SIMON 轻量级密码算法的唯密文故障分析

李玮[1,2,3,4]，吴益鑫[1]，谷大武[2]，李嘉耀[1]，曹珊[1]，汪梦林[1]，蔡天培[1]，丁祥武[1]，刘志强[2]

（1. 东华大学计算机科学与技术学院，上海 201620；2. 上海交通大学计算机科学与工程系，上海 200240；
3. 上海市可扩展计算与系统重点实验室，上海 200240；4. 上海市信息安全综合管理技术研究重点实验室，上海 200240）

摘 要：在随机半字节故障模型下，针对 Feistel 结构的 SIMON 密码进行了唯密文故障攻击。导入随机半字节故障产生错误密文，对每个错误密文解密生成中间状态，利用统计学的知识分析中间状态的分布，在原有的 SEI 区分器、GF 区分器、MLE 区分器、MLE-SEI 双重区分器、GF-SEI 双重区分器和 GF-MLE 双重区分器的基础上，提出了新型的GF-MAP双重区分器、HW-MLE双重区分器、GF-HW双重区分器和HW-MAP双重区分器，对SIMON密码全部版本进行了统计分析。结果表明，SIMON 密码不能抵抗唯密文故障攻击，并且所提新型区分器在 SIMON 密码中需要故障数更少，攻击效果更好。研究成果为其他类似结构的算法提供了重要的借鉴。

关键词：轻量级密码；SIMON；唯密文故障分析

中图分类号：TP309. 7

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019204

Ciphertext-only fault analysis of the SIMON lightweight cipher

LI Wei[1,2,3,4], WU Yixin[1], GU Dawu[2], LI Jiayao[1], CAO Shan[1], WANG Menglin[1],
CAI Tianpei[1], DING Xiangwu[1], LIU Zhiqiang[2]

1. School of Computer Science and Technology, Donghua University, Shanghai 201620, China
2. Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
3. Shanghai Key Laboratory of Scalable Computing and Systems, Shanghai 200240, China
4. Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai 200240, China

Abstract: The ciphertext-only fault analysis on the SIMON cipher was proposed by injecting a random nibble fault under the random nibble fault model. After injecting faults, every faulty ciphertext could be decrypted and the statistical distribution of all intermediate states were analyzed by the attackers. On the basis of the previous distinguishers of SEI, GF, MLE, MLE-SEI, GF-SEI and GF-MLE, four novel distinguishers of GF-MAP, HW-MLE, GF-HW and HW-MAP were proposed to reduce faults. The results show that the SIMON cipher cannot resist against the ciphertext-only fault analysis. It provides an important reference for security analysis of other ciphers.

Key words: lightweight cipher, SIMON, ciphertext-only fault analysis

1 引言

随着信息技术与计算机技术的高速发展，物联网正逐步深入人们生活中，如何保障其中的信息安全问题已成为行业关注的焦点[1-2]。由于物联网环境中的传感器设备和射频识别技术等计算能力弱，存储量少，无法承载传统的密码算法，这就要求设计出执行效率高且吞吐量低的轻量级密码算法。轻量级密码算法由于其自身优势得到广泛应用，作为实现保密、完整性保护及认证

收稿日期：2019−05−27；**修回日期**：2019−08−28

通信作者：丁祥武，dingxw@dhu.edu.cn

基金项目：国家自然科学基金资助项目（No.61772129, No.61672347）；国家密码发展基金资助项目（No.MMJJ20180101）

Found Items: The National Natural Science Foundation of China (No.61772129, No.61672347), The National Cryptography Development Fund (No.MMJJ20180101)

的核心体制，其设计、分析和实现方法成为密码学研究的主流[3-5]。研究学者相继提出了多种轻量级密码算法，适用于物联网环境中类似 RFID（radio frequency identification）、智能卡和密码芯片等计算能力有限的微型计算设备[6-7]。

轻量级密码算法在快速发展的同时，其安全性分析也受到人们的广泛关注。例如，传统密码分析方法中的线性攻击、差分攻击、不可能差分攻击、立方攻击和差分−线性攻击等[8-10]。然而，在物联网环境中，单纯从密码算法的设计结构上研究安全性已经远远不够，攻击者可以借助激光照射、异常时钟和涡流磁场等方式干扰加密实现过程使其出错，从而泄露一些中间状态信息，利用中间状态信息获取密钥，这种攻击被称为“故障分析”[11-15]。由于其高效的攻击效果和潜在的威胁性，故障分析已成为国内外密码学领域的主流研究方向之一。

故障分析在发展过程中，逐步出现了多种类型的分析方法。1997 年，Biham 等[16]提出了一种新型的故障分析——差分故障攻击（DFA, differential fault attack），它是目前应用范围较广的一种故障分析技术。之后，又出现了不可能故障分析[17]、线性故障攻击[18]、中间相遇故障分析[19]、代数故障攻击[20]、无效故障分析[21]、碰撞故障分析[22]和唯密文故障分析[23]等攻击方法。上述方法均属于选择明文攻击（CPA, chosen plaintext attack）。然而，选择明文攻击有一定局限性，攻击者需要明确地知道明文以及对应的正确密文与错误密文，从而得到正确的密钥。

在故障分析中，唯密文故障攻击（CFA, ciphertext-only fault attack）是目前唯一一种能够在唯密文攻击（COA, ciphertext-only attack）的假设下进行攻击的技术[24]。攻击者在仅得到错误密文的情况下对密码算法进行破译，通过在加密过程的特定轮数导入随机故障，获得错误密文，解密密文获得中间状态，利用统计学的原理分析中间状态的分布律，即可获得正确密钥。由于唯密文攻击对攻击者能力要求最低，因此一旦攻击成功，会对密码算法的安全性造成巨大威胁。目前，在国内外的研究中，唯密文故障攻击 Feistel 结构的密码算法仅有 LBlock 轻量级密码算法，因此本文针对 Feistel 结构的 SIMON 密码算法进行唯密文故障攻击[25]。

2　相关工作

1997 年，Boneh 等利用随机故障成功破译了 RSA 算法，此后，故障分析在评测新型密码体制安全的方法中占据了重要的位置。SIMON 密码是美国国家安全局在 2013 年所提出的一种 Feistel 结构的轻量级密码算法[26]。SIMON 密码被设计出后受到了人们的广泛关注，研究者对该算法进行了大量的故障分析研究。2014 年，Tupsamudre 等[27]首次对 SIMON 密码进行差分故障分析，通过单比特故障模型和单字节故障模型在倒数第二轮导入故障。其中，若要恢复最后一轮密钥的 16 bit，则需要 8 个单比特故障或者 2 个单字节故障。为了进一步减少导入故障数，2015 年，Takahashi 等[28]针对 SIMON 密码进行了差分故障攻击，在随机“与”故障模型下，在 SIMON128/128 版本中，通过在倒数第二轮导入 7.8 个故障数成功恢复出整个密钥，这是首次通过随机故障模型成功恢复整个密钥。2016 年，Chen 等[29]提出了改进的差分故障攻击，在字节故障模型下使用最多 6.0 个故障数就能破译出密钥，成功减少了所需故障数。除了差分故障分析外，2017 年，Ma 等[30]对 SIMON32/64 版本与 SIMON128/128 版本进行代数故障攻击（AFA, algebraic fault attack）。结果表明，在 SIMON 32/64 版本中，通过单比特故障模型将故障导入第 26 轮，只需 5.0 个故障数就能恢复整个密钥；在 SIMON128/128 版本中，将故障导入第 65 轮，只需 2 个故障数即可求得密钥。上述分析方式都是选择明文攻击，本文对 SIMON 密码进行的唯密文故障分析研究是一种在唯密文攻击假设下进行攻击的密码分析技术。表 1 列出了目前针对 SIMON 密码的故障分析研究，分别是差分故障攻击和代数故障攻击，这 2 种分析方法都属于选择明文攻击，本文针对 SIMON 密码提出了唯密文故障攻击，该分析方法属于唯密文攻击。

表 1　针对 SIMON 密码的故障分析研究

类型	故障假设	模型	提出文献
DFA	CPA	Bit/Byte	文献[27-29]
AFA	CPA	Bit	文献[30]
CFA	COA	Nibble	本文

唯密文故障攻击是 Fuhr 等[24]于 2013 年针对 SPN 结构的 AES（advanced encryption standard）密

码算法提出的一种新型故障攻击，通过在算法加密过程中导入随机故障，获得大量错误密文样本，统计某一轮中的中间状态值，利用统计学中的理论恢复出密钥。其中，在字节故障模型下，通过在倒数第二轮导入 80 个故障数，利用 SEI（square Euclidean imbalance）区分器恢复出密钥；通过在倒数第一轮导入 56 个故障数，利用 MLE（maximum likelihood estimate）区分器恢复出正确密钥。李玮等[31]于 2017 年针对代换置换结构的 LED 轻量级密码算法改进了唯密文故障攻击，除了原有的区分器外，又提出了 2 种效率更高的新型区分器，分别是拟合优度 GF（goodness of fit）区分器和 GF-SEI 双重区分器。2018 年，李玮等[25]提出了针对 Feistel 结构的 LBlock 轻量级密码算法的唯密文故障攻击，同时提出了 2 种新型双重区分器 GF-MLE 和 MLE-SEI，减少了导入故障数，提高了攻击效率。

本文提出了 SIMON 密码的新型唯密文故障攻击，将故障导入在倒数第三轮，在已有的区分器 SEI、GF、MLE、MLE-SEI、GF-SEI 和 GF-MLE 的基础上，提出了新型的双重区分器 GF-MAP、HW-MLE、GF-HW 和 HW-MAP。表 2 总结了 AES 密码、LBlock 密码和 SIMON 密码中所使用的区分器。在 AES 密码中，仅使用了 2 种区分器对其进行破译；在 LBlock 密码中，使用了 6 种区分器；在 SIMON 密码中，除了原先的 6 种区分器，又使用新提出的 4 种新型区分器对密码进行破译。表 3 列出了针对各个版本 SIMON 密码的唯密文故障分析部分子密钥结果对比，展示了使用不同的区分器破译各个 SIMON 密码所需要的故障数。

表 2 SIMON、LBlock 和 AES 密码的唯密文故障分析区分器使用对比

区分器	版本		
	AES	LBlock	SIMON
SEI	Y	Y	Y
GF	—	Y	Y
MLE	Y	Y	Y
MLE-SEI	—	Y	Y
GF-SEI	—	Y	Y
GF-MLE	—	Y	Y
GF-MAP	—	—	Y
HW-MLE	—	—	Y
GF-HW	—	—	Y
HW-MAP	—	—	Y

表 3 SIMON 密码各版本的唯密文故障分析部分子密钥结果对比

区分器	版本				
	32/64	48/96	64/128	96/144	128/256
SEI	∞	∞	∞	∞	∞
GF	99	100	102	89	104
MLE	64	61	66	68	62
MLE-SEI	98	90	96	107	114
GF-SEI	76	80	94	87	101
GF-MLE	66	70	72	66	74
GF-MAP	59	65	67	63	68
HW-MLE	63	60	66	66	57
GF-HW	59	60	62	69	62
HW-MAP	60	62	62	69	57

3 SIMON 密码简介

3.1 符号说明

记 $M = X_1 \| X_0$ 为明文。其中，将明文分成左右 2 个分支，$C = X_{T+1} \| X_T$ 为密文，$C^* = X^*_{T+1} \| X^*_T$ 为错误密文，T 为算法轮数；K 为密码算法的主密钥，k_i 为轮密钥，每个轮密钥由主密钥通过密钥编排算法生成，其中 $i \in [0, T-1]$；S^t 表示向左移 t 位，S^{-t} 表示向右移 t 位。

3.2 SIMON 密码算法

SIMON 密码是一种典型的 Feistel 结构的迭代型分组密码。SIMON 密码的分组长度为 $2n$，密钥长度为 mn，其中，$n \in \{16, 24, 32, 48, 64\}$，$m \in \{2, 3, 4\}$，本文中记算法版本名称为 SIMON2$n$/$mn$。以 SIMON32/64 版本为例，其明文长度为 32 bit，密钥长度为 64 bit。SIMON 密码的版本信息如表 4 所示。

表 4 SIMON 密码各版本

版本名称	明文长度/bit	密文长度/bit	轮数
SIMON32/64	32	64	32
SIMON48/72	48	72	36
SIMON48/96		96	36
SIMON64/96	64	96	42
SIMON64/128		128	44
SIMON96/96	96	96	52
SIMON96/144		144	54
SIMON128/128	128	128	68
SIMON128/192		192	69
SIMON128/256		256	72

在加密算法中将消息明文分成左右2个等长的分支进行左右交替变换。SIMON 密码主要由加密、解密与密钥编排 3 个部分组成。其中，解密过程是加密过程的逆运算。SIMON 密码的结构如图 1 所示。

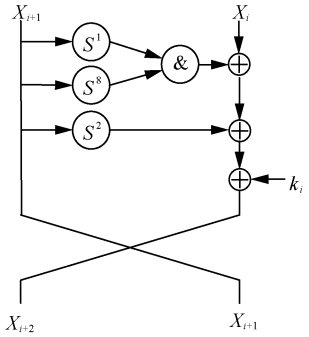


图 1　SIMON 密码的结构

第 i 轮的计算式为

$$X_{i+2}=\left(X_{i+1}\lll 1\&X_{i+1}\lll 8\right)\oplus Y_i\oplus\left(X_{i+1}\lll 2\right)\oplus k_i$$

其中，$0\leqslant i\leqslant T-1$。首先左分支左移 1 bit 与左分支左移 8 bit 进行与运算，然后与右分支进行异或运算，将得到的结果与左分支左移 2 bit 进行异或，最后与该轮子密钥异或成为下一轮的左分支，下一轮的右分支即为上一轮的左分支。该运算方式迭代运行 T 轮。

3.3　密钥编排方案

主密钥K通过密钥编排方案产生每一轮的子密钥$\{k_0,k_1,k_2,\cdots,k_{T-1}\}$，在 SIMON 密码中，每个版本的密钥编排方案根据密钥 mn 的值进行分类，密钥编排方案如下。

$$\begin{cases}k_{i+m}=c\oplus(z_j)_i\oplus k_i\oplus(I\oplus S^{-1})S^{-3}k_{i+1}, & m=2\\ k_{i+m}=c\oplus(z_j)_i\oplus k_i\oplus(I\oplus S^{-1})S^{-3}k_{i+2}, & m=3\\ k_{i+m}=c\oplus(z_j)_i\oplus k_i\oplus(I\oplus S^{-1})(S^{-3}\oplus k_{i+3}\oplus k_{i+1}), & m=4\end{cases}$$

其中，$c=2^n-4$，z_j 为固定常数序列值，I 为原值。

4　唯密文故障分析

4.1　基本假设和故障模型

本文算法中，唯密文故障攻击的基本假设为攻击者对随机明文使用同一个密钥进行加密，并在加密过程的特定轮数导入随机故障，获得大量的错误密文样本。

本文针对 SIMON32/64、SIMON48/96、SIMON64/128、SIMON96/144 和 SIMON128/256 这 5 个版本进行了攻击实验，采用的故障模型都是半字节随机故障模型，在加密过程中倒数第三轮的左分支导入故障，使其产生随机半字节故障值。

4.2　基本步骤

针对 SIMON 密码的唯密文故障攻击过程可以分为以下几个步骤。

步骤 1　确定导入故障模型，保证明文随机产生，用同一个密钥对其进行加密。在加密过程中指定轮数导入随机故障，生成错误密文。

步骤 2　对密文进行解密，求出中间状态值受密钥与密文影响的关系，对中间状态值进行统计分析，通过区分器得到每个候选密钥值的区分器值，选择区分器最大值或最小值求出子密钥的部分比特位。

步骤 3　重复上述步骤，更换故障导入位置，求出子密钥其余部分的比特位，之后可以用密钥编排方案推出主密钥。

4.3　具体过程

本文提出了针对 SIMON 轻量级密码算法的唯密文故障攻击，在已有的 6 种区分器的基础上，针对 SIMON 密码提出了 4 种新型区分器，分别是 GF-MAP 双重区分器、HW-MLE 双重区分器、GF-HW 双重区分器和 HW-MAP 双重区分器。具体攻击过程如下。

步骤 1　选择一个密钥，用该密钥对随机明文进行加密，导入随机半字节故障，得到错误密文样本。以 SIMON64/128 版本为例，导入位置可以是图 2 中 X_{42} 左分支上的任意半字节，若导入位置为第一个半字节，则扩散路径如图 2 所示。导入位置不同故障扩散的路径也不同。

步骤 2　穷举密钥候选值，推算出每个密钥候选值所对应的中间状态样本组，中间状态可以用密文与密钥来表示，计算式为

$$\begin{cases}X_{T-1}=X_{T+1}^*\oplus(X_T^*\lll 2)\oplus(X_T^*\lll 1\&X_T^*\lll 8)\oplus k_{T-1}\\ X_{T-2}=X_T\oplus(X_{T-1}\lll 2)\oplus(X_{T-1}\lll 1\&X_{T-1}\lll 8)\oplus k_{T-2}\\ X_{T-3}=X_{T-1}\oplus(X_{T-2}\lll 2)\oplus(X_{T-2}\lll 1\&X_{T-2}\lll 8)\oplus k_{T-3}\end{cases}$$

步骤 3　得到中间状态样本组之后，用区分器对中间状态进行统计分析。每个密钥候选值都对应导入故障数的错误密文，每个错误密文都可以根据密钥候选值求出一个中间状态值。因此，每个密钥候选值对应一组中间状态，每组样本值都可以用区分器计算出所对应的区分器值，选择不同的区分器进行统计分析，选取区分器最大值或最小值所对应的密钥候选值就是所求的正确子密钥。

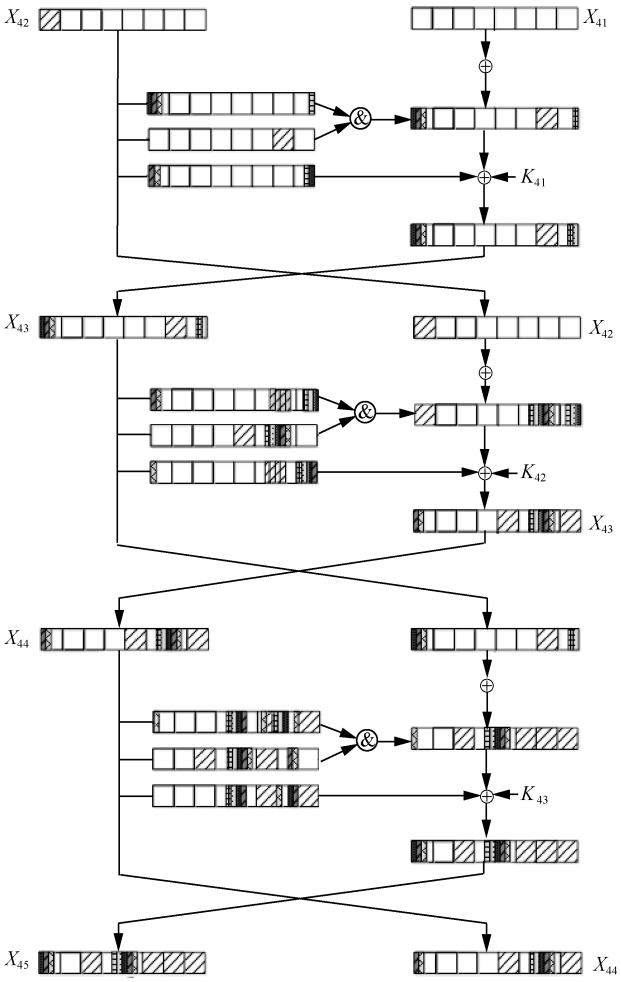


图 2　SIMON64/128 中故障导入在倒数第三轮的路径扩散

在 SIMON32/64 版本中，上述步骤可恢复出 k_{31} 的半字节与 k_{30} 的 9 bit，重复上述步骤 4 次，即可恢复出 k_{31} 的 4 个半字节和 k_{30} 的 4 个半字节，之后,通过密钥编排方案求出主密钥。在其余 4 个版本中，由于密钥编排的特殊性，每次能获得 2 个密钥候选值，这 2 个密钥候选值中将会有 11 bit 是相同的值且是正确值，将这 2 个候选值进行比较，选取比特位相同的数值，即为所求位置正确的值，每次可恢复出倒数第二轮子密钥的 3 bit 和倒数第一轮中子密钥的 8 bit。

4.3　区分器

本文对 SIMON 密码进行唯密文攻击过程中所使用到的区分器一共有 10 种。本节先介绍已有的 6 种区分器，再介绍本文提出的 4 种新型双重区分器，分别是 GF-MAP、HW-MLE、GF-HW 和 HW-MAP。

4.3.1　SEI 区分器

平方欧氏距离（SEI, square Euclidean imbalance）区分器主要用于统计未知分布与均匀分布之间的距离，求出最不满足均匀分布的样本即为所求正确密钥对应样本组。计算式为

$$\mathrm{SEI}=\sum_{\varepsilon=0}^{\eta-1}\left(\frac{\gamma[\varepsilon]}{N}-\frac{1}{\eta}\right)^2$$

其中，$\eta=2^4$，由于本文使用的是随机半字节故障，因此 η 表示半个字节所有排列组合个数；$\varepsilon\in[0,15]$；N 为导入故障数；$\gamma[\varepsilon]$ 统计中间状态为 ε 时的个数。针对每个密钥候选值都有对应的样本组，样本容量为 N，求出每个样本组所对应的 SEI 值，越不符合均匀分布所得 SEI 值越大，该样本所对应的密钥候选值即为正确子密钥。

4.3.2　GF 区分器

拟合优度（GF, goodness of fit）区分器在使用时要求先求出理论分布律。通过比较实际求得的分布律与理论分布律之间的差值，差值最小时，说明该样本是所求样本。图 3 为本文中间状态的理论分布律。区分器计算式为

$$\mathrm{GF}=\sum_{\varepsilon=0}^{\eta-1}\frac{(O_\varepsilon-\Upsilon_\varepsilon)^2}{\Upsilon_\varepsilon}$$

其中，η 表示半个字节所有排列组合个数，O_ε 表示在密钥候选值对应样本里中间状态值为 ε 时的实际个数，Υ_ε 表示同等样本量条件下中间状态值为 ε 时的理论个数。通过比较对应中间状态值相同时实际与理论个数之差，判断出最接近理论分布的样本。GF 值越小，越接近理论分布。

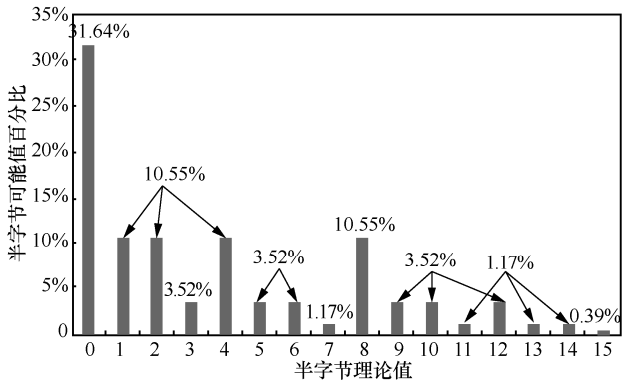


图 3　半字节故障按位与导入后的分布律

4.3.3　MLE 区分器

极大似然估计（MLE, maximum likelihood estimate）区分器是 Fuhr 等针对 AES 密码算法提出的一种区分器。区分器计算式为

$$\mathrm{MLE}=\prod_{m=0}^{M-1}P(\Psi_{T-2})$$

其中，M 为导入故障数，$m\in[0,M-1]$，Ψ_{T-3} 表示倒数第三轮的中间状态值。将样本中所有的中间状态值的理论概率相乘，求出每个密钥候选值对应的极大似然估计值，其值越大，越满足概率分布，从而可以求得对应正确子密钥。

4.3.4　MLE-SEI 区分器

将 MLE 区分器与 SEI 区分器相结合，构建双重区分器，首先用极大似然估计求出部分密钥候选值集合，将其记为 $\chi(k)$，再用 SEI 区分器在剩下密钥中选出最优解。计算式为

$$\mathrm{SEI}(\chi)=\sum_{\varepsilon=0}^{\eta-1}\left(\frac{\gamma[\varepsilon]}{N}-\frac{1}{\eta}\right)^2$$

$$\mathrm{SP}=\max(\mathrm{SEI})$$

针对 $\chi(k)$ 集合中的每一个密钥候选值 k 求出对应的 SEI 值，进行二次筛选，最后选择 SEI 值最大的样本 SP，该样本对应候选值即为正确子密钥。

4.3.5　GF-SEI 双重区分器

将 GF 区分器与 SEI 区分器结合，先用拟合优度筛选出接近理论分布样本 $\chi(k)$，由于实际分布不可能与理论分布完全一致，因此设定一个临界值 χ_α^2，通过自由度 df 查找上侧位卡方分布表 χ^2 中对应的临界值 χ_α^2，规定当 $\chi^2\leqslant\chi_\alpha^2$ 时，样本服从该已知分布，在本文中定义精度为 0.05。再用 SEI 区分器筛选出正确子密钥。

4.3.6　GF-MLE 双重区分器

GF-MLE 双重区分器先用拟合优度过滤不满足分布的密钥候选值，得到密钥集合 $\chi(k)$，再使用 MLE 区分器进行筛选。

$$\mathrm{MLE}(\chi)=\prod_{m=0}^{M-1}P(\Psi_{T-2})$$

$$\mathrm{SP}=\max(\mathrm{MLE})$$

求出剩下集合中每个密钥候选值对应的 MLE 值，选取 MLE 值最大的样本组，即为正确样本。

4.3.7　GF-MAP 双重区分器

为了进一步减少故障数，本文将 GF 区分器与参数估计之最大后验估计（MAP, maximum a posteriori）区分器相结合，提出了新型区分器 GF-MAP 双重区分器。实验证明，该区分器能有效减少导入故障数，在较短时间内实现算法破译。与前 2 种区分器相似，先用拟合优度选出接近理论分布律的密钥候选值集合 $\chi(k)$，再用 MAP 区分器进一步选出最优子密钥。

$$\mathrm{MAP}(\chi)=\frac{p(\gamma)\tilde{p}(\gamma)}{\sum_{t=0}^{n-1}p(\gamma)\tilde{p}(\gamma)}$$

$$\mathrm{SP}=\max(\mathrm{MAP})$$

其中，$p(\gamma)$ 表示中间状态值为 γ 的概率，$\tilde{p}(\gamma)$ 表示对应密钥候选值的先验概率，n 表示密钥候选值的穷举范围。选取 MAP 值最大的样本组 SP，该样本所对应的密钥候选值为正确密钥。

4.3.8　HW-MLE 双重区分器

汉明重量（HW, hamming weight）可用于统计半字节或字节中非 0 的位数。该区分器可适用于更深的轮数中随机故障模型的统计。计算式为

$$\mathrm{HW}=\frac{1}{N}\sum_{n=0}^{N-1}\mathrm{hw}\left(\tilde{\Psi}_{l-1}\right)$$

其中，N 表示故障数，$0\leqslant n\leqslant N-1$，$\tilde{\Psi}_{l-1}$ 表示每一组错误的中间状态样本，hw 表示求出的中间状态样本所对应的汉明重量值。在随机半字节故障中，理论上得到的半字节中比特位为 0 的概率最大，所以 HW 区分器中所求得的值越小，说明所得密钥越正确。本文结合 HW 区分器与 MLE 区分器构建了双重区分器。先用 HW 区分器筛选，排除错误样本，剩下密钥候选值集合 $\chi(k)$，再用 MLE 区分器进行筛选。

$$\mathrm{MLE}(\chi)=\prod_{m=0}^{M-1}P(\Psi_{T-2})$$

$$\mathrm{SP}=\max(\mathrm{MLE})$$

针对集合 $\chi(k)$ 中的每个密钥候选值求出对应的 MLE 值，选取值最大的 MLE 值样本所对应的密钥候选值为所求正确子密钥。

4.3.9　GF-HW 双重区分器

为了进一步提高攻击效率，本文将 GF 区分器与 HW 区分器结合，先用 GF 区分器筛选出符合分布的候选值集合 $\chi(k)$，再将其用 HW 区分器进行统计分析，筛选出最优密钥，计算式为

$$\mathrm{HW}(\chi)=\frac{1}{N}\sum_{n=0}^{N-1}\mathrm{hw}\left(\tilde{\Psi}_{l-1}\right)$$

$$\mathrm{SP}=\min(\mathrm{HW})$$

取 HW 最小值的样本 SP，找出该样本对应的密钥候选值就是最后所求的正确子密钥。

4.3.10　HW-MAP 双重区分器

本文还提出了 HW-MAP 双重区分器，先用 HW 区分器进行筛选，求出候选值集合 $\chi(k)$，再用 MAP

区分器进一步筛选出最优密钥，计算式为

$$\mathrm{MLE}(\chi)=\prod_{m=0}^{M-1}P(\Psi_{T-2})$$

$$\mathrm{SP}=\max(\mathrm{MLE})$$

求出 $\chi(k)$ 集合中的每个密钥候选值对应的 MLE 值，选取值最大的 MLE 值样本对应候选值即为所求正确子密钥。

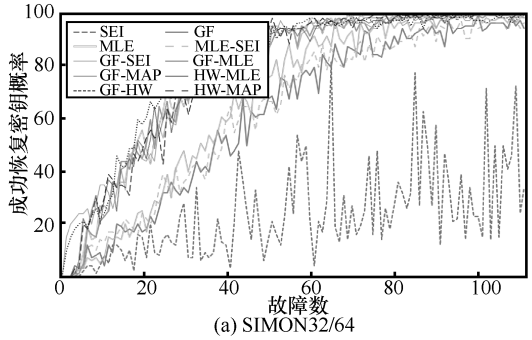
5 实验分析

本文实验在PC端（CPU为Inter Core I7-9700K，4.9 GHz，内存为 16GB）使用 Java 编程语言对 SIMON 密码进行模拟唯密文故障攻击。在攻击过程中，模拟实现导入故障操作，之后对算法进行唯密文故障分析，用区分器恢复出主密钥。本文经过 1 000 次实验操作，以 99%的成功概率分别破译了 SIMON32/64 、 SIMON48/96 、 SIMON64/128 、 SIMON96/144 和 SIMON128/256 共 5 个版本的 SIMON 密码，成功恢复出倒数第一轮与倒数第二轮子密钥。在实验过程中，分别记录了针对 5 种版本 SIMON 密码的唯密文故障攻击过程中使用不同的区分器所需故障数、成功恢复密钥概率和耗费时间。

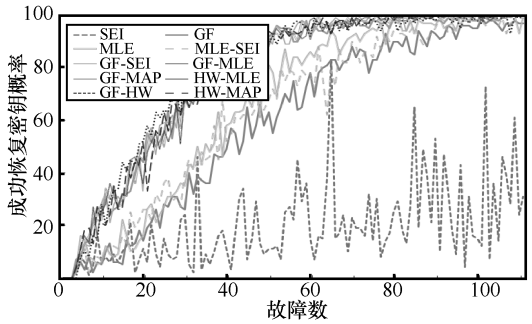
图 4 展示了 SIMON 密码中 5 个典型版本恢复子密钥所需故障数对应的成功恢复密钥概率。图 4 中 10 种不同线型表示不同的区分器，分别为区分器 SEI、GF、 MLE、MLE-SEI、GF-SEI、GF-MLE 、 GF-MAP 、 HW-MLE 、 GF-HW 和 HW-MAP，可以看出，各版本成功恢复密钥需要的最少故障数分别为 59、60、62、63 和 57；SEI 区分器的攻击成功概率最高仅达到 83%，其他区分器均达到 99%以上。

图 5 为 SIMON 密码中故障数对应的消耗时间。图 5 中分别展示了 SEI、GF 和 MLE 单区分器，MLE-SEI、GF-SEI、GF-MLE、GF-MAP、HW-MLE、GF-HW 和 HW-MAP 双重区分器所需消耗时间，可以看出，各版本成功恢复密钥需要的最少消耗时间为 2.2 s、13.0 s、24.3 s、36.3 s 和 41.2 s；SEI 区分器的攻击成功概率达到最高时消耗时间需要 12.8 s。

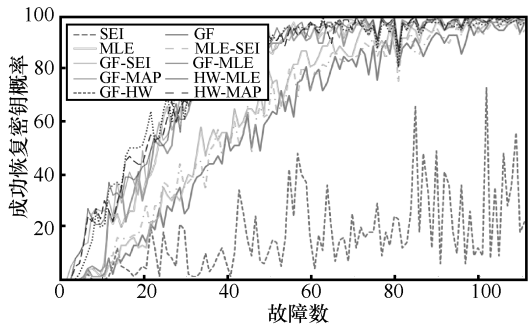
由图 4 和图 5 可知，随机“与”故障导入之后，受分布律以及数据量的影响，每个区分器都呈现各自的统计效率。按照攻击效果分类，10 种区分器可以分成以下 3 组：SEI 区分器的攻击效率最低，



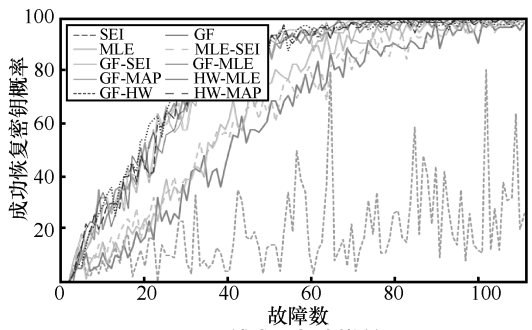
(a) SIMON32/64



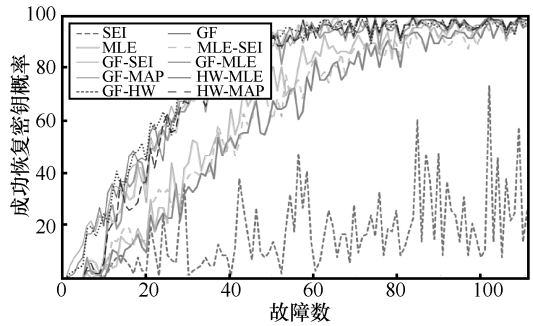
(b) SIMON48/96



(c) SIMON64/128

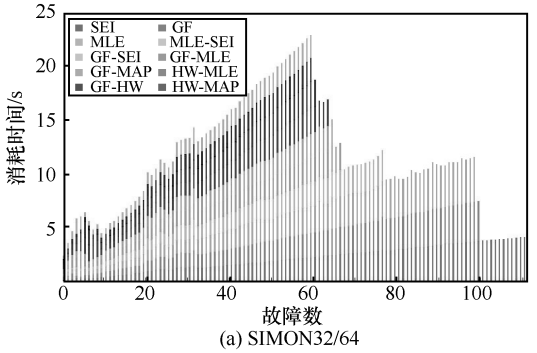


(d) SIMON96/144

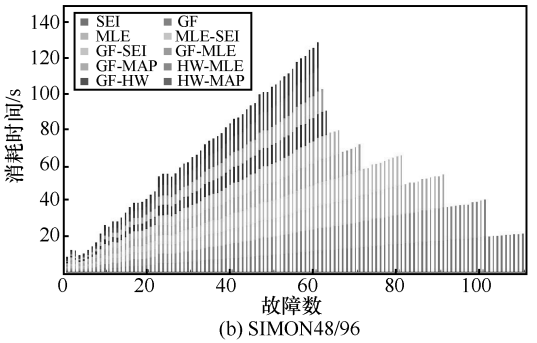


(e) SIMON128/256

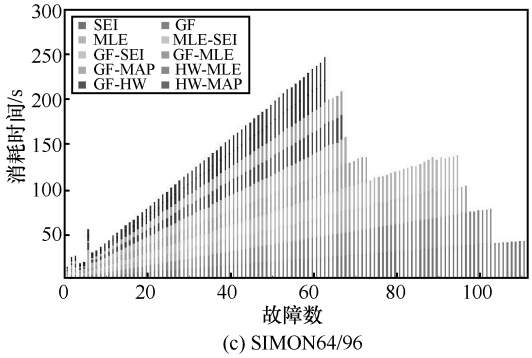
图 4 各版本中故障数对应成功恢复密钥概率



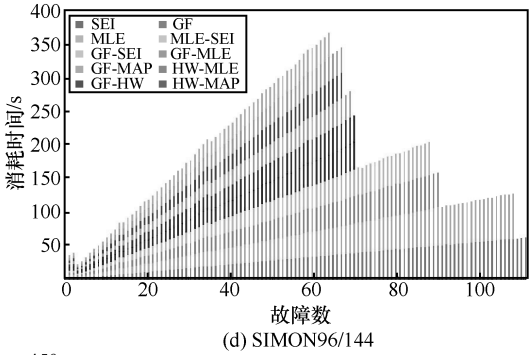
(a) SIMON32/64



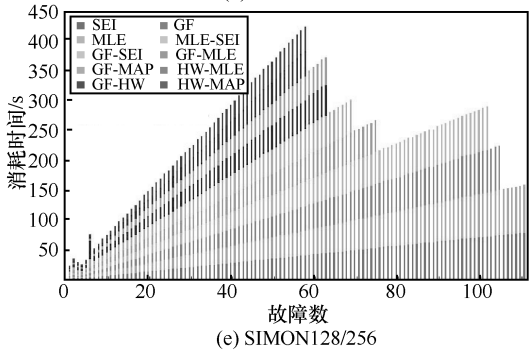
(b) SIMON48/96



(c) SIMON64/96



(d) SIMON96/144



(e) SIMON128/256

图 5　各版本中故障数对应的消耗时间

在 SIMON 密码中基本无效；其次是 GF-SEI 双重区分器、MLE-SEI 双重区分器和 GF 区分器，这 3 种区分器攻击效果并不显著；攻击效率明显较好的是 MLE 区分器、GF-MLE 双重区分器、GF-MAP 双重区分器、HW-MLE 双重区分器、GF-HW 双重区分器和 HW-MAP 双重区分器。在 SIMON32/64 版本中，GF-MAP 双重区分器和 GF-HW 双重区分器攻击效果最好，所需故障数最少且消耗时间最短，是该版本中最好的区分器。在 SIMON48/96 版本中，HW-MLE 双重区分器与 HW-MAP 双重区分器所需故障数最少。在 SIMON64/128 版本中，GF-HW 双重区分器和 HW-MAP 双重区分器所需故障数最少，双重区分器结合了单区分器的优点，在短时间内就能以 99%的概率恢复出密钥。在 SIMON96/144 版本中 GF-MAP 双重区分器所需故障数最少。在 SIMON128/256 版本中 HW-MLE 双重区分器和 HW-MAP 双重区分器仅需要 57 个故障数就能恢复正确密钥，HW-MLE 区分器所需时间最短，是该版本中最优区分器。

6　结束语

本文提出了针对 Feistel 结构的 SIMON 密码的新型唯密文故障分析。实验结果表明，在随机半字节故障模型下，本文新提出的 4 种新型区分器比已有的 6 种区分器所需故障数更少，在同等故障数的情况下，成功恢复出密钥的概率更高。由此证明，Feistel 结构的 SIMOM 密码并不能抵抗唯密文故障攻击，这为其他类似结构的密码算法提供了借鉴，并为抵御唯密文故障攻击研究提供了重要的参考价值。

附录 A　实验数据及结果

明文　随机生成

密钥　SIMON32/64 版本主密钥为 0123456789ABCDEF，SIMON48/96 版本主密钥为 0123456789ABCDEF01234567，SIMON64/128 版本主密钥为 0123456789ABCD EF0123456789AB CDEF，SIMON96/144 版本主密钥为 0123456789ABCD EF0123456789 ABCDEF0123，SIMON128/256 版本主密钥为 0123456789ABCDEF0123456789ABCDEF0123456789ABC DEF 01234，56789ABCDEF。

实验结果　10 种区分器均能恢复主密钥，实验数据分别如表 5 和表 6 所示。

表5 不同区分器破译SIMON密码的成功概率

故障数	成功恢复密钥概率									
	SEI	GF	MLE	MLE-SEI	GF-SEI	GF-MLE	GF-MAP	HW-MLE	GF-HW	HW-MAP
0	0/0/0/0/0	0/0/0/0/0	0/0/0/0/0	0/0/0/0/0	0/0/0/0/0	/0/0/0/0	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	0/0/0/0/0	0/0/0/0/0	15/0/0/0/0	0/0/0/0/0	10/0/0/0/0	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	0/0/0/0/0	0/0/0/0/0	20/0/5/0/5	0/0/0/0/1	15/0/0/0/2	0/0/0/0/0
3	2/4/0/6/0	4/2/0/4/0	1/5/0/2/0	2/2/0/2/0	0/3/0/8/0	0/7/0/3/0	22/2/8/4/8	1/5/8/0/2	18/0/0/3/3	3/4/5/3/0
4	0/8/0/7/0	3/6/0/5/0	3/10/0/12/0	2/6/0/11/0	4/16/0/13/0	1/8/0/6/0	24/11/10/5/10	6/11/10/7/6	20/8/2/7/4	3/11/6/9/0
5	2/6/0/13/0	3/3/0/5/0	9/13/0/18/0	5/11/0/12/0	3/14/0/11/0	5/13/1/9/0	24/13/13/11/13	22/16/13/13/8	21/10/6/6/5	20/18/13/14/0
6	4/1/2/3/0	12/8/4/11/3	19/16/4/14/6	11/2/2/9/3	7/8/3/1/2	18/14/4/15/8	26/12/14/12/20	18/13/27/20/17	19/8/10/14/19	18/19/24/22/4
7	4/4/0/2/0	7/2/1/4/3	14/20/4/15/7	12/7/4/9/4	6/7/1/7/0	16/21/5/19/2	20/16/25/15/22	25/27/23/23/17	23/16/15/20/20	23/13/22/19/6
8	1/16/0/6/0	8/6/1/5/2	15/22/3/23/6	10/8/4/8/3	7/5/1/10/1	15/27/4/16/2	27/24/27/20/18	31/16/21/22/20	26/15/26/21/16	30/27/27/26/2
9	4/6/0/3/0	9/5/1/6/1	27/22/1/32/2	14/7/3/14/0	5/6/1/9/1	21/24/3/35/1	35/28/26/18/24	20/25/21/30/27	22/28/20/26/20	24/21/23/20/2
10	8/8/0/8/0	4/10/2/11/0	27/34/7/32/8	13/10/2/15/1	7/12/1/15/4	23/31/5/20/4	35/32/26/29/22	29/28/23/34/20	24/20/21/29/25	30/20/30/24/6
11	5/6/1/4/3	12/13/8/7/4	25/30/25/32/26	17/12/9/11/7	15/9/5/7/8	25/24/26/25/24	32/21/30/30/26	37/36/37/30/33	29/29/34/33/21	39/24/26/29/18
12	12/9/5/10/6	9/6/2/5/11	36/35/21/26/21	17/12/9/17/15	14/8/7/10/4	36/26/22/28/28	26/28/24/27/35	35/31/32/21/36	31/33/36/36/33	37/35/22/30/21
13	12/6/12/13/8	20/6/8/10/10	35/27/25/30/24	16/11/16/12/14	15/9/6/15/5	34/27/28/35/19	32/31/37/29/35	25/27/33/26/31	46/34/37/25/41	34/26/29/30/22
14	10/10/5/7/9	19/5/7/9/6	36/28/20/35/26	19/16/15/19/17	14/22/13/11/16	44/32/35/36/22	41/29/29/32/34	41/32/31/32/37	42/44/35/38/35	35/26/35/28/38
15	6/12/4/16/7	17/14/10/14/11	36/34/24/27/33	22/13/16/22/20	20/16/13/13/14	44/32/22/35/38	33/34/35/37/29	42/31/39/38/37	42/41/47/39/36	34/42/45/40/28
16	10/21/3/18/5	18/12/9/9/12	46/44/26/43/30	20/25/16/24/19	15/10/15/21/13	41/33/28/36/35	47/39/41/35/41	45/45/39/28/47	49/45/50/44/42	31/38/47/40/26
17	2/2/1/2/2	17/13/13/13/14	48/36/26/38/31	18/19/17/21/13	19/11/16/18/13	50/40/33/40/37	44/43/37/41/43	42/46/38/48/49	49/43/50/45/48	47/44/45/45/27
18	16/7/3/7/8	20/18/13/19/17	52/46/38/34/42	16/22/17/28/17	24/14/12/21/19	47/46/41/37/45	51/49/32/40/44	52/43/40/45/45	60/51/50/42/49	44/43/44/38/29
19	15/11/5/12/3	17/14/17/15/12	56/45/32/47/42	24/26/22/16/14	25/16/13/20/15	45/44/30/45/44	45/33/49/48/37	50/36/43/51/46	58/52/51/54/52	48/52/44/48/36
20	7/6/4/6/3	18/19/14/17/10	49/49/38/46/29	22/26/29/23/15	17/26/12/24/12	51/55/36/53/36	44/55/36/51/37	45/48/44/43/45	61/58/56/54/45	53/33/50/44/37
21	20/20/20/17/20	23/21/21/23/24	43/57/40/38/54	20/22/17/25/28	24/28/22/19/30	60/52/43/40/50	47/54/49/51/50	53/52/49/53/56	67/54/64/60/60	56/45/55/41/50
22	9/9/12/16/11	20/26/19/16/18	53/50/44/49/49	24/32/28/32/30	29/21/22/26/18	49/50/53/42/50	44/47/52/58/49	65/55/55/57/59	64/63/52/62/57	53/56/53/42/42
23	8/4/1/0/1	26/19/27/32/22	58/57/53/64/54	34/29/28/24/34	28/24/24/23/27	65/52/51/50/55	58/58/60/49/56	54/49/53/51/51	67/61/55/63/60	54/54/54/60/50
24	14/15/18/14/24	32/28/20/23/25	63/50/62/60/56	39/36/37/29/32	32/27/35/30/27	60/55/51/57/57	53/59/53/58/58	60/56/51/49/45	69/64/64/55/64	43/63/55/59/59
25	16/9/10/10/9	32/27/28/27/23	72/60/66/60/53	35/38/36/34/34	39/31/32/39/21	64/63/48/64/53	61/59/55/67/60	67/52/53/56/63	75/63/70/65/59	64/56/62/65/63
26	13/7/8/10/7	36/31/26/22/23	65/59/57/63/57	30/29/31/35/27	30/31/30/31/44	61/53/51/65/60	59/62/60/60/66	55/57/62/57/60	68/71/60/69/55	59/69/68/64/56
27	12/8/5/9/6	33/31/32/26/36	63/65/60/66/56	42/31/33/40/32	41/33/32/36/33	59/67/64/68/63	58/57/61/57/62	64/66/67/58/61	74/70/74/72/64	69/65/60/62/57
28	23/22/21/23/25	31/27/35/24/22	69/57/61/68/65	32/27/44/31/32	45/36/30/34/26	71/62/61/62/64	66/75/70/59/72	67/51/56/64/68	82/62/72/73/80	71/62/66/75/65
29	28/24/19/23/36	34/26/25/37/32	65/78/73/58/66	36/40/35/38/36	48/35/36/34/42	72/68/61/70/64	75/71/64/63/71	71/70/72/65/68	79/83/61/73/77	69/69/68/75/68
30	7/5/2/7/1	32/40/27/31/35	71/71/72/58/71	38/45/37/40/39	40/43/40/39/44	67/65/64/65/67	66/71/70/71/66	77/69/66/69/80	72/72/72/77/79	62/65/67/67/67
31	7/2/1/3/3	38/32/36/42/33	83/76/70/69/68	42/41/39/40/41	46/42/39/39/53	73/69/71/73/81	75/72/68/69/70	78/66/74/72/71	75/80/71/78/79	68/78/69/76/72
32	34/46/1/33/4	44/39/39/43/35	72/74/70/69/69	43/44/45/46/40	45/50/48/44/52	79/69/74/78/82	77/70/69/67/75	70/72/78/69/74	83/81/79/72/80	75/66/70/81/70
33	6/3/3/6/5	40/37/40/42/40	81/77/70/76/78	41/48/45/53/39	51/43/58/43/41	71/72/76/76/78	69/72/83/77/83	75/82/69/71/79	82/77/77/76/75	74/72/71/72/69
34	9/9/10/8/8	42/36/43/48/39	71/73/74/77/76	37/45/34/46/40	48/51/47/40/47	78/73/74/73/64	84/78/86/84/76	79/75/71/82/74	85/80/83/84/88	84/80/73/74/66
35	7/5/3/5/5	40/36/44/36/44	76/79/81/75/81	47/46/49/50/41	54/48/53/53/47	79/74/79/73/74	78/75/83/78/75	75/76/82/76/82	88/83/78/85/83	80/81/81/81/73
36	9/10/5/7/5	49/47/44/42/38	84/78/70/78/80	48/58/51/52/50	51/51/57/51/52	80/80/71/79/83	80/78/85/75/77	84/73/84/73/82	95/81/80/83/79	86/80/81/71/83
37	22/16/9/13/13	56/46/47/43/54	82/72/82/81/83	45/45/57/57/59	55/63/53/54/56	81/90/88/76/80	78/88/74/79/74	84/68/73/82/83	83/86/81/81/82	90/74/80/84/75

（续表）

故障数	成功恢复密钥概率									
	SEI	GF	MLE	MLE-SEI	GF-SEI	GF-MLE	GF-MAP	HW-MLE	GF-HW	HW-MAP
38	13/18/12/11/9	51/46/44/36/47	78/80/84/83/88	49/68/47/56/53	61/46/56/60/48	78/85/74/81/74	85/83/76/81/81	83/82/86/80/77	86/85/81/87/85	89/87/80/82/82
39	12/11/6/4/9	54/49/56/44/52	83/71/87/87/79	60/52/55/57/49	59/58/56/58/49	85/84/77/77/85	84/79/81/81/88	89/79/80/89/84	93/89/87/91/86	91/85/73/81/78
40	3/3/1/4/1	46/57/49/50/54	88/83/84/85/84	65/54/52/55/55	61/59/52/62/65	80/87/83/85/82	82/83/79/81/86	86/87/83/82/85	88/81/87/88/86	84/77/83/84/84
41	21/17/10/14/12	48/55/51/56/50	87/93/79/85/83	55/61/60/61/47	70/63/65/69/55	88/92/83/79/78	82/78/92/84/85	84/80/81/79/84	88/89/89/86/83	82/85/83/83/78
42	48/30/34/35/38	51/47/51/55/55	89/84/88/87/77	60/60/52/60/52	64/63/58/59/60	88/90/84/81/87	83/87/88/89/82	89/88/90/83/86	85/88/89/88/90	91/78/92/82/88
43	36/34/26/31/27	68/52/55/63/56	87/79/78/87/94	65/62/56/57/63	69/64/60/58/73	84/84/83/89/83	87/85/90/87/78	89/84/86/82/94	86/84/89/92/95	90/85/91/81/89
44	25/7/15/17/17	50/65/63/53/56	87/92/82/89/91	65/62/66/66/59	67/69/65/64/66	85/88/78/89/89	88/92/84/83/92	91/88/87/89/88	92/89/87/88/87	92/90/85/93/88
45	14/15/9/16/7	63/53/50/58/63	91/90/86/88/83	65/62/48/67/60	62/65/65/74/69	93/85/80/90/88	89/92/86/92/86	90/92/87/88/88	96/89/88/88/90	88/88/91/91/85
46	33/29/24/19/27	61/58/59/58/68	90/88/88/89/85	56/65/60/68/72	79/73/63/67/71	95/92/87/87/90	91/90/87/91/92	86/87/91/88/89	90/85/88/92/93	92/85/87/86/91
47	19/13/7/13/10	62/66/49/57/56	88/85/91/88/84	66/67/66/62/72	75/61/71/70/71	90/90/93/89/88	91/83/90/90/89	91/95/91/87/87	94/90/89/92/90	96/92/86/89/86
48	6/9/6/3/8	62/58/59/59/55	87/90/89/97/90	68/64/62/69/72	71/78/63/71/71	90/89/87/93/89	90/89/84/88/91	94/85/90/93/95	90/91/95/94/96	94/93/90/92/88
49	14/11/10/13/10	68/63/61/61/60	91/90/87/90/93	67/68/63/65/65	76/81/80/75/77	87/92/88/93/96	83/91/96/91/89	96/88/89/89/92	87/90/89/85/91	94/94/93/88/86
50	21/11/15/14/14	69/55/64/69/68	96/93/86/86/94	67/72/76/69/61	77/78/75/76/81	90/93/90/85/92	96/89/87/92/89	93/92/91/94/92	96/92/93/94/92	99/93/91/94/93
51	16/12/14/14/9	64/61/63/69/65	96/93/90/92/88	62/68/64/61/69	83/69/76/81/72	94/96/90/91/94	94/96/88/91/95	95/95/96/94/93	91/89/91/94/92	94/93/91/92/89
52	12/7/5/4/2	76/65/72/64/65	95/92/90/96/90	66/80/66/70/62	73/78/66/79/81	92/95/90/89/82	98/94/91/91/95	92/93/93/91/88	93/93/93/95/93	95/91/94/94/89
53	23/25/15/20/19	75/70/64/69/66	95/95/92/95/93	77/75/66/76/78	83/87/72/78/70	95/95/92/93/91	95/89/92/95/93	95/95/95/92/93	96/96/96/97/96	95/94/89/98/90
54	42/27/42/34/32	68/67/70/71/72	95/92/94/94/93	72/79/80/77/70	89/78/77/77/73	93/95/96/93/93	95/89/91/96/89	94/93/97/93/96	95/93/96/88/96	89/92/95/93/93
55	24/22/24/19/18	77/75/62/67/73	94/93/98/94/90	76/78/81/74/74	80/84/82/83/72	95/90/91/94/91	95/94/95/96/92	95/93/93/95/91	94/97/95/93/95	96/94/96/91/91
56	54/45/48/50/48	68/64/75/75/61	95/90/94/93/97	75/73/69/70/76	83/84/82/83/81	88/90/93/93/93	87/97/97/96/95	92/93/97/92/93	97/98/96/96/95	95/93/93/93/92
57	44/29/40/39/27	77/65/76/72/64	94/98/94/95/94	81/79/81/74/69	78/81/87/80/89	96/93/94/91/96	93/98/94/97/90	95/91/98/96/99	97/97/96/97/91	95/94/95/96/99
58	50/36/37/34/41	79/73/81/79/77	96/95/96/95/98	81/77/78/79/77	87/84/87/82/82	95/98/91/94/95	94/97/94/95/94	93/92/92/94/93	98/95/95/98/97	96/96/96/96/91
59	22/15/16/11/14	77/78/72/72/72	97/93/97/96/94	83/78/72/82/81	90/86/81/86/83	92/91/92/91/96	99/92/92/94/94	90/98/98/94/98	99/92/97/97/95	97/94/98/94/97
60	4/7/4/3/3	80/69/78/77/84	97/96/97/88/96	86/72/79/76/85	92/84/82/90/87	96/96/96/95/95	95/94/96/94/96	94/99/97/97/95	99/99/97/96/94	99/97/96/94/92
61	21/16/17/12/7	70/78/80/84/76	98/100/92/92/96	80/88/78/73/77	88/88/85/90/85	96/94/90/95/92	95/97/93/96/93	97/97/96/96/95	96/96/94/93/98	97/96/94/97/97
62	17/15/11/15/17	85/80/72/73/76	93/95/94/92/99	89/77/82/80/79	89/89/89/85/93	94/94/90/94/94	97/97/96/92/98	97/94/97/98/99	97/95/100/96/99	99/99/99/97/97
63	29/38/36/37/26	82/81/75/76/78	98/96/94/96/95	79/62/81/69/75	92/88/89/94/88	98/93/98/95/94	96/95/97/99/97	99/97/97/96/99	96/98/96/98/98	97/97/95/97/97
64	82/83/20/80/20	80/83/80/87/82	99/97/95/96/99	88/79/86/82/82	88/94/92/87/89	96/96/98/93/95	96/97/96/96/96	98/93/96/97/96	98/93/97/96/95	98/93/90/93/96
65	19/15/7/8/8	89/83/85/81/83	95/96/97/95/100	83/73/87/84/81	98/92/86/87/86	98/97/94/98/96	99/99/96/95/96	97/98/97/98/98	97/98/98/97/97	96/97/98/97/95
66	13/17/15/12/17	84/79/80/82/76	99/97/99/97/96	81/87/84/87/86	91/85/89/95/87	99/98/98/100/93	96/98/92/95/97	97/95/99/99/98	96/94/99/97/99	98/98/97/96/96
67	31/24/16/16/17	80/82/85/78/78	97/96/92/98/91	80/82/83/84/77	89/88/87/88/87	95/95/89/97/94	95/96/99/95/97	99/98/97/99/92	97/98/95/97/97	99/98/99/97/94
68	14/10/7/6/6	88/83/83/89/83	100/99/97/99/98	84/82/83/90/85	92/91/85/94/86	98/98/95/97/94	97/96/99/98/99	98/97/96/96/97	98/94/95/97/99	99/95/99/97/98
69	27/23/25/22/28	87/88/84/86/82	99/96/98/100/96	83/90/84/81/88	94/92/85/92/90	98/96/94/99/95	100/99/99/91/95	97/96/96/99/92	99/98/97/99/95	95/99/95/99/93
70	16/19/12/4/10	86/84/81/85/87	97/99/97/98/100	88/88/85/85/85	84/93/90/92/93	94/99/97/99/94	97/100/98/96/100	99/99/100/99/95	99/97/98/98/100	98/96/100/97/99
71	19/19/20/12/16	85/87/88/82/80	100/98/97/100/100	90/82/86/87/87	97/90/95/91/90	97/96/98/95/95	97/99/97/98/96	98/98/97/98/99	97/97/99/98/99	98/98/97/97/100
72	25/16/16/17/17	94/86/86/84/90	99/98/97/98/100	82/86/90/89/91	93/93/97/91/88	97/96/99/97/98	97/97/98/97/98	98/99/100/99/96	98/96/95/99/98	99/97/95/99/100
73	46/32/18/31/24	93/78/78/92/85	99/97/95/100/93	89/86/89/87/85	93/94/93/91/90	94/95/96/98/90	96/99/97/97/91	97/99/97/100/94	99/97/93/96/90	99/97/95/99/92
74	16/14/18/18/16	85/83/89/89/89	99/98/98/99/99	84/84/92/95/87	95/95/96/93/90	96/98/99/100/100	95/98/98/99/96	98/100/99/99/99	97/99/97/97/99	99/100/97/99/98
75	48/30/29/34/33	85/83/76/88/81	99/100/91/100/93	92/92/85/89/86	95/94/88/97/86	97/98/89/98/88	99/98/89/97/93	98/100/91/100/94	95/97/88/99/95	99/100/91/100/94

（续表）

故障数	成功恢复密钥概率									
	SEI	GF	MLE	MLE-SEI	GF-SEI	GF-MLE	GF-MAP	HW-MLE	GF-HW	HW-MAP
76	14/8/9/11/9	84/87/88/86/88	99/98/100/100/100	89/87/89/93/84	99/97/91/95/91	99/97/100/97/99	96/99/99/99/99	98/98/100/99/98	97/94/97/97/98	99/98/99/98/97
77	26/14/18/11/19	90/93/91/90/91	100/99/97/99/98	87/93/84/87/89	91/89/88/96/94	97/97/97/99/95	99/98/98/97/96	97/99/98/98/97	97/99/97/96/95	100/97/97/98/99
78	18/17/13/16/18	87/86/86/90/88	98/98/96/100/97	87/90/90/86/92	98/96/96/92/84	97/95/97/98/95	99/97/97/98/96	98/100/97/100/97	97/99/94/99/97	97/99/98/98/98
79	27/25/24/26/26	92/90/97/91/88	100/99/100/98/98	88/94/93/92/90	95/98/88/98/96	99/99/96/97/97	100/98/95/97/96	99/98/99/100/97	98/100/98/99/98	99/99/100/99/99
80	36/29/23/27/9	89/90/81/90/81	99/100/87/98/91	90/93/75/90/84	97/99/85/98/90	98/98/84/96/91	99/97/85/99/91	100/100/87/100/92	98/94/81/99/91	100/99/87/100/92
81	32/18/12/17/12	95/88/88/89/93	100/99/99/99/97	90/93/92/95/92	97/94/92/94/91	99/98/99/99/95	96/100/98/99/97	98/100/98/100/97	98/98/98/99/97	99/99/97/99/97
82	26/13/14/15/18	91/92/90/89/93	100/99/95/99/98	91/92/91/85/88	98/94/92/98/93	99/98/98/99/96	97/94/97/99/97	100/100/97/99/97	99/97/95/99/97	100/100/97/100/97
83	32/27/26/31/23	91/86/88/92/94	100/100/99/100/100	93/94/94/93/96	94/98/96/96/96	100/99/96/99/100	100/97/97/98/100	99/100/98/97/100	96/100/99/98/97	99/99/99/99/100
84	78/65/66/59/61	93/85/92/91/94	100/98/100/100/99	88/96/86/94/91	97/93/95/98/96	99/99/99/100/97	98/98/98/99/98	100/98/98/100/96	99/97/98/98/98	100/99/100/95/97
85	27/19/18/18/14	94/94/89/89/92	99/99/95/99/98	95/92/86/93/91	97/98/90/95/96	100/100/94/100/98	99/99/94/97/99	99/100/95/99/99	99/99/93/97/98	99/99/96/99/99
86	63/49/48/48/48	95/91/85/89/87	100/100/98/100/99	92/89/89/94/88	97/97/96/97/98	97/100/98/99/97	99/98/97/98/99	100/99/97/100/99	95/98/95/100/97	100/100/96/99/99
87	49/39/34/41/37	93/88/89/95/94	98/100/99/100/99	95/91/92/91/94	99/97/95/99/95	98/99/99/100/96	100/100/98/100/99	100/100/98/99/99	100/99/100/99/98	100/98/99/99/99
88	27/21/12/22/15	96/94/92/93/90	99/100/99/99/99	97/93/94/93/96	97/97/94/97/96	99/99/98/97/99	100/99/98/100/97	99/99/98/100/99	98/99/98/100/97	100/99/99/99/99
89	58/53/49/44/48	93/93/94/100/90	99/100/100/99/97	90/95/96/95/92	95/96/98/97/92	99/98/100/99/97	95/100/100/99/98	100/100/100/99/98	100/98/98/97/96	99/100/99/99/98
90	12/10/6/9/9	94/91/93/89/93	100/100/100/99/98	96/99/93/94/92	98/99/97/96/95	99/98/99/99/95	98/99/100/100/97	99/100/98/99/98	100/100/98/98/99	99/99/99/100/97
91	47/47/41/42/37	88/92/90/95/92	100/99/97/99/95	95/98/92/93/89	98/95/95/96/93	97/97/95/99/95	99/99/97/100/94	99/99/95/99/95	97/100/97/98/95	100/100/95/98/96
92	37/33/36/28/26	98/96/93/98/92	100/100/96/100/99	98/93/90/96/90	98/96/98/99/97	100/99/96/98/96	99/100/97/99/99	100/100/98/100/99	98/100/98/96/99	99/100/98/98/99
93	21/18/18/17/24	93/95/93/94/95	99/99/98/100/99	95/93/93/94/94	99/97/98/98/99	100/98/96/99/99	100/99/99/98/100	99/100/99/100/99	100/97/96/100/98	99/99/99/99/99
94	22/9/10/14/14	95/91/93/96/94	100/100/100/99/97	95/96/96/97/93	99/94/99/96/94	99/99/100/100/96	99/98/100/99/97	100/100/98/100/97	98/99/97/97/97	100/100/99/100/96
95	39/43/36/35/31	95/96/86/96/94	100/99/96/99/99	98/97/93/98/92	99/100/94/100/96	100/99/96/100/98	100/99/95/97/99	100/100/96/99/98	100/95/95/99/97	100/99/96/100/99
96	14/4/6/8/9	96/96/90/100/92	99/98/100/100/96	91/99/99/96/88	100/99/97/95/96	100/99/100/99/95	98/100/99/98/96	100/100/100/100/97	99/100/99/99/96	100/99/100/100/97
97	34/31/26/26/21	96/96/97/95/92	100/98/99/100/96	91/98/95/94/94	100/98/98/98/94	100/100/98/99/95	98/99/99/99/95	100/100/97/100/96	100/97/96/100/96	99/100/99/100/95
98	23/16/9/14/15	96/95/93/96/95	100/99/100/100/97	99/98/96/96/89	98/99/97/95/94	100/98/99/99/96	100/100/100/100/97	100/100/100/99/95	98/99/97/98/96	100/99/99/98/96
99	23/15/12/12/8	100/95/96/91/92	100/100/99/100/97	95/98/97/95/93	99/98/94/100/97	100/98/100/100/96	100/100/97/100/97	100/100/99/100/97	98/98/98/99/97	100/100/100/99/96
100	15/12/9/11/11	94/99/94/98/96	99/99/99/99/99	96/98/93/97/97	97/99/96/99/98	99/100/98/98/98	100/100/99/99/98	100/98/98/100/99	98/97/97/99/97	100/99/99/100/98
101	72/73/73/81/74	95/97/96/97/98	100/100/98/100/100	97/96/95/97/95	99/99/97/99/99	100/99/98/100/99	100/100/97/98/100	100/100/98/100/100	97/100/97/98/99	100/99/98/100/100
102	14/7/8/12/14	97/98/99/99/92	100/100/100/99/99	97/98/97/98/98	98/100/99/98/98	100/98/98/100/99	100/99/99/98/99	100/98/100/100/99	98/100/99/100/99	100/99/99/100/99
103	50/36/35/28/46	97/98/96/96/96	100/99/100/99/99	97/99/97/95/98	98/98/100/97/99	100/99/98/100/98	100/100/100/100/96	100/99/100/99/99	99/99/100/98/96	100/100/100/99/99
104	15/14/9/12/8	97/96/95/97/99	100/100/99/100/99	97/96/96/98/95	99/98/97/98/99	100/98/99/100/97	99/100/99/98/99	99/100/99/100/98	100/99/96/98/98	100/100/99/100/99
105	50/46/48/38/38	97/94/95/97/92	100/100/100/100/95	97/99/97/98/91	99/99/99/100/95	100/99/100/100/95	99/100/99/100/94	100/99/99/100/95	99/99/99/98/94	100/100/99/100/95
106	41/39/28/31/22	95/97/97/97/96	100/100/99/100/98	94/93/97/97/94	97/99/97/100/97	100/99/99/98/98	99/100/99/100/98	100/100/98/99/98	99/100/98/99/98	100/100/99/100/98
107	46/28/36/32/25	99/96/98/97/94	100/100/100/99/98	98/97/99/99/96	100/100/100/98/97	100/100/100/100/97	100/100/100/99/98	100/99/99/100/97	97/93/98/97/93	99/100/100/100/98
108	73/61/56/64/58	96/98/99/98/99	100/100/100/100/100	98/98/96/97/98	97/100/100/99/99	99/100/100/100/99	100/100/100/100/99	100/100/100/100/100	98/100/99/100/100	100/99/99/100/100
109	24/24/18/20/14	98/97/94/96/96	100/100/99/100/99	95/99/93/99/98	99/93/97/100/97	100/100/98/100/98	100/100/99/99/99	100/100/99/100/99	100/99/97/98/97	100/100/99/100/99
110	34/31/22/26/26	95/97/98/99/97	99/100/99/100/99	97/99/95/99/98	99/99/98/99/97	99/100/99/100/99	99/100/99/99/99	100/100/99/100/99	100/100/98/97/98	100/100/99/100/99

注：表中数值均乘 1%。

表 6　不同区分器破译 SIMON 密码的消耗时间

故障数	消耗时间/s									
	SEI	GF	MLE	MLE-SEI	GF-SEI	GF-MLE	GF-MAP	HW-MLE	GF-HW	HW-MAP
0	0.2/0.8/0.9/1.6/1.5	0.3/0.7/1.0/2.0/2.7	0.2/0.4/1.0/1.8/2.0	0.2/0.9/1.3/1.9/2.0	0.1/0.9/1.9/1.9/2.2	0.3/1.0/2.0/2.8/2.2	0.4/1.1/2.0/2.5/2.7	0.4/1.1/1.5/2.8/3.0	0.3/1.1/1.5/3.4/2.4	0.2/0.8/0.9/2.6/2.6
1	0.2/1.2/1.3/4.0/2.6	0.3/1.1/2.9/3.5/3.4	0.3/0.6/2.0/3.2/2.1	0.3/1.1/1.5/3.3/2.0	0.3/1.3/2.0/2.2/3.4	0.5/2.1/4.2/4.1/4.5	0.5/1.6/3.3/4.1/5.3	0.3/1.2/2.4/3.2/3.3	0.5/1.3/2.6/5.1/5.1	0.3/1.2/2.4/3.8/4.0
2	0.2/1.1/1.9/2.8/2.5	0.5/0.8/2.2/3.3/2.3	0.5/0.8/3.4/4.2/2.6	0.5/1.7/1.8/4.0/2.1	0.1/1.1/2.0/3.2/2.4	0.7/1.3/2.9/4.3/3.3	0.7/1.1/2.3/4.3/4.0	0.5/2.1/3.7/4.5/3.5	0.5/1.3/2.5/5.4/3.9	0.5/1.0/3.4/4.1/2.9
3	0.3/0.8/1.5/2.0/2.2	0.2/0.8/1.5/2.2/2.3	0.6/0.8/1.4/1.9/2.2	0.6/0.9/1.6/2.3/2.5	0.2/0.9/1.6/2.1/2.4	0.9/1.2/2.0/2.8/3.0	1.5/1.1/2.0/2.8/3.1	0.7/0.9/2.4/2.0/2.3	0.3/1.2/2.2/3.0/3.2	0.7/0.9/1.5/2.0/2.3
4	0.2/0.9/1.7/2.4/2.9	0.2/1.0/1.8/2.5/3.0	0.8/0.9/1.7/2.4/3.0	0.5/1.0/1.6/2.7/3.2	0.3/1.0/1.7/2.5/3.1	0.8/1.3/2.4/3.3/4.1	1.2/1.3/2.3/3.3/4.1	0.9/1.0/1.7/2.5/3.0	0.3/1.4/2.6/3.3/4.1	0.8/1.0/1.7/2.5/3.0
5	0.3/1.1/2.1/2.9/3.7	0.3/1.1/2.2/3.0/3.8	0.6/1.1/2.2/2.9/3.7	0.5/1.1/1.9/3.3/4.0	0.3/1.1/2.2/3.1/3.8	0.6/1.5/2.9/4.0/5.1	0.4/1.6/21.8/4.1/14.0	1.5/1.2/7.4/3.0/3.8	0.4/1.7/6.2/4.1/30.1	1.5/1.2/7.1/2.9/3.8
6	0.3/1.3/2.4/3.5/4.4	0.3/1.3/2.4/3.8/4.4	0.3/1.3/2.4/3.6/4.5	0.4/1.3/2.3/4.0/5.6	0.3/1.4/2.5/3.6/4.5	0.4/1.7/3.4/4.7/5.6	0.4/1.7/5.3/4.7/7.6	1.5/1.4/3.1/3.6/4.5	0.4/1.9/3.5/4.7/7.2	1.5/1.4/2.9/3.7/4.5
7	0.3/1.5/2.9/4.2/5.1	0.3/1.5/2.8/4.2/5.2	0.3/1.5/2.7/4.2/5.2	0.4/1.6/2.6/4.7/5.6	0.3/1.6/3.1/4.1/5.3	0.4/2.0/3.8/5.3/6.7	0.4/2.0/4.3/5.3/8.7	1.2/1.6/3.1/4.3/5.3	0.4/2.2/3.9/5.5/8.3	0.7/1.6/3.1/4.2/5.3
8	0.3/1.9/3.3/4.7/5.8	0.4/2.0/3.2/4.8/5.9	0.3/2.0/3.2/4.6/5.9	0.4/2.0/2.9/5.1/6.2	0.3/2.0/3.4/4.7/6.1	0.4/2.4/4.2/5.9/7.3	0.4/2.5/4.7/5.9/9.8	1.6/2.1/3.4/4.8/6.0	0.4/2.7/4.4/5.9/9.1	0.6/2.1/3.6/4.8/6.0
9	0.4/2.4/3.7/5.2/6.6	0.4/2.4/3.6/5.4/6.7	0.4/2.5/3.5/5.1/6.6	0.4/2.5/3.3/5.8/6.6	0.4/2.5/3.7/5.4/6.7	0.5/3.0/4.6/6.4/7.9	0.5/3.1/5.0/6.6/10.4	0.6/2.6/4.0/5.4/6.7	0.5/3.4/4.7/6.6/9.9	0.5/2.6/3.9/5.4/6.8
10	0.4/2.3/4.0/5.7/7.4	0.5/2.4/4.0/5.9/7.4	0.5/2.4/4.0/5.7/7.4	0.5/2.4/3.7/6.4/7.3	0.5/2.4/4.1/5.9/7.6	0.5/2.9/5.0/6.9/8.6	0.5/2.9/5.4/7.0/11.2	0.5/2.5/4.2/5.8/7.5	0.6/3.1/5.0/7.1/10.5	0.5/2.5/4.3/5.8/7.5
11	0.5/2.6/4.4/6.3/8.1	0.5/2.7/4.4/6.6/8.0	0.5/2.6/4.4/6.3/8.1	0.6/2.6/4.1/7.2/8.1	0.5/2.8/4.5/6.4/8.2	0.6/3.2/5.3/7.5/9.3	0.6/3.2/5.9/7.7/12.1	0.6/2.8/4.9/6.6/8.2	0.6/3.4/5.8/7.6/11.4	0.6/2.9/5.0/6.4/8.2
12	0.5/2.6/4.8/6.9/8.9	0.5/2.6/4.7/7.3/8.9	0.5/2.7/4.9/6.9/8.9	0.6/2.7/4.4/7.8/9.3	0.5/2.7/4.9/7.1/9.0	0.6/3.0/5.7/8.0/10.2	0.6/3.1/6.2/8.0/13.0	0.6/2.8/5.3/7.1/8.9	0.6/3.4/5.7/8.1/12.2	0.6/2.9/5.3/7.1/9.0
13	0.6/2.8/5.3/8.2/9.5	0.6/2.9/5.1/8.3/9.5	0.6/2.9/5.2/7.7/9.5	0.7/2.9/4.8/8.8/9.8	0.6/2.9/5.3/7.9/9.5	0.7/3.3/6.0/9.0/10.8	0.6/3.4/6.6/9.2/13.8	0.6/3.0/5.7/7.9/9.6	0.7/3.7/6.2/9.3/13.0	0.6/3.1/5.7/7.8/9.6
14	0.6/3.1/5.6/8.0/10.0	0.6/3.2/5.6/8.3/10.2	0.6/3.2/5.7/8.0/10.2	0.7/3.2/5.0/9.1/10.2	0.6/3.2/5.7/8.1/10.3	0.7/3.6/6.4/9.0/11.3	0.7/3.6/7.4/9.1/14.5	0.6/3.3/6.2/8.3/10.3	0.7/3.9/6.6/9.2/13.6	0.7/3.4/6.3/8.2/10.2
15	0.6/3.3/5.9/8.7/10.8	0.6/3.5/5.9/9.0/10.9	0.6/3.5/6.0/8.7/11.0	0.7/3.5/5.4/9.7/11.6	0.6/3.5/6.1/8.7/11.0	0.7/3.9/6.7/9.8/12.0	0.7/3.9/7.5/9.8/15.2	0.7/3.6/6.3/8.8/11.1	0.7/4.3/6.9/9.9/14.4	0.7/3.7/6.4/8.8/11.1
16	0.6/3.6/6.3/9.2/11.7	0.7/3.8/6.3/9.6/11.6	0.7/3.7/6.3/9.1/11.6	0.7/3.8/5.7/10.2/11.7	0.7/3.7/6.5/9.3/11.6	0.8/4.0/7.1/10.1/12.7	0.7/4.1/7.8/10.2/16.0	0.7/3.9/6.8/9.5/11.7	0.8/4.6/7.1/10.3/15.1	0.8/3.9/6.8/9.4/11.7
17	0.7/3.5/6.8/9.8/12.2	0.7/3.7/6.7/10.0/12.3	0.7/3.8/6.7/9.7/12.3	0.8/3.7/6.0/10.7/12.2	0.7/3.8/6.9/9.8/12.4	0.8/4.1/7.5/10.7/13.5	0.8/4.1/8.2/10.8/16.6	0.8/3.9/7.1/9.8/12.3	0.8/4.5/7.5/10.9/16.0	0.8/3.9/7.2/9.8/12.5
18	0.7/3.6/7.1/10.5/13.2	0.7/3.8/7.2/10.8/13.1	0.8/3.8/7.1/10.4/13.3	0.8/3.8/6.3/11.7/13.1	0.7/3.8/7.4/10.5/13.4	0.8/4.1/7.9/11.3/14.3	0.8/4.1/8.7/11.5/17.8	0.8/4.0/7.6/10.7/13.4	0.8/4.6/7.9/11.8/16.8	0.9/4.0/7.6/10.6/13.4
19	0.8/3.8/7.5/11.2/14.0	0.8/4.0/7.4/11.5/13.6	0.8/4.0/7.5/11.0/13.9	0.9/4.0/6.5/12.3/13.8	0.8/4.0/7.8/11.0/13.8	0.9/4.3/8.4/11.9/14.7	0.9/4.3/9.0/12.0/18.4	0.8/4.2/8.0/11.3/13.9	0.9/4.8/8.3/12.4/17.6	0.9/4.2/8.1/11.3/13.9
20	1.0/4.0/7.9/11.3/14.4	1.0/4.2/7.9/11.6/14.5	1.0/4.2/7.9/11.3/14.4	1.0/4.2/6.8/12.8/15.4	1.0/4.3/8.0/11.4/14.5	1.1/4.5/8.7/12.4/15.5	1.1/4.5/9.5/12.5/19.3	0.9/4.4/8.4/11.7/14.6	1.1/5.1/8.6/12.3/18.5	0.9/4.4/8.4/11.7/14.6
21	1.0/4.2/8.3/11.8/15.3	1.0/4.3/8.2/12.3/15.1	1.0/4.5/8.3/12.1/15.2	1.0/4.4/7.1/13.3/16.0	0.9/4.4/8.6/12.1/15.3	1.1/4.7/8.8/12.9/16.2	1.0/4.7/9.7/13.1/19.8	0.9/4.6/8.8/12.1/15.3	1.1/5.3/9.1/13.1/19.3	1.0/4.6/8.9/12.1/15.4
22	1.1/5.1/8.8/12.6/16.1	1.0/5.2/8.5/13.1/15.9	1.0/5.2/8.6/12.4/16.0	1.1/5.3/7.7/14.0/16.0	1.0./5.2/8.8/12.7/16.1	1.1/5.6/9.3/13.6/16.8	1.1/5.7/10.3/13.7/20.2	1.0/5.4/9.2/12.8/16.1	1.1/6.2/9.3/13.9/19.8	1.0/5.4/9.4/12.6/16.1
23	1.1/5.1/9.2/13.2/16.6	1.2/5.4/8.9/13.7/16.4	1.2/5.4/9.2/13.1/16.7	1.2/5.4/8.4/14.7/17.2	1.1/5.3/9.2/13.1/16.6	1.2/5.6/9.7/13.9/17.4	1.2/5.6/10.9/14.0/21.5	1.0/5.7/9.7/13.5/16.9	1.2/6.2/10.0/14.6/21.0	1.0/5.7/9.7/13.5/16.9
24	1.1/5.1/9.4/13.6/17.3	1.1/5.4/9.3/14.3/17.2	1.1/5.4/9.5/13.8/17.4	1.1/5.4/8.7/15.4/17.6	1.1/5.3/9.6/13.7/17.3	1.2/5.6/10.1/14.5/18.2	1.1/5.6/11.1/14.8/21.6	1.0/5.6/10/14.1/17.4	1.1/6.3/9.9/14.8/21.6	1.0/5.6/10.2/13.9/17.6
25	1.0/5.0/9.9/14.3/18.1	1.1/5.2/9.8/14.8/18.1	1.0/5.2/9.9/14.6/18.2	1.1/5.2/9.0/15.9/18.7	1.0/5.3/9.9/14.6/18.2	1.1/5.4/10.6/14.9/18.9	1.1/5.4/11.5/15.1/22.4	1.1/5.4/10.6/14.4/18.2	1.1/6.2/10.6/15.4/22.3	1.1/5.5/10.6/14.5/18.3
26	1.1/5.2/10.1/14.8/19.0	1.1/5.4/10.0/15.6/18.8	1.1/5.4/10.5/14.9/19.0	1.2/5.4/9.4/16.4/19.4	1.1/5.5/10.3/15.2/19.3	1.1/5.6/10.8/15.7/19.9	1.2/5.7/12.1/16.0/23.0	1.1/5.6/10.9/15.2/19.1	1.1/6.4/10.9/16.2/23.1	1.1/5.7/10.9/15.3/19.2
27	1.3/5.5/10.8/15.6/19.6	1.3/5.7/10.5/16.2/19.5	1.4/5.8/10.6/15.4/19.8	1.2/5.7/10.0/17.3/19.6	1.3/5.8/10.7/15.6/19.9	1.4/5.9/11.2/16.3/20.5	1.4/6.0/12.4/16.4/24.1	1.2/6.0/11.4/15.9/19.9	1.4/6.7/11.2/16.7/23.9	1.2/6.0/11.3/16.0/20.0
28	1.3/5.7/11.1/15.8/20.2	1.4/5.9/10.9/16.5/20.0	1.4/6.0/11.0/15.9/20.5	1.2/6.0/10.6/17.8/21.1	1.3/6.0/11.2/16.0/20.3	1.4/6.2/11.6/16.7/20.8	1.4/6.2/12.9/16.9/24.6	1.2/6.2/11.7/16.5/20.3	1.4/7.0/11.6/17.2/24.5	1.2/6.3/11.8/16.2/20.5
29	1.3/5.8/11.4/16.9/20.9	1.3/6.0/11.3/17.6/20.7	1.4/6.0/11.4/16.6/21.2	1.2/6.1/11.2/18.5/20.9	1.4/6.1/11.6/17.1/21.0	1.4/6.2/11.9/17.4/21.7	1.4/6.3/13.2/17.6/25.9	1.2/6.3/12.2/17.3/21.1	1.4/7.0/12.1/17.9/25.4	1.3/6.3/12.2/17.0/21.3
30	1.3/6.1/11.7/17.2/21.5	1.4/6.3/11.4/17.7/21.4	1.4/6.4/11.9/17.1/21.7	1.3/6.3/10.6/19.0/21.6	1.3/6.3/11.8/16.9/21.7	1.4/6.5/12.4/17.9/22.4	1.4/6.5/13.7/18.0/25.9	1.3/6.6/12.6/17.6/21.8	1.4/7.4/12.3/18.4/25.8	1.3/6.6/12.6/17.4/21.8
31	1.4/6.2/12.3/18.2/22.4	1.5/6.4/12.0/18.7/22.4	1.5/6.5/12.2/17.9/22.7	1.4/6.5/11.5/20.2/23.1	1.5/6.6/12.3/18.3/22.4	1.5/6.6/12.9/18.5/23.2	1.5/6.7/14.1/19.1/26.7	1.3/6.7/12.9/18.2/22.7	1.5/7.4/12.7/19.2/26.8	1.3/6.8/13.1/18.1/22.9
32	1.2/6.4/12.6/18.7/22.9	1.3/6.7/12.4/19.4/22.8	1.3/6.7/12.6/18.7/23.1	1.4/6.7/11.6/21.0/23.1	1.3/6.7/12.7/18.8/23.1	1.3/6.8/13.2/19.4/23.5	1.3/6.9/14.5/19.7/27.6	1.3/7.0/13.4/19.3/23.2	1.3/7.8/13.2/20.1/27.5	1.4/7.0/13.4/19.0/23.5
33	1.2/6.8/13.0/19.4/23.6	1.3/7.0/12.7/20.6/23.5	1.3/7.1/13.2/19.4/23.9	1.5/7.1/11.8/21.7/23.8	1.3/7.1/13.2/19.6/23.9	1.3/7.2/13.4/19.9/24.5	1.3/7.2/14.8/20.4/28.3	1.4/7.3/13.7/20.0/23.9	1.3/8.1/13.3/20.7/28.2	1.5/7.4/13.7/19.9/24.0
34	1.3/6.9/13.3/20.0/24.3	1.3/7.2/13.1/21.2/24.3	1.3/7.2/13.5/20.6/24.6	1.6/7.3/11.4/22.7/25.3	1.3/7.3/13.6/20.5/24.6	1.3/7.2/13.8/20.6/25.1	1.3/7.5/15.2/20.9/29.3	1.5/7.6/14.1/20.6/24.7	1.3/8.4/13.8/21.3/29.1	1.5/7.6/14.3/20.5/24.7
35	1.3/7.1/13.8/19.9/25.0	1.3/7.3/13.6/20.5/25.1	1.4/7.4/13.8/20.1/25.3	1.6/7.4/12.5/22.2/25.4	1.4/7.5/13.9/20.0/25.3	1.4/7.4/14.3/20.2/25.6	1.4/7.5/15.7/20.5/30.3	1.5/7.7/14.6/20.5/25.6	1.4/8.4/14.1/21.0/30.0	1.5/7.8/14.6/20.4/25.7
36	1.4/7.2/14.2/20.5/25.9	1.4/7.4/13.9/21.7/25.6	1.4/7.6/14.2/20.4/26.1	1.7/7.5/12.7/23.0/26.3	1.4/7.5/14.4/20.7/26.1	1.4/7.6/14.5/21.0/26.5	1.4/7.6/16.1/21.1/30.6	1.5/7.8/15.0/21.2/26.3	1.4/8.5/14.4/21.2/30.3	1.5/8.0/14.9/21.1/26.4
37	1.4/7.4/14.6/21.2/26.8	1.4/7.6/14.3/21.9/26.3	1.4/7.7/14.5/21.2/26.7	1.7/7.7/13.6/23.8/27.1	1.4/7.7/14.7/21.4/26.8	1.5/7.7/14.9/21.8/27.1	1.4/7.8/16.6/21.7/32.1	1.5/8.0/15.4/21.6/26.8	1.4/8.7/14.8/21.9/31.8	1.6/8.0/15.3/21.5/26.9

（续表）

故障数	消耗时间/s									
	SEI	GF	MLE	MLE-SEI	GF-SEI	GF-MLE	GF-MAP	HW-MLE	GF-HW	HW-MAP
38	1.4/7.6/15.0/21.7/27.3	1.5/7.9/14.8/22.8/27.2	1.5/8.0/14.9/21.8/27.4	1.7/8.0/14.0/23.9/27.3	1.5/8.1/15.1/21.8/27.7	1.5/8.0/15.4/22.1/28.3	1.5/8.1/16.9/22.5/32.6	1.6/8.3/15.7/22.0/27.6	1.5/9.1/15.4/22.9/32.4	1.6/8.4/15.8/22.3/27.8
39	1.5/7.9/15.5/22.5/28.1	1.5/8.1/15.1/23.0/27.7	1.5/8.2/15.4/22.3/28.1	1.8/8.2/14.0/24.7/28.9	1.5/8.3/15.4/22.4/28.0	1.5/8.3/15.7/22.4/28.4	1.5/8.4/17.3/23.0/33.1	1.6/8.6/16.1/22.6/28.2	1.5/9.3/15.6/23.7/32.9	1.6/8.7/16.2/22.4/28.5
40	1.5/8.1/15.8/22.7/28.9	1.5/8.4/15.4/23.7/28.5	1.6/8.5/15.7/22.6/28.9	1.8/8.5/14.8/25.1/28.7	1.6/8.5/15.9/22.8/29.1	1.6/8.5/16.1/23.1/29.2	1.6/8.6/17.6/23.5/34.1	1.6/8.9/16.6/23.0/29.3	1.6/9.7/16.0/23.8/33.5	1.7/8.9/16.5/23.2/29.4
41	1.5/8.2/16.1/23.5/29.9	1.6/8.5/15.8/24.5/29.3	1.6/8.6/16.1/23.4/29.6	1.8/8.5/14.6/26.0/30.2	1.6/8.6/16.2/23.6/29.8	1.6/8.5/16.5/23.7/30.2	1.6/8.7/18.2/24.2/34.5	1.7/9.0/17.0/23.9/29.9	1.6/9.7/16.3/24.3/34.4	1.7/9.0/17.0/23.9/30.3
42	1.6/8.4/16.6/23.6/30.4	1.6/8.7/16.3/25.2/29.9	1.6/8.7/16.7/23.8/30.3	2.0/8.7/14.6/26.7/30.9	1.6/8.7/16.6/23.9/30.5	1.6/8.8/16.8/24.6/30.8	1.6/8.9/18.5/24.7/35.4	1.7/9.1/17.4/24.4/30.8	1.6/9.9/16.7/25.0/35.5	1.7/9.1/17.5/24.3/30.6
43	1.6/8.6/17.0/24.8/31.1	1.7/8.9/16.7/25.5/30.7	1.7/9.0/17.0/24.8/31.5	2.0/9.0/15.3/27.6/31.5	1.6/9.0/17.0/24.6/31.1	1.7/9.0/17.2/25.0/31.3	1.7/9.1/18.9/25.5/35.9	1.8/9.4/18.1/25.1/31.1	1.7/10.2/17.0/25.6/36.0	1.8/9.4/17.9/24.9/31.1
44	1.7/8.8/17.4/24.8/31.7	1.7/9.1/16.9/25.9/31.5	1.7/9.2/17.5/25.1/32.1	2.1/9.2/15.0/28.0/31.6	1.7/9.3/17.4/25.2/31.9	1.7/9.3/17.7/25.7/32.1	1.7/9.3/19.3/25.6/37.5	1.8/9.6/18.3/25.7/31.9	1.7/10.5/17.4/26.1/37.3	1.8/9.6/18.3/25.6/32.1
45	1.7/8.9/17.7/25.3/32.7	1.7/9.3/17.3/26.6/32.4	1.7/9.4/17.8/25.7/32.9	2.1/9.4/15.6/28.6/32.8	1.7/9.4/17.9/25.9/32.7	1.7/9.3/17.9/26.1/33.2	1.7/9.5/19.8/26.3/37.5	1.9/9.8/18.7/26.2/33.1	1.8/10.6/17.8/26.7/37.4	1.9/9.8/18.6/26.1/33.5
46	1.8/9.5/18.1/26.0/32.9	1.7/9.7/17.9/27.1/33.0	1.8/9.8/18.1/26.3/33.4	2.2/9.8/16.2/29.0/33.7	1.8/9.8/18.3/26.2/33.4	1.8/9.9/18.4/26.6/33.7	1.7/9.8/20.2/27.0/37.6	1.9/10.3/18.9/26.7/33.4	1.8/11.2/18.2/27.4/38.0	2.0/10.4/19.0/26.6/33.3
47	1.8/9.4/18.5/26.9/33.6	1.8/10.3/18.1/28.0/33.5	1.8/9.9/18.5/26.9/33.9	2.2/9.9/16.6/30.5/34.8	1.8/10.1/18.5/27.1/34.5	1.8/9.9/18.8/27.2/34.4	1.8/10.0/20.8/27.9/39.5	1.9/10.3/19.2/27.6/34.0	1.8/11.1/18.6/28.0/39.5	1.9/10.5/19.6/27.3/34.5
48	1.8/9.5/18.9/27.2/34.4	1.8/9.9/18.5/28.9/34.2	1.9/10.0/18.9/27.2/35.0	2.1/9.9/16.0/30.4/34.9	1.8/10.3/18.9/28.0/34.6	1.9/10.1/19.1/27.9/34.9	1.8/10.0/21.2/28.1/40.4	2.0/10.4/19.8/28.3/34.7	1.9/11.2/19.0/28.4/40.5	2.1/10.4/19.9/28.2/35.0
49	1.9/9.8/19.3/27.9/35.3	1.9/10.1/18.9/28.9/35.0	1.9/10.3/19.3/27.9/35.4	2.0/10.2/16.6/31.0/35.7	1.8/10.3/19.4/27.9/35.2	1.9/10.2/19.5/28.1/35.5	1.9/10.4/21.5/28.7/40.6	2.0/10.7/20.3/28.7/35.5	1.9/11.6/19.3/28.9/40.6	2.0/10.7/20.4/28.4/35.7
50	1.9/10.0/19.7/28.4/36.0	1.9/10.2/19.3/29.5/35.5	2.0/10.4/19.5/28.3/36.2	2.0/10.3/17.7/31.9/36.2	1.9/10.4/19.8/28.5/36.1	1.9/10.3/20.1/29.0/36.2	1.9/10.6/21.9/29.2/41.6	2.0/10.8/20.7/28.8/36.3	1.9/11.7/20.0/29.6/41.7	2.1/11.0/20.8/29.2/36.5
51	1.9/10.1/20.0/29.4/36.7	2.0/10.5/19.6/30.4/36.3	2.0/10.6/20.1/29.1/37.1	2.2/10.5/17.7/32.3/37.7	2.0/10.7/20.3/29.5/37.0	2.0/10.6/20.4/29.5/37.1	2.0/10.6/22.4/30.0/42.7	2.1/11.1/21.3/30.0/37.2	1.9/12.0/20.2/30.2/42.5	2.1/11.2/21.2/29.5/37.3
52	2.0/10.4/20.4/29.4/37.4	2.0/10.8/20.1/30.5/37.1	2.0/10.9/20.5/29.5/37.8	2.2/10.8/18.1/32.6/37.3	2.0/10.9/20.7/29.6/37.7	2.0/10.8/20.7/29.9/37.8	2.0/10.9/23.1/30.3/43.5	2.1/11.3/21.6/30.5/37.7	2.0/12.3/20.7/30.5/43.8	2.1/11.4/21.8/30.1/38.0
53	2.0/10.5/20.9/30.2/38.0	2.0/11.0/20.4/31.6/37.7	2.1/11.0/21.0/30.4/38.5	2.2/11.0/18.5/33.8/38.6	2.0/11.1/20.9/30.4/38.3	2.0/10.9/21.0/30.4/38.3	2.0/11.1/23.6/31.1/45.1	2.2/11.5/22.2/30.7/38.4	2.0/12.4/21.3/31.4/45.1	2.2/11.6/22.1/30.4/38.2
54	2.0/10.8/21.1/30.7/38.6	2.1/11.2/20.8/31.6/38.1	2.1/11.3/21.4/30.4/38.8	2.3/11.2/18.5/34.0/40.2	2.0/11.3/21.4/30.6/39.1	2.1/11.2/21.4/30.8/39.3	2.1/11.4/23.9/31.3/45.1	2.2/11.8/22.5/31.4/39.3	2.1/12.8/21.4/31.8/44.7	2.2/11.8/22.6/31.0/39.4
55	2.1/11.1/21.7/31.0/39.3	2.1/11.5/21.0/32.5/38.9	2.1/11.7/21.7/31.2/39.7	2.3/11.6/19.1/34.9/39.5	2.1/11.8/21.8/31.1/39.9	2.1/11.6/21.9/31.5/40.1	2.1/11.8/24.3/31.7/45.7	2.2/12.2/22.7/32.0/39.9	2.1/13.2/21.7/32.5/46.2	2.3/12.2/22.7/31.6/40.4
56	2.1/11.4/22.0/31.9/40.4	2.2/11.7/21.5/32.5/40.0	2.2/11.9/22.0/31.8/40.4	2.3/11.8/19.5/35.1/40.8	2.1/11.9/22.1/32.1/40.3	2.1/11.7/22.2/32.4/40.6	2.1/11.9/24.6/32.3/46.2	2.3/12.4/23.3/33.1/41.0	2.1/13.4/22.0/33.1/47.1	2.3/12.4/23.1/32.2/40.8
57	2.1/11.5/22.3/32.9/40.7	2.2/11.8/21.9/34.1/40.5	2.2/12.0/22.6/32.5/41.1	2.4/12.0/19.9/36.7/41.0	2.2/12.0/22.6/32.6/41.5	2.1/11.9/22.6/33.0/41.1	2.1/12.0/24.8/33.0/47.1	2.3/12.6/23.5/33.8/41.2	2.1/13.6/22.4/33.7/47.2	2.4/12.5/23.5/33.1/41.8
58	2.2/11.8/22.7/33.3/41.9	2.2/12.1/22.2/34.6/41.4	2.2/12.4/22.9/33.2/42.2	2.4/12.3/20.3/37.3/43.3	2.2/12.4/23.0/33.2/42.0	2.2/12.3/22.9/33.6/42.1	2.2/12.4/25.5/34.1/48.7	2.4/12.8/23.9/34.0/42.6	2.2/14.0/22.8/34.7/48.5	2.4/12.9/24.1/33.8/42.2
59	2.2/11.9/23.2/33.6/42.6	2.3/12.3/22.7/34.4/42.0	2.3/12.6/23.4/33.7/43.5	2.5/12.4/21.1/37.5/42.8	2.2/12.4/23.4/33.4/42.6	2.2/12.4/23.5/33.7/42.5	2.2/12.5/25.7/34.3/49.7	2.4/13.0/24.3/34.7/43.1	2.3/14.1/23.3/34.6/49.9	2.5/12.9/24.5/34.2/42.9
60	2.3/12.2/23.6/34.0/43.1	2.3/12.6/23.1/35.3/42.8	2.3/12.8/23.7/34.0/44.2	2.5/12.6/20.9/37.7/43.6	2.3/12.8/23.7/34.6/43.2	2.3/12.6/23.9/34.5/43.4	2.3/12.8/26.1/34.5/50.6	2.4/13.3/24.8/34.9/43.5	2.3/14.4/23.5/34.9/50.4	2.5/13.4/24.8/34.8/43.8
61	2.3/12.3/23.8/34.6/43.7	2.3/12.9/23.3/36.5/43.6	2.3/13.0/24.0/34.6/45.7	2.9/12.9/21.8/38.8/44.2	2.3/13.0/24.0/34.3/44.3	2.3/12.9/24.2/34.7/44.4	2.3/13.0/26.6/35.7/51.3	2.4/13.5/25.1/35.1/44.4	2.3/14.6/24.1/36.0/51.0	2.5/13.5/25.4/35.3/44.6
62	2.3/12.5/24.4/35.1/44.2	2.4/12.9/23.7/36.4/43.9	2.4/13.1/24.5/35.3/45.7	2.5/13.0/23.4/39.1/45.5	2.3/13.1/24.4/35.0/44.7	2.3/12.9/24.7/35.7/44.6	2.3/13.0/27.1/35.8/51.6	2.5/13.6/25.6/35.8/44.9	2.4/14.7/24.3/36.5/51.4	2.5/13.7/25.6/35.5/45.0
63	2.4/12.6/24.7/35.9/45.4	2.4/13.0/24.2/36.8/45.4	2.4/13.4/24.8/35.9/46.6	2.5/13.3/23.0/39.8/45.9	2.4/13.4/24.9/35.9/45.6	2.4/13.2/25.1/36.0/45.7	2.4/13.3/27.9/36.3/51.9	2.5/13.9/26.2/36.7/46.0	2.4/15.0/25.1/37.1/52.2	2.6/13.9/26.3/36.3/46.4
64	2.4/12.8/25.1/36.4/46	2.5/13.2/24.7/37.5/45.7	2.5/13.4/25.2/36.4/46.8	3.0/13.4/22.6/40.7/46.4	2.4/13.3/25.3/36.6/46.6	2.4/13.3/25.4/36.8/46.3	2.4/13.4/27.9/37.2/53.3	2.6/13.9/26.4/37.0/46.6	2.4/15.1/25.5/37.4/53.3	2.6/14.1/26.6/36.9/46.8
65	2.4/12.8/25.7/37.0/46.5	2.5/13.3/24.9/38.2/46.4	2.5/13.5/25.5/36.9/46.8	2.7/13.5/22.0/40.5/47.4	2.4/13.6/25.6/37.0/46.9	2.5/13.3/25.9/36.9/47.0	2.4/13.5/28.3/37.9/54.3	2.6/14.1/26.9/37.8/47.1	2.5/15.2/25.6/37.9/54.9	2.7/14.2/26.9/37.6/47.4
66	2.5/13.2/25.9/37.4/47.2	2.5/13.6/25.3/38.6/46.8	2.6/13.8/26.0/37.6/47.8	2.9/13.7/24.2/41.6/47.9	2.5/13.8/26.0/37.7/47.4	2.5/13.6/26.2/37.7/47.6	2.5/13.7/28.8/38.0/54.9	2.6/14.3/27.2/38.1/48.0	2.5/15.5/25.7/38.7/54.7	2.7/14.4/27.4/37.9/48.1
67	2.5/13.3/26.3/38.0/48.0	2.5/13.8/26.0/39.4/47.5	2.6/14.0/26.5/38.2/48.5	2.9/13.9/24.3/42.6/48.4	2.5/13.9/26.5/38.3/48.4	2.5/13.7/26.5/38.4/48.4	2.5/13.9/29.2/39.2/55.8	2.8/14.5/27.7/39.5/48.6	2.6/15.7/26.1/39.2/55.8	2.8/14.6/27.7/38.9/48.8
68	2.6/13.5/26.6/38.8/49.1	2.5/14.0/26.1/40.3/48.4	2.6/14.2/26.7/38.9/49.4	3.0/14.0/24.2/42.9/49.6	2.6/14.1/26.8/38.7/49.4	2.6/14.0/26.9/38.9/49.2	2.5/14.2/29.6/39.8/54.9	2.8/14.7/27.9/39.8/49.4	2.6/15.9/26.5/40.6/55.1	2.8/14.8/28.1/39.7/49.7
69	2.6/13.7/27.1/39.3/49.6	2.6/14.1/26.5/40.9/49.1	2.7/14.4/27.3/39.2/50.1	3.0/14.2/23.8/43.9/50.6	2.6/14.4/27.3/39.4/49.8	2.6/14.2/27.3/39.7/50.0	2.6/14.4/29.9/40.4/49.8	2.8/15.0/28.3/40.2/50.0	2.6/16.1/26.8/40.7/51.2	2.8/15.0/28.6/40.0/50.3
70	2.6/13.9/27.6/40.2/50.3	2.7/14.5/26.8/41.4/50.0	2.7/14.6/27.5/40.4/50.6	2.9/14.6/24.9/44.8/50.8	2.7/14.6/27.5/40.4/50.3	2.6/14.4/27.7/40.8/50.3	2.6/14.6/27.5/41.1/51.1	2.9/15.2/27.7/41.1/51.1	2.6/16.4/30.3/41.6/51.5	2.9/15.2/27.6/40.5/51.0
71	2.7/14.2/27.8/40.3/51.0	2.7/14.6/27.2/41.3/50.2	2.7/14.9/27.9/40.4/51.4	2.9/14.7/25.1/44.7/51.8	2.7/14.8/27.9/40.1/51.0	2.7/14.6/28.1/40.3/51.2	2.7/14.9/27.9/41.5/51.8	2.9/15.3/28.1/41.2/51.7	2.7/16.5/30.7/41.5/52.5	2.9/15.4/28.0/40.5/51.9
72	2.7/14.2/28.2/41.3/52.0	2.7/14.8/27.6/42.4/51.4	2.8/15.2/28.3/41.0/52.5	2.9/14.8/23.5/45.3/51.6	2.7/14.9/28.4/40.8/52.3	2.7/14.7/28.6/41.0/51.8	2.7/15.0/28.3/41.9/52.4	2.9/15.5/28.7/42.0/52.4	2.7/16.8/31.2/42.0/52.7	2.9/15.7/28.4/41.9/52.6
73	2.7/14.6/28.6/41.5/52.2	2.7/15.2/28.0/43.0/51.7	2.8/15.3/28.7/41.8/52.5	2.9/15.3/25.0/46.4/52.8	2.8/15.4/28.9/41.6/52.5	2.8/15.2/28.9/41.6/52.6	2.7/15.4/28.5/41.9/53.2	3.0/16.0/29.0/42.8/53.0	2.8/17.3/31.7/42.8/53.7	3.0/16.1/28.7/42.4/53.5
74	2.8/14.8/29.0/41.9/53.2	2.8/15.3/28.3/43.5/52.5	2.9/15.5/29.2/42.3/53.6	3.0/15.4/27.3/46.4/54.5	2.8/15.5/29.2/42.3/53.4	2.8/15.3/29.3/42.6/53.3	2.8/15.5/28.9/42.9/54.1	3.0/16.2/29.4/42.9/53.4	2.8/17.5/32.0/43.7/54.6	3.0/16.2/29.1/42.7/53.6
75	2.8/14.9/29.4/42.3/53.6	2.8/15.5/28.6/43.7/53.5	2.9/15.6/29.5/42.7/54.6	3.2/15.6/26.9/48.0/54.7	2.8/15.7/29.6/42.7/54.5	2.9/15.4/29.7/43.0/54.5	2.8/15.6/29.4/44.3/55.2	3.1/16.3/29.8/44.1/54.2	2.9/17.6/32.4/43.2/54.5	3.0/16.4/29.5/43.1/54.9

（续表）

故障数	消耗时间/s									
	SEI	GF	MLE	MLE-SEI	GF-SEI	GF-MLE	GF-MAP	HW-MLE	GF-HW	HW-MAP
76	3.0/15.3/29.7/43.2/54.7	3.0/15.7/29.2/44.3/54.1	3.1/16.0/29.9/43.3/54.9	3.3/15.8/26.4/49.4/55.9	2.9/16.0/29.9/43.5/55.0	3.0/15.8/30.1/44.7/54.5	3.0/15.9/29.7/44.0/55.6	3.2/16.6/30.2/43.5/55.2	3.0/18.0/32.9/44.2/56.0	3.2/16.7/29.9/42.9/55.4
77	2.9/15.4/30.3/43.9/55.9	2.9/16.0/29.5/45.6/54.7	3.0/16.2/30.2/43.7/55.7	3.7/16.1/26.6/49.2/55.4	2.9/16.2/30.4/43.9/56.0	2.9/16.0/30.3/44.7/55.7	2.9/16.2/30.2/44.9/56.6	3.1/16.8/30.4/44.7/56.1	2.9/18.2/33.3/45.8/56.3	3.1/16.9/30.4/44/56.7
78	2.9/15.7/30.5/43.8/55.9	3.0/16.1/29.9/45.6/55.4	3.0/16.3/30.7/44.7/56.7	3.7/16.3/27.9/49.6/56.9	2.9/16.4/30.8/44.4/56.6	2.9/16.1/30.8/44.5/56.1	2.9/16.3/30.5/45.0/57.0	3.1/17.0/30.9/45.5/56.6	2.9/18.4/33.8/45.5/56.8	3.1/17.1/30.8/44.9/56.9
79	3.0/15.8/31.0/45.4/56.6	3.0/16.4/30.2/46.5/56.3	3.0/16.6/31.1/44.7/57.0	3.8/16.4/28.2/50.3/57.7	3.0/16.5/31.2/45.0/56.6	3.0/16.4/31.2/45.4/56.7	2.9/16.5/30.9/45.4/57.2	3.2/17.3/31.3/45.6/57.5	3.0/18.6/34.2/46.6/57.8	3.2/17.2/31.1/45.8/57.6
80	3.0/15.9/31.3/45.2/57.2	3.0/16.5/30.5/46.5/56.7	3.1/16.8/31.5/45.5/57.8	3.5/16.6/27.9/50.9/57.9	3.0/16.8/31.6/45.5/57.8	3.0/16.5/31.5/46.0/57.6	3.0/14.1/31.4/46.2/58.3	3.3/17.4/31.7/46.1/58.0	3.0/18.9/34.7/47.0/58.6	3.2/17.4/31.5/45.8/58.1
81	3.0/16.2/31.7/46.1/58.1	3.1/16.7/31.0/47.3/57.7	3.1/16.9/31.8/45.8/59.0	3.5/16.8/28.9/51.5/58.9	3.1/16.9/31.9/45.8/59.1	3.1/16.7/32.1/46.3/58.4	3.0/16.9/31.7/46.6/59.2	3.3/17.6/32.1/47.2/59.1	3.0/19.0/35.0/47.2/59.4	3.3/17.7/32.0/46.4/59.9
82	3.1/16.4/32.1/46.6/59.0	3.1/17.0/31.4/47.8/58.5	3.2/17.2/32.2/46.2/59.3	3.6/17.1/28.3/51.4/59.8	3.1/17.2/32.2/46.3/59.8	3.1/17.0/32.4/47.2/59.6	3.1/17.1/32.0/47.3/60.3	3.3/17.8/32.5/47.5/59.6	3.1/19.2/35.4/47.4/60.1	3.3/18.0/32.5/47.1/60.0
83	3.1/16.5/32.5/47.2/59.3	3.2/17.0/31.8/48.9/58.8	3.2/17.3/32.7/47.5/60.0	4.1/17.2/29.1/52.4/60.1	3.1/17.4/32.6/47.6/59.8	3.1/17.0/32.8/48.1/59.8	3.1/17.3/32.4/48.6/60.6	3.4/18.0/32.9/48.6/60.3	3.1/19.4/35.9/48.7/60.9	3.4/18.1/32.7/47.8/60.7
84	3.2/16.8/32.8/48.0/60.6	3.2/17.1/32.0/49.5/60.0	3.2/17.5/32.9/47.9/60.8	3.8/17.4/28.8/53.1/60.9	3.2/17.5/33.0/48.1/60.6	3.2/17.2/33.1/48.1/60.2	3.1/17.4/32.8/49.0/61.4	3.4/18.2/33.7/49.0/61.0	3.2/19.6/36.2/49.6/61.3	3.4/18.2/33.4/48.7/61.0
85	3.2/17.0/33.2/48.4/61.1	3.2/17.7/32.5/49.8/60.7	3.3/17.9/33.4/48.1/61.6	3.7/17.7/29.8/53.5/61.6	3.2/17.9/33.4/47.6/61.2	3.2/17.6/33.5/48.2/61.4	3.2/17.8/33.4/49.2/62.1	3.4/18.5/33.7/49.5/61.9	3.2/20.1/36.7/49.4/62.6	3.4/18.6/33.6/49.2/61.9
86	3.2/17.2/33.7/48.6/62.1	3.3/17.8/32.9/50.5/61.3	3.3/18.0/33.7/48.8/62.4	4.0/17.9/30.6/54.1/62.2	3.2/17.9/33.8/48.6/62.4	3.2/17.7/33.8/49.1/62.1	3.3/17.9/33.6/49.3/62.8	3.5/18.7/34.0/49.8/62.8	3.2/20.2/37.2/50.1/63.4	3.4/18.8/33.9/49.0/63.0
87	3.3/17.4/34.1/49.3/62.4	3.3/17.9/33.3/50.8/61.6	3.4/18.3/34.1/49.3/62.9	3.9/18.1/31.3/55.2/64.0	3.3/18.3/34.3/49.7/62.5	3.3/17.9/34.4/49.4/62.8	3.3/18.3/34.1/50.3/64.1	3.5/19.0/34.5/50.8/63.1	3.3/20.4/37.5/50.4/63.7	3.5/19.0/34.6/50.2/63.6
88	3.3/17.5/34.4/50.1/62.7	3.4/18.2/33.7/51.4/62.2	3.4/18.5/34.5/50.0/63.9	4.4/18.3/33.5/55.9/63.3	3.3/18.4/34.8/50.3/63.1	3.3/18.2/34.7/50.7/63.2	3.3/18.4/34.3/51.4/64.3	3.6/19.2/34.9/51.1/63.9	3.3/20.7/38.0/51.5/64.4	3.5/19.4/34.8/50.5/64.2
89	3.4/17.6/34.8/50.9/63.8	3.4/18.2/33.9/51.6/63.3	3.4/18.5/35.0/50.9/64.2	4.2/18.3/29.2/56.6/65.2	3.4/18.6/35.2/50.3/64.4	3.3/18.2/35.0/50.7/64.2	3.4/18.4/34.8/51.3/65.5	3.6/19.2/35.3/52.1/64.8	3.3/20.8/38.4/51.5/65.4	3.6/19.1/35.3/51.3/65.1
90	3.4/17.9/35.2/51.0/64.4	3.4/18.6/34.4/53.9/64.0	3.5/18.9/35.4/51.2/65.5	4.0/18.7/31.3/57.1/65.9	3.4/18.8/35.4/51.1/64.7	3.4/18.5/35.7/50.9/64.9	3.4/18.7/35.0/51.8/65.8	3.7/19.6/35.6/52.5/64.9	3.4/21.1/38.9/52.5/65.7	3.6/19.5/35.7/52.8/65.7
91	3.5/18.1/35.6/52.2/65.1	3.5/18.7/34.9/54.2/64.6	3.5/19.0/35.7/52.0/65.7	3.9/18.9/28.3/58.2/66.5	3.4/18.9/35.8/52.5/66.0	3.4/18.7/35.9/52.2/65.6	3.4/19.0/35.5/53.3/66.4	3.7/19.7/36.0/53.1/66.5	3.4/21.3/39.3/54.0/66.4	3.7/19.7/36.1/52.6/66.7
92	3.5/18.4/36.0/52.0/65.7	3.5/18.9/35.2/53.4/65.6	3.5/19.2/36.1/52.3/66.6	4.2/19.2/28.6/58.3/67.1	3.4/19.2/36.3/53.0/66.6	3.5/18.9/36.3/52.7/66.1	3.4/19.1/35.9/54.2/67.0	3.7/20.0/36.4/52.7/66.8	3.5/21.5/39.7/53.4/67.2	3.7/19.9/36.5/53.0/67.2
93	3.5/18.5/36.4/52.8/66.6	3.5/19.1/35.5/54.6/65.9	3.6/19.4/36.6/52.2/67.4	4.1/19.2/29.0/58.7/68.1	3.5/19.4/36.5/53.3/67.1	3.5/19.1/36.7/52.8/67.1	3.5/19.3/36.4/54.6/67.6	3.8/20.2/36.7/53.4/67.3	3.5/21.7/40.0/54.3/68.4	3.7/20.1/36.9/53.5/68.2
94	3.6/18.6/36.7/53.7/67.6	3.6/19.1/35.9/54.4/66.4	3.6/19.5/37.0/53.0/68.0	4.0/19.3/29.3/59.3/68.4	3.5/19.4/36.9/53.0/67.6	3.5/19.2/37.2/53.2/67.9	3.5/19.4/36.6/54.2/69.5	3.8/20.3/37.1/53.6/68.2	3.6/21.8/40.5/54.4/68.6	3.8/20.2/37.4/53.9/68.4
95	3.6/18.8/37.3/54.2/68.3	3.6/19.4/36.4/56.2/67.6	3.6/19.8/37.2/53.9/68.6	4.3/19.6/29.5/59.7/70.5	3.6/19.8/37.5/54.1/67.9	3.6/19.4/37.4/54.6/67.9	3.5/19.6/37.0/55.2/69.1	3.9/20.5/37.6/54.4/68.9	3.6/22.1/41.2/55.2/69.4	3.8/20.5/37.8/55.0/69.0
96	3.6/18.8/37.6/54.5/68.5	3.7/19.5/36.7/56.2/68.2	3.7/19.8/37.8/54.5/69.6	4.1/19.8/29.9/60.4/70.7	3.6/19.8/37.8/54.2/69.3	3.6/19.5/37.9/54.4/68.9	3.6/19.9/37.5/55.4/70.0	3.9/20.9/38.1/55.6/70.0	3.6/22.4/41.4/55.9/69.9	3.9/20.8/38.1/55.7/69.9
97	3.6/19.5/38.0/55.3/69.7	3.7/19.9/37.2/56.1/68.7	3.7/20.1/38.1/54.8/70.1	4.2/20.0/30.2/61.4/70.3	3.6/20.1/38.3/55.8/70.1	3.7/19.8/38.2/55.4/69.4	3.6/20.1/37.9/56.6/70.4	3.9/21.0/38.4/55.2/70.3	3.7/22.6/42.0/56.7/71.0	3.9/20.8/38.4/56.0/70.5
98	3.7/19.6/38.2/55.4/70.0	3.7/20.2/37.4/58.4/69.2	3.7/20.5/38.7/55.5/71.0	4.2/20.2/30.9/62.5/71.8	3.7/20.4/38.8/56.4/70.6	3.7/20.1/38.6/56.7/70.5	3.7/20.3/38.1/57.0/71.6	4.0/21.2/38.8/56.9/71.2	3.7/22.8/42.3/57.7/71.2	4.0/21.0/38.8/56.9/71.6
99	3.7/19.8/38.8/56.2/71.2	3.7/20.5/37.9/58.4/70.4	3.8/20.9/38.9/56.4/71.2	4.2/20.7/31.0/62.6/71.6	3.7/20.7/39.0/56.4/71.1	3.7/20.5/38.9/56.2/71.0	3.7/20.8/38.8/57.7/71.7	4.0/21.7/39.2/57.1/71.9	3.7/23.4/42.7/58.4/71.9	4.0/21.6/39.3/57.2/72.2
100	3.8/20.1/39.2/56.7/71.7	3.8/20.9/38.1/58.8/70.9	3.9/21.1/39.2/56.8/72.3	4.5/20.8/31.3/62.8/72.8	3.8/21.1/39.5/56.9/72.3	3.8/20.7/39.3/57.0/72.3	3.8/20.9/39.1/58.1/72.8	4.1/21.8/39.5/57.3/73.1	3.8/23.6/43.2/58.4/72.7	4.1/21.8/39.7/57.4/73.1
101	3.8/20.3/39.6/57.2/72.7	3.8/21.0/38.5/59.3/71.2	3.8/21.2/39.7/57.5/72.8	4.2/21.1/31.3/64.5/73.1	3.8/21.3/39.7/57.2/73.5	3.8/20.9/39.8/57.9/73.0	3.8/21.2/39.4/58.5/74.0	4.1.0/22.1/39.9/57.8/73.5	3.8/23.9/43.5/59.3/73.7	4.1/22.0/40.2/58.3/74.4
102	3.8/20.4/39.9/57.5/72.6	3.9/21.0/39.0/59.6/72.4	3.9/21.4/40.0/58.2/73.7	4.2/21.3/31.7/64.2/74.2	3.8/21.4/40.1/57.5/73.5	3.8/21.0/40.2/58.1/73.2	3.8/21.2/40.0/59.2/74.6	4.1.0/22.1/40.4/57.9/73.9	3.9/24.0/43.9/59.1/74.4	4.1/22.1/40.5/58.4/74.3
103	3.9/20.5/40.2/58.3/73.4	3.9/21.2/39.3/61.1/72.6	3.9/21.4/40.5/58.8/74.4	4.4/21.3/33.9/65.9/76.3	3.8/21.4/40.6/58.8/74.6	3.9/21.1/40.6/58.6/74.1	3.8/21.3/40.2/59.5/75.2	4.2/22.4/40.8/59.6/74.4	3.9/24.1/44.4/60.2/75.3	4.2/22.3/40.8/60.0/74.5
104	3.9/20.7/40.7/59.3/74.2	3.9/21.3/39.8/61.5/73.5	4.0/21.7/40.7/59.5/75.3	4.6/21.4/32.3/66.2/75.8	3.9/21.5/41.0/59.2/75.5	3.9/21.3/40.9/59.7/74.7	3.9/21.6/40.5/60.0/76.1	4.2/22.5/41.2/59.9/75.3	3.9/24.2/44.9/61.2/75.8	4.2/22.4/41.2/60.8/75.8
105	4.0/21.1/41.2/59.9/74.8	4.0/21.7/40.0/61.4/74.4	4.0/22.1/41.3/60.0/75.8	4.4/21.9/32.7/66.4/76.4	3.9/22.1/41.4/59.2/75.8	3.9/21.7/41.5/59.5/75.5	3.9/22.0/40.9/60.5/76.6	4.2/23.0/41.6/59.9/76.3	3.9/24.7/45.4/61.2/76.5	4.3/22.9/41.5/60.5/77.2
106	4.0/21.3/41.4/59.9/75.8	4.0/21.8/40.4/62.8/75.2	4.1/22.3/41.7/60.2/76.9	4.8/22.1/33.2/66.5/77.0	4.0/22.3/41.7/60.4/76.0	4.0/22.0/41.9/60.4/76.0	4.0/22.2/41.4/61.2/76.9	4.3.0/23.2/41.9/60.7/76.4	4.0/25.0/45.6/61.8/77.0	4.3/23.1/42.1/60.8/77.3
107	4.0/21.3/41.9/60.4/76.5	4.1/22.0/41.0/62.9/76.3	4.1/22.4/42.0/60.6/77.4	4.4/22.2/33.5/67.5/77.2	4.0/22.4/42.1/61.2/76.8	4.0/22.1/42.2/61.3/76.6	4.0/22.3/41.7/61.9/77.8	4.3/23.2/42.3/61.4/77.7	4.0/25.1/46.1/63.2/78.4	4.3/23.2/42.5/61.6/77.6
108	4.1/21.6/42.3/61.1/77.8	4.1/22.2/41.4/62.7/77.7	4.2/22.6/42.3/61.3/78.7	4.7/22.4/33.6/67.9/77.8	4.0/22.6/42.5/60.9/78.1	4.1/22.2/42.6/61.4/77.8	4.0/22.5/42.1/62.3/78.8	4.4/23.5/42.7/61.9/78.3	4.0/25.2/46.5/62.4/78.4	4.3/23.3/42.9/62.6/78.6
109	4.1/21.9/42.8/61.8/77.9	4.1/22.4/41.6/64.0/77.1	4.2/22.8/42.8/62.3/78.9	4.7/22.8/33.8/69.2/78.6	4.1/22.8/42.9/61.8/78.5	4.1/22.4/42.9/62.2/78.4	4.1/22.8/42.6/63.8/78.9	4.4/23.8/43.1/62.4/78.9	4.1/25.6/47.0/64.0/78.9	4.4/23.6/43.4/62.7/79.2
110	4.2/22.1/42.9/62.8/78.6	4.2/22.9/41.9/64.6/78.0	4.2/23.3/43.1/63.2/79.5	4.5/23.1/34.1/70.1/80.6	4.1/23.3/43.3/63.5/79.5	4.1/22.8/43.3/63.1/78.8	4.1/23.1/42.9/63.8/79.8	4.4/24.2/43.5/63.3/79.3	4.1/26/47.4/65.4/80.1	4.4/24.0/43.7/63.7/80.4

参考文献：

[1] AHANGER T A, ALJUMAH A. Internet of things: a comprehensive study of security issues and defense mechanisms[J]. IEEE Access, 2019(7):11020-11028.

[2] ALIOTO M, SHAHGHASEMI M. The Internet of things on its edge: trends toward its tipping point[J]. IEEE Consumer Electronics Magazine, 2018, 7(1):77-87.

[3] MOHD B J, HAYAJNEH T. Lightweight block ciphers for IoT: energy optimization and survivability techniques[J]. IEEE Access, 2018, 6:35966-35978.

[4] ABED S, JAFFAL R, MOHD B J, et al. FPGA modeling and optimization of a SIMON lightweight block ciphers[J]. Sensors, 2019, 19(3): 913.

[5] 王元昊, 李宏博, 崔钰钊, 等. 具有密文等值测试功能的公钥加密技术综述[J]. 网络与信息安全学报, 2018, 4(11) : 13-22.
WANG Y H, LI H B, CUI Y Z, et al. Survey on public key encryption with equality test[J]. Chinese Journal of Network and Information Security, 2018, 4(11):13-22.

[6] LI T, OTA K, WANG T, et al. Optimizing the coverage via the UAVs with lower costs for information-centric Internet of things[J]. IEEE Access, 2019(7): 15292-15309.

[7] MAYER C P. Security and privacy challenges in the internet of things[J]. Electronic Communications of the European Association of Software Science and Technology, 2009, 17(3):11-22.

[8] 陈彦琴. SIMECK32/64 算法的不可能差分分析[J]. 计算机工程, 2017, 43(4) : 141-153.
CHEN Y Q, ZHANG W Y. Impossible differential cryptanalysis of SIMECK32/64 algorithm[J]. Computer Engineering, 2017,43(4): 141-153.

[9] 万刘蝉, 韦永壮. 简化 SIMON 类算法的立方测试与分析[J]. 计算机应用研究, 2017, 34(1) : 246-250.
WAN L C, WEI Y Z. Cube test and analysis for reduced SIMON family of block ciphers[J]. Application Research of Computers, 2017, 34(1):246-250.

[10] 董向忠, 关杰. SIMON类算法轮函数的差分性质分析[J]. 密码学报, 2015, 2(3) : 207-216.
DONG X Z, GUAN J. Analysis on differential properties of the round function of SIMON family of block ciphers[J]. Journal of Cryptologic Research, 2015, 2(3):207-216.

[11] GHOSHAL A, PATRANABIS S, MUKHOPADHYAY D. Template-based fault injection analysis of block ciphers[C]// International Conference of Security, Privacy, and Applied Cryptography Engineering. 2018:21-36.

[12] BIEHL I, MEYER B, MÜLLER V. Differential fault attacks on elliptic curve cryptosystems[C]// International Conference of Advances in Cryptology. 2000:131-146.

[13] FISCHER W, REUTER C A. Differential fault analysis on Grøstl[C]// International Workshop of Fault Diagnosis and Tolerance in Cryptography. 2012:44-54.

[14] HEMME L, HOFFMANN L. Differential fault analysis on the SHA1 compression function[C]// International Workshop of Fault Diagnosis and Tolerance in Cryptography. 2011:54-62.

[15] 王永娟, 任泉宇, 张诗怡. 轻量级分组密码 Klein 的差分故障攻击[J]. 通信学报, 2016(S1) : 115-119.
WANG Y J, REN Q Y, ZHANG S Y. Differential fault attack on lightweight block cipher Klein[J]. Journal on Communications, 2016(S1):115-119.

[16] BIHAM E, SHAMIR A. Differential fault analysis of secret key cryptosystems[C]// International Conference of Advances in Cryptology. 1997:513-525.

[17] ZONG R, DONG X Y, WANG X Y. Impossible differential attack on Simpira v2[J]. Science China Information Sciences, 2018, 61(3), 032106:1-032106:13.

[18] WANG D, WANG A, ZHENG X. Fault-tolerant linear collision attack: a combination with correlation power analysis[C]// International Conference of Information Security Practice and Experience. 2014: 232-246.

[19] LI R, JIN C. Meet-in-the-middle attacks on reduced-round QARMA-64/128[J]. The Computer Journal, 2018, 61(8):1158-1165.

[20] JOVANOVIC P, KREUZER M, POLIAN I. An algebraic fault attack on the LED block cipher[C]// International Conference of IACR Cryptology ePrint Archive. 2012:400.

[21] KORKIKIAN R, PELISSIER S, NACCACHE D. Blind fault attack against SPN ciphers[C]// International Workshop of Fault Diagnosis and Tolerance in Cryptography.2014:94-103.

[22] WANG A, ZHANG Y, TIAN W, et al. Right or wrong collision rate analysis without profiling: full-automatic collision fault attack[J]. Science China Information Sciences, 2018, 61(3):032101:1- 032101: 11.

[23] SANTIS F D, GUILLEN O, SAKIC E, et al. Ciphertext-only fault attack on PRESENT[C]// International Workshop of Lightweight Cryptography for Security and Privacy. 2014:85-108.

[24] FUHR T, JAULMES E, LOMNE V, et al. Fault attacks on AES with faulty ciphertexts only[C]// International Workshop of Fault Diagnosis and Tolerance in Cryptography. 2013:108-118.

[25] 李玮, 吴益鑫, 谷大武, 等. LBlock 轻量级密码算法的唯密文故障分析[J]. 计算机研究与发展, 2018, 55(10) : 82-92.
LI W, WU Y X, GU D W, et al. Ciphertext-only fault analysis of the LBlock lightweight cipher[J]. Journal of Computer Research and Development, 2018, 55(10) : 82-92.

[26] BEAULIEU R, SHORS D, SMITH J, et al. The SIMON and SPECK families of lightweight block ciphers[J]. IACR Cryptology ePrint Archive, 2013:404.

[27] TUPSAMUDRE H, BISHT S, MUKHOPADHYAY D. Differential fault analysis on the families of SIMON and SPECK ciphers[C]// International Workshop of Fault Diagnosis and Tolerance in Cryptography, 2014:40-48.

[28] TAKAHASHI J, FUKUNAGA T. Fault analysis on SIMON family of lightweight block ciphers[C]//International Conference on Information Security and Cryptology. Springer, 2014:175-189.

[29] CHEN H, FENG J Y, RIJIMEN V, et al. Improved fault analysis on SIMON block cipher family[C]// International Workshop of Fault Diagnosis and Tolerance in Cryptography. 2016:16-24.

[30] 马云飞, 王韬, 陈浩, 等. 轻量级分组密码 SIMON 代数故障攻击[J]. 计算机应用, 2017, 37(7) : 1953-1959.
MA Y F, WANG T, CHEN H, et al. Algebraic fault attack on lightweight block ciphers SIMON[J]. Journal of Computer Applications, 2017, 37(7): 1953-1959.

[31] 李玮, 葛晨雨, 谷大武, 等. 物联网环境中 LED 轻量级密码算法的统计故障分析研究[J]. 计算机研究与发展, 2017, 54(10): 2205-2214.
LI W, GE C Y, GU D W, et al. Research on the LED lightweight cipher against the statistical fault analysis in Internet of things[J]. Journal of Computer Research and Development, 2017, 54(10): 2205-2214.

[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，主要研究方向为密码分析。

吴益鑫（1995− ），女，浙江湖州人，东华大学硕士生，主要研究方向为分组密码的安全性分析。

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与计算机安全。

李嘉耀（1996− ），男，广东广州人，东华大学硕士生，主要研究方向为对称密码的安全性分析。

曹珊（1995− ），女，湖南株洲人，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。

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

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

丁祥武（1963− ），男，湖北荆门人，博士，东华大学副教授、硕士生导师，主要研究方向为区块链安全。

刘志强（1970− ），男，江西南昌人，博士，上海交通大学副研究员，主要研究方向为密码学与计算机安全。