计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2019.20190406
56(10):2216-2228,2019

物联网中 MIBS 轻量级密码的唯密文故障分析

李 玮[1,2,3,4] 曹 珊[1] 谷大武[2] 李嘉耀[1] 汪梦林[1] 蔡天培[1] 石秀金[1]
[1](东华大学计算机科学与技术学院 上海 201620)
[2](上海交通大学计算机科学与工程系 上海 200240)
[3](上海市可扩展计算与系统重点实验室(上海交通大学) 上海 200240)
[4](上海市信息安全综合管理技术研究重点实验室(上海交通大学) 上海 200240)
(liwei.cs.cn@gmail.com)

Ciphertext-Only Fault Analysis of the MIBS Lightweight Cryptosystem in the Internet of Things

Li Wei[1,2,3,4], Cao Shan[1], Gu Dawu[2], Li Jiayao[1], Wang Menglin[1], Cai Tianpei[1], and Shi Xiujin[1]
[1](*School of Computer Science and Technology, Donghua University, Shanghai* 201620)
[2](*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240)
[3](*Shanghai Key Laboratory of Scalable Computing and Systems (Shanghai Jiao Tong University), Shanghai* 200240)
[4](*Shanghai Key Laboratory of Integrate Administration Technologies for Information Security (Shanghai Jiao Tong University), Shanghai* 200240)

Abstract The lightweight cryptosystem MIBS was proposed at the CANS conference in 2009. It has high efficiency in both hardware implementation and software implementation. MIBS can resist against classical cryptanalysis, such as differential analysis and linear analysis, etc. It is suitable for the resource-limited devices in the Internet of things. This paper proposes new ciphertext-only fault analysis of the MIBS cryptosystem. The attackers can apply a new fault model of Double AND and two novel distinguishers of Parzen-HW and Parzen-HW-MLE to break MIBS. The experiments only require at least 72 fault injections to recover the secret key with a success probability of no less than 99%. The method can further reduce fault injections and time, and effectively improve the attacking efficiency. It shows that the ciphertext-only fault analysis poses a serious threaten to the security of MIBS. The research also provides an important reference for the security analysis of other lightweight cryptosystems.

Key words lightweight cryptosystem; MIBS; ciphertext-only fault analysis; Internet of things; distinguisher

摘 要 MIBS 密码是在 2009 年的密码学和网络安全(CANS)会议上提出的一种轻量级算法,它具有较高的软硬件实现效率,并且能够抵抗差分分析、线性分析等传统密码分析方法,适合运行在资源受限,并

收稿日期:2019-06-12;**修回日期**:2019-08-01
基金项目:国家自然科学基金项目(61772129);国家密码发展基金项目(MMJJ20180101);上海市可扩展计算与系统重点实验室开放课题;上海市信息安全综合管理技术研究重点实验室开放课题(AGK201703);上海市青年科技英才扬帆计划(17YF1405500);东华大学研究生创新基金项目(GSIF-DH-M-2019013)
This work was supported by the National Natural Science Foundation of China (61772129), the National Cryptography Development Fund (MMJJ20180101), the Open Fund of Shanghai Key Laboratory of Scalable Computing and Systems, the Open Fund of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (AGK201703), the Shanghai Sailing Program (17YF1405500), and the Graduate Student Innovation Fund of Donghua University (GSIF-DH-M-2019013).
通信作者:石秀金(sxj@dhu.edu.cn)

有一定安全要求的物联网环境中.提出了一种针对 MIBS 密码的新型唯密文故障攻击,即利用新型双重"与"故障模型、新型 Parzen-HW 和 Parzen-HW-MLE 区分器对中间状态进行分析,进而破译 MIBS 密码.实验表明:该方法最少使用 72 个故障注入即可破译出主密钥,并且成功率不小于 99%.该方法可以进一步降低故障注入数和时间,有效地提高了攻击效率.研究表明:唯密文故障攻击对 MIBS 密码算法的安全性造成极大的威胁,为其他轻量级密码的安全性分析提供了重要参考.

关键词　轻量级密码;MIBS;唯密文故障攻击;物联网;区分器

中图法分类号　TP309.7

物联网是物物相连的网络,它通过信息传感设备,按照某种协议把任何物品接入互联网,进行信息交换和通信,以实现对物品的智能化识别、定位、跟踪、监控和管理,广泛应用于智能家居、食品安全、智能电网、智慧医疗、智能交通、精准农业、智能环保、智慧物流、智能零售和公共安全等领域中[1-5].物联网的普及为人们的工作、学习和生活带来了极大的便利,但是,与传统的网络相比,它遭受到更大的安全风险.原因在于物联网中使用的终端设备存储和计算能力有限,不能有效地使用传统的密码算法实现信息的保密性、完整性和认证性.为了保护物联网中的数据免遭截获、篡改和伪造等威胁,国内外学者设计了具有一系列功耗低、吞吐量小、执行效率高和安全性能佳的轻量级密码,包括 MIBS 密码、LBlock 密码、Simon 密码和 Simeck 密码等[6-9].

2009 年 Lzadi 等学者[6]于密码学和网络安全(CANS)会议上提出了 MIBS 轻量级分组密码,该密码具有典型的 Feistel 结构,分组长度为 64 b,密钥长度分为 64 b 和 80 b,具有功耗低、存储占用小等优点,适合在资源受限的 RFID 设备上使用.MIBS 算法可以进行抵抗差分攻击、线性攻击、不可能差分攻击、积分攻击、中间相遇攻击和碰撞攻击等分析[10-15].

在物联网环境中,RFID 等设备易受到故障分析(fault analysis, FA)的攻击.1996 年 Boneh 等学者[16-18]针对 RSA 密码系统首次提出故障分析,以较低的攻击代价破译了密钥,引起了国内外研究学者的广泛关注.1997 年 Biham 等学者[18]提出了差分故障分析(differential fault analysis, DFA),并成功破译了 DES 密码.攻击者通过利用强磁场、电源电压毛刺、时钟毛刺、激光干扰、外界温度变化等方式对密码模块执行过程中的中间状态进行扰乱,从而获得错误的密文,并结合其他有效信息来破译主密钥.在物联网环境中,RFID 等设备易受到这种攻击.

在故障攻击的实现中,基本假设至关重要,分为选择明文攻击(chosen plaintext attack, CPA)和唯密文攻击(ciphertext-only attack, COA).例如差分故障攻击、线性故障攻击、积分故障攻击、不可能差分故障攻击等的基本假设均为选择明文攻击,即攻击者可以选择获取任意明文的密文及相对应的错误密文.而仅有唯密文故障攻击的基本假设为唯密文攻击,即攻击者可以获得任意密文或错误密文.在唯密文攻击假设下,攻击者的能力最弱,一旦获得成功,将对密码系统的安全造成巨大威胁.因此,分析轻量级密码算法能否抵抗唯密文攻击假设下的故障攻击,对于物联网安全具有十分重要的意义.

目前,国内外还未有公开发表关于 MIBS 轻量级密码算法是否抵抗唯密文故障攻击方法的结果.本文深度剖析了 MIBS 密码的内部结构和运算,使用唯密文故障攻击对其进行了安全性分析,不仅实现了已有的"与"故障模型下的平方欧氏距离等 7 种区分器,而且提出了新型的双重"与"故障模型、新型 Parzen-HW 双重区分器和 Parzen-HW-MLE 三重区分器.结果表明,使用新型故障模型和区分器不仅提高了故障攻击效率,而且降低了故障攻击需要的故障注入数.该方法的提出,对于保护物联网等环境中的数据传输安全、增强密码系统的自主开发和分析能力,无疑都具有重要的现实意义和价值.

1　相关工作

自 MIBS 轻量级密码提出后,国内外研究学者相继使用差分攻击、线性攻击、不可能差分攻击、积分攻击、中间相遇攻击和碰撞攻击等传统密码分析方法对其安全性进行了分析.如表 1 所示,这些结果检测了 MIBS 密码缩减轮的安全性.

在故障攻击分析 MIBS 密码方面,研究学者通常使用选择明文假设下的差分故障攻击,完成破译 MIBS 密码全部轮.2011 年王素贞等学者[19]在加密部分的最后 2 轮分别注入 32 b 故障,将密钥搜索空

间降低到 $2^{21.7}$.2018 年王永娟等学者[20]基于 S 盒差分传播特性,在加密部分的最后一轮注入 4 b 故障,进而恢复最后一轮密钥的 47 b,所需要的时间复杂度为 2^{17}.2019 年 Gao 等学者[21]通过计算 S 盒的差分分布的统计规律,在最后 3 轮中分别注入 4 b 故障,恢复主密钥的时间复杂度仅为 2^2.本文分析了在唯密文攻击假设下,MIBS 密码抵抗唯密文故障攻击的安全性.表 2 给出了针对 MIBS 算法的故障分析对比.

Table 1 Classical Cryptanalysis of MIBS

表 1 针对 MIBS 密码的传统密码分析

Type	Rounds	Data	Time	Reference
Collision Attack	10	$2^{11.5}$	$2^{48.32}$	Ref [10]
Integral Attack	10	$2^{61.67}$	2^{40}	Ref [11]
Meet-in-the-middle Attack	11	$2^{39.65}$	$2^{68.46}$	Ref [12]
Differential Attack	13	2^{61}	2^{56}	Ref [13]
Impossible Differential Attack	15	$2^{52.8}$	$2^{55.5}$	Ref [14]
Linear Attack	19	$2^{57.8}$	$2^{74.23}$	Ref [15]

Table 2 Comparison of Fault Analysis of MIBS

表 2 针对 MIBS 算法的故障分析对比

Type	Assumption	Model/b	References
DFA	CPA	4/32	Ref [19-21]
CFA	COA	4	This paper

2013 年 Fuhr 等学者[22]首次针对 AES 密码提出了唯密文故障攻击方法,结合平方欧氏距离、汉明重量和极大似然估计等区分器,仅需要 320,288 和 224 个故障注入,可以恢复最后一轮密钥.2017 年李玮等学者[23]将唯密文故障攻击应用在 LED 密码上,并新增了拟合优度区分器和拟合优度—平方欧氏距离双重区分器,用于降低所需的故障注入数.以上 2 种分析方法都是针对 SPN 结构的密码.2018 年李玮等学者针对 Feistel 结构的 LBlock 轻量级密码,新增了双重区分器,提高了故障攻击的效率[24].从目前的研究可以看出,改进的唯密文故障攻击的方法均是通过优化选择单区分器和双重区分器来降低故障注入数.结合物联网环境和 MIBS 密码的设计特点,本文提出的唯密文故障攻击不仅增加了新型的双重区分器和三重区分器,而且构建了新型的双重"与"故障模型,进一步提高了故障导入效率,减少了故障注入数.表 3 总结了 AES 算法、LBlock 算法和 MIBS 算法的唯密文故障攻击所需故障注入的结果对比.

Table 3 Comparison of Fault Injections to Decrypting the Last Subkey of AES, LBlock and MIBS

表 3 破译 AES,LBlock 和 MIBS 密码最后一轮子密钥所需故障数对比

Distinguisher	AES	LBlock	MIBS	
	AND	AND	AND	Double AND
SEI	320	124	108	46
GF		114	110	38
HW	288		74	28
MLE	224	92	70	28
GF-SEI		70	86	36
GF-MLE		90	92	34
MLE-SEI		58	92	34
Parzen-HW			68	26
Parzen-HW-MLE			64	24

2 MIBS 算法介绍

2.1 符号说明

设明文为 $X=L_1 \| R_1 \in (F_2^4)^{16}$,密文为 $Y=L_{33} \| R_{33} \in (F_2^4)^{16}$,主密钥为 K,子密钥为 $k_l \in (F_2^4)^{16}$,$\|$ 表示级联,$L_l \in (F_2^4)^8$ 和 $R_l \in (F_2^4)^8$ 分别为第 l 轮输入的左右两块各 32 b,其中 $l \in [1,32]$.

2.2 MIBS 密码简介

MIBS 密码的分组长度为 64 b,MIBS-64 版本和 MIBS-80 版本分别对应密钥长度为 64 b,80 b,其迭代轮数均为 32 轮.算法由加密、解密和密钥编排 3 部分组成.解密与加密相同,所使用的子密钥顺序相反.结构如图 1 所示:

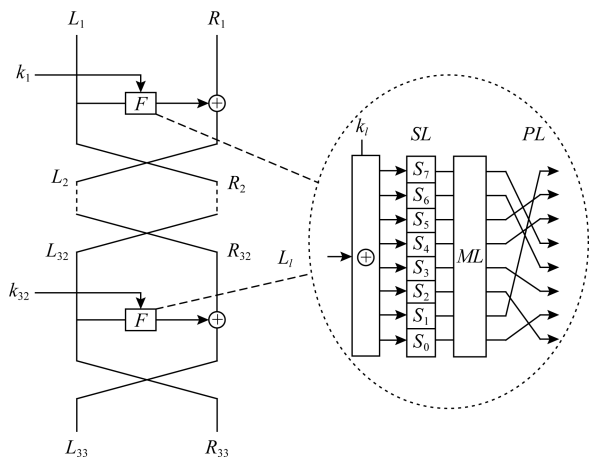


Fig. 1 The structure of MIBS

图 1 MIBS 算法的结构

轮函数 F 由子密钥加、非线性层和线性层组成,表示为

$$L_{l+1}=F(L_l,k_l)\oplus R_l=$$
$$PL(ML(SL(L_l\oplus k_l)))\oplus R_l,$$
$$R_{l+1}=L_l,$$

其中,SL 为非线性层,ML 和 PL 分别为线性层的混淆变换和置换.ML 表达式为

$$L_{l,1}=L_{l,2}\oplus L_{l,3}\oplus L_{l,4}\oplus L_{l,5}\oplus L_{l,6}\oplus L_{l,7},$$
$$L_{l,2}=L_{l,1}\oplus L_{l,3}\oplus L_{l,4}\oplus L_{l,6}\oplus L_{l,7}\oplus L_{l,8},$$
$$L_{l,3}=L_{l,1}\oplus L_{l,2}\oplus L_{l,4}\oplus L_{l,5}\oplus L_{l,7}\oplus L_{l,8},$$
$$L_{l,4}=L_{l,1}\oplus L_{l,2}\oplus L_{l,3}\oplus L_{l,5}\oplus L_{l,6}\oplus L_{l,8},$$
$$L_{l,5}=L_{l,1}\oplus L_{l,2}\oplus L_{l,4}\oplus L_{l,5}\oplus L_{l,6},$$
$$L_{l,6}=L_{l,1}\oplus L_{l,2}\oplus L_{l,3}\oplus L_{l,6}\oplus L_{l,7},$$
$$L_{l,7}=L_{l,2}\oplus L_{l,3}\oplus L_{l,4}\oplus L_{l,7}\oplus L_{l,8},$$
$$L_{l,8}=L_{l,1}\oplus L_{l,3}\oplus L_{l,4}\oplus L_{l,5}\oplus L_{l,8}.$$

MIBS 的加密部分如算法 1 所示.

算法 1. MIBS 密码的加密算法.

输入:明文 X、密钥 K;

输出:密文 Y.

① $L_1\|R_1=X$;
② for $l=1$ to 32
③　$k_l=Keyschedule(K)$;
④ end for
⑤ for $l=1$ to 32
⑥　$L_{l+1}=PL(ML(SL(L_l\oplus k_l)))\oplus R_l$;
⑦　$R_{l+1}=L_l$;
⑧ end for
⑨ $Y=L_{33}\|R_{33}$.

3　唯密文故障分析

3.1　基本假设和故障模型

本文使用的基本假设为唯密文攻击,即攻击者可以利用同一个密钥对多组随机明文进行加密,并在加密过程中导入任意故障,从而获得多组相对应的错误密文.

唯密文故障攻击中常使用的是“与”故障模型,在此基础上,本文构建了双重“与”故障模型,即

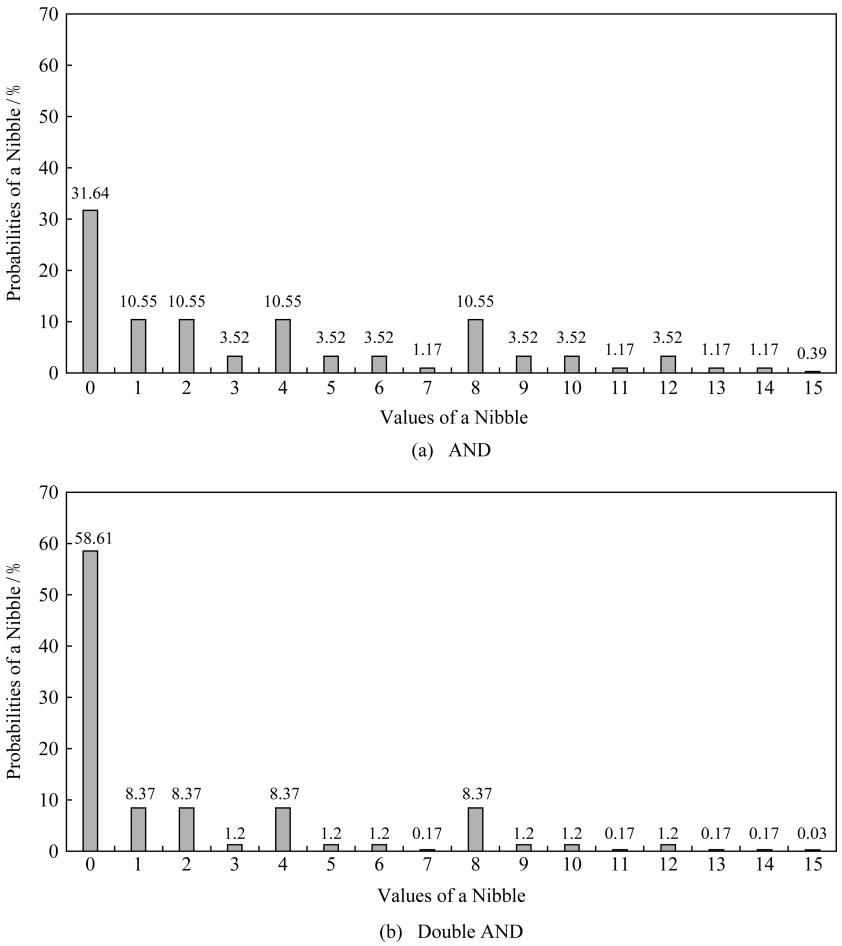


Fig. 2　The distribution of a nibble after fault injections

图 2　半字节被影响后的分布律

$$\begin{cases}\text{“与”}:\tilde{I}=I\wedge e_1,\\ \text{双重“与”}:\tilde{I}=I\wedge e_1\wedge e_2,\end{cases}$$

其中,I 表示加密过程的中间状态值,$\tilde{I}$ 表示导入故障后的错误值,$\wedge$ 表示按位与操作,e_1 和 e_2 是随机未知半字节,其中 $e_1\in[0,15]$,$e_2\in[0,15]$.

图 2 统计了上述故障模型的半字节分布,图 2(b)双重“与”模型中的半字节分布比图 2(a)“与”模型中的半字节分布差异更大.

3.2 攻击步骤

针对 MIBS 算法,本文验证了前人提出的 SEI,HW,ML,GF,GF-SEI,GF-MLE 和 MLE-SEI 等区分器,并提出了 2 种新型区分器 Parzen-HW 和 Parzen-HW-MLE 用于唯密文故障分析,均可以破译 MIBS 算法,具体有 3 个步骤.

步骤 1. 攻击者使用主密钥 K 对随机明文进行加密,迭代加密到第 30 轮,在右分组的任意一个半字节单元中导入随机故障,得到错误密文 $\tilde{Y}$,对随机明文重复多次故障导入得到若干错误密文.故障扩散路径和导入故障的位置相关,在不同的位置导入故障可以恢复出密钥的不同的位,本文以故障导入在右分支的第 6 个半字节为例,故障扩散路径如图 3 所示:

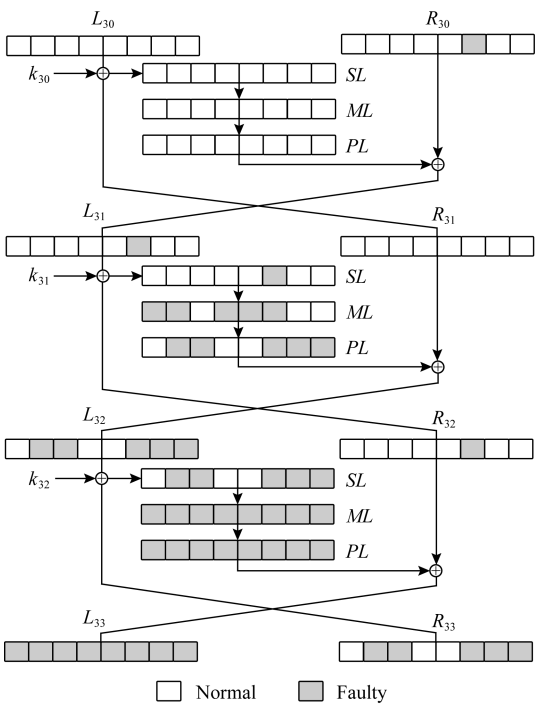


Fig. 3 Faulty diffusion path in the last three rounds

图 3 最后 3 轮的故障扩散路径

步骤 2. 攻击者通过逆向运算,推导出导入故障的中间状态、错误密文和子密钥之间的关系式,通过穷举部分子密钥,得到一组中间状态的猜测值,使用区分器对中间状态的分布进行统计分析,推导出最后一轮的正确子密钥.由 MIBS 密码的操作可知,在 R_{30} 处的故障并未直接影响子密钥 k_{30},且 $R_{32}=L_{31}$,故只需利用 R_{32} 与 $\tilde{Y}$ 和 k_{32} 之间的关系式得到猜测值 $\hat{R}_{32}$,然后对其进行统计区分从而恢复 k_{32},即:

$$\hat{R}_{32}=PL(ML(SL(\tilde{R}_{33}\oplus k_{32})))\oplus\tilde{L}_{33}.$$

通过中间状态、子密钥和错误密文之间的关系式可以求出 k_{32} 的第 1,2,4,5,6 个半字节的值,由此可推出 R_{32} 与 k_{32} 的 20 位相关,依次可以求解 k_{32} 的 20 个位.同步骤 1,在第 7 个半字节导入故障,即可求得 k_{32} 剩余 12 个位.

步骤 3. 与步骤 2 类似,可以推出最后 3 轮所有子密钥,通过密钥编排方案即可恢复出主密钥.

3.3 区分器介绍

本文使用了 9 种区分器对 MIBS 密码进行分析,其中最后 2 种是本文所提出的新型区分器.

1) 平方欧氏距离区分器

平方欧氏距离(square Euclidean imbalance, SEI)区分器[22]是通过计算样本值与理论值之间的距离来估计密钥候选值为正确密钥的可能性.理论上每一个中间状态的取值都处于均匀分布,只有当候选密钥为正确的子密钥时,中间状态值会偏离均匀分布,当 $SEI(\hat{k}_l)$ 取最大值时,所对应的密钥猜测值为正确的子密钥:

$$SEI(\hat{k}_l)=\sum_{r=0}^{15}\left(\frac{\#\{i\mid\hat{R}^i_{l,j}=r\}}{N}-\frac{1}{16}\right)^2,$$

其中,$\hat{k}_l$ 为第 l 轮子密钥的猜测值,$R^i_{l,j}$ 为第 i 组密文右分支的第 j 个字节,$\hat{R}^i_{l,j}$ 为 $R^i_{l,j}$ 的猜测值,N 为故障注入的总数,$\#\{i\mid\hat{R}^i_{l,j}=r\}$ 表示中间状态的猜测值取值为 r 出现的次数.

2) 拟合优度区分器

拟合优度(goodness of fit, GF)区分器[23]是在已知样本分布率的情况下,通过计算一组样本与给定分布的拟合程度,从而找出正确的子密钥.图 2 给出了“与”、双重“与”故障模型下的理论分布.样本与已知分布率的拟合相似度越大,即误差越小,所对应的密钥候选值为正确子密钥的可能性越大,因此当 GF 取值最小时,所对应的密钥猜测值为正确子密钥:

$$GF(\hat{k}_l)=\sum_{r=0}^{15}\frac{(\#\{i\mid\hat{R}^i_{l,j}=r\}-\#\{i\mid\overline{R}^i_{l,j}=r\})^2}{\#\{i\mid\overline{R}^i_{l,j}=r\}},$$

其中,$\#\{i|\hat{R}^i_{l,j}=r\}$表示中间状态的猜测值为 r 出现的次数,$\#\{i|\overline{R}^i_{l,j}=r\}$表示在检验假设的条件下每个中间状态理论值为 r 的个数.

3) 汉明重量区分器

汉明重量(Hamming weight, HW)区分器[22]是计算中间状态和等长非零字符串的汉明距离,导入故障后会打破中间状态 0,1 的平衡,

$$HW(\hat{k}_l)=\frac{1}{N}\sum_{i=1}^{N}hw(\hat{R}^i_{l,j}),$$

其中,N 为故障注入的总数,$hw(\hat{R}^i_{l,j})$表示中间状态的汉明重量.当汉明重量取值最小时,该组样本对应的密钥为正确子密钥.

4) 极大似然估计区分器

极大似然估计(maximum likelihood estimate, MLE)区分器[22]是通过利用观察到的样本信息,反推最具有可能出现此样本结果的模型参数值.通过建立似然函数,计算每一组中间状态理论应该出现概率的乘积:

$$MLE(\hat{k}_l)=\prod_{i=1}^{N}p(\widetilde{R}^i_{l,j}=\hat{R}^i_{l,j}),$$

其中,$\widetilde{R}^i_{l,j}$表示第 i 组错误密文的第 j 个字节的错误中间状态,$p(\widetilde{R}^i_{l,j}=\hat{R}^i_{l,j})$表示每一个错误中间状态的取值对应的理论概率.当使 MLE 取值最大时,所属样本对应的密钥候选值即为正确的子密钥.

5) 拟合优度——平方欧氏距离区分器

拟合优度——平方欧氏距离(GF-SEI)区分器[23]先利用拟合优度算法过滤一部分明显不符合理论分布的样本所对应的密钥候选值,再利用平方欧氏距离进一步计算选择出最优的样本.该区分器的使用可以提高攻击效率,减少需要的故障注入数:

$$GF(\hat{k}_l)\leqslant\chi^2_\alpha,$$

其中,χ^2_α 表示精度为 α 的 χ^2_α 分布上侧分位数表中查询的临界值,α 的精度可以适当调整.当 $GF(\hat{k}_l)\geqslant\chi^2_\alpha$ 时,该密钥猜测值对应的中间状态不符合已知分布,因此该密钥猜测值将被筛选掉,接着使用 $SEI(\hat{k}_l)$继续过滤剩下的密钥候选值,当密钥候选值 $\hat{k}_r$ 使得 $GF(\hat{k}_l)$取最小值且 $SEI(\hat{k}_l)$取最大值时,该密钥猜测值即为正确的子密钥.

6) 拟合优度—极大似然估计区分器

拟合优度—极大似然估计(GF-MLE)区分器[24]先利用 GF 区分器挑选出与理论分布最接近的部分密钥候选值,再使用 MLE 区分器计算挑选出来的样本对应的概率,达到减少故障注入数和提高攻击效率的目的:

$$GF(\hat{k}_l)\leqslant\chi^2_\alpha.$$

当 $GF(\hat{k}_l)\geqslant\chi^2_\alpha$ 时,该密钥猜测值对应的中间状态不符合已知分布,因此该密钥猜测值被剔除,然后,当 $MLE(\hat{k}_l)$达到最大值时,所对应的密钥猜测值即为正确的子密钥.

7) 极大似然估计—平方欧氏距离区分器

极大似然估计—平方欧氏距离(MLE-SEI)区分器[24]先利用 MLE 区分器筛选出密钥候选值,再计算出这些值对应样本的平方欧氏距离,从而达到减少故障注入数:

$$MLE(\hat{k}_l)\geqslant\theta,$$

其中,θ 表示给定的一个概率标准.当 $SEI(\hat{k}_l)$达到最大值时,所对应密钥猜测值即为正确的子密钥.

8) 窗估计—汉明重量区分器

窗估计—汉明重量(Parzen-HW)区分器是本文提出的一种新型双重复合区分器.Parzen 窗估计是一种无参估计,由于 Parzen 区分器不需要假设数据分布,所以具有通用性的优点,但是要准确地估计窗函数需要大量的样本,因此使用 Parzen 区分器理论上需要更多的故障注入.通过结合 HW 区分器可以有效地避免上述问题,具体方法为先利用 Parzen 方法过滤大部分密钥候选值,然后再使用 HW 方法作精确筛选:

$$Parzen(\hat{k}_l)=\frac{1}{N}\sum_{i=1}^{N}f(u),$$

$$u=\frac{\overline{R}^i_{l,j}-\hat{R}^i_{l,j}}{h},$$

其中,$f(u)$为概率密度函数,表示以 $\overline{R}^i_{l,j}$ 为中心长度为 h 的区域内的样本数,N 为故障注入总数.当 $HW(\hat{k}_l)$达到最小值时,对应的密钥候选值即为正确的子密钥.

9) 窗估计—汉明重量—极大似然估计区分器

现有的区分器均为单区分器和双重区分器,本文提出的窗估计—汉明重量—极大似然估计(Parzen-HW-MLE)区分器是一种新型的三重区分器,有效地发挥了 3 种单区分器的优点,进一步提高了攻击效率,减少故障注入数.首先,攻击者构造窗函数,使用 Parzen 过滤大量密钥候选值

$$Parzen(\hat{k}_l)=\frac{1}{N}\sum_{i=1}^{N}f(u),$$

$$u=\frac{\bar{R}^{i}_{l,j}-\hat{R}^{i}_{l,j}}{h},$$

然后,结合汉明重量区分器进一步筛选:

$$HW(\hat{k}_l)\leqslant\mu,$$

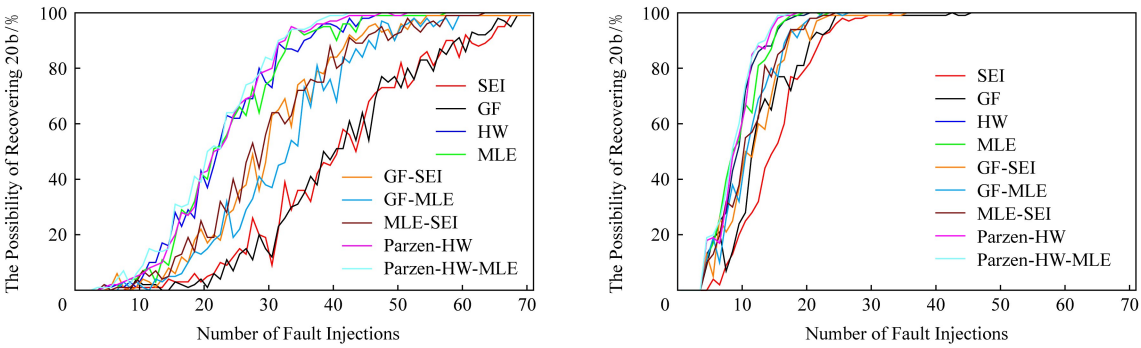
其中,μ 代表一个标准值,当 $HW(\hat{k}_l)\leqslant\mu$ 时,会筛选掉较多密钥候选值;最后,攻击者利用 MLE 区分器进一步筛选剩余的候选密钥值,当 MLE 取最大值时,所对应的密钥候选值为正确的子密钥.

4 唯密文故障破译 MIBS 密码的实验分析

实验使用的 PC 配置为 Intel Core I5-4200M,实验平台为 Eclipse.使用 Java 编程语言软件模拟攻击环境.本文共进行了 1 000 次实验,均以超过 99% 的成功概率破译 MIBS-64 版本和 MIBS-80 版本的密钥.附录 A 列出了实验所有数据.

图 4(a)(b)表示在"与"、双重"与"故障模型下,所有区分器恢复子密钥的 20 b 所需要的成功概率和所需故障注入数的关系,其中横坐标表示故障注入数,纵坐标表示攻击成功率.不同颜色表示 SEI, GF, HW, MLE, GF-SEI, GF-MLE, MLE-SEI, Parzen-HW 和 Parzen-HW-MLE 等区分器的变化趋势.最终每一种区分器恢复子密钥的成功概率不小于 99%.因而,在"与"、双重"与"故障模型下,攻击者恢复出最后一轮子密钥最少需要的故障注入为 64 个、24 个,破译主密钥最少需要的故障注入为 192 个、72 个.由表 3 可知,新型区分器 Parzen-HW 和 Parzen-HW-MLE 所需的故障注入数均较少.

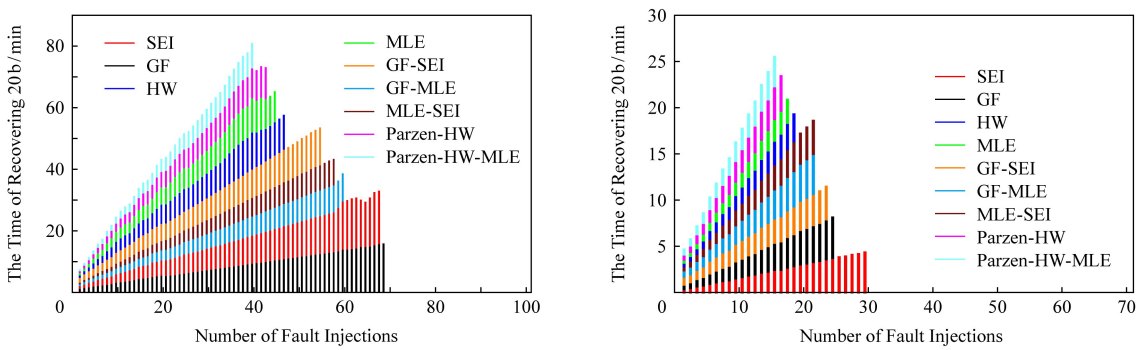
图 5(a)(b)表示在"与"、双重"与"故障模型下,使用所有区分器恢复子密钥 20 b 需要消耗的时间堆积图和故障注入数的关系.其中,横坐标表示故障注入数,纵坐标表示需要消耗的时间堆积,不同颜色线条分别代表各区分器.图 6 表示在相同区分器中,"与"、双重"与"故障模型下恢复出子密钥的平均时间对比图.其中,横坐标表示区分器,纵坐标表示时间,不同色块分别代表各故障模型.由图 5 和图 6 可知,SEI 区分器和 GF 区分器所耗时间最多.和原有的"与"故障模型相比,双重"与"故障模型下各区分器需要的时间都大幅度减少.



(a) AND (b) Double AND

Fig. 4 Comparison of success probability of recovering 20 b in two fault models

图 4 2 种故障模型下恢复出 20 b 的成功率对比



(a) AND (b) Double AND

Fig. 5 Comparison of time of recovering 20 b using two fault models

图 5 2 种不同故障模型下恢复 20 b 所需的时间对比

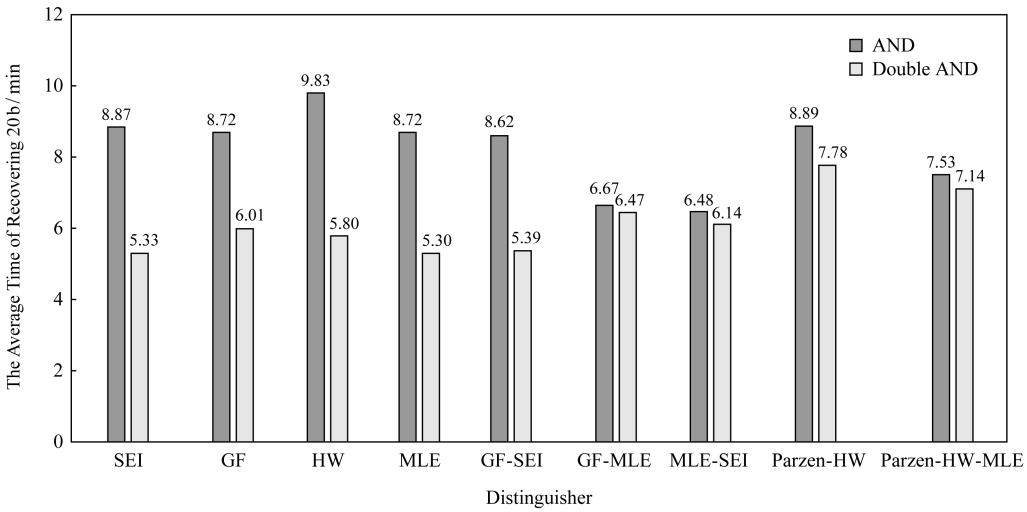


Fig. 6　Comparison of average time of recovering 20 b

图 6　恢复 20 b 所需的平均时间对比

在双重“与”故障模型中,所有区分器可以以较短时间和较少故障注入破译子密钥.并且,双重区分器 Parzen-HW 和三重区分器 Parzen-HW-MLE 在故障注入和时间消耗上均少于原有的区分器,因而,使用新型故障模型和新型区分器有效地提升了提高了故障攻击的效率,降低故障注入数和攻击时间.

5　结束语

本文提出并讨论了 MIBS 密码算法抵抗唯密文故障攻击的安全性.仿真结果表明:以 MIBS 密码为代表的 Feistel 结构密码算法易受到唯密文故障分析的威胁,在新型双重“与”故障模型下,新型 Parzen-HW 二重区分器和 Parzen-HW-MLE 三重区分器可以以较少的故障注入数、较低的时间花费破译 MIBS 密码,该方法的提出优化了唯密文故障攻击方法的效率和性能,为物联网中轻量级密码算法的安全性分析提供了参考.

参　考　文　献

[1] Zamanifar A, Nazemi E. An approach for predicting health status in IoT health care [J]. Journal of Network and Computer Applications, 2014, 134(15): 100-113

[2] García M I, González L F. Collaboration of smart IoT devices exemplified with smart cupboards [J]. IEEE Access, 2019, 7(1): 9881-9892

[3] Muangprathub J, Boonnam N, Kajornkasirat S, et al. IoT and agriculture data analysis for smart farm [J]. Computers and Electronics in Agriculture, 2019, 156(1): 467-474

[4] Gope P, Sikdar B. Lightweight and privacy-preserving two-factor authentication scheme for IoT devices [J]. IEEE Internet of Things Journal, 2019, 6(1): 580-589

[5] Tiburski R T, Moratelli C R, Filho S J, et al. Lightweight security architecture based on embedded virtualization and trust mechanisms for IoT edge devices [J]. IEEE Communications Magazine, 2019, 57(2): 67-73

[6] Lzadi M, Sadeghiyan B, Sadeghian S S, et al. MIBS: A new lightweight block cipher [C] //Proc of the 8th Int Conf on Cryptology and Network Security. Berlin: Springer, 2009: 334-348

[7] Wu Wenling, Zhang Lei. LBlock: A lightweight block cipher [C] //Proc of the 9th Int Conf on Applied Cryptography and Network Security. Berlin: Springer, 2011: 327-344

[8] Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK families of lightweight block ciphers [J]. IACR Cryptology ePrint Archive, 2013, 2013(1): 404-449

[9] Yang Gangqiang, Zhu Bo, Suder V, et al. The simeck family of lightweight block ciphers [C] //Proc of the 17th Int Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2015: 307-329

[10] Duan Danqing, Wei Hongru. Collision attack on MIBS algorithm [J]. Computer Science, 2018, 45(2): 222-225 (in Chinese)
(段丹青, 卫宏儒. 对 MIBS 算法的碰撞攻击[J]. 计算机科学, 2018, 45(2): 222-225)

[11] Yu Xiaoli, Wu Wenlin, Li Yanjun. Integral attack of reduced-round MIBS block cipher [J]. Journal of Computer Research and Development, 2013, 50(10): 2117-2125 (in Chinese)
(于晓丽, 吴文玲, 李艳俊. 低轮 MIBS 分组密码的积分分析[J]. 计算机研究与发展, 2013, 50(10): 2117-2125)

[12] Liu Chao, Liao Fucheng, Wei Hongru. Intermediate encounter attack on MIBS algorithm [J]. Journal of Inner Mongolia University: Natural Science Edition, 2013, 44(3): 308-315 (in Chinese)

(刘超, 廖福成, 卫宏儒. 对 MIBS 算法的中间相遇攻击[J]. 内蒙古大学学报: 自然科学版, 2013, 44(3): 308-315)

[13] Bay A, Nakahara J, Vaudenay S. Cryptanalysis of reduced-round MIBS block cipher [C] //Proc of the 9th Int Conf on Cryptology and Network Security. Berlin: Springer, 2010: 1-19

[14] Cheng Lu, Xu Peng, Wei Yuechuan. New related-key impossible differential attack on MIBS-80 [C] //Proc of the 8th Int Conf on Intelligent Networking and Collaborative Systems. Piscataway, NJ: IEEE, 2016: 203-206

[15] Bay A, Huang Jialin, Vaudenay S. Improved linear cryptanalysis of reduced-round MIBS [C] //Proc of the 9th Int Conf on Advances in Information and Computer Security. Berlin: Springer, 2014: 204-220

[16] Boneh D, Demillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults [C] //Proc of the 16th Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1997: 37-51

[17] Boneh D, Lipton R J. On the importance of eliminating errors in cryptographic computations [J]. Journal of Cryptology, 2001, 14(2): 101-119

[18] Biham E, Shamir A. Differential fault analysis of secret key cryptosystems [C] //Proc of the 17th Annual Int Cryptology Conf on Advances in Cryptology. Berlin: Springer, 1997: 513-525

[19] Wang Suzhen, Zhao Xinjie, Wang Tao, et al. Differential fault attack on block cipher MIBS [J]. Computer Science, 2011, 38(4): 122-124 (in Chinese)
(王素贞, 赵新杰, 王韬, 等. 针对 MIBS 的宽度差分故障分析[J]. 计算机科学, 2011, 38(4): 122-124)

[20] Wang Yongjuan, Zhang Shiyi, Wang Tao, et al. Differential fault attack on block cipher MIBS [J]. Journal of University of Electronic Science and Technology of China, 2018, 47(4): 601-605 (in Chinese)
(王永娟, 张诗怡, 王涛, 等. 对 MIBS 分组密码的差分故障攻击[J]. 电子科技大学学报, 2018, 47(4): 601-605)

[21] Gao Yang, Wang Yongjuan, Yuan Qingjun, et al. Probabilistic analysis of differential fault attack on MIBS [J]. IEICE Transactions on Information & Systems, 2019, 102(2): 299-306

[22] Fuhr T, Jaulmes E, Lomné V, et al. Fault attacks on AES with faulty ciphertexts only [C] //Proc of the 8th Int Workshop on Fault Diagnosis and Tolerance in Cryptography. Piscataway, NJ: IEEE, 2013: 108-118

[23] Li Wei, Ge Chenyu, Gu Dawu, 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 (in Chinese)
(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)

[24] Li Wei, Wu Yixin, Gu Dawu, et al. Ciphertext-only fault analysis of the LBlock lightweight cipher [J]. Journal of Computer Research and Development, 2018, 55(10): 2174-2184 (in Chinese)
(李玮, 吴益鑫, 谷大武, 等. LBlock 轻量级密码算法的唯密文故障分析[J]. 计算机研究与发展, 2018, 55(10): 2174-2184)

Li Wei, born in 1980. PhD, professor and PhD supervisor. Senior member of CCF. Her main research interests include the design and analysis of symmetric ciphers.

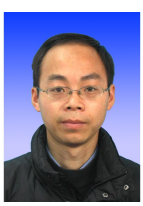
Cao Shan, born in 1995. Master candidate. Her main research interests include security analysis of lightweight ciphers.

Gu Dawu, born in 1970. PhD, professor and PhD supervisor. His main research interests include cryptology and computer security.

Li Jiayao, born in 1996. Master candidate. His main research interests include security analysis of symmetric ciphers.

Wang Menglin, born in 1998. Master candidate. Her main research interests include security analysis of symmetric ciphers.

Cai Tianpei, born in 1996. Master candidate. His main research interests include security analysis of lightweight block ciphers.



Shi Xiujin, born in 1975. PhD, associate professor. His main research interests include security analysis of the Internet of things.

附录 A. 唯密文故障分析 MIBS 密码的实验数据及结果.

明文:随机生成.

MIBS-64 版本主密钥:0123456789ABCDEF.

MIBS-80 版本主密钥:0123456789ABCDEF0123.

结果表明:各区分器均能恢复主密钥,数据如表 A1 和表 A2 所示.

Table A1　Success Probability of Breaking MIBS Using AND/Double AND Fault Model for Different Distinguishers

表 A1　"与"模型/双重"与"模型下不同区分器破译 MIBS 密码的成功率　　%

# Fault Injections	SEI	GF	HW	MLE	GF-SEI	GF-MLE	MLE-SEI	Parzen-HW	Parzen-HW-MLE
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
2	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	1/0
4	0/0	0/9	2/13	0/12	0/13	0/11	2/10	1/18	1/19
5	0/4	0/19	1/17	0/17	1/5	0/19	0/13	2/19	1/20
6	0/2	1/21	2/25	1/26	6/26	0/10	1/20	2/17	4/25
7	0/9	1/7	1/28	3/40	1/21	3/26	1/32	3/31	7/36
8	1/13	0/14	3/43	4/50	0/25	1/38	1/30	4/48	2/51
9	1/20	4/24	1/52	4/54	1/37	3/32	3/38	5/56	6/60
10	1/25	2/28	5/72	7/67	4/50	1/48	7/55	6/66	9/74
11	1/28	2/50	10/81	8/64	3/48	0/59	5/57	8/85	15/84
12	1/32	2/63	10/86	3/81	1/60	4/69	7/62	9/88	14/89
13	1/44	0/69	17/88	11/83	4/58	3/73	4/81	10/87	14/90
14	4/49	0/65	16/88	9/87	8/70	5/80	5/77	16/94	15/95
15	3/53	3/77	28/94	19/95	6/81	5/77	12/85	20/98	31/99
16	3/60	2/77	23/97	29/97	12/83	6/89	13/87	28/99	30/99
17	3/77	1/72	29/98	27/99	10/93	10/94	19/94	27/99	31/100
18	6/76	2/81	26/99	32/99	18/94	14/91	14/94	30/100	41/100
19	3/79	4/81	43/99	42/100	22/96	13/96	25/94	42/100	39/100
20	5/82	1/90	37/100	40/100	17/90	15/98	19/98	43/100	50/100
21	6/87	6/93	45/100	51/100	20/97	18/98	19/98	50/100	52/100
22	10/92	4/92	54/100	52/100	18/98	20/100	32/99	51/100	51/100
23	9/93	11/94	63/100	56/100	27/99	32/100	28/99	55/100	64/100
24	12/96	7/99	62/100	62/100	29/99	19/100	40/100	63/100	64/100
25	15/98	13/99	62/100	66/100	36/99	22/99	32/100	67/100	67/100
26	13/97	15/99	69/100	63/100	38/99	29/100	46/100	69/100	74/100
27	26/98	11/99	69/100	73/100	49/99	33/100	53/100	70/100	75/100
28	20/98	20/99	80/100	64/100	36/99	41/100	44/100	78/100	78/100
29	19/99	15/99	75/100	74/100	46/99	38/100	56/100	79/100	84/100
30	19/99	12/99	73/100	76/100	63/99	37/100	64/100	80/100	83/100
31	22/99	23/99	89/100	82/100	65/99	45/100	64/100	89/100	90/100
32	39/99	26/99	87/100	86/100	69/99	46/100	60/100	90/100	91/100
33	29/100	30/99	87/100	94/100	59/99	54/100	63/100	95/100	94/100

Continued (Table A1) %

# Fault Injections	SEI	GF	HW	MLE	GF-SEI	GF-MLE	MLE-SEI	Parzen-HW	Parzen-HW-MLE
34	36/100	31/99	86/100	94/100	74/99	52/100	72/100	94/100	94/100
35	36/100	35/99	90/100	92/100	76/100	73/100	72/100	93/100	94/100
36	32/100	41/99	91/100	93/100	68/100	66/100	76/100	94/100	95/100
37	42/100	38/99	94/100	94/100	79/100	81/100	75/100	96/100	97/100
38	46/100	50/99	96/100	95/100	78/100	72/100	75/100	96/100	98/100
39	45/100	47/99	96/100	95/100	84/100	76/100	88/100	97/100	99/100
40	49/100	51/99	95/100	90/100	84/100	68/100	80/100	97/100	99/100
41	58/100	51/99	93/100	96/100	87/100	84/100	82/100	98/100	99/100
42	56/100	61/100	98/100	96/100	92/100	82/100	91/100	99/100	100/100
43	50/100	54/99	95/100	93/100	90/100	87/100	89/100	99/100	100/100
44	59/100	64/99	98/100	99/100	92/100	84/100	89/100	99/100	100/100
45	68/100	54/100	98/100	99/100	95/100	90/100	92/100	99/100	100/100
46	71/100	69/100	99/100	99/100	96/100	87/100	93/100	99/100	100/100
47	73/100	77/100	100/100	99/100	93/100	97/100	95/100	100/100	100/100
48	73/100	75/100	100/100	99/100	94/100	96/100	90/100	100/100	100/100
49	73/100	77/100	100/100	99/100	90/100	90/100	92/100	99/100	100/100
50	82/100	73/100	100/100	99/100	96/100	95/100	93/100	99/100	100/100
51	73/100	80/100	100/100	99/100	94/100	96/100	98/100	100/100	100/100
52	76/100	76/100	100/100	99/100	98/100	98/100	95/100	100/100	100/100
53	84/100	83/100	100/100	99/100	96/100	95/100	93/100	100/100	100/100
54	86/100	83/100	100/100	99/100	99/100	98/100	96/100	100/100	100/100
55	81/100	79/100	100/100	99/100	99/100	95/100	97/100	100/100	100/100
56	85/100	87/100	100/100	99/100	99/100	97/100	95/100	100/100	100/100
57	90/100	85/100	100/100	100/100	99/100	98/100	99/100	100/100	100/100
58	90/100	89/100	100/100	100/100	99/100	94/100	99/100	100/100	100/100
59	84/100	91/100	100/100	100/100	99/100	99/100	99/100	100/100	100/100
60	92/100	86/100	100/100	100/100	99/100	99/100	99/100	100/100	100/100
61	89/100	93/100	100/100	100/100	99/100	99/100	99/100	100/100	100/100
62	88/100	92/100	100/100	100/100	99/100	99/100	99/100	100/100	100/100
63	89/100	92/100	100/100	100/100	99/100	100/100	100/100	100/100	100/100
64	91/100	94/100	100/100	100/100	99/100	100/100	100/100	100/100	100/100
65	95/100	98/100	100/100	100/100	99/100	100/100	100/100	100/100	100/100
66	95/100	97/100	100/100	100/100	99/100	100/100	100/100	100/100	100/100
67	99/100	95/100	100/100	100/100	99/100	100/100	100/100	100/100	100/100
68	99/100	99/100	100/100	100/100	99/100	100/100	100/100	100/100	100/100
69	99/100	99/100	100/100	100/100	99/100	100/100	100/100	100/100	100/100
70	99/100	99/100	100/100	100/100	99/100	100/100	100/100	100/100	100/100

Table A2　Time in Breaking MIBS Using AND/Double AND Fault Model for Different Distinguishers

表 A2　“与”模型/双重“与”模型下不同区分器破译 MIBS 需要的时间　　min

# Fault Injections	SEI	GF	HW	MLE	GF-SEI	GF-MLE	MLE-SEI	Parzen-HW	Parzen-HW-MLE
0	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00
1	0.86/0.36	1.22/0.50	0.75/0.39	0.70/0.33	1.67/0.86	0.70/0.68	0.41/0.44	0.63/0.55	0.65/0.64
2	1.13/0.49	1.48/0.63	0.99/0.49	0.92/0.44	1.83/0.87	0.87/0.83	0.64/0.65	0.91/0.69	0.80/0.78
3	1.44/0.66	1.78/0.80	1.25/0.61	1.13/0.56	2.08/0.98	0.96/0.98	0.69/0.76	1.23/0.95	0.99/0.95
4	1.60/0.76	1.98/0.92	1.66/0.78	1.57/0.72	2.33/1.15	1.08/1.10	0.84/0.92	1.41/1.17	1.20/1.14
5	1.97/0.95	2.15/1.13	2.07/0.95	1.86/0.86	2.55/1.39	1.24/1.29	0.98/1.05	1.72/1.39	1.40/1.34
6	2.14/1.11	2.37/1.29	2.20/1.11	2.01/1.04	2.67/1.50	1.39/1.47	1.13/1.21	1.91/1.60	1.64/1.53
7	2.34/1.24	2.55/1.43	2.76/1.25	2.54/1.16	3.02/1.67	1.54/1.64	1.28/1.39	2.21/1.85	1.83/1.77
8	2.45/1.32	2.80/1.57	3.22/1.41	2.92/1.31	3.15/1.75	1.70/1.77	1.52/1.53	2.41/2.07	1.97/1.88
9	2.75/1.53	3.24/1.84	3.56/1.56	3.22/1.45	3.58/1.89	1.84/2.01	1.58/1.70	2.64/2.22	2.20/2.09
10	2.97/1.68	3.40/2.00	3.84/1.74	3.55/1.59	3.70/2.03	1.99/2.17	2.71/1.85	2.95/2.45	2.40/2.27
11	3.18/1.85	3.61/2.18	3.96/1.89	3.63/1.74	3.83/2.15	2.15/2.37	2.89/2.04	3.09/2.65	2.60/2.46
12	3.44/1.95	3.80/2.32	3.75/2.06	3.49/1.89	4.00/2.25	2.28/2.52	2.99/2.17	3.35/2.89	2.83/2.68
13	3.65/2.17	4.07/2.56	4.34/2.23	3.99/2.04	4.24/2.41	2.43/2.72	3.17/2.36	3.6/3.17	2.99/2.85
14	4.02/2.27	4.40/2.74	4.67/2.39	4.39/2.20	4.51/2.51	2.56/2.93	3.30/2.51	3.82/3.32	3.23/3.04
15	4.09/2.44	4.62/2.93	4.98/2.55	4.57/2.32	4.71/2.64	3.22/3.14	3.45/2.70	4.06/3.58	3.45/3.24
16	4.19/2.44	4.78/3.09	4.92/2.69	4.50/2.45	4.86/2.73	3.84/3.40	3.58/2.86	4.30/3.82	3.62/3.44
17	4.69/2.70	5.08/3.31	5.12/2.84	4.66/2.59	5.12/2.86	4.02/3.61	3.76/3.01	4.56/3.95	3.80/3.61
18	4.68/2.84	5.35/3.47	5.82/3.01	5.39/2.74	5.35/3.00	4.12/3.82	3.89/3.21	4.79/4.24	4.02/3.81
19	4.90/3.04	5.56/3.72	6.22/3.19	5.66/2.92	5.53/3.16	4.27/3.99	4.05/3.36	5.00/4.27	4.21/3.99
20	5.10/3.14	5.39/3.85	6.19/3.32	5.66/3.04	5.35/3.25	4.44/4.17	4.19/3.52	5.25/4.52	4.45/4.18
21	5.33/3.30	5.57/3.99	6.47/3.49	5.92/3.20	5.50/3.38	4.57/4.30	4.35/3.69	5.48/4.78	4.60/4.35
22	5.56/3.43	5.75/4.09	6.96/3.64	6.43/3.33	5.70/3.51	4.72/4.47	4.47/3.85	5.70/5.05	4.79/4.55
23	5.81/3.61	5.95/4.29	7.20/3.79	6.69/3.48	5.92/3.63	4.87/4.52	4.64/3.95	5.95/5.24	5.00/4.76
24	6.23/3.73	6.18/4.47	7.27/3.96	6.74/3.62	6.08/3.77	5.03/4.84	4.78/4.20	6.18/5.56	5.27/4.97
25	6.27/3.89	6.43/4.62	6.98/4.13	6.47/3.77	6.28/3.91	5.17/4.98	4.94/4.35	6.44/5.76	5.41/5.21
26	6.35/3.99	6.66/4.64	7.27/4.26	6.73/3.91	6.49/4.01	5.33/5.07	5.08/4.54	6.65/5.94	5.61/5.37
27	6.52/4.16	6.85/4.87	7.56/4.45	6.92/4.07	6.70/4.17	5.45/5.29	5.23/4.69	6.95/6.09	5.79/5.54
28	6.76/4.25	7.04/5.00	7.83/4.57	7.19/4.18	6.87/4.28	5.62/5.41	5.41/4.90	7.14/6.38	6.01/5.74
29	6.95/4.42	7.27/5.14	8.04/4.75	7.42/4.36	7.10/4.43	5.72/5.57	5.52/5.06	7.38/6.59	6.21/5.89
30	7.18/4.59	7.48/5.40	8.34/4.92	7.65/4.50	7.31/4.57	5.88/5.74	5.67/5.21	7.61/6.78	6.41/6.13
31	7.41/4.76	7.72/5.52	8.60/5.12	7.91/4.69	7.48/4.77	6.01/5.87	5.81/5.39	7.84/6.75	6.59/6.29
32	7.47/4.76	7.92/5.61	8.79/5.24	8.21/4.80	7.70/4.85	6.20/5.98	5.98/5.56	8.07/7.07	6.80/6.55
33	7.79/4.98	8.08/5.67	9.33/5.39	8.56/4.94	7.88/4.97	6.35/6.15	6.12/5.71	8.30/7.18	7.02/6.68
34	8.02/5.23	8.30/6.01	10.00/5.55	9.28/5.07	8.12/5.14	6.49/6.30	6.28/5.88	8.60/7.39	7.20/6.85
35	8.22/5.28	8.53/5.97	10.63/5.74	9.76/5.24	8.29/5.27	6.64/6.46	6.40/6.15	8.78/7.59	7.38/6.99
36	8.42/5.47	8.74/6.33	11.03/5.84	10.12/5.34	8.51/5.38	6.76/6.69	6.55/6.33	9.01/7.80	7.60/7.26
37	8.62/5.60	8.96/6.32	11.32/6.04	10.50/5.51	8.74/5.51	6.90/6.73	6.70/6.45	9.23/7.94	7.79/7.42
38	8.97/5.71	9.16/6.55	11.16/6.19	10.26/5.65	8.94/5.66	7.08/7.28	6.87/6.69	9.51/9.86	8.01/7.61

Continued (Table A2) min

# Fault Injections	SEI	GF	HW	MLE	GF-SEI	GF-MLE	MLE-SEI	Parzen-HW	Parzen-HW-MLE
39	9.11/5.89	9.40/6.73	12.02/6.40	11.11/5.84	9.17/5.83	7.21/7.13	7.03/6.71	9.75/8.87	8.20/7.82
40	9.30/6.10	9.59/7.07	11.15/6.56	10.29/6.00	9.36/5.99	7.37/7.37	7.17/6.99	9.95/8.63	8.44/8.09
41	9.53/6.17	9.79/6.99	11.27/6.67	10.39/6.10	9.58/6.06	7.44/7.55	7.26/7.14	10.19/8.70	8.59/8.21
42	9.74/6.33	10.03/7.22	10.44/6.83	9.64/6.24	9.81/6.23	7.64/7.74	7.44/7.31	10.41/9.12	8.78/8.43
43	10.01/6.39	10.22/7.37	10.59/6.96	9.75/6.36	9.97/ 6.31	7.73/7.75	7.55/7.46	10.64/9.13	9.01/8.66
44	10.17/6.58	10.48/7.37	10.82/7.13	9.99/6.51	10.20/6.48	7.91/7.99	7.73/7.65	10.89/9.40	9.23/8.77
45	10.39/6.70	10.66/7.50	11.06/7.30	10.13/6.67	10.42/6.61	8.05/8.04	7.86/7.76	11.26/9.57	9.40/9.03
46	10.72/6.83	10.87/7.64	11.28/7.45	10.40/6.80	10.58/6.76	8.21/8.26	8.04/7.97	11.36/9.77	9.66/9.14
47	10.78/6.95	11.13/7.80	11.50/7.63	10.64/6.98	10.82/6.89	8.33/8.55	8.16/8.13	11.58/9.97	9.81/9.30
48	10.99/7.10	11.27/7.88	11.68/7.74	10.86/7.11	11.02/7.01	8.53/8.55	8.35/8.29	11.81/10.26	10.01/9.55
49	11.27/7.27	11.49/8.14	11.93/7.91	11.05/7.24	11.23/7.17	8.61/8.91	8.44/8.47	12.05/10.47	10.20/9.80
50	11.52/7.39	11.74/8.14	12.40/8.09	11.42/7.39	11.47/7.30	8.77/8.87	8.63/8.62	12.28/10.67	10.44/9.94
51	11.69/7.55	11.88/8.38	12.58/8.25	11.62/7.53	11.66/7.45	8.91/9.21	8.75/8.83	12.52/10.81	10.61/10.12
52	11.90/7.64	12.17/8.37	12.82/8.41	11.86/7.67	11.89/7.62	9.09/8.98	8.94/8.92	12.75/11.12	10.78/10.27
53	12.16/7.84	12.34/8.65	13.02/8.55	11.99/7.81	12.10/7.74	9.21/9.42	9.04/9.12	12.98/11.23	11.00/10.57
54	12.28/7.94	12.52/8.65	13.09/8.80	12.13/8.06	12.29/7.93	9.34/9.33	9.18/9.21	13.42/11.48	11.22/10.69
55	12.50/8.05	12.75/8.75	13.34/8.88	12.32/8.10	12.53/8.01	9.51/9.78	9.35/9.45	13.52/11.67	11.41/10.95
56	12.69/8.18	12.98/8.92	13.61/9.05	12.52/8.27	12.74/8.20	9.65/9.61	9.50/9.52	13.89/14.26	11.64/10.99
57	12.90/8.37	13.15/9.08	13.90/9.21	12.79/8.42	12.91/8.33	9.71/9.94	10.60/9.80	13.96/12.03	11.86/11.24
58	14.11/8.46	13.41/9.23	14.08/9.37	13.01/8.58	13.17/8.46	9.88/9.87	10.77/9.82	14.16/12.28	12.00/11.36
59	15.59/8.65	14.00/9.34	14.29/9.51	13.23/8.67	13.72/8.60	10.10/10.28	10.99/10.11	14.37/12.47	12.38/11.52
60	15.99/8.78	14.03/9.89	41.08/9.68	13.54/8.85	13.78/8.72	10.17/10.32	10.06/10.18	14.61/12.72	12.59/11.71
61	16.43/8.88	14.12/9.79	15.11/9.87	14.02/9.03	13.87/8.88	10.33/10.48	10.21/10.42	14.91/13.19	13.09/11.90
62	16.50/9.04	14.36/10.00	14.81/10.00	13.64/9.17	14.08/8.98	10.51/10.63	10.39/10.50	15.13/13.12	12.87/12.13
63	15.33/9.20	14.86/9.93	15.06/10.16	13.92/9.27	14.55/9.18	10.67/10.77	10.54/10.73	15.35/13.35	13.06/12.30
64	14.64/9.20	14.81/10.28	15.25/10.34	14.07/9.42	14.52/9.25	10.75/10.78	10.61/10.83	15.56/13.56	13.19/12.41
65	15.90/9.53	14.97/10.65	15.52/10.50	14.32/9.56	14.69/9.43	10.99/11.07	10.86/10.93	15.81/13.94	13.53/12.70
66	17.23/9.68	15.37/10.58	15.99/10.69	14.64/9.73	15.12/9.57	11.02/11.16	10.93/11.07	16.02/13.81	13.59/12.78
67	17.35/9.81	15.74/10.78	15.98/10.80	14.73/9.84	15.41/9.70	11.20/11.41	11.11/11.33	16.25/14.33	13.80/13.16
68	21.43/10.00	15.96/10.83	16.21/11.02	14.93/10.02	15.52/9.86	11.30/11.40	11.23/11.39	16.49/14.23	14.28/13.26
69	21.37/10.09	16.03/10.89	19.53/11.19	17.92/10.18	15.78/10.02	11.53/11.70	11.45/11.62	16.74/14.73	14.20/13.41
70	20.00/10.20	16.03/10.98	19.91/11.33	18.36/10.30	15.76/10.12	11.58/11.82	11.50/11.81	16.95/14.83	14.38/13.55