轻量级密码算法 TWINE 的唯密文故障分析

李玮[1,2,3,4]，汪梦林[1]，谷大武[2]，李嘉耀[1]，蔡天培[1]，徐光伟[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 200204；
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 200204；
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 200093）

摘 要：研究了唯密文攻击下 TWINE 密码的安全性，即在唯密文故障攻击下，利用 SEI、MLE、HW、GF、GF-SEI、GF-MLE、Parzen-HW、MLE-HE、HW-HE 和 HW-MLE-HE 等一系列区分器进行分析，能够以至少 99%的成功概率恢复 TWINE 密码的主密钥。仿真实验表明，所提新型区分器 MLE-HE、HW-HE 和 HW-MLE-HE 可以有效地减少故障数并提高攻击效率。研究结果为分析物联网中轻量级密码算法的安全性提供了重要参考。

关键词：轻量级密码；TWINE；唯密文故障分析；物联网

中图分类号：TP309.7

文献标识码：A

DOI: 10.11959/j.issn.1000−436x.2021039

Ciphertext-only fault analysis of the TWINE lightweight cryptogram algorithm

LI Wei[1,2,3,4], WANG Menglin[1], GU Dawu[2], LI Jiayao[1], CAI Tianpei[1], XU Guangwei[1]

1. School of Computer Science and Technology, Donghua University, Shanghai 201620, China
2. Department of Computer and Science and Engineering, Shanghai Jiao Tong University, Shanghai 200204, China
3. Shanghai Key Laboratory of Scalable Computing and System, Shanghai Jiao Tong University, Shanghai 200204, China
4. Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai Jiao Tong University, Shanghai 200093, China

Abstract: The security analysis of TWINE against the ciphertext-only fault analysis was proposed. The secret key of TWINE could be recovered with a success probability at least 99% using a series of distinguishers of SEI、MLE、HW、GF、GF-SEI、GF-MLE、Parzen-HW、MLE-HE、HW-HE and HW-MLE-HE. Among them, the novel proposed distinguishers of MLE-HE、HW-HE and HW-MLE-HE can effectively reduce the faults and improve the attack efficiency in simulating experiments. It provides a significant reference for analyzing the security of lightweight ciphers in the Internet of Things.

Keywords：lightweight cryptogram, TWINE, ciphertext-only fault analysis, Internet of things

1 引言

物联网是一种物与物进行信息交换和通信的网络。它通过智能设备和机器感知收集有关数据，提取数据中有用的信息并提供方便快捷的服务。物联网的发展促进了大量新兴领域的发展，例如智能家居、智慧医疗、精准农业、智慧交通等[1-4]。由于物联网中的智能设备及传感器的处理、存储资源有限，在收集、传送和处理网络中的大量数据时，传统的密码算法较难有效地保证信息的机密性、完整

收稿日期：2020−08−05；**修回日期：**2020−11−05

通信作者：李嘉耀，gaajiulei@gmail.com

基金项目：国家自然科学基金资助项目（No.61772129）；国家密码发展基金资助项目（No.MMJJ20180101）；上海市自然科学基金资助项目（No.19ZR1402000）；上海市可扩展计算与系统重点实验室开放课题基金资助项目；上海市信息安全综合管理技术研究重点实验室开放课题基金资助项目

Foundation Items: The National Natural Science Foundation of China (No.61772129), The National Cryptography Development Fund (No.MMJJ20180101), The Natural Science Foundation of Shanghai (No.19ZR1402000), Shanghai Key Laboratory of Scalable Computing and Systems, Shanghai Key Laboratory of Integrate Administration Technologies for Information Security

性和认证性，因此，运行效率高、吞吐量小和安全性高的轻量级密码算法适用于物联网中的安全数据处理[5-7]。

TWINE 是 2012 年在 SAC（selected areas in cryptography）会议上提出的一种具有广义 Feistel 结构的轻量级分组密码，旨在保护资源受限的终端设备的数据安全[8]。现有的 TWINE 的传统密码分析包括不可能差分故障分析、饱和分析、Biclique 分析、零相关线性分析、中间相遇分析等[8-11]。但是，在物联网环境中，攻击者可以通过激光照射、异常时钟、涡流磁场等方式注入故障，干扰密码的加密过程，这些故障会使中间状态的计算产生偏差，通过分析或者统计错误中间状态即可恢复密钥并破译密码，这种攻击方法称为故障分析（FA, fault analysis）。

故障分析是在 1997 年由 Boneh 等[12]提出的一种密码分析方法，它通过在密码设备运行过程中注入随机的故障，干扰正常运行过程，从而恢复出密钥并破译密码。后来，故障分析衍生出差分故障分析（DFA, differential fault analysis）、不可能差分故障分析（IDFA, impossible differential fault analysis）、中间相遇故障分析（MFA, meet-in-the-middle fault analysis）、统计故障分析（SFA, statistical fault analysis）和唯密文故障分析（CFA, ciphertext-only fault analysis）等[13-17]。这些分析方法是轻量级安全密码实现的重要实际威胁之一。

根据攻击能力的强弱，密码分析方法的攻击假设可以分为选择明文攻击（CPA, chosen-plaintext attack）、已知明文攻击（KPA, known-plaintext attack）和唯密文攻击（COA, ciphertext-only attack）等。针对 TWINE 的传统密码分析、现有故障分析的攻击假设主要集中在已知明文攻击和选择明文攻击，即攻击者需要获取当前密钥下的一些明文密文对，或特定明文对应的密文，这对攻击者的能力要求较强。在资源受限的物联网环境中，唯密文攻击对攻击者的能力要求最弱，攻击者仅需获取密文，因此容易在实际中应用，并可以有效地检测密码算法的实现安全性。

基于唯密文攻击的攻击假设，唯密文故障分析通过密码设备运行过程中注入随机故障，利用错误密文推导出的中间状态，分析相关的统计信息，在仅获得错误密文的情况下即可破译密码。TWINE 作为广义 Feistel 结构的典型密码之一，目前国内外都没有针对该密码的唯密文故障分析的相关研究，本文提出了针对 TWINE 的新型唯密文故障分析方法，设计并实现了 3 种新型区分器，从而降低了攻击代价，有效地提高了攻击效率。该方法的提出对于分析轻量级密码算法的安全性具有参考价值，同时对于增强物联网中信息的保护具有现实意义。

2 相关工作

密码分析是评测密码算法安全性的重要手段，国内外学者使用多种密码分析技术对 TWINE 进行了安全性分析。在传统密码分析方面，TWINE 的设计者分别利用不可能差分分析、饱和分析等对 TWINE 的安全性进行评估[8]。2012 年，Çoban 等[9]使用 Biclique 构造和中间相遇分析搜索密钥，对 TWINE 进行了 Biclique 分析。2014 年，Wang 等[10]使用改进的零相关线性分析检验 TWINE 的安全性，利用密钥编排方法的弱点并使用部分压缩技术降低了零相关线性分析的计算复杂度。2016 年，Tolba 等[11]利用广义中间相遇攻击，通过允许将密钥划分为 3 个子集来消除中间相遇攻击的限制，实现对 TWINE 的全密码攻击。以上攻击的假设均为选择明文攻击或者已知明文攻击。

在故障分析方面，2013 年，Yoshikawa 等[18]提出了差分故障分析，利用与同一明文相对应的一个正确密文和不同轮注入故障产生的错误密文，恢复了 TWINE 的 80 bit 主密钥。2015 年，Li 等[19]对 TWINE 进行了差分故障分析，在 31 轮利用故障模型“与”导入半字节故障，分别利用 8 个和 18 个故障恢复了 TWINE 的 80 bit 和 128 bit 主密钥。2017 年，高杨等[20]利用 S 盒的差分分布特性进行差分故障分析，采用随机半字节模型，在 33 轮、34 轮、35 轮平均注入 9 个故障，即可恢复 TWINE 的 80 bit 主密钥。此外，Nozaki 等[16]使用统计故障分析，通过在时钟中插入毛刺产生故障，统计 40 对正确密文和错误密文对应的中间状态的汉明权重最小平均值，恢复了 TWINE 的 80 bit 主密钥。现有的故障分析方法都是选择明文攻击的假设。

本文结合唯密文攻击的假设，对 TWINE 密码进行了唯密文故障分析。此时攻击者仅依赖错误密文，攻击能力最弱，因此，唯密文故障分析

的分析方案在现实的操作环境中具有更加灵活的应用前景。TWINE-80 和 TWINE-128 的安全性分析对比如表 1 所示。

表 1　TWINE-80 和 TWINE-128 的安全性分析对比

分析类型	基本假设	攻击轮数/轮	文献
不可能差分故障分析	CPA	23/24	文献[8]
饱和分析	CPA	22/23	文献[8]
Biclique 分析	CPA	36/36	文献[9]
零相关线性分析	KPA	23/25	文献[10]
中间相遇分析	KPA	36/36	文献[11]
差分故障分析	CPA	36/36	文献[18-20]
统计故障分析	CPA	36/36	文献[16]
唯密文故障分析	COA	36/36	本文

在唯密文故障分析方面，2013 年，Fuhr 等[17]针对 AES（advanced encryption standard）进行了唯密文故障分析，利用“与”故障模型，诱导随机字节故障生成错误密文，接着推导出对应的错误中间状态，利用平方欧氏距离（SEI，square Euclidean distance）、极大似然估计（MLE，maximum likelihood estimate）和汉明权重（HW，Hamming weight）等区分器筛选密钥候选值。实验结果表明，对于区分器 SEI、MLE 和 HW，分别导入 320、224 和 288 个随机字节故障就可以恢复 AES 的子密钥。2016 年，Dobraunig 等[21]提出，攻击者可以在基于 AES 的认证加密算法中注入故障进行破译。文献[22-24]采用唯密文故障分析的方法分别对轻量级密码算法 LED（light encryption device）、SIMON 和 MIBS 等进行安全性分析，扩展了唯密文故障分析的范围。然而，对于具有广义 Feistel 结构的 TWINE 能否抵御唯密文故障分析，国内外尚无文献发表。

本文给出了 TWINE 的新型唯密文故障分析，提出了新型区分器极大似然估计−直方图估计（MLE-HE，maximum likelihood estimate-histogram estimate）、汉明权重−直方图估计（HW-HE，Hamming weight-histogram estimate）和汉明权重−极大似然估计−直方图估计（HW-MLE-HE，maximum likelihood estimate-hamming weight-histogram estimate）等区分器，不仅减少了故障数，而且提高了分析效率。唯密文故障分析破译 AES、LED、SIMON、MIBS 和 TWINE 子密钥的结果对比如表 2 所示。

3　TWINE 密码介绍

3.1　术语说明

记 $X\in(\{0,1\}^4)^{16}$ 为明文，$Y\in(\{0,1\}^4)^{16}$ 为正确密文，$X_j^i\in\{0,1\}^4$ 表示第 i 轮中输入的第 j 个半字节，其中，$i\in[1,36]$ 且 $j\in[0,15]$。

记 K 为主密钥，k_l 为主密钥的第 l 个半字节，z 表示主密钥半字节个数，$\mathrm{RK}_t^i\in\{0,1\}^4$ 表示第 i 轮子密钥的第 t 个半字节，$\mathrm{CON}^i=\mathrm{CON}_{\mathrm{H}}^i\|\mathrm{CON}_{\mathrm{L}}^i$ 为第 i 轮密钥编排时的轮常数，其中，H 表示高 4 位，L 表示低 4 位，$z\in\{19,31\}$，$l\in[0,z]$，$i\in[1,36]$ 且 $t\in[0,7]$。

记 F 为轮函数，S 为混淆层，π 为扩散层。

记 ~ 为导入故障后的错误值，<<< 为循环左移，‖为级联。

3.2　TWINE 描述

TWINE 的分组长度为 64 bit，主密钥长度为 80 bit 或 128 bit，分别表示为 TWINE-80 版本和 TWINE-128 版本，迭代轮数为 36 轮，TWINE 结构

表 2　唯密文故障分析破译 AES、LED、SIMON、MIBS 和 TWINE 子密钥的结果对比

区分器	中文全称	AES-128[17]	LED-128[22]	SIMON-128[23]	MIBS-80[24]	TWINE-80/128
SEI	平方欧氏距离	320	280	∞	108	240/236
MLE	极大似然估计	224	160	264	70	144/144
HW	汉明权重	288	156	—	74	148/148
GF(goodness of fit)	拟合优度	—	240	408	110	216/224
GF-SEI	拟合优度−平方欧氏距离	—	212	376	86	224/216
GF-MLE	拟合优度−极大似然估计	—	—	288	92	224/216
Parzen-HW	窗估计−汉明权重	—	—	—	68	164/180
MLE-HE	极大似然估计−直方图估计	—	—	—	—	132/132
HW-HE	汉明权重−直方图估计	—	—	—	—	128/128
HW-MLE-HE	汉明权重−极大似然估计−直方图估计	—	—	—	—	124/124

如图 1 所示。加密部分和解密部分的结构相同，子密钥的使用顺序相反。算法 1～算法 3 分别给出了 TWINE 的加密算法和不同版本的密钥编排方案。

算法 1 TWINE 的加密算法

输入 $P=X_0^1\|X_1^1\|\cdots\|X_{15}^1$，

$\mathrm{RK}=\mathrm{RK}^1\|\mathrm{RK}^2\|\cdots\|\mathrm{RK}^{36}$

输出 Y

1) for i=1 to 35 do

2) $\mathrm{RK}^i=\mathrm{RK}_0^i\|\mathrm{RK}_1^i\|\cdots\|\mathrm{RK}_7^i$

3) for t=0 to 7 do

4) $X_{2t+1}^i=S(X_{2t}^i\oplus\mathrm{RK}_t^i)\oplus X_{2t+1}^i$

5) end for

6) for j=0 to 15 do

7) $X_{\pi[j]}^{i+1}=X_j^i$

8) end for

9) end for

10) for t=0 to 7 do

11) $X_{2t+1}^{36}=S(X_{2t}^{36}\oplus RK_t^{36})\oplus X_{2t+1}^{36}$

12) end for

13) $Y=Y_0\|Y_1\|\cdots\|Y_{15}=X_0^{36}\|X_1^{36}\|\cdots\|X_{15}^{36}$

算法 2 TWINE-80 版本的密钥编排方案

输入 $K=k_0\|k_1\|\cdots\|k_{18}\|k_{19}$

输出 $\mathrm{RK}^1,\mathrm{RK}^2,\cdots,\mathrm{RK}^{36}$

1) for i=1 to 35 do

2) $\mathrm{RK}^i=k_1\|k_3\|k_4\|k_6\|k_{13}\|k_{14}\|k_{15}\|k_{16}$

3) $k_1=k_1\oplus S(k_0),k_4=k_4\oplus S(k_{16})$

4) $k_7=k_7\oplus(0\|\mathrm{CON}_{\mathrm{H}}^i),k_{19}=k_{19}\oplus(0\|\mathrm{CON}_{\mathrm{L}}^i)$

5) $k_0\|\cdots\|k_3=(k_0\|\cdots\|k_3)<<<4$

6) $k_0\|\cdots\|k_{19}=(k_0\|\cdots\|k_{19})<<<16$

7) $\mathrm{RK}^{36}=k_1\|k_3\|k_4\|k_6\|k_{13}\|k_{14}\|k_{15}\|k_{16}$

算法 3 TWINE-128 版本的密钥编排方案

输入 $K=k_0\|k_1\|\cdots\|k_{30}\|k_{31}$

输出 $\mathrm{RK}^1,\mathrm{RK}^2,\cdots,\mathrm{RK}^{36}$

1) for i=1 to 35 do

2) $\mathrm{RK}^i=k_2\|k_3\|k_{12}\|k_{15}\|k_{17}\|k_{18}\|k_{28}\|k_{31}$

3) $k_1=k_1\oplus S(k_0),k_4=k_4\oplus S(k_{16})$

4) $k_{23}=k_{23}\oplus S(k_{30}),k_7=k_7\oplus(0\|\mathrm{CON}_{\mathrm{H}}^i)$

5) $k_{19}=k_{19}\oplus(0\|\mathrm{CON}_{\mathrm{L}}^i)$

6) $k_0\|\cdots\|k_3=(k_0\|\cdots\|k_3)<<<4$

7) $k_0\|\cdots\|k_{31}=(k_0\|\cdots\|k_{31})<<<16$

8) end for

9) $\mathrm{RK}^{36}=k_2\|k_3\|k_{12}\|k_{15}\|k_{17}\|k_{18}\|k_{28}\|k_{31}$

4 唯密文故障分析

4.1 基本假设和故障模型

唯密文故障分析的基本假设是唯密文攻击，此时，攻击者可以使用相同主密钥对随机明文进行加密，运行过程中导入随机故障获取相应的错误密文；再利用故障导入前后对应的中间状态分布的偏离，从而破译密码。根据 TWINE 的数据单元，本文采用了随机半字节的“与”故障模型，即

$$\tilde{X}_j^i=X_j^i\&e$$

其中，X_j^i 表示第 i 轮的第 j 个半字节中间状态值，$i\in[1,36]$ 且 $j\in[0,15]$，$\tilde{X}_j^i$ 表示对应的错误中间状态值，e 表示随机半字节故障且 $e\in[0,15]$，& 表示按位“与”操作。半字节被影响后的分布规律如图 2 所示。在具体实现时，软件通过结合中间状态与随

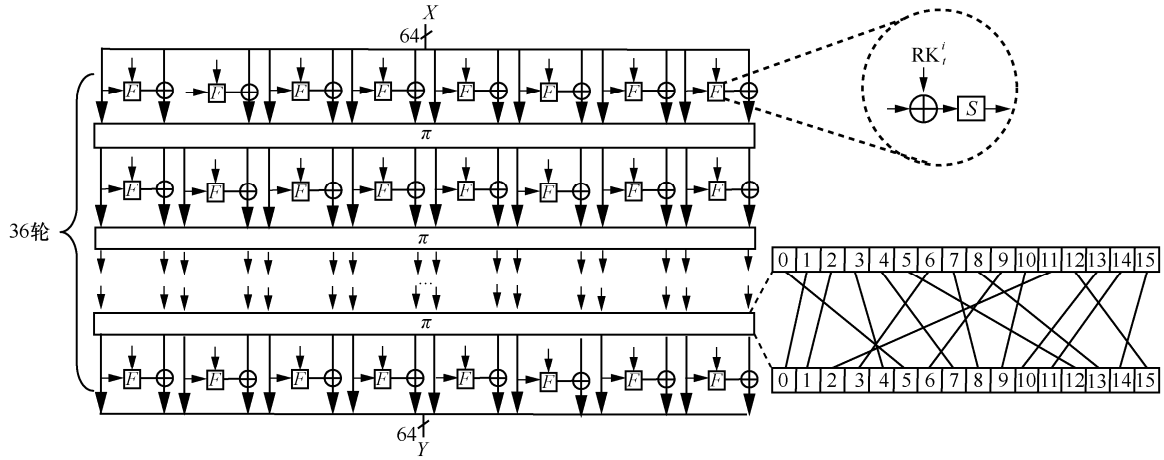


图 1 TWINE 结构

机半字节故障，进行“与”代码操作实现，硬件通过外部时钟信号注入毛刺实现[25]。

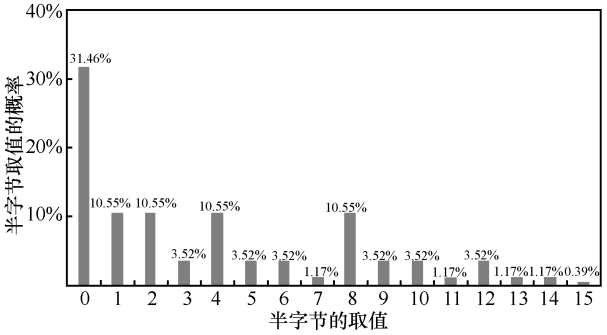


图 2　半字节被影响后的分布规律

4.2　攻击步骤

针对 TWINE 密码的唯密文故障分析包括以下 3 个步骤。

步骤 1　故障注入。攻击者使用相同主密钥对随机明文进行加密，在加密运行过程中注入指定轮的随机半字节故障，并获取相应的错误密文。图 3 给出了半字节故障注入第 33 轮随机位置时的故障扩散路径，以故障位置在首个半字节为例。

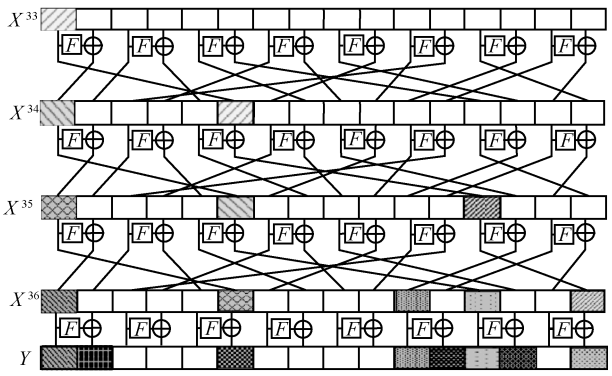


图 3　半字节故障注入第 33 轮随机位置时的故障扩散路径

步骤 2　恢复子密钥。攻击者分析错误中间状态、子密钥和错误密文之间的关系。首先，解密错误密文，利用区分器判定错误中间状态的实际分布与理论分布是否一致。若一致，则可以筛选出正确子密钥。具体实施如下，通过猜测子密钥中的 RK_1^{36}、RK_3^{35}、RK_7^{36} 和 RK_2^{34} 解密错误密文，获取密钥候选值对应的错误中间状态 $\tilde{X}_0^{33}$，推导如下。

$$\tilde{X}_0^{33}=\tilde{X}_5^{34}=S(X_7^{35}\oplus \mathrm{RK}_2^{34})\oplus \tilde{X}_{12}^{35}=$$
$$S((S(X_3^{36}\oplus \mathrm{RK}_3^{35})\oplus X_8^{36})\oplus \mathrm{RK}_2^{34})\oplus$$
$$\tilde{X}_{15}^{36}=S((S((S(Y_2\oplus \mathrm{RK}_1^{36})\oplus Y_3)\oplus$$
$$\mathrm{RK}_3^{35})\oplus Y_8)\oplus \mathrm{RK}_2^{34}\oplus (S(Y_{14}\oplus \mathrm{RK}_7^{36})\oplus \tilde{Y}_{15})$$

然后，计算区分器最大值或最小值，该错误中间状态 $\tilde{X}_0^{33}$ 对应的 RK_1^{36}、RK_3^{35}、RK_7^{36} 和 RK_2^{34} 候选值，即为正确子密钥中的字节。同理，攻击者重复上述步骤，利用故障注入 X_4^{33}、X_6^{33} 和 X_{12}^{33}，可以分别推导出子密钥中的 RK_3^{34}、RK_1^{35}、RK_0^{36}、RK_6^{36}、RK_1^{34}、RK_0^{35}、RK_2^{36}、RK_3^{36}、RK_7^{34}、RK_5^{35}、RK_4^{36} 和 RK_5^{36}，即可求解出最后一轮子密钥 RK^{36}。

步骤 3　破译主密钥。利用 RK^{36} 解密最后一轮，获得第 35 轮的输出，将故障注入第 32 轮，同理可恢复出倒数第二轮子密钥 RK^{35}。依次类推，破译 TWINE-80 版本主密钥 K，最少需要 3 轮子密钥 RK^{36}、RK^{35} 和 RK^{34}，过程如下。

$$K=(\mathrm{RK}_6^{36}\oplus(0\|\mathrm{CON}_{\mathrm{L}}^{35}))\|(\mathrm{RK}_7^{35}\oplus S(\mathrm{RK}_6^{36}\oplus$$
$$(0\|\mathrm{CON}_{\mathrm{L}}^{35})))\|\mathrm{RK}_4^{36}\|\mathrm{RK}_5^{36}\|\mathrm{RK}_2^{34}\|\mathrm{RK}_0^{35}\|$$
$$\mathrm{RK}_3^{34}\|\mathrm{RK}_1^{35}\|\mathrm{RK}_2^{35}\|\mathrm{RK}_0^{36}\|\mathrm{RK}_3^{35}\|(\mathrm{RK}_1^{36}\oplus$$
$$(0\|\mathrm{CON}_{\mathrm{H}}^{35}))\|\mathrm{RK}_2^{36}\|\mathrm{RK}_4^{34}\|\mathrm{RK}_3^{36}\|\mathrm{RK}_6^{34}\|$$
$$\mathrm{RK}_7^{34}\|\mathrm{RK}_4^{35}\|\mathrm{RK}_5^{35}\|(\mathrm{RK}_6^{35}\oplus(0\|\mathrm{CON}_{\mathrm{L}}^{34}))$$

破译 TWINE-128 版本主密钥 K，最少需要 5 轮子密钥 RK^{36}、RK^{35}、RK^{34}、RK^{33} 和 RK^{32}，过程如下。

$$K=\mathrm{RK}_7^{33}\|(\mathrm{RK}_6^{33}\oplus S(\mathrm{RK}_7^{33}))\|\mathrm{RK}_4^{36}\|\mathrm{RK}_5^{36}\|$$
$$(\mathrm{RK}_7^{34}\oplus S(\mathrm{RK}_2^{33}))\|(\mathrm{RK}_6^{34}\oplus S(\mathrm{RK}_7^{34}))\|$$
$$\mathrm{RK}_0^{33}\|(\mathrm{RK}_1^{33}\oplus(0\|\mathrm{CON}_{\mathrm{H}}^{32}))\|(\mathrm{RK}_7^{35}\oplus$$
$$S(\mathrm{RK}_2^{34}))\|(\mathrm{RK}_6^{35}\oplus S(\mathrm{RK}_7^{35}))\|\mathrm{RK}_0^{34}\|$$
$$(\mathrm{RK}_1^{34}\oplus(0\|\mathrm{CON}_{\mathrm{H}}^{33}))\|(\mathrm{RK}_7^{36}\oplus S(\mathrm{RK}_2^{35}))\|$$
$$(\mathrm{RK}_6^{36}\oplus S(\mathrm{RK}_7^{36}))\|\mathrm{RK}_0^{35}\|(\mathrm{RK}_1^{35}\oplus(0\|$$
$$\mathrm{CON}_{\mathrm{H}}^{34}))\|\mathrm{RK}_2^{33}\|\mathrm{RK}_4^{32}\|\mathrm{RK}_0^{36}\|((\mathrm{RK}_1^{36}\oplus$$
$$(0\|\mathrm{CON}_{\mathrm{H}}^{35}))\oplus(0\|\mathrm{CON}_{\mathrm{L}}^{32}))\|\mathrm{RK}_2^{34}\|\mathrm{RK}_4^{33}\|$$
$$\mathrm{RK}_5^{33}\|((\mathrm{RK}_3^{34}\oplus(0\|\mathrm{CON}_{\mathrm{L}}^{33}))\oplus S(\mathrm{RK}_5^{35}))\|$$
$$\mathrm{RK}_2^{35}\|\mathrm{RK}_4^{34}\|\mathrm{RK}_5^{34}\|((\mathrm{RK}_3^{35}\oplus(0\|\mathrm{CON}_{\mathrm{L}}^{34}))$$
$$\oplus S(\mathrm{RK}_5^{36}))\|\mathrm{RK}_2^{36}\|\mathrm{RK}_4^{35}\|\mathrm{RK}_5^{35}\|\mathrm{RK}_7^{32}$$

4.3　区分器

4.3.1　已有区分器

1) SEI

SEI 由 Fuhr 等[17]提出，用于计算实际分布与均匀分布之间的距离。在错误中间状态呈现不均匀分布时，若密钥候选值对应的错误中间状态的 SEI 值越大，则错误中间状态的实际分布与均匀分布距离越大。此时，SEI 最大值对应于正确的子密钥。SEI 表示为

$$\mathrm{SEI}=\sum_{\varepsilon=0}^{T-1}\left(\frac{\rho(\varepsilon)}{N}-\frac{1}{T}\right)^2$$

其中，T 表示半字节所有可能取值的个数，N 表示与密钥候选值相对应的一组错误中间状态个数，$\rho(\varepsilon)$ 表示错误中间状态值为 ε 的个数，$T=2^4$ 且 $\varepsilon\in[0,15]$。

2) MLE

MLE 由 Fuhr 等[17]提出，适用于已知错误中间状态的理论分布率的情况，如图 2 所示。将每个错误中间状态的理论分布率相乘，计算与密钥候选值对应的错误中间状态发生的概率。此时，MLE 值越大，表示错误中间状态实际分布满足理论分布的可能性越大，即 MLE 最大值对应于正确的子密钥。MLE 表示为

$$\mathrm{MLE}=\prod_{n=0}^{N-1}P(\tilde{X}_j^i)$$

其中，$P(\tilde{X}_j^i)$ 表示错误中间状态值 $\tilde{X}_j^i$ 的理论概率，N 表示与密钥候选值相对应的错误中间状态个数。

3) HW

HW 由 Fuhr 等[17]提出，用于计算错误中间状态与相同长度的零字符串之间的汉明距离，其值等于错误中间状态的非零个数。密钥候选值对应的错误中间状态的 HW 值越小，表示错误中间状态的零个数越多。此时，HW 最小值对应于正确的子密钥。HW 表示为

$$\mathrm{HW}=\frac{1}{N}\sum_{n=0}^{N-1}\mathrm{hw}(\tilde{X}_j^i)$$

其中，$\mathrm{hw}(\tilde{X}_j^i)$ 表示错误中间状态 $\tilde{X}_j^i$ 的汉明权重值，N 表示与密钥候选值对应的错误中间状态个数。

4) GF

GF 用于测量实际分布与理论分布之间的拟合度[22]。密钥候选值对应的错误中间状态的 GF 值越小，表示错误中间状态实际分布与理论分布之间的差异越小，即拟合度越大。此时，GF 的最小值对应于正确的子密钥。GF 表示为

$$\mathrm{GF}=\sum_{\varepsilon=0}^{T-1}\frac{(\rho(\varepsilon)-\gamma(\varepsilon))^2}{\gamma(\varepsilon)}$$

其中，T 表示半字节所有可能取值的个数，$\rho(\varepsilon)$ 表示错误中间状态值为 ε 的个数，$\gamma(\varepsilon)$ 表示理论上错误中间状态值为 ε 的个数，$T=2^4$ 且 $\varepsilon\in[0,15]$。

5) GF-SEI

GF-SEI 结合了 GF 和 SEI[22]。首先，攻击者使用 GF 过滤掉不符合理论分布的密钥候选值，满足

$$\mathrm{GF}=\sum_{\varepsilon=0}^{T-1}\frac{(\rho(\varepsilon)-\gamma(\varepsilon))^2}{\gamma(\varepsilon)},\quad \mathrm{GF}(\lambda)\leqslant\chi_\alpha^2$$

其中，χ_α^2 表示从 χ^2 分布上侧分位数表中查找的具有确定精度 α 的 GF 临界值，λ 表示筛选后的密钥候选值。然后，攻击者使用 SEI 过滤保留的密钥候选值 λ，满足

$$\mathrm{SEI}=\sum_{\varepsilon=0}^{T-1}\left(\frac{\rho(\varepsilon)}{N}-\frac{1}{T}\right)^2$$

对于 GF-SEI，正确的子密钥所对应的错误中间状态具有最小的 GF 值和最大的 SEI 值。

6) GF-MLE

GF-MLE 是由 GF 和 MLE 组合的双重区分器[23]。攻击者首先利用 GF 区分器筛选出与密钥候选值对应的错误中间状态，保留符合理论分布的错误中间状态，满足

$$\mathrm{GF}=\sum_{\varepsilon=0}^{T-1}\frac{(\rho(\varepsilon)-\gamma(\varepsilon))^2}{\gamma(\varepsilon)},\quad \mathrm{GF}(\lambda)\leqslant\chi_\alpha^2$$

然后，攻击者使用 MLE 选择使似然函数最大化的错误中间状态所对应的密钥候选值，满足

$$\mathrm{MLE}=\prod_{n=0}^{N-1}P(\tilde{X}_j^i)$$

对于 GF-MLE，正确的子密钥所对应的错误中间状态具有最小的 GF 值和最大的 MLE 值。

7) Parzen-HW

Parzen-HW 结合了 Parzen 和 HW 的优点[24]。首先，使用 Parzen 进行无参估计，缩小密钥候选值的搜索空间。Parzen 的值越大，表示区域内样本数越多即对应可能的密钥候选值。Parzen 满足

$$\mathrm{Parzen}=\frac{1}{N}\sum_{n=0}^{N-1}f(u)=\frac{1}{N}\sum_{n=0}^{N-1}f\left(\frac{\bar{X}_j^i-\tilde{X}_j^i}{h}\right)$$

其中，$f(u)$ 是窗函数，表示以 $\bar{X}_j^i$ 为中心，窗宽为 h 的区域内样本数量，N 表示与密钥候选值对应的错误中间状态个数。然后，攻击者使用 HW 对可能的密钥候选值进行筛选，满足

$$\mathrm{HW}=\frac{1}{N}\sum_{n=0}^{N-1}\mathrm{hw}(\tilde{X}_j^i)$$

对于 Parzen-HW，正确的子密钥所对应的错误中间状态具有最大的 Parzen 值和最小的 HW 值。

4.3.2 新型区分器

1) MLE-HE

直方图估计（HE, histogram estimate）以直方

图法作为基础来计算密钥候选值的概率密度。由图 2 可知，值较小的半字节出现概率较高，因此错误中间状态值的理论个数累加和占比越大，表示其出现较小半字节的次数越多，即对应正确的子密钥，HE 表达式为

$$\mathrm{HE}=\frac{\sum_{n=0}^{N-1}h(\tilde{X}_j^i)}{\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}h(\tilde{X}_j^i)}$$

其中，N 表示与密钥候选值相对应的错误中间状态个数，M 表示所有密钥候选值的个数，$h(\tilde{X}_j^i)$ 表示错误中间状态 $\tilde{X}_j^i$ 的理论个数。

MLE-HE 结合了 MLE 和 HE 这 2 种统计方法。首先，攻击者使用 MLE 统计错误中间状态，筛选出部分可能的密钥候选值，满足

$$\mathrm{MLE}=\prod_{n=0}^{N-1}P(\tilde{X}_j^i)$$

然后，攻击者使用 HE 进一步筛选。对于 MLE-HE，当错误中间状态同时具有最大的 MLE 值和 HE 值，即该错误中间状态的分布满足理论分布且具有最大的概率密度时，则对应正确子密钥。

2) HW-HE

HW-HE 结合了 HW 和 HE 的优点，能够提高唯密文故障分析的效率。首先，攻击者使用 HW 筛选出具有较小汉明距离的错误中间状态，满足

$$\mathrm{HW}=\frac{1}{N}\sum_{n=0}^{N-1}\mathrm{hw}(\tilde{X}_j^i)$$

然后，攻击者使用 HE 进一步筛选，概率密度最大的一组中间状态对应正确的子密钥，满足

$$\mathrm{HE}=\frac{\sum_{n=0}^{N-1}h(\tilde{X}_j^i)}{\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}h(\tilde{X}_j^i)}$$

对于 HW-HE，基于按位“与”操作，半字节中出现 0、1 的比例为 3:1。当一组错误中间状态同时具有最小的 HW 值和最大的 HE 值时，则这组错误中间状态的 0 和 1 比例最大，因而最接近图 2 的理论分布，那么该错误中间状态对应正确子密钥。

3) HW-MLE-HE

HW-MLE-HE 是在 MLE-HE 和 HW-HE 基础上的改进。首先，攻击者使用 HW 缩小密钥候选值的搜索空间，满足

$$\mathrm{HW}=\frac{1}{N}\sum_{n=0}^{N-1}\mathrm{hw}(\tilde{X}_j^i)$$

然后，攻击者利用 MLE 进一步统计密钥候选值对应的错误中间状态，选择似然函数值较大的错误中间状态，满足

$$\mathrm{MLE}=\prod_{n=0}^{N-1}P(\tilde{X}_j^i)$$

最后，攻击者使用 HE 在剩余的密钥候选值中进行筛选、验证，确定唯一正确的子密钥。满足

$$\mathrm{HE}=\frac{\sum_{n=0}^{N-1}h(\tilde{X}_j^i)}{\sum_{m=0}^{M-1}\sum_{n=0}^{N-1}h(\tilde{X}_j^i)}$$

对于 HW-MLE-HE，在筛选过程中，攻击者选择汉明权重较小的若干组错误中间状态，再比较各组错误中间状态的极大似然估计值，保留具有最大值的错误中间状态，其对应的密钥候选值中可能包含正确子密钥。为了保证所筛选的密钥的正确性和唯一性，利用 HE 比较各组错误中间状态的概率密度，具有最大值的错误中间状态与图 2 的理论分布最接近，即对应正确子密钥。所有区分器的对比如表 3 所示。

5　实验分析

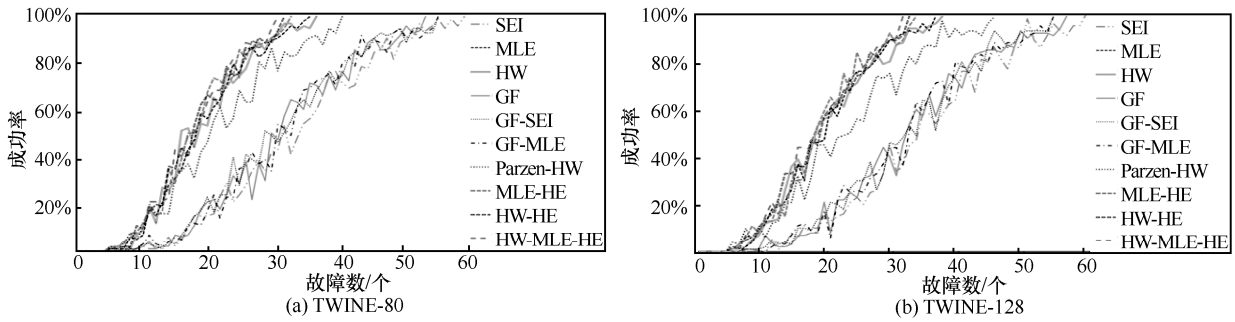
本实验采用 Java 语言编程，利用计算机软件来模拟故障产生和注入，在密码算法运行过程中注入半字节故障。以 TWINE-128 版本为例，唯密文故障分析每次恢复子密钥的 16 bit，重复 4 次，即可恢复最后一轮子密钥，依次类推，恢复最后 5 轮子密钥，即可推导出 128 bit 主密钥。在故障数、准确度、耗时和复杂度指标上，恢复 TWINE 各版本的主密钥与恢复子密钥的 16 bit 具有固定的比例关系。本节以恢复子密钥的 16 bit 的实验数据为单元，计算衡量各区分器分析 TWINE 各版本的效果。附录 1 给出了所有实验数据。

5.1　故障数

故障数指破译密码主密钥或子密钥时，所需要注入的故障个数。在相同的成功率下，破译密码所需要的故障数越少，表明攻击代价越少。图 4 给出了不同区分器恢复 TWINE 子密钥的 16 bit 的故障数与成功率之间的关系。其中，横坐标表示故障数，纵坐标表示成功率，不同曲线表示不同区分器唯密

表 3　区分器对比

区分器	中文全称	取值范围	对比
SEI	平方欧氏距离	最大值	通过最大化实际分布和均匀分布的平方距离和，筛选最不符合均匀分布的实际分布
MLE	极大似然估计	最大值	通过最大化变量的理论概率乘积，筛选出现概率最大的实际分布
HW	汉明权重	最小值	通过最小化变量与相同长度零字符串的汉明距离，筛选使变量二进制字符串中 1 的个数最少的实际分布
GF	拟合优度	最小值	通过对变量的理论个数与实际个数作运算，找出与理论分布差异最小的实际分布
GF-SEI	拟合优度−平方欧氏距离	GF 取最小值，SEI 取最大值	先使用 GF 筛选与理论分布较拟合的实际分布，再使用 SEI 筛选与均匀分布距离最大的实际分布
GF-MLE	拟合优度−极大似然估计	GF 取最小值，MLE 取最大值	先使用 GF 筛选与理论分布较拟合的实际分布，再使用 MLE 筛选似然函数值最大的实际分布
Parzen- HW	窗估计−汉明权重	Parzen 取最大值，HW 取最小值	先使用 Parzen 筛选在指定区域内样本数较多的实际分布，再使用 HW 筛选汉明距离最小的实际分布
MLE-HE	极大似然估计−直方图估计	MLE 和 HE 均取最大值	先使用 MLE 筛选变量的理论概率乘积较大的实际分布，再使用 HE 筛选理论个数累加和占比最大的实际分布
HW-HE	汉明权重−直方图估计	HW 取最小值，HE 取最大值	先使用 HW 筛选变量二进制字符串中 1 的个数较少的实际分布，再使用 HE 筛选概率密度最大的分布
HW-MLE-HE	汉明权重−极大似然估计−直方图估计	HW 取最小值，MLE 和 HE 取最大值	先使用 HW 筛选汉明权重较小的分布，再使用 MLE 筛选似然函数值较大的分布，最后 HE 筛选概率密度最大的分布



(a) TWINE-80　　(b) TWINE-128

图 4　不同区分器恢复 TWINE 子密钥的 16 bit 故障数与的成功率的关系

文故障分析的结果。以 TWINE-128 版本为例，利用区分器 SEI、MLE、HW、GF、GF-SEI、GF-MLE、Parzen-HW、MLE-HE、HW-HE 和 HW-MLE-HE 以至少 99%的成功率恢复子密钥，最少需要注入的故障数为 236、144、148、224、216、216、180、132、128 和 124。与已有区分器相比，本文提出的 3 种新型区分器 MLE-HE、HW-HE 和 HW-MLE-HE 需要的故障数较少，攻击效率高。此时，HW-MLE-HE 具有最少故障数。

5.2　准确度

准确度用于衡量各区分器筛选出的密钥候选值个数与理论值个数之间的差距。本节使用平均绝对误差（MAE, mean absolute error）来衡量各个区分器的准确度。MAE 表示为

$$\mathrm{MAE}=\frac{1}{V}\left(\sum_{v=1}^{V}\left|Q_v-1\right|\right)$$

其中，$V=1\,000$ 表示实验次数，Q_v 表示第 v 次实验筛选出的候选值个数，第 v 次实验理论候选值个数为 1。MAE 值越小，表示实验准确度越高。图 5 给出了不同区分器恢复 TWINE 子密钥的 16 bit 的故障数与 MAE 的关系。在相同故障数下，MLE-HE、HW-HE 和 HW-MLE-HE 的 MAE 值小于已有区分器的 MAE 值，且快速逼近于 0，此时，HW-MLE-HE 具有最小 MAE 值。

5.3　耗时

耗时是指恢复密钥所花费的时间，包括导入故障、遍历候选密钥和统计中间状态所消耗的时间。图 6 给出了不同区分器恢复 TWINE 子密钥的 16 bit 的故障数与耗时之间的关系，其中横坐标表示故障数，纵坐标表示耗时，不同的曲线表示不同区分器。以 TWINE-128 版本为例，利用区分器 SEI、MLE、HW、GF、GF-SEI、GF-MLE、Parzen-HW、MLE-HE、

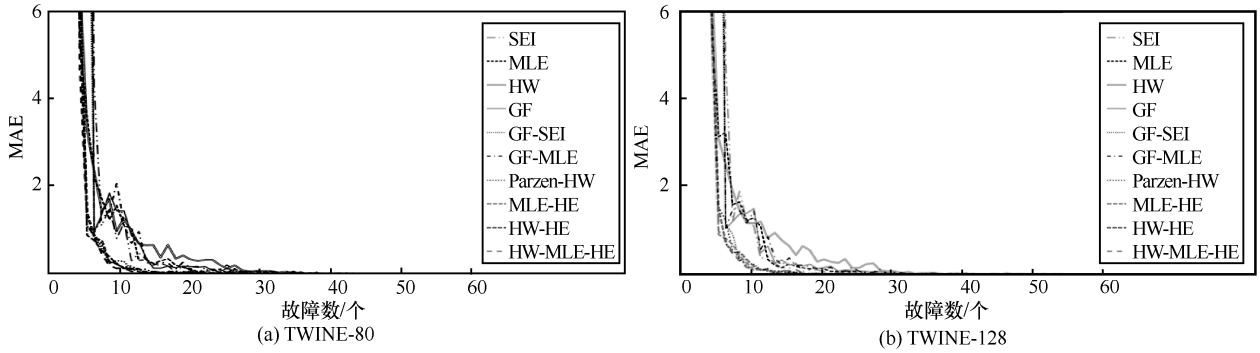


图 5　各区分器恢复 TWINE 子密钥的 16 bit 的故障数与 MAE 的关系

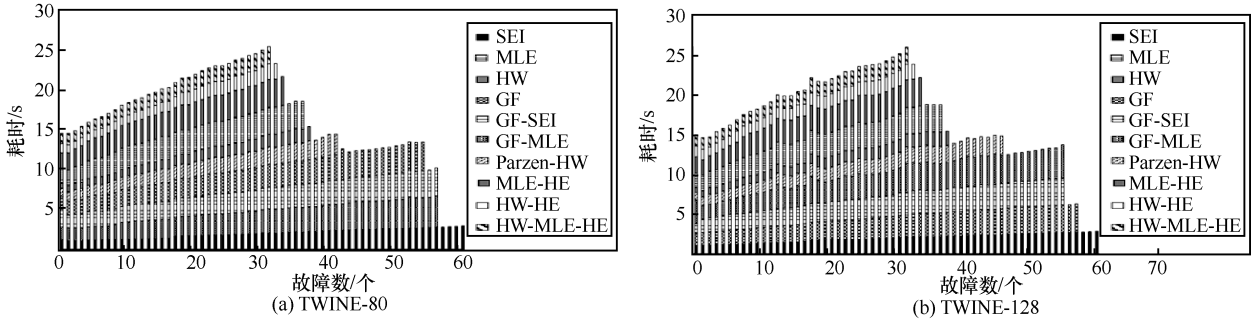


图 6　各区分器恢复 TWINE 子密钥的 16 bit 的故障数与耗时的关系

HW-HE 和 HW-MLE-HE 恢复子密钥最少需要的时间分别为 11.6 s、14 s、7.2 s、14 s、13.6 s、16.8 s、9.6 s、14.4 s、7.2 s 和 8.4 s。此时，HW 和 HW-HE 耗时最少，HW-MLE-HE 次之。

5.4　复杂度

时间复杂度和数据复杂度用于衡量破译密码时所需要的时间量和数据量。表 4 给出了不同区分器恢复 TWINE 子密钥的时间复杂度和数据复杂度。新型区分器 MLE-HE、HW-HE 和 HW-MLE-HE 的复杂度均小于现有区分器的复杂度，其中 HW-MLE-HE 的复杂度最小。

本节采用故障数、准确度、耗时和复杂度等指标衡量各个区分器对 TWINE 密码进行唯密文故障分析的效果。从图 4～图 6 和表 4 可以看出，新型区分器 MLE-HE、HW-HE 和 HW-MLE-HE 均有效减少了故障数，成功率达到 99%及以上，其中，HW-MLE-HE 所需要的故障数较少、准确度较高、复杂度较小；HW-HE 和 HW-MLE-HE 耗时较少。一般情况下，故障数是衡量唯密文故障攻击的首要标准。因此，在资源受限的物联网环境下，建议采用 HW-MLE-HE 对 TWINE 密码进行唯密文故障分析，可以达到相对较好的攻击效果。

表 4　不同区分器恢复 TWINE 子密钥的复杂度

区分器	TWINE-80		TWINE-128	
	时间复杂度	数据复杂度	时间复杂度	数据复杂度
SEI	$2^{27.91}$	$2^{23.91}$	$2^{27.88}$	$2^{23.88}$
MLE	$2^{27.26}$	$2^{23.17}$	$2^{27.26}$	$2^{23.17}$
HW	$2^{27.30}$	$2^{23.21}$	$2^{27.30}$	$2^{23.21}$
GF	$2^{28.75}$	$2^{23.75}$	$2^{28.81}$	$2^{23.81}$
GF-SEI	$2^{28.81}$	$2^{23.81}$	$2^{28.75}$	$2^{23.75}$
GF-MLE	$2^{28.81}$	$2^{23.81}$	$2^{28.75}$	$2^{23.75}$
Parzen-HW	$2^{28.45}$	$2^{23.36}$	$2^{28.58}$	$2^{23.49}$
MLE-HE	$2^{27.13}$	$2^{23.04}$	$2^{27.13}$	$2^{23.04}$
HW-HE	$2^{27.09}$	$2^{23.00}$	$2^{27.09}$	$2^{23.00}$
HW-MLE-HE	$2^{27.04}$	$2^{22.95}$	$2^{27.04}$	$2^{22.95}$

6　结束语

本文针对 TWINE 密码抵抗唯密文故障分析的安全性进行了研究，提出的新型区分器 MLE-HE、HW-HE 和 HW-MLE-HE，均可以减少攻击所需的故障数，并提高攻击效率。研究表明，TWINE 密码易受到唯密文故障分析的威胁，在物联网中使用该密码时，设计人员需采取有效措施用于抵御唯密文故障分析的攻击。

附录 1　实验数据

明文：随机生成

TWINE-80 版本主密钥：00112233445566778899

TWINE-128 版本主密钥：00112233445566778899AABBCCDDEEFF

本文中所有实验数据如表 5～表 7 所示。

表 5　　各区分器恢复 TWINE-80 和 TWINE-128 子密钥的 16 bit 的 MAE 值

故障数	SEI	MLE	HW	GF	GF-SEI	GF-MLE	Parzen-HW	MLE-HE	HW-HE	HW-MLE-HE
0	65535.00/ 65535.00	65535.00/ 65535.00	65535.00/ 65535.00	65535.00/ 65535.00	65535.00/ 65535.00	65535.00/ 65535.00	65535.00/ 65535.00	65535.00/ 65535.00	65535.00/ 65535.00	65535.00/ 65535.00
1	65535.00/ 65535.00	4095.00/ 4095.00	4095.00/ 4095.00	4095.00/ 4095.00	4095.00/ 4095.00	4095.00/ 4095.00	4095.00/ 4095.00	4095.00/ 4095.00	4095.00/ 4095.00	4095.00/ 4095.00
2	4087.32/ 4722.52	255.84/ 288.64	249.80/ 251.20	2312.88/ 2296.44	256.92/ 260.44	2323.32/ 2299.72	251.32/ 257.12	253.00/ 253.04	252.12/ 257.92	252.12/ 257.92
3	253.32/254.44	15.31/16.18	15.02/21.31	756.71/769.79	191.23/191.91	773.40/770.70	16.62/13.59	16.20/17.38	15.41/18.72	15.41/18.72
4	15.91/15.37	5.38/5.73	6.76/6.81	60.90/58.96	11.52/11.10	59.34/58.22	7.31/5.58	6.80/5.49	5.83/6.05	5.83/6.05
5	27.27/30.61	3.63/3.15	3.26/3.11	21.38/21.80	14.34/14.13	20.99/21.68	1.09/1.55	0.88/0.91	1.41/1.51	1.41/1.51
6	4.28/4.95	2.23/3.25	2.31/2.51	0.97/1.05	0.90/1.14	0.95/1.04	0.89/1.22	0.76/0.82	0.81/0.71	0.81/0.71
7	1.10/1.22	1.73/1.60	1.42/1.93	1.35/1.21	0.59/0.92	1.27/1.50	0.67/0.56	0.53/0.69	0.77/0.49	0.77/0.49
8	1.49/1.90	1.24/1.66	1.72/1.46	1.85/1.38	0.24/0.33	1.41/1.47	0.28/0.37	0.40/0.42	0.28/0.51	0.28/0.51
9	0.81/1.23	1.56/1.24	0.97/1.17	1.44/1.40	0.30/0.26	2.08/1.18	0.23/0.18	0.23/0.25	0.24/0.33	0.24/0.33
10	1.18/1.10	1.10/1.29	1.27/1.17	1.44/1.51	0.28/0.23	1.11/1.44	0.15/0.14	0.13/0.09	0.13/0.19	0.13/0.19
11	0.30/0.36	1.05/1.09	0.99/1.21	0.88/0.49	0.10/0.11	0.70/0.57	0.18/0.11	0.13/0.12	0.12/0.09	0.12/0.09
12	0.47/0.40	0.31/0.34	0.70/0.83	0.73/0.64	0.11/0.09	0.97/0.86	0.08/0.07	0.05/0.09	0.12/0.13	0.12/0.13
13	0.34/0.25	0.33/0.20	0.65/0.95	0.37/0.26	0.02/0.03	0.27/0.36	0.11/0.08	0.02/0.02	0.03/0.04	0.03/0.04
14	0.13/0.15	0.24/0.15	0.66/0.77	0.13/0.33	0.02/0.02	0.20/0.21	0.02/0.07	0.03/0.01	0.05/0.06	0.05/0.06
15	0.25/0.13	0.30/0.24	0.38/0.66	0.13/0.21	0.02/0.05	0.27/0.37	0.02/0.09	0.02/0.02	0.03/0.05	0.03/0.05
16	0.18/0.26	0.35/0.18	0.66/0.44	0.18/0.22	0.04/0.05	0.25/0.20	0.04/0.02	0.00/0.03	0.04/0.04	0.04/0.04
17	0.05/0.07	0.20/0.15	0.35/0.65	0.14/0.19	0.00/0.02	0.11/0.21	0.07/0.02	0.02/0.00	0.03/0.02	0.03/0.02
18	0.18/0.09	0.15/0.12	0.42/0.55	0.18/0.23	0.03/0.02	0.27/0.17	0.02/0.03	0.01/0.02	0.01/0.00	0.01/0.00
19	0.09/0.10	0.12/0.15	0.33/0.29	0.17/0.13	0.03/0.02	0.16/0.13	0.06/0.03	0.02/0.02	0.04/0.02	0.04/0.02
20	0.06/0.06	0.05/0.12	0.30/0.34	0.15/0.16	0.00/0.01	0.17/0.12	0.03/0.01	0.03/0.01	0.02/0.01	0.02/0.01
21	0.10/0.03	0.06/0.07	0.32/0.29	0.17/0.18	0.00/0.00	0.12/0.16	0.03/0.01	0.00/0.00	0.02/0.00	0.02/0.00
22	0.10/0.08	0.07/0.07	0.32/0.26	0.09/0.08	0.00/0.01	0.11/0.05	0.01/0.00	0.00/0.00	0.02/0.00	0.02/0.00
23	0.03/0.02	0.11/0.08	0.21/0.35	0.04/0.10	0.01/0.00	0.10/0.07	0.00/0.00	0.00/0.00	0.02/0.00	0.02/0.00
24	0.01/0.06	0.03/0.06	0.12/0.14	0.13/0.09	0.01/0.01	0.20/0.16	0.01/0.01	0.00/0.00	0.00/0.01	0.00/0.01
25	0.03/0.03	0.12/0.07	0.20/0.14	0.07/0.08	0.00/0.00	0.09/0.07	0.02/0.00	0.01/0.00	0.00/0.02	0.00/0.02
26	0.04/0.07	0.03/0.02	0.09/0.23	0.02/0.07	0.00/0.00	0.06/0.05	0.01/0.00	0.00/0.00	0.00/0.00	0.00/0.00
27	0.07/0.02	0.02/0.06	0.06/0.25	0.05/0.03	0.00/0.00	0.03/0.05	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00
28	0.04/0.06	0.02/0.06	0.07/0.09	0.08/0.06	0.01/0.00	0.05/0.11	0.00/0.00	0.00/0.01	0.00/0.01	0.00/0.01
29	0.02/0.02	0.04/0.02	0.07/0.07	0.06/0.02	0.00/0.00	0.02/0.02	0.00/0.00	0.00/0.00	0.00/0.01	0.00/0.01
30	0.06/0.03	0.06/0.03	0.07/0.07	0.01/0.02	0.00/0.00	0.02/0.05	0.02/0.00	0.00/0.00	0.00/0.00	0.00/0.00
31	0.01/0.00	0.02/0.00	0.03/0.03	0.02/0.03	0.00/0.01	0.02/0.04	0.00/0.01	0.00/0.00	0.00/0.00	0.00/0.00
32	0.05/0.04	0.01/0.02	0.05/0.05	0.03/0.03	0.00/0.00	0.02/0.01	0.00/0.01	0.00/0.00	0.00/0.00	—
33	0.03/0.01	0.04/0.00	0.02/0.02	0.02/0.02	0.00/0.00	0.05/0.00	0.00/0.00	0.00/0.00	—	—
34	0.01/0.00	0.01/0.01	0.02/0.03	0.04/0.04	0.00/0.00	0.01/0.00	0.00/0.00	—	—	—
35	0.02/0.02	0.01/0.00	0.00/0.04	0.00/0.00	0.00/0.00	0.02/0.03	0.00/0.00	—	—	—

（续表 5）

故障数	SEI	MLE	HW	GF	GF-SEI	GF-MLE	Parzen-HW	MLE-HE	HW-HE	HW-MLE-HE
36	0.04/0.01	0.00/0.00	0.02/0.03	0.01/0.02	0.00/0.00	0.01/0.02	0.00/0.00	—	—	—
37	0.02/0.02	—	0.00/0.00	0.01/0.00	0.00/0.00	0.01/0.00	0.00/0.00	—	—	—
38	0.01/0.01	—	—	0.02/0.02	0.00/0.00	0.00/0.02	0.00/0.00	—	—	—
39	0.02/0.00	—	—	0.00/0.03	0.00/0.00	0.02/0.01	0.00/0.00	—	—	—
40	0.03/0.02	—	—	0.01/0.01	0.00/0.00	0.00/0.02	0.00/0.00	—	—	—
41	0.02/0.00	—	—	0.00/0.02	0.00/0.00	0.01/0.02	0.00/0.00	—	—	—
42	0.01/0.00	—	—	0.01/0.01	0.00/0.00	0.00/0.00	—/0.00	—	—	—
43	0.00/0.01	—	—	0.01/0.00	0.00/0.00	0.00/0.00	—/0.00	—	—	—
44	0.02/0.00	—	—	0.00/0.02	0.00/0.00	0.00/0.00	—/0.00	—	—	—
45	0.00/0.00	—	—	0.00/0.01	0.00/0.00	0.00/0.00	—/0.00	—	—	—
46	0.00/0.03	—	—	0.00/0.00	0.00/0.00	0.00/0.00	—	—	—	—
47	0.01/0.01	—	—	0.00/0.01	0.00/0.00	0.00/0.00	—	—	—	—
48	0.01/0.00	—	—	0.01/0.02	0.00/0.00	0.00/0.00	—	—	—	—
49	0.01/0.01	—	—	0.00/0.01	0.00/0.00	0.00/0.00	—	—	—	—
50	0.00/0.00	—	—	0.00/0.00	0.00/0.00	0.01/0.01	—	—	—	—
51	0.00/0.00	—	—	0.00/0.01	0.00/0.00	0.00/0.01	—	—	—	—
52	0.00/0.01	—	—	0.00/0.00	0.00/0.00	0.00/0.00	—	—	—	—
53	0.00/0.00	—	—	0.01/0.01	0.00/0.00	0.00/0.00	—	—	—	—
54	0.00/0.01	—	—	0.00/0.00	0.00/0.00	0.00/0.00	—	—	—	—
55	0.00/0.00	—	—	—/0.00	0.00/—	0.00/—	—	—	—	—
56	0.00/0.00	—	—	—/0.00	0.00/—	0.00/—	—	—	—	—
57	0.00/0.00	—	—	—	—	—	—	—	—	—
58	0.00/0.00	—	—	—	—	—	—	—	—	—
59	0.00/0.00	—	—	—	—	—	—	—	—	—
60	0.00/−	—	—	—	—	—	—	—	—	—

表 6　　各区分器恢复 TWINE-80 和 TWINE-128 子密钥的 16 bit 的成功概率

故障数	SEI	MLE	HW	GF	GF-SEI	GF-MLE	Parzen-HW	MLE-HE	HW-HE	HW-MLE-HE
0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
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	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
5	0/0	1/0	2/1	0/0	0/0	0/0	2/4	1/1	1/2	2/0
6	0/0	1/0	0/1	0/0	0/0	1/0	1/3	1/3	1/1	2/2
7	2/0	1/2	1/2	0/1	1/1	4/1	3/10	4/6	2/7	3/5
8	0/1	6/4	1/5	1/1	0/1	1/1	8/4	6/11	2/6	7/6
9	1/0	5/9	7/7	1/1	1/1	1/0	5/11	8/8	11/10	9/8
10	2/0	7/12	9/12	2/7	3/2	3/0	10/6	12/13	10/14	10/15
11	1/4	19/18	19/13	4/4	3/5	7/2	20/12	18/13	17/16	21/21
12	1/1	15/19	12/14	1/2	2/3	3/4	16/13	15/21	20/22	21/16
13	3/3	21/21	27/26	2/2	1/4	2/3	16/20	17/15	19/33	21/22
14	6/8	28/26	26/36	2/3	4/3	4/7	16/21	35/30	36/33	23/27
15	2/6	31/37	30/39	7/7	3/10	6/11	31/32	29/30	35/36	43/44
16	5/11	35/30	51/33	6/7	7/10	5/12	34/22	39/31	44/36	40/44

（续表 6）

故障数	SEI	MLE	HW	GF	GF-SEI	GF-MLE	Parzen-HW	MLE-HE	HW-HE	HW-MLE-HE
17	10/10	43/46	52/43	7/8	11/9	11/9	37/31	50/46	40/47	49/43
18	15/10	47/46	44/53	11/8	15/14	12/8	31/45	50/53	53/45	50/49
19	15/17	58/47	54/56	18/21	17/14	11/17	42/45	56/59	62/57	55/57
20	15/13	56/61	53/57	21/8	23/21	17/6	46/40	67/65	66/59	63/61
21	16/15	61/57	65/64	22/22	17/20	24/21	55/48	73/61	64/61	68/64
22	23/16	64/65	61/61	18/22	24/18	14/28	61/49	72/75	64/68	68/65
23	29/21	70/72	75/69	24/25	24/27	23/25	52/50	69/67	78/68	76/74
24	21/23	79/76	71/71	32/23	40/30	23/26	56/56	74/84	74/74	81/75
25	24/20	75/76	74/76	29/31	28/30	35/25	68/55	85/77	75/75	73/78
26	28/25	83/78	77/78	38/32	41/38	36/31	63/65	81/78	86/84	88/81
27	34/26	86/81	84/83	22/38	39/26	42/33	63/74	89/84	85/82	87/86
28	38/33	82/85	88/79	37/44	37/33	37/37	80/73	87/86	90/87	86/87
29	34/45	84/89	85/80	30/40	51/46	39/44	77/75	88/92	88/89	87/89
30	42/34	89/90	90/87	50/32	49/45	34/44	86/66	90/87	88/89	94/90
31	43/36	90/92	92/88	47/45	46/48	54/36	76/76	91/89	93/91	99/99
32	53/45	92/93	96/94	57/54	50/53	52/51	84/82	94/95	99/99	—
33	41/47	95/92	96/94	64/60	55/49	49/63	82/79	99/99	—	—
34	48/58	94/96	93/92	63/57	61/64	61/59	83/86	—	—	—
35	54/58	97/93	95/95	60/66	64/63	68/66	88/87	—	—	—
36	56/54	99/99	94/96	71/57	61/51	69/71	90/86	—	—	—
37	60/58	—	99/99	70/65	68/64	72/72	91/97	—	—	—
38	66/62	—	—	66/75	72/70	73/62	87/90	—	—	—
39	75/64	—	—	74/73	76/74	75/80	94/94	—	—	—
40	76/76	—	—	68/69	72/80	70/78	92/91	—	—	—
41	71/76	—	—	76/78	74/75	79/77	99/93	—	—	—
42	69/67	—	—	72/83	82/80	82/82	—/93	—	—	—
43	70/81	—	—	85/84	84/76	78/83	—/91	—	—	—
44	78/80	—	—	82/85	82/87	91/80	—/96	—	—	—
45	77/86	—	—	88/85	86/93	85/88	—/99	—	—	—
46	84/81	—	—	90/84	90/90	89/85	—	—	—	—
47	85/77	—	—	85/87	92/86	88/88	—	—	—	—
48	90/86	—	—	85/86	91/88	84/88	—	—	—	—
49	81/86	—	—	88/93	92/92	92/88	—	—	—	—
50	88/98	—	—	91/90	94/93	94/91	—	—	—	—
51	90/89	—	—	95/92	88/93	90/92	—	—	—	—
52	90/86	—	—	92/92	94/93	93/95	—	—	—	—
53	96/91	—	—	93/92	94/93	90/92	—	—	—	—
54	93/96	—	—	99/91	92/99	92/99	—	—	—	—
55	95/93	—	—	—/94	92/—	94/—	—	—	—	—
56	98/91	—	—	—/99	99/—	99/—	—	—	—	—
57	94/95	—	—	—	—	—	—	—	—	—
58	98/95	—	—	—	—	—	—	—	—	—
59	95/100	—	—	—	—	—	—	—	—	—
60	99/–	—	—	—	—	—	—	—	—	—

表 7　　各区分器恢复 TWINE-80 和 TWINE-128 子密钥的 16 bit 的时间

故障数	SEI	MLE	HW	GF	GF-SEI	GF-MLE	Parzen-HW	MLE-HE	HW-HE	HW-MLE-HE
0	1.20/1.06	1.73/1.73	0.64/0.66	1.63/1.61	2.19/1.22	1.72/2.95	1.03/0.95	2.06/2.08	1.17/1.34	1.27/1.39
1	1.08/1.05	1.91/1.91	0.81/0.80	1.72/1.70	1.64/1.69	1.70/1.70	1.17/1.09	2.17/1.92	1.02/1.34	1.42/1.42
2	1.08/1.06	2.06/2.05	0.83/0.84	1.83/1.80	1.73/1.77	1.70/1.70	1.25/1.23	2.25/1.94	0.92/1.08	1.30/1.27
3	1.09/1.09	2.16/2.14	0.81/0.84	1.86/1.80	1.73/1.78	1.67/1.72	1.36/1.23	2.42/2.12	1.03/1.27	1.39/1.39
4	1.14/1.13	2.25/2.22	0.86/0.86	1.87/1.83	1.89/1.92	1.80/1.81	1.39/1.28	2.48/2.17	0.97/1.20	1.36/1.36
5	1.17/1.17	2.34/2.31	0.87/0.87	1.95/1.89	1.92/1.98	1.84/1.87	1.41/1.31	2.58/2.23	1.00/1.20	1.36/1.38
6	1.20/1.19	2.42/2.42	0.91/0.91	1.98/1.95	1.87/1.94	1.80/2.05	1.42/1.31	2.66/2.31	1.03/1.39	1.42/1.42
7	1.23/1.22	2.52/2.48	0.94/0.94	2.03/1.95	1.92/1.97	1.83/2.19	1.45/1.39	2.75/2.62	1.03/1.34	1.44/1.42
8	1.28/1.25	2.56/2.56	0.97/0.95	2.08/2.02	1.95/2.02	1.94/2.22	1.50/1.41	2.78/2.80	1.08/1.27	1.47/1.45
9	1.30/1.31	2.66/2.59	0.98/0.97	2.13/2.06	1.98/2.03	2.20/2.22	1.53/1.41	2.84/2.81	1.08/1.33	1.48/1.48
10	1.33/1.33	2.70/2.64	1.00/1.03	2.19/2.09	2.05/2.09	2.23/2.33	1.53/1.45	2.86/2.86	1.11/1.30	1.50/1.50
11	1.39/1.36	2.72/2.69	1.03/1.05	2.20/2.16	2.08/2.13	2.28/2.47	1.58/1.47	2.91/2.94	1.13/1.34	1.53/1.53
12	1.36/1.38	2.75/2.77	1.08/1.08	2.22/2.17	2.11/2.17	2.30/3.03	1.62/1.50	2.97/2.97	1.14/1.38	1.55/1.56
13	1.42/1.41	2.80/2.80	1.09/1.09	2.28/2.23	2.14/2.17	2.34/2.62	1.66/1.53	3.01/3.00	1.17/1.42	1.61/1.58
14	1.45/1.44	2.84/2.81	1.11/1.13	2.30/2.23	2.17/2.17	2.34/2.44	1.70/1.56	3.03/3.06	1.22/1.44	1.63/1.61
15	1.47/1.45	2.88/2.86	1.16/1.16	2.38/2.28	2.20/2.23	2.41/2.62	1.73/1.59	3.08/3.06	1.23/1.47	1.69/1.69
16	1.44/1.59	2.89/2.86	1.19/1.20	2.39/2.30	2.23/2.25	2.42/2.48	1.70/1.59	3.11/3.08	1.28/1.48	1.72/1.77
17	1.70/1.72	2.91/2.94	1.23/1.23	2.42/2.34	2.25/2.30	2.47/3.41	1.75/1.63	3.12/3.12	1.41/1.53	1.75/1.92
18	1.77/1.72	2.98/2.92	1.27/1.30	2.45/2.41	2.31/2.33	2.48/2.84	1.80/1.69	3.16/3.14	1.56/1.55	1.78/1.78
19	1.81/1.78	3.00/2.97	1.28/1.28	2.42/2.34	2.27/2.31	2.47/2.66	1.80/1.69	3.20/3.19	1.59/1.61	1.83/1.80
20	1.80/1.78	3.02/2.98	1.33/1.33	2.50/2.47	2.37/2.39	2.55/2.67	1.84/1.72	3.20/3.22	1.59/1.61	1.84/1.84
21	1.84/1.83	3.06/3.02	1.36/1.34	2.58/2.42	2.34/2.39	2.58/2.89	1.91/1.75	3.22/3.22	1.69/1.69	1.92/1.83
22	1.86/1.84	3.08/3.03	1.38/1.38	2.61/2.52	2.41/2.45	2.66/3.05	1.94/1.77	3.27/3.25	1.73/1.72	1.92/1.91
23	1.88/1.84	3.08/3.06	1.39/1.41	2.64/2.52	2.45/2.52	2.69/2.89	1.98/1.83	3.30/3.28	1.75/1.73	1.97/1.89
24	1.91/1.89	3.11/3.13	1.41/1.42	2.62/2.58	2.47/2.52	2.67/3.17	1.95/1.84	3.31/3.37	1.73/1.70	1.94/1.92
25	1.91/1.89	3.13/3.12	1.44/1.44	2.69/2.59	2.50/2.56	2.70/2.97	1.98/1.84	3.34/3.53	1.73/1.73	1.98/1.95
26	1.95/1.94	3.19/3.16	1.47/1.48	2.72/2.67	2.55/2.61	2.76/2.83	2.00/1.88	3.41/3.39	1.78/1.80	2.00/2.02
27	1.95/1.98	3.20/3.17	1.49/1.48	2.72/2.64	2.56/2.61	2.77/2.87	2.03/1.91	3.44/3.41	1.83/1.81	2.05/2.00
28	2.02/2.00	3.25/3.20	1.52/1.52	2.78/2.72	2.63/2.66	2.81/2.94	2.08/1.95	3.44/3.41	1.83/1.84	2.06/2.03
29	2.03/2.03	3.27/3.23	1.56/1.53	2.81/2.72	2.62/2.69	2.83/3.16	2.08/1.97	3.44/3.48	1.88/1.86	2.11/2.06
30	2.19/2.16	3.27/3.25	1.58/1.59	2.83/2.75	2.67/2.83	2.87/3.10	2.17/1.97	3.46/3.48	1.91/1.91	2.14/2.11
31	2.16/2.14	3.31/3.30	1.62/1.63	2.86/2.83	2.70/2.78	3.03/3.66	2.19/2.06	3.51/3.48	1.97/1.95	2.17/2.14
32	2.11/2.11	3.36/3.33	1.66/1.66	2.91/2.98	2.72/2.89	3.03/3.48	2.14/1.98	3.52/3.55	1.95/1.84	—
33	2.20/2.25	3.36/3.36	1.67/1.68	2.92/2.91	2.80/2.95	2.98/3.31	2.22/2.11	3.61/3.58	—	—
34	2.27/2.23	3.39/3.36	1.72/1.73	2.94/2.89	2.80/2.92	3.05/3.58	2.22/2.08	—	—	—
35	2.31/2.27	3.44/3.44	1.77/1.80	2.98/2.89	2.80/2.88	3.09/3.41	2.30/2.11	—	—	—
36	2.27/2.30	3.45/3.45	1.77/1.77	3.00/2.92	2.81/2.87	3.09/3.30	2.28/2.16	—	—	—
37	2.34/2.31	—	1.80/1.80	3.05/2.98	2.86/2.92	3.11/3.28	2.33/2.16	—	—	—
38	2.33/2.36	—	—	3.06/3.05	2.91/2.98	3.14/3.34	2.36/2.22	—	—	—
39	2.39/2.34	—	—	3.17/3.03	2.92/2.97	3.20/3.66	2.45/2.20	—	—	—

（续表 7）

故障数	SEI	MLE	HW	GF	GF-SEI	GF-MLE	Parzen-HW	MLE-HE	HW-HE	HW-MLE-HE
40	2.44/2.42	—	—	3.20/3.09	3.02/3.06	3.23/3.73	2.64/2.30	—	—	—
41	2.45/2.44	—	—	3.25/3.08	2.98/3.03	3.30/3.61	2.56/2.36	—	—	—
42	2.50/2.50	—	—	3.83/3.14	3.06/3.11	3.31/3.67	—/2.34	—	—	—
43	2.52/2.45	—	—	3.31/3.16	3.05/3.09	3.45/3.67	—/2.33	—	—	—
44	2.58/2.48	—	—	3.31/3.14	3.06/3.11	3.50/3.87	—/2.33	—	—	—
45	2.56/2.52	—	—	3.36/3.22	3.11/3.16	3.53/3.56	—/2.39	—	—	—
46	2.58/2.53	—	—	3.41/3.30	3.12/3.16	3.50/3.53	—	—	—	—
47	2.59/2.56	—	—	3.37/3.44	3.22/3.19	3.52/3.55	—	—	—	—
48	2.67/2.61	—	—	3.37/3.33	3.25/3.22	3.53/3.62	—	—	—	—
49	2.64/2.61	—	—	3.41/3.34	3.25/3.23	3.59/3.73	—	—	—	—
50	2.69/2.64	—	—	3.48/3.34	3.26/3.27	3.66/3.77	—	—	—	—
51	2.70/2.67	—	—	3.55/3.39	3.31/3.33	3.67/3.80	—	—	—	—
52	2.75/2.70	—	—	3.56/3.44	3.31/3.36	3.94/3.83	—	—	—	—
53	2.77/2.72	—	—	3.62/3.44	3.34/3.34	3.76/3.87	—	—	—	—
54	2.80/2.75	—	—	3.61/3.45	3.37/3.37	3.77/4.16	—	—	—	—
55	2.83/2.77	—	—	—/3.47	3.39/—	3.80/—	—	—	—	—
56	2.91/2.83	—	—	—/3.53	3.51/—	3.89/—	—	—	—	—
57	2.91/2.83	—	—	—	—	—	—	—	—	—
58	2.95/2.87	—	—	—	—	—	—	—	—	—
59	3.00/2.92	—	—	—	—	—	—	—	—	—
60	3.05/−	—	—	—	—	—	—	—	—	—

参考文献：

[1] SABIT H, CHONG P H J, KILBY J. Ambient intelligence for smart home using the Internet of Things[C]//2019 International Telecommunication Networks and Applications Conference. Piscataway: IEEE Press, 2019: 1-3.

[2] XIAO F, MIAO Q W, XIE X H, et al. Indoor anti-collision alarm system based on wearable Internet of things for smart healthcare[J]. IEEE Communications Magazine, 2018, 56(4): 53-59.

[3] VALECCE G, STRAZZELLA S, RADESCA A, et al. Solarfertigation: Internet of things architecture for smart agriculture[C]//2019 IEEE International Conference on Communications Workshops. Piscataway: IEEE Press, 2019: 1-6.

[4] BRINCAT A A, PACIFICI F, MARTINAGLIA S, et al. The Internet of things for intelligent transportation systems in real smart cities scenarios[C]//2019 IEEE World Forum on Internet of Things. Piscataway: IEEE Press, 2019: 128-132.

[5] BUTUN I, ÖSTERBERG P, SONG H. Security of the Internet of things: vulnerabilities, attacks and countermeasures[J]. IEEE Communications Surveys and Tutorials, 2020, 22(1): 616-644.

[6] ZHOU L, SU C H, YEH K H. A lightweight cryptographic protocol with certificateless signature for the Internet of things[J]. ACM Transactions on Embedded Computing Systems, 2019, 18(3): 1-10.

[7] HE D J, YE R, CHAN S, et al. Privacy in the Internet of things for smart healthcare[J]. IEEE Communications Magazine, 2018, 56(4): 38-44.

[8] SUZAKI T, MINEMATSU K, MORIOKA S, et al. TWINE: a lightweight block cipher for multiple platforms[C]//2012 International Conference on Selected Areas in Cryptography. Berlin: Springer, 2012: 339-354.

[9] ÇOBAN M, KARAKOÇ F, BOZTAŞ Ö. Biclique cryptanalysis of TWINE[C]//2012 International Conference on Cryptology and Network Security. Berlin: Springer, 2012: 43-55.

[10] WANG Y F, WU W L. Improved multidimensional zero-correlation linear cryptanalysis and applications to LBlock and TWINE[C]//2014 Australasian Conference on Information Security and Privacy. Berlin: Springer, 2014: 1-16.

[11] TOLBA M, YOUSSEF A M. Generalized MitM attacks on full TWINE[J]. Information Processing Letters, 2016, 116(2): 128-135.

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

[13] DUSRAT P, LETOURNEUX G, VIVOLO O. Differential fault analy-

sis on AES[C]//2003 International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2003: 293-306.

[14] BLÖMER J, SEIFERT J P. Fault based cryptanalysis of the advanced encryption standard (AES)[C]//2003 International Conference on Financial Cryptography. Berlin: Springer, 2003: 162-181.

[15] DERBEZ P, FOUQUE P A, LERESTEUX D. Meet-in-the-middle and impossible differential fault analysis on AES[C]//2011 International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2011: 274-291.

[16] NOZAKI Y, ASAHI K, YOSHIKAWA M. Statistical fault analysis for a lightweight block cipher TWINE[C]//2015 IEEE Global Conference on Consumer Electronics. Piscataway: IEEE Press, 2015: 477-478.

[17] FUHR T, JAULMES E, LOMNÉ V, et al. Fault attacks on AES with faulty ciphertexts only[C]//2013 Fault Diagnosis and Tolerance in Cryptography. Piscataway: IEEE Press, 2013: 108-118.

[18] YOSHIKAWA H, KAMINAGA M, SHIKODA A, et al. Round addition DFA on 80-bit piccolo and TWINE[J]. IEICE Transactions on Information and Systems, 2013, 96(9): 2031-2035.

[19] LI W, ZHANG W W, GU D W, et al. Security analysis of the lightweight cryptosystem TWINE in the Internet of Things[J]. KSII Transactions on Internet and Information Systems, 2015, 9(2): 793-810.

[20] 高杨, 王永娟, 王磊, 等. 轻量级分组密码算法TWINE差分故障攻击的改进[J]. 通信学报, 2017, 38(Z2): 178-184.
GAO Y, WANG Y J, WANG L, et al. Improvement differential fault attack on TWINE[J]. Journal on Communications, 2017, 38(Z2): 178-184.

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

[22] 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.

[23] 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.

[24] 李玮, 曹珊, 谷大武, 等. 物联网中 MIBS 轻量级密码的唯密文故障分析[J]. 计算机研究与发展, 2019, 56(10): 2216-2228.
LI W, CAO S, GU D W, et al. Ciphertext-only fault analysis of the MIBS lightweight cryptosystem in the Internet of things[J]. Journal of Computer Research and Development, 2019, 56(10): 2216-2228.

[25] KORAK T, HUTTER M, EGE B, et al. Clock glitch attacks in the presence of heating[C]//2014 Fault Diagnosis and Tolerance in Cryptography. Piscataway: IEEE Press, 2014: 104-114.

[作者简介]

李玮（1980− ），女，安徽寿县人，博士，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。

汪梦林（1998− ），女，河南信阳人，东华大学硕士生，主要研究方向为轻量级密码的安全性分析。

谷大武（1970− ），男，河南漯河人，博士，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。

李嘉耀（1996− ），男，广东广州人，东华大学博士生，主要研究方向为对称密码的故障分析。

蔡天培（1996− ），男，浙江温州人，东华大学硕士生，主要研究方向为对称密码的安全性分析。

徐光伟（1969− ），男，湖南衡阳人，博士，东华大学教授、硕士生导师，主要研究方向为网络与信息安全。