI、MAP、GF、MLE、HW及RF六种区分器所需的故障数分别为340、277、258、229、217与145个。使用滑动差分统计故障分析方法恢复128比特原始密钥时，上述六种区分器对应的故障数依次为212、176、167、143、139及78个。与统计故障分析方法相比，滑动差分统计故障分析方法降低了所需故障数。两种方法中，本文提出的RF区分器所需故障数最少。

3.2　耗时

耗时是评估故障分析攻击效率与实用价值的核心量化指标，它表示攻击者从注入故障到最终成功恢复出原始密钥的全过程总耗时。图8与图9分别呈现了两种方法在采用不同区分器恢复128比特原始密钥过程中的累积耗时情况。其中，横轴表示故障注入次数，纵轴表示所需时间。在使用统计故障分析方法时，当SEI、MAP、GF、MLE、HW及RF六种区分器均能达到99.0%及以上的密钥恢复成功率时，各自对应的耗时依次为4.58秒、3.29秒、3.03秒、2.54秒、2.37秒与1.51秒。使用滑动

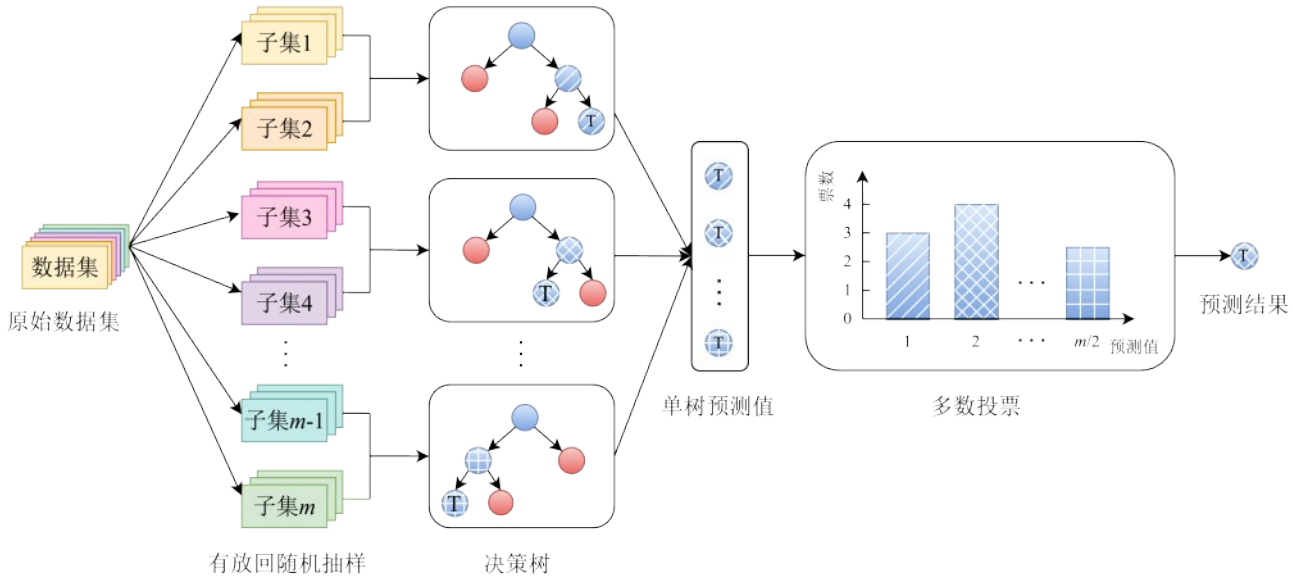

图7　随机森林区分器密钥筛选流程图

差分统计故障分析方法时，不同区分器耗时分别为2.27分钟、2.18分钟、2.28分钟、2.01分钟、1.09分钟和0.61分钟。两种方法中，本文提出的RF区分器相较于其他区分器缩短了恢复密钥所需的总时长。

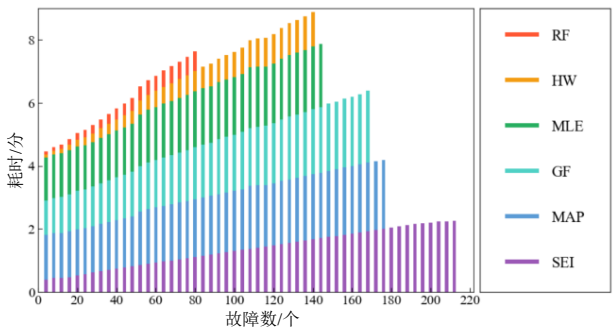

图9　滑动差分统计故障分析恢复128比特密钥耗时累加

3.3　成功率

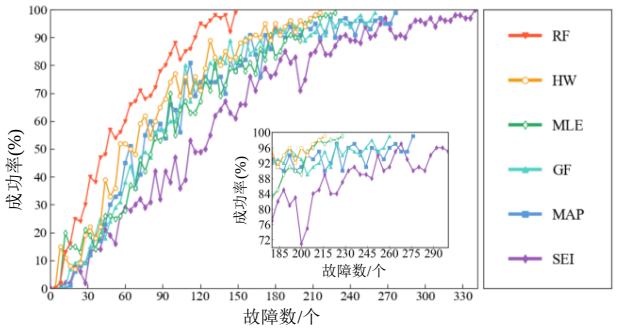

图10　统计故障分析恢复128比特密钥的成功率

成功率是指攻击者注入指定数量故障后，在限定攻击次数或攻击时间内成功破译主密钥的概率，是衡量故障分析攻击实用性的关键指标。分析过程中将剩余候选密钥个数不大于2且该集合中包含正确密钥的情况定义为成功。图10与图11分别呈现了统计故障分析方法与滑动差分统计故障分析方法在不同故障注入数量下的密钥恢复成功率。横轴表示故障注入次数，纵轴表示原始密钥的破译成功率。实验结果表明，SEI、MAP、GF、MLE、HW和RF六种区分器均能成功破译SAEAES-128算法，成功率达到99.9%及以上。在相同故障注入数量的条件下，本文提出的RF区分器的成功率表现优于传统区分器，能够在更少的故障注入次数下率先收敛至99.9%及以上的高成功率区间，展现出更优的破译效率与稳定性。

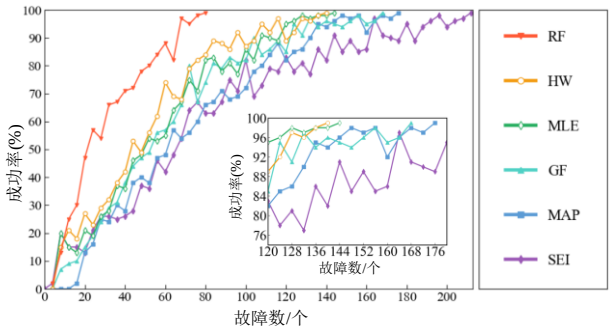

图 11　滑动差分统计故障分析恢复 128 比特密钥的成功率

3.4　复杂度

评估攻击方法效能与安全性的两个关键参数是数据复杂度和存储复杂度。前者指破解密码算法所需的数据量，后者指所需的空间量，两者共同反映了攻击实施过程中资源消耗与效率水平。数据复杂度的表达式如下：

$$\sigma \cdot 2^{\alpha}, \tag{15}$$

存储复杂度的表达式为：

$$\sigma \cdot 2^{\alpha} \cdot \varepsilon, \tag{16}$$

其中，σ为恢复原始密钥所需注入的故障数，α为候选密钥的比特数，2^{α}为候选密钥的个数，ε为所需存储的密文比特数。

表 3 对比了统计故障分析方法与滑动差分统计故障分析方法在恢复 SAEAES-128 算法 128 比特原始密钥时，达到最大成功概率所需的存储复杂度和数据复杂度。从表中可以看出，本文提出的 RF 区分器在两项指标上均优于传统区分器，展现出明显的性能优势。

表 3　区分器恢复 128 比特原始密钥的复杂度分析

区分器	统计故障分析		滑动差分统计故障分析	
	存储复杂度	数据复杂度	存储复杂度	数据复杂度
SEI	$2^{32.42}$	$2^{24.42}$	$2^{63.73}$	$2^{47.73}$
MAP	$2^{32.11}$	$2^{24.11}$	$2^{63.46}$	$2^{47.46}$
GF	$2^{32.01}$	$2^{24.01}$	$2^{63.38}$	$2^{47.38}$
MLE	$2^{31.84}$	$2^{23.84}$	$2^{63.16}$	$2^{47.16}$
HW	$2^{31.76}$	$2^{23.76}$	$2^{63.12}$	$2^{47.12}$
RF	$2^{31.18}$	$2^{23.18}$	$2^{62.28}$	$2^{46.28}$

4　结束语

本文研究了 SAEAES 算法抵抗滑动差分统计故障分析的安全性能。实验结果表明，本文所提分析方法在破解认证加密算法 SAEAES 时，成功率可达 99.9% 以上，且能够将故障注入到更深轮次。新型区分器随机森林区分器在保持高可靠性的同时，还降低了所需故障次数。

综上所述，滑动差分统计故障分析对轻量级认证加密算法 SAEAES 以及低空智联网中资源受限设备的安全性构成了严重威胁。

参考文献：

[1] ZHANG M, LU L, WU Y H, et al. A Lightweight Acoustic Fingerprint Based Drone Authentication System for Secure Drone the Delivery[J]. IEEE Transactions on Information Forensics and Security, 2025, 21(50): 1447-1461.

[2] CHEN J, CHEN R, KOU G. Unifying Attribute and Structure about Preservation for the Enhanced Graph Contrastive Learning[J]. IEEE Transactions on Neural Networks and Learning Systems, 2025, 3(4): 45-61.

[3] 何乐生, 靳亚灿, 张孝蔚等. 抗侧信道攻击对称算法的逐比特分析与功耗均衡防护[J]. 通信学报, 2025, 46(12): 213-221.
HE L S, JIN Y C, ZHANG X W, et al. Bitwise Analysis and Power Balanced Protection of Symmetric Algorithms Against Side Channel Attacks[J]. Journal on Communications, 2025, 46(12): 213-221.

[4] 李庚松, 刘艺, 郑奇斌, 等. 无人机多传感器数据融合研究综述[J]. 软件学报, 2025, 33(4): 1881-1905.
LI G S, LIU Y, ZHENG Q B, et al. Research Survey on Multi Sensor Data Fusion for to UAVs[J]. Journal of Software, 2025, 33(4): 1881-1905.

[5] 何乐生, 冯毅, 岳远康, 等. 针对物联网设备的旁路攻击及防御方法的研究[J/OL]. 通信学报, 2025, 22(4): 1-10.
HE L S, FENG Y, YUE K Y, et al. Research on Bypass Attacks and Defense Methods for Iot Devices[J/OL]. Journal on Communications, 2025, 22(4): 1-10.

[6] 黄韬, 刘江, 汪硕, 等. 未来网络技术与发展趋势综述[J]. 通信学报, 2021, 42(1): 130-150.
HUANG T, LIU J, WANG S, et al. Review on Future Network Technologies and the Development[J]. Journal on Communications, 2021, 42 (1): 130-150.

[7] 史殿习, 洪臣, 康颖, 等. 面向多无人机协同飞行控制的云系统架构[J]. 计算机学报, 2020, 24(12): 2352-2371.
SHI D X, HONG C, KANG Y, et al. Cloud System Architecture for Cooperative Flight Control Multiple UAVs[J]. Journal of Computer Science and Technology, 2020, 24(12): 2352-2371.

[8] NAITO Y, MATSUI M, SUGAWARA T, et al. About the Lightweight Blockcipher Based AEAD Mode of Operation[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 11(2): 192-217.

[9] SUGAWARA T. Hardware Performance Evaluation of Authenticated Encryption about the SAEAES with Threshold Implementation[J]. Cryptography, 2020, 16(3): 4-23.

[10] DATTA N, DUTTA A, GHOSH S. INT-RUP Security of SAEB and about TinyJAMBU[C]// Proceedings of International Conference on Cryptology in India. 2022: 146-170.

[11] DINUR I. New Techniques for Analyzing Differentials Application to AES[J]. IACR Cryptology ePrint Archive, 2025, 44(42): 166-174.

[12] BONEH D, DEMILLO R A, LIPTON R J. On the Importance of the Checking Cryptographic Protocols for about Faults[C]//Proceedings of the Theory and Applications of the Cryptographic Techniques. 1997: 37-51.

[13] SAYANDEEP S, DIRMANTO J, DEBAPRIYA R B, et al. About the Framework to about Counter Statistical Ineffective Fault Analysis of the Block Ciphers Using of the Domain Transformation and Error about Correction[J]. IEEE Transactions on Information Forensics and Security, 2020, 33(15): 1905-1919.

[14] BEYNE T, BOUVIER C. Exponential Sums in the Linear about Cryptanalysis[J]. Journal of Cryptology, 2026, 55(27): 1-16.

[15] DOBRAUNIG C, EICHLSEDER M, KORAK T, et al. SIFA: The Exploiting about the Ineffective Fault Inductions on Symmetric Cryptography[J]. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018, 52(22): 547-572.

[16] SAYANDEEP S, DIRMANTO J, DEBAPRIYA R B, et al. About Framework to Counter Statistical Ineffective Fault Analysis of Block Ciphers Using Domain Transformation and Error Correction[J]. IEEE Transactions on Information Forensics and Security, 2020, 55(15): 1905-1919.

[17] BIRYUKOV A, WAGNER D A. Slide Attacks[C]//Proceedings of Fast Software Encryption. 1999: 245-259.

[18] BIRYUKOV A, WAGNER D A. Advanced Slide Attacks[C]// Proceedings of European Cryptology Conference. 2000: 589-606.

[19] 李玮, 刘春, 谷大武, 等. Saturnin-Short轻量级认证加密算法的统计故障分析[J]. 通信学报, 2023, 22(44): 167-175.
LI W, LIU C, GU D W, et al. Statistical Invalid Fault Analysis of Saturnin-Short Lightweight Authenticated Encryption Algorithm[J]. Journal on Communications, 2023, 22(44): 167-175.

[20] DOBRAUNIG C, EICHLSEDER M, KORAK T, et al. Statistical Fault Attacks on Nonce-based Authenticated Encryption Schemes [C]//Proceedings of the Theory and Application of Cryptology and Information Security. 2016: 369-395.

[21] FUHR T, JAULMES E, LOMNE V, et al. Fault Attacks on AES with the Faulty Ciphertexts Only[C]//Proceedings of Fault Diagnosis and Tolerance in Cryptography. 2013: 108-118.

[22] WANG T, YE S, FANG F, et al. Deep Maximum about the Posterior Estimator for Accelerated MRI Reconstruction[J]. Knowledge-based Systems, 2025, 45(31): 938-956.

[23] ZHANG A, ZHOU W, XIE L, et al. Recurrent Neural about the Goodness-of-fit Test for a Time Series[C]//Proceedings of Artificial Intelligence and Statistics. 2025: 2917-2925.

[24] FISHER R A. On the Mathematical Foundations of the Theoretical about Statistics[J]. Philosophical Transactions of the Royal Society of London, 1922, 88(222): 309-368.

[25] REED I. A Class of Multiple-error-correcting Codes and Decoding about Scheme[J]. Transactions of the IRE Professional Group on Information Theory, 1954, 24(4): 38-49.

[26] GHOSAL A K, SARDAR A. Differential Fault the Analysis Attack-tolerant Hardware Implementation of Fault Analysis AES[J]. Journal of Supercomputing, 2023, 45(34): 4648-4681.

[27] ANTONIO G F, GAËTAN L, MARÍA P, et al. Internal Symmetries and Linear Properties Full-permutation Distinguishers and Improved Collisions on Gimli[J]. Journal of Cryptology, 2021, 56(14): 49-76.

[28] 苏睿韬, 任炯炯, 陈少真. 基于深度学习的GIFT-128与ASCON算法神经差分区分器研究[J]. 计算机学报, 2026, 55(23): 453-458.
SU R T, REN J J, CHEN S Z. Research on the Neural Differential Distinguishers of GIFT-128 and ASCON Algorithms Based on Deep Learning[J]. Journal of Computer Science and Technology, 2026, 55 (23): 453-458.

[29] HAGRASS O, SRIPERUMBUDUR B K, LI B. Spectral Regularized the Kernel Goodness-of-fit Tests[J]. Journal of Machine Learning Research, 2024, 56(25): 1-52.

[30] FACCIOLI M, MOELTNER K. Random Forests for Dichotomous Choice about the Contingent Valuation[J]. Journal of Environmental Economics and Management, 2026, 34(13): 303-324.