轻量级密码算法Piccolo的统计故障分析

李 玮[1),2),3),4)] 李嘉耀[1)] 谷大武[2)] 汪梦林[1)] 蔡天培[1)]

[1)](东华大学计算机科学与技术学院 上海 201620)

[2)](上海交通大学计算机科学与工程系 上海 200240)

[3)](上海交通大学上海市可扩展计算与系统重点实验室 上海 200240)

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

摘 要 Piccolo算法是于2011年CHES会议上提出的一种轻量级分组密码算法,用于物联网环境中保护RFID、传感器、智能卡等电子设备的通信安全.目前国内外安全性分析研究集中在该算法的已知明文攻击和选择明文攻击,在攻击者能力最弱条件下的唯密文攻击尚无相关研究.文中提出了统计故障分析下Piccolo密码的安全性,即在唯密文条件下,使用SEI、HW、ML、GF、MAP、GF-SEI、GF-ML、ML-SEI、ML-MAP、MM-HW及MM-HW-ML等一系列区分器,恢复Piccolo密码的主密钥.实验结果表明,Piccolo算法不能抵御统计故障分析的攻击,文中提出的新型区分器ML-MAP、MM-HW和MM-HW-ML仅需164和262个故障,可以分别恢复出80比特和128比特主密钥,有效地减少了故障数,并提升了攻击效率.该结果为物联网环境中轻量级密码的安全设计与实现提供有价值的参考.

关键词 Piccolo;轻量级密码算法;密码分析;唯密文攻击;统计故障分析

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2021.02104

Statistical Fault Analysis of the Piccolo Lightweight Cryptosystem

LI Wei[1),2),3),4)] LI Jia-Yao[1)] GU Da-Wu[2)] WANG Meng-Lin[1)] CAI Tian-Pei[1)]

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

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

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

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

Abstract With a typical structure of generalized Feistel networks (GFN), the Piccolo lightweight cryptosystem was proposed at the workshop on Cryptographic Hardware and Embedded System (CHES) in 2011. It has a 64-bit block size and flexible 80-bit and 128-bit block sizes, corresponding to 25 and 31 rounds in the encryption and decryption, respectively. The Piccolo lightweight cryptosystem can protect the communication among electronic devices like RFIDs, sensors, and smart cards in the Internet of Things. It is vital and necessary to do security analysis of the Piccolo lightweight cryptosystem. On the circumstance, the attackers can obtain different types of information, including plaintext and ciphertexts, etc. Up to now, the attacking assumptions of the previous security analysis of the Piccolo lightweight cryptosystem focus on the known-plaintext attack (KPA) and the chosen-plaintext attack (CPA), such as the

收稿日期:2020-06-28;在线发布日期:2021-03-02.本课题得到国家自然科学基金项目(61772129,61932014)、国家密码发展基金项目(MMJJ20180101)、上海市自然科学基金(19ZR1402000)、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和中央高校基本科研业务费专项专项资金资助.**李 玮**,博士,教授,中国计算机学会(CCF)会员,主要研究领域为对称密码算法的设计与分析.E-mail:liwei.cs.cn@gmail.com.**李嘉耀**(通信作者),博士生,主要研究领域为分组密码的故障分析.E-mail:gaajiulei@gmail.com.**谷大武**,博士,教授,主要研究领域为密码学与计算机安全.**汪梦林**,硕士生,主要研究领域为轻量级密码的安全性分析.**蔡天培**,硕士生,主要研究领域为分组密码的安全性分析.

differential analysis, the linear analysis, the impossible differential analysis, the boomerang analysis, the meet-in-the-middle analysis, and the zero-correlation linear analysis etc. In the classical attacking scenario, the attackers require some information of the plaintexts. However, in the literature, there is no security analysis of the Piccolo lightweight cryptosystem against the ciphertext-only attack (COA), which is the weakest attacking assumption. In this case, the attackers can only obtain the ciphertexts. Owing to the limitation of hardware and portability in the Internet of Things, the COA attack is easier to implement. This paper proposes the security analysis of Piccolo against the statistical fault analysis (SFA) in the assumption of COA. It investigates the applications of a series of distinguishers of Square Euclidean Imbalance (SEI), Hamming Weight (HW), Maximum Likelihood (ML), Goodness of Fit (GF), Maximum a Posterior (MAP), Goodness of Fit-Square Euclidean Imbalance (GF-SEI), Goodness of Fit-Maximum Likelihood (GF-ML), Maximum Likelihood-Square Euclidean Imbalance (ML-SEI), Maximum Likelihood-Maximum a Posterior (ML-MAP), Method of Moments-Hamming Weight (MM-HW) and Method of Moments-Hamming Weight-Maximum Likelihood (MM-HW-ML). In order to descript the performance of all distinguishers, accuracy, reliability, latency, and complexity are taken into consideration. The accuracy represents the value of root mean squared error (RMSE). The smaller the value of RMSE is, the more accurate the distinguisher is. The reliability stands for the successful rate of the SFA in recovering the subkeys of Piccolo. When the reliability reaches at least 99%, the attackers have a strong capability in most cases. The latency represents the time in recovering the subkeys of Piccolo. The complexity is composed of time complexity, data complexity and memory complexity of the SFA. Both latency and complexity reflect the effectiveness of the distinguishers in practice. The experimental results show that Piccolo cannot resist against the statistical fault analysis. When the reliability reaches at least 99%, the novel proposed distinguishers of ML-MAP, MM-HW and MM-HW-ML can recover the 80-bit and 128-bit secret keys with 164 and 262 faults, respectively. The experiments show that the novel distinguishers have good performance in accuracy, reliability, latency, and complexity. They can be applied to decrease faults and increase efficiency. The results offer valuable references for the designing and implementation of the lightweight cryptosystems in the Internet of Things.

Keywords　piccolo; lightweight cryptosystem; cryptanalysis; ciphertext-only attack; statistical fault analysis

1　引　言

随着物联网的快速发展，射频识别标签(RFID)、传感器、智能卡等电子设备使得智慧物流、智能制造、精准农业、智能医疗、智慧交通等广泛应用于人们衣食住行中. 在开放的网络中，信息的存储、处理和传输不可避免地会遭受截获、篡改和伪造等攻击的威胁. 然而，由于物联网中电子设备计算能力、存储能力和能量的限制，传统密码算法不能有效地保证信息的保密性、完整性和认证性等. 因此，轻量级密码一经提出，即受到国外内研究学者的广泛关注，其设计与分析已受到学术界和工业界的高度重视[1-8].

2011年，Shibutani等学者在国际密码硬件安全顶级会议CHES中提出了Piccolo轻量级密码[2]. 该分组密码算法基于广义Feistel网络的结构，包括Piccolo-80版本和Piccolo-128版本，在硬件实现的芯片面积和能量消耗以及软件实现的代码大小和内存消耗均具有较大优势，并且可以有效地抵御差分攻击、线性攻击、不可能差分攻击、Boomerang攻击以及中间相遇攻击等传统密码分析的攻击[2].

不同于上述传统密码分析方法，故障分析通常利用激光、电磁辐射、篡改软件等手段诱导故障，干扰密码算法正常运行并产生错误输出. 攻击者通过

分析错误密文与正确密文之间的一系列关系，达到恢复密钥，实现快速破译密码的目的. 1997年，Boneh等学者提出故障分析的方法，并破译了RSA公钥密码[9]. 后来，故障分析发展迅速，种类涉及差分故障分析(differential fault analysis，DFA)，代数故障分析(algebraic fault analysis，AFA)、中间相遇故障分析(meet-in-the-middle fault analysis，MFA)和统计故障分析(statistical fault analysis，SFA)等，目前已成为分组密码、流密码和公钥密码安全实现的现实威胁之一[10-13].

在密码分析中，攻击者会根据自身能力的强弱，获得不同量别的信息，譬如明文、密文等. 大多数传统密码分析方法以及一些故障分析方法采用的是已知明文攻击(KPA)和选择明文攻击(CPA)，即攻击者获得当前密钥下的一些明/密文对，或者特定的明文所对应的密文. 然而，在物联网环境中，由于受到硬件设备制造成本和便携性的限制，上述攻击假设难以有效应用. 然而，基于唯密文攻击(COA)的统计故障分析方法对攻击者能力要求最弱，仅需截获密文即可，因此，若该假设下的攻击可以实现，必然对密码算法的安全性造成更大的威胁性. 如何利用唯密文攻击发现轻量级密码的设计与实现漏洞，近年来已成为故障攻击研究的热点和难点.

目前国内外已公开发表的文献中，尚未有Piccolo算法抵御统计故障分析的成果. 本文结合Piccolo算法的结构，提出了基于唯密文攻击的统计故障分析方法，分析了平方欧氏距离(SEI)、汉明重量(HW)、极大似然估计(ML)、拟合优度(GF)、最大后验概率(MAP)、拟合优度—平方欧氏距离(GF-SEI)、拟合优度—极大似然估计(GF-ML)、极大似然估计—平方欧氏距离(ML-SEI)、极大似然估计—最大后验概率(ML-MAP)、矩估计—汉明重量(MM-HW)及矩估计—汉明重量—极大似然估计(MM-HW-ML)等区分器的攻击效果. 结果表明，本文提出的ML-MAP、MM-HW和MM-HW-ML等新型区分器在准确度、可靠度、故障数、耗时和数据复杂度具有优势，有效地提升了攻击效果. 该方法的提出，为物联网中轻量级密码算法的安全设计与实现提供了重要的参考.

2 相关工作

近年来，国内外学者使用多种密码分析方法对Piccolo算法进行安全性分析. 2014年，Azimi等学者利用S盒的特性，使用不可能差分分析对13轮Piccolo-80版本和15轮Piccolo-128版本进行了安全性分析[14]. 2015年，Tolba等学者结合密钥使用筛选技术与6轮区分器，将针对Piccolo-128缩减轮版本的中间相遇分析扩展到17轮[15]. 2016年，Fu等学者提出针对Piccolo-128版本的多维零相关线性分析，利用多维度线性密码分析方法中的统计法来检测所猜测密钥的正确性[16]. 除了上述的传统密码分析方法以外，故障分析也应用于Piccolo算法的安全性分析. 2012年，赵光耀等学者提出了差分故障攻击，通过注入半字节故障，将Piccolo-80版本的主密钥搜索空间降低至2^{22}[17]. 次年，赵新杰等学者利用代数故障分析方法，分别推导出Piccolo-80版本和Piccolo-128版本的主密钥[18]. 表1总结了Piccolo算法的密码分析方法，可以看出，现有研究的基本假设均集中在已知明文攻击和选择明文攻击.

表1 针对Piccolo-80/128算法的安全性分析汇总

分析类型	基本假设	攻击轮数	参考文献
差分分析	CPA	7/7	[2]
线性分析	KPA	8/8	[2]
Boomerang分析	CPA	9/9	[2]
不可能差分分析	CPA	13/15	[14]
中间相遇分析	CPA	14/17	[15]
零相关线性分析	KPA	-/15	[16]
差分故障分析	CPA	25/-	[17]
代数故障分析	CPA	25/31	[18]
统计故障分析	COA	25/31	本文

2013年，Fuhr等学者提出了基于唯密文攻击假设的统计故障分析，并利用SEI、HW和ML区分器以320个随机半字节故障、288个全零半字节故障和224个全零字节故障，成功恢复出AES密码的128比特子密钥[13]. 2016年，Dobraunig等学者在硬件上实现了基于AES密码构造的认证加密算法的统计故障分析[19]. 近年来，Li等学者利用统计故障分析，对LED密码、LBlock密码和MIBS密码进行安全性分析，使用GF、MAP和GF-SEI等多个区分器降低了故障数[20-22]. 表2以AES密码、LED密码、LBlock密码、MIBS密码以及Piccolo密码的子密钥恢复为例，总结了可靠度为99%及以上时，统计故障分析中各区分器的结果对比. 可以看出，新型区分器ML-MAP、MM-HW和MM-HW-ML所需故障数最少.

表2　针对AES、LED、MIBS和Piccolo的统计故障分析结果比较

区分器	算法				
	AES-128[13]	LED-128[20]	LBlock-80[21]	MIBS-80[22]	Piccolo-80/128
SEI	320	280	124	108	—
HW	288	156	—	74	49
ML	224	160	92	70	57
GF	—	240	114	110	72
MAP	—	152	—	—	50
GF-SEI	—	212	70	86	68
GF-ML	—	—	90	92	58
ML-SEI	—	—	58	92	59
ML-MAP	—	—	—	—	48
MM-HW	—	—	—	—	44
MM-HW-ML	—	—	—	—	41

3　Piccolo算法

3.1　符号定义

设e比特的二进制向量集为Z_2^e.

记$X\in(Z_2^4)^{16}$为明文，$Y\in(Z_2^4)^{16}$为密文，r为迭代轮数且$r\in\{25,31\}$，$t_l^j\in(Z_2^4)^4$为第l轮的中间状态的第j个16比特串，$l\in[0,r-1]$，$j\in[0,3]$；

记F、RP以及RP^{-1}分别为轮函数、轮置换及轮置换的逆；

记$K\in(Z_2^4)^{4(n+1)}$为80比特和128比特主密钥，$K=k_0\|k_1\|\cdots\|k_n$且$n\in\{4,7\}$，$rk_i\in(Z_2^4)^4$和$wk_i\in(Z_2^4)^4$分别为轮密钥和白化密钥，con^{80}和con^{128}为两个版本中密钥编排方案的轮常数，且$i\in[0,2r-1]$，$j\in[0,3]$；

记$\mathcal{HW}(\cdot)$为计算二进制串的汉明重量的函数，$\mathcal{P}(\cdot)$为半字节的概率分布函数，$\mathcal{Q}(\cdot)$是先验分布函数；

记f为故障导入次数，u_q、v_q分别为中间状态值q的理论个数、实验个数且$q\in[0,15]$，g_m为密钥的第m个猜测值，$m\in[0,M-1]$且$M\in\{2^4,2^{20}\}$；

记$\tilde{}$和$\hat{}$分别代表元素的理论值和实际值符号，$\oplus$和$\|$分别为比特串的按位异或和级联.

3.2　算法简述

Piccolo算法的分组长度为64比特，密钥长度为80或者128比特，版本分别表示为Piccolo-80和Piccolo-128，如表3所示，对应的迭代轮数r分别为25和31.

表3　各版本的Piccolo算法简介

算法版本	分组长度/bit	密钥长度/bit	迭代轮数/round
Piccolo-80	64	80	25
Piccolo-128	64	128	31

Piccolo算法由加密算法、解密算法和密钥编排组成，如图1所示. 其中，加密算法所使用的轮函数F，由S盒及矩阵M组成. 除了最后一轮，每轮的中间状态需要以字节为单位进行轮置换RP. 解密与加密的区别在于轮密钥和白化密钥的使用顺序，其他相同. Piccolo的结构如算法1所示，密钥编排方案如

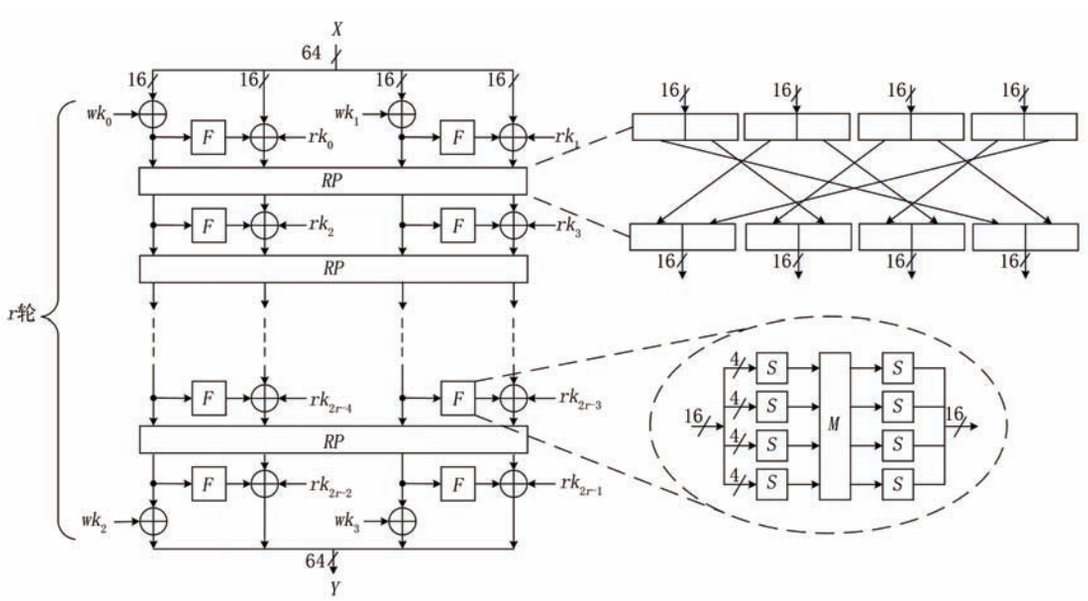

图1　Piccolo算法的结构

算法2和3所示.

算法1. Piccolo-80/128的加密.

输入： $X, rk_0, rk_1, \cdots, rk_{2r-1}, wk_0, wk_1, wk_2, wk_3$.

输出： Y.

1. $t_0^0 \| t_0^1 \| t_0^2 \| t_0^3 \leftarrow X$;
2. $t_0^0 \leftarrow t_0^0 \oplus wk_0$;
3. $t_0^2 \leftarrow t_0^2 \oplus wk_1$;
4. FOR $l \leftarrow 0$ TO $r-1$ DO
5. $t_l^1 \leftarrow t_l^1 \oplus F(t_l^0) \oplus rk_{2l}$;
6. $t_l^3 \leftarrow t_l^3 \oplus F(t_l^2) \oplus rk_{2l+1}$;
7. $t_{l+1}^0 \| t_{l+1}^1 \| t_{l+1}^2 \| t_{l+1}^3 \leftarrow RP(t_l^0 \| t_l^1 \| t_l^2 \| t_l^3)$;
8. END FOR
9. $t_{r-1}^1 \leftarrow t_{r-1}^1 \oplus F(t_{r-1}^0) \oplus rk_{2r-2}$;
10. $t_{r-1}^3 \leftarrow t_{r-1}^3 \oplus F(t_{r-1}^2) \oplus rk_{2r-1}$;
11. $t_{r-1}^0 \leftarrow t_{r-1}^0 \oplus wk_2$;
12. $t_{r-1}^2 \leftarrow t_{r-1}^2 \oplus wk_3$;
13. $Y \leftarrow t_{r-1}^0 \| t_{r-1}^1 \| t_{r-1}^2 \| t_{r-1}^3$;
14. RETURN Y.

算法2. Piccolo-80的密钥编排方案.

输入： $k_0 \| k_1 \| k_2 \| k_3 \| k_4 \leftarrow K$.

输出： $rk_0, rk_1, \cdots, rk_{2r-1}, wk_0, wk_1, wk_2, wk_3$.

1. $wk_0 \leftarrow k_0^L \| k_1^R$;
2. $wk_1 \leftarrow k_1^L \| k_0^R$;
3. $wk_2 \leftarrow k_4^L \| k_3^L$;
4. $wk_3 \leftarrow k_3^L \| k_4^L$;
5. FOR $l \leftarrow 0$ TO $r-1$ DO
6. IF $l \bmod 5 = 0$ or 2 THEN
7. $rk_{2l} \leftarrow con_{2l}^{80} \oplus k_2$;
8. $rk_{2l+1} \leftarrow con_{2l+1}^{80} \oplus k_3$;
9. ELSE IF $l \bmod 5 = 1$ or 4 THEN
10. $rk_{2l} \leftarrow con_{2l}^{80} \oplus k_0$;
11. $rk_{2l+1} \leftarrow con_{2l+1}^{80} \oplus k_1$;
12. ELSE
13. $rk_{2l} \leftarrow con_{2l}^{80} \oplus k_4$;
14. $rk_{2l+1} \leftarrow con_{2l+1}^{80} \oplus k_4$;
15. END IF
16. END FOR
17. RETURN $rk_0, rk_1, \cdots, rk_{2r-1}, wk_0, wk_1, wk_2, wk_3$.

算法3. Piccolo-128的密钥编排方案.

输入： $k_0 \| k_1 \| \cdots \| k_7 \leftarrow K$.

输出： $rk_0, rk_1, \cdots, rk_{2r-1}, wk_0, wk_1, wk_2, wk_3$.

1. $pos \leftarrow \{4, 1, 0, 5, 6, 7, 2, 3\}$;
2. $wk_0 \leftarrow k_0^L \| k_1^R$;
3. $wk_1 \leftarrow k_1^L \| k_0^R$;
4. $wk_2 \leftarrow k_4^L \| k_7^L$;
5. $wk_3 \leftarrow k_7^L \| k_4^R$;
6. FOR $i \leftarrow 0$ TO $2r-1$ DO
7. IF $(i+2) \bmod 8 = 0$ THEN
8. FOR $n \leftarrow 0$ TO 7 DO
9. $k_{pos[n]} \leftarrow k_n$;
10. END IF
11. $rk_i \leftarrow con_i^{128} \oplus k_{(i+2) \bmod 8}$;
12. END IF
13. END FOR
14. RETURN $rk_0, rk_1, \cdots, rk_{2r-1}, wk_0, wk_1, wk_2, wk_3$.

4 统计故障分析

4.1 基本假设和故障模型

统计故障分析采用的基本假设是唯密文攻击，即攻击者除了所截获的密文，没有其它可利用的信息. 与已知明文攻击、选择明文攻击相比，唯密文攻击的攻击者分析能力最弱，若密码算法在唯密文攻击假设下是不安全的，则在其它攻击假设下也一定是不安全的.

根据Piccolo算法的数据单元，本文采用了随机半字节故障模型. 攻击者在监听通信信道时，在密码运行过程中随机导入半字节故障，以按位“与”操作的方式使得故障导入位置的值的分布发生偏离，由原来的均匀分布变成非均匀分布，如图2所示.

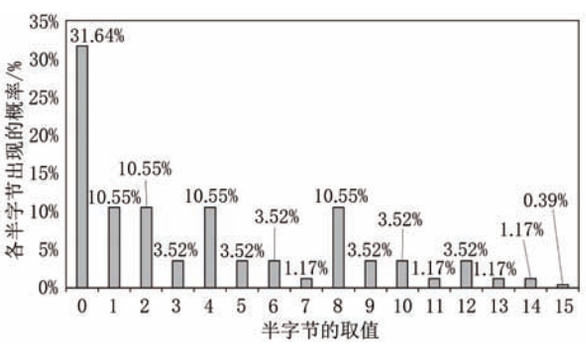

图2 按位“与”后的半字节值分布

4.2 攻击步骤

统计故障分析Piccolo算法包括以下四个步骤：

步骤一. 故障导入. 攻击者使用同一主密钥加密随机明文，并在运行过程中注入半字节故障，获取错误密文. 图3以故障注入在倒数第二轮为例，给出了故障位置在 t_{r-2}^0 首个半字节时的传播路径.

步骤二. 恢复白化密钥和轮密钥. 攻击者将错误密文和密钥候选值进行解密操作，计算出故障导入位置的中间状态值. 此时，$\hat{t}_{r-2}^0$ 或 $\hat{t}_{r-2}^2$ 的推导如下：

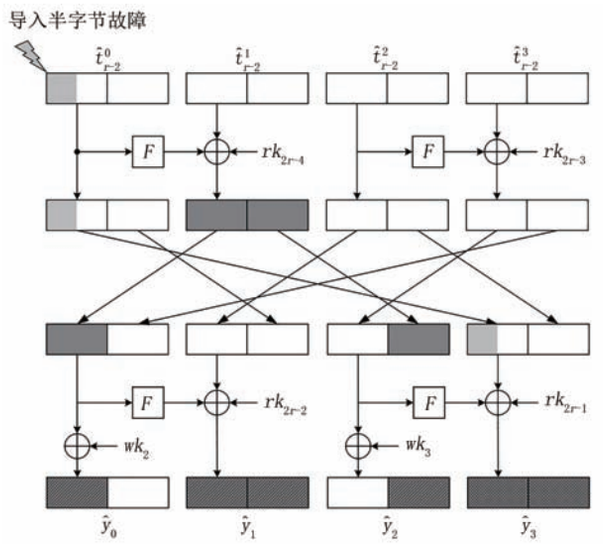

图3　Piccolo−80/128算法的故障传播路径

$$\hat{y}_0\|\hat{y}_1\|\hat{y}_2\|\hat{y}_3=\hat{Y},$$
$$\hat{t}^0_{r-2}=RP^{-1}(\hat{t}^3_{r-1})$$
$$=RP^{-1}(F(\hat{y}_2\oplus wk_3)\oplus rk_{2r-1}\oplus\hat{y}_3),$$
$$\hat{t}^2_{r-2}=RP^{-1}(\hat{t}^1_{r-1})$$
$$=RP^{-1}(F(\hat{y}_0\oplus wk_2)\oplus rk_{2r-2}\oplus\hat{y}_1).$$

攻击者选用4.3节中区分器，计算中间状态值的区分器最大(小)值，该值对应的即为正确密钥. 利用$\hat{t}^0_{r-2}$、$\hat{t}^2_{r-2}$可以分别恢复wk_3和4比特rk_{2r-1}，或wk_2和4比特rk_{2r-2}. 通过多次故障注入，可以完整恢复rk_{2r-1}和rk_{2r-2}.

步骤三. 恢复主密钥. 攻击者利用wk_2、wk_3、rk_{2r-1}和rk_{2r-2}解密最后一轮，获得倒数第二轮的输出，再将故障注入到倒数第三轮，同理可恢复出倒数第二轮的轮密钥rk_{2r-3}和rk_{2r-4}，$r\in\{25,31\}$. 依次类推，直至恢复出Piccolo算法的主密钥. 根据密钥编排方案，攻击者需恢复出wk_3、wk_2、rk_{49}、rk_{48}及rk_{44}，即可计算出Piccolo-80版本的主密钥如下：

$$K=(rk_{48}\oplus con^{80}_{48})\|(rk_{48}\oplus con^{80}_{48})\|(rk_{48}\oplus con^{80}_{48})$$
$$\|\,wk^L_3\|\,wk^R_2\|\,wk^L_2\|\,wk^R_3.$$

同理，攻击者需恢复出wk_3、wk_2、rk_{61}、rk_{60}、rk_{59}、rk_{58}、rk_{56}和rk_{55}，可推导出Piccolo-128版本的主密钥，如下所示：

$$K=(rk_{56}\oplus con^{128}_{56})\|(rk_{55}\oplus con^{128}_{55})\|(rk_{60}\oplus con^{128}_{60})$$
$$\|(rk_{59}\oplus con^{128}_{59})\|(wk^L_2\|\,wk^R_3)\|(rk_{61}\oplus con^{128}_{61})$$
$$\|(rk_{58}\oplus con^{128}_{58})\|(wk^L_3\|\,wk^R_2).$$

4.3　区分器

攻击者采用以下11个区分器对Piccolo算法进行统计故障分析，其中Fuhr等学者提出了SEI、HW和ML区分器[13]，Li等学者提出了GF、MAP、GF-SEI、GF-ML和ML-SEI区分器[20-22]，本节提出了新型区分器ML-MAP、MM-HW和MM-HW-ML.

4.3.1　已有区分器

(1) SEI区分器

SEI区分器用于测量实际分布与均匀分布之间距离，由Fuhr等学者提出并应用在AES算法的统计故障分析中[13]. 若密钥候选值对应的中间状态的SEI值最大，表示当前密钥候选值为正确密钥. SEI区分器表示为：

$$\mathrm{SEI}=\sum_{q=0}^{15}\left(\frac{v_q}{f}-\frac{1}{16}\right).$$

(2) HW区分器

HW区分器用于计算二进制串与同等长度的全零串之间的差异，二进制串的汉明重量被定义为该串中“1”的个数[13]. 若密钥候选值对应的中间状态的汉明重量最小，则此候选值即为正确密钥. HW区分器表示为：

$$\mathrm{HW}=\frac{1}{f}\sum_{q=0}^{15}(\mathcal{HW}(q)\cdot v_q).$$

(3) ML区分器

ML区分器是一种利用已知分布律推导参数的方法[13]. 在导入故障后，该位置的半字节分布律如图2所示. 对于所有的密钥候选值，攻击者挑选出区分器值最大的一组中间状态，其对应的密钥候选值为正确密钥的概率最大. ML区分器定义为：

$$\mathrm{ML}=\prod_{q=0}^{15}\mathcal{P}(q)^{v_q}.$$

(4) GF区分器

GF区分器用于比较实际分布与理论分布的拟合优度，应用于LED算法的统计故障分析中[20]. 若拟合优度越小，说明两个分布差异越小. 当GF值最小时，对应的密钥候选值为正确密钥. GF区分器表示为：

$$\mathrm{GF}=\sum_{q=0}^{15}\frac{(u_q-v_q)^2}{u_q}.$$

(5) MAP区分器

MAP区分器是贝叶斯统计模型的一种应用，它的先验假设为如图2所示的按位“与”故障模型的概率分布函数[20]. 攻击者计算每一组中间状态的MAP值，其中最大值所对应的密钥候选值，即为正确密钥. MAP区分器定义为：

$$\mathrm{MAP}=\frac{(\tilde{t}^0_{r-2}|g_m)\cdot\mathcal{Q}(g_m)}{\sum_{m=0}^{M-1}(\tilde{t}^0_{r-2}|g_m)\cdot\mathcal{Q}(g_m)},$$

其中，以$\hat{t}^0_{r-2}$为例，$(\tilde{t}^0_{r-2}|g_m)$是以g_m为条件的$\tilde{t}^0_{r-2}$的概率分布函数.

(6) GF-SEI区分器

GF-SEI区分器结合两个单区分器GF与SEI的优势，旨在提高统计故障攻击LED算法的攻击效率[20]. 首先，攻击者利用GF区分器筛除与理论分布相差较大的样本，即拟合优度较大的中间状态，满足：

$$\mathrm{GF}=\sum_{q=0}^{15}\frac{(u_q-v_q)^2}{u_q},$$

接着，攻击者在剩余样本中，利用SEI区分器计算并比较，得到SEI值最大的中间状态，满足：

$$\mathrm{SEI}=\sum_{q=0}^{15}\left(\frac{v_q}{f}-\frac{1}{16}\right),$$

这组中间状态所对应的密钥候选值，即为正确密钥.

(7) GF-ML区分器

GF-ML区分器是结合GF区分器和ML区分器结合的二重区分器[21]. 攻击者通过利用GF区分器筛除拟合优度较大的中间状态，满足：

$$\mathrm{GF}=\sum_{q=0}^{15}\frac{(u_q-v_q)^2}{u_q}.$$

然后，攻击者使用ML区分器计算出ML值最大的一组中间状态，满足：

$$\mathrm{ML}=\prod_{q=0}^{15}\mathcal{P}(q)^{v_q},$$

这组中间状态所对应的密钥候选值，即为正确密钥.

(8) ML-SEI区分器

ML-SEI区分器将ML区分器和SEI区分器充分结合[21]，先利用ML区分器筛除极大似然估计值较小的中间状态，满足：

$$\mathrm{ML}=\prod_{q=0}^{15}\mathcal{P}(q)^{v_q},$$

再用SEI区分器计算剩余各组中间状态的SEI值，并挑选出最大值的一组中间状态，满足：

$$\mathrm{SEI}=\sum_{q=0}^{15}\left(\frac{v_q}{f}-\frac{1}{16}\right),$$

这组中间状态所对应的密钥候选值，即为正确密钥.

4.3.2 新型区分器

(1) ML-MAP区分器

ML-MAP区分器是结合ML单区分器和MAP单区分器的双重区分器，用于降低攻击所需的故障数. 首先，攻击者使用ML区分器筛除区分器值较小的密钥候选值，满足：

$$\mathrm{ML}=\prod_{q=0}^{15}\mathcal{P}(q)^{v_q},$$

再利用MAP区分器，筛选出具有MAP最大值的一组中间状态，满足：

$$\mathrm{MAP}=\frac{(\tilde{t}^0_{r-2}|g_m)\cdot\mathcal{Q}(g_m)}{\sum_{m=0}^{M-1}(\tilde{t}^0_{r-2}|g_m)\cdot\mathcal{Q}(g_m)}.$$

此时，该中间状态对应的密钥，为正确密钥. 由图2可知，值较小的半字节出现概率较高. 当一组中间状态的ML或MAP值越大，表明这组中间状态值小的半字节比例越大，与图2的分布越接近，那么所对应的密钥候选值越有可能是正确密钥.

(2) MM-HW区分器

MM-HW区分器通过结合MM区分器和HW区分器的优点，旨在提高攻击效率. MM区分器以参数估计中的矩估计作为基础，计算出每组中间状态的一阶矩，排除区分器较大值，满足：

$$\mathrm{MM}=\frac{1}{f}\sum_{q=0}^{15}(q\cdot v_q),$$

再利用HW区分器在剩余值的集合中，挑选出最小值，满足：

$$\mathrm{HW}=\frac{1}{f}\sum_{q=0}^{15}(\mathcal{HW}(q)\cdot v_q).$$

此时，HW区分器的最小值对应的密钥候选值，即为正确密钥. 基于按位“与”操作，半字节中出现‘0’、‘1’的比例为3∶1. 当一组中间状态的汉明重量或者一阶矩越小，则这组中间状态的‘0’和‘1’比例越大，因而与图2的分布越接近，那么所对应的密钥候选值越有可能是正确密钥.

(3) MM-HW-ML区分器

MM-HW-ML区分器是结合了三个单区分器MM、HW和ML的三重区分器. 首先，攻击者利用MM区分器，排除一阶矩较大的密钥候选值，降低密钥的搜索空间，满足：

$$\mathrm{MM}=\frac{1}{f}\sum_{q=0}^{15}(q\cdot v_q),$$

然后，利用HW区分器进一步筛除较大值的密钥候选值，满足：

$$\mathrm{HW}=\frac{1}{f}\sum_{q=0}^{15}(\mathcal{HW}(q)\cdot v_q),$$

最后，使用ML区分器，对剩余的候选值进行筛选、验证，确保唯一恢复密钥，满足：

$$\mathrm{ML}=\prod_{q=0}^{15}\mathcal{P}(q)^{v_q}.$$

在筛选过程中，攻击者选择一阶矩较小的若干组中

间状态，从中再挑选出汉明重量的最小值所对应的一组中间状态，若这组中间状态的汉明重量最小，其所对应的密钥候选值，有可能为正确密钥. 为了验证所筛选密钥的正确性，攻击者利用ML区分器，比较各组中间状态的极大似然估计值，具有最大值的中间状态与图2的分布越接近，所对应的密钥候选值越有可能是正确密钥.

5　软件模拟及分析

本实验采用JAVA语言编程实现产生随机故障的产生，分别破译Piccolo-80版本和Piccolo-128版本，并使用准确度、可靠度、故障数、耗时和复杂度，来衡量不同区分器在统计故障分析中的效果.

5.1　准确度

准确度用于衡量候选密码与正确密钥之间的数量. 本文采用均方根误差(RMSE)来衡量区分器的准确度，定义如下：

$$\mathrm{RMSE}=\sqrt{\frac{1}{N}\sum_{\varepsilon=1}^{N}\left(h(\varepsilon)-1\right)},$$

其中，N表示实验次数，ε为实验序号，$h(\varepsilon)$表示序号为ε的实验所筛选出的候选密钥个数，正确密钥个数为1. 若RMSE的计算值越趋近于0，则表明该区分器的准确度越高. 本软件模拟采用N=1000，图4给出了故障数、RMSE值和各区分器之间的关系图，其中，x轴为故障注入数，y轴表示不同区分器，z轴为RMSE值. 随着故障数的增加，SEI区分器的RMSE值难以逼近0，说明准确度低；其它区分器的RMSE值呈现下降并逼近0的趋势，说明这些区分器恢复密钥的准确度高. 与现有区分器相比，在相同故障数下，区分器MM-HW-ML、MM-HW、GF-SEI和ML-MAP的RMSE值更逼近于0，如附录表A1所示.

5.2　可靠度

可靠度是指各区分器破译密码的成功概率. 图5说明了故障数与主密钥恢复之间的关系，其中x轴表示导入的故障数，y轴为恢复出正确密钥的成功百分比，每条折线表示不同的区分器. 以Piccolo-128版本为例，HW、ML、GF、MAP、GF-SEI、GF-ML、ML-SEI、ML-MAP、MM-HW以及MM-HW-ML区分器分别以364、460、320、435、371、377、403、307、281以及262个故障，可以恢复出正确主密钥，可靠度达到99%及以上；SEI区分器的可靠度最低，最大值为28%，如表4和附录表A2所示. 与现有区分器相比，新型区分器MM-HW-ML、MM-HW和ML-MAP以更少的故障数达到成功率99%及以上.

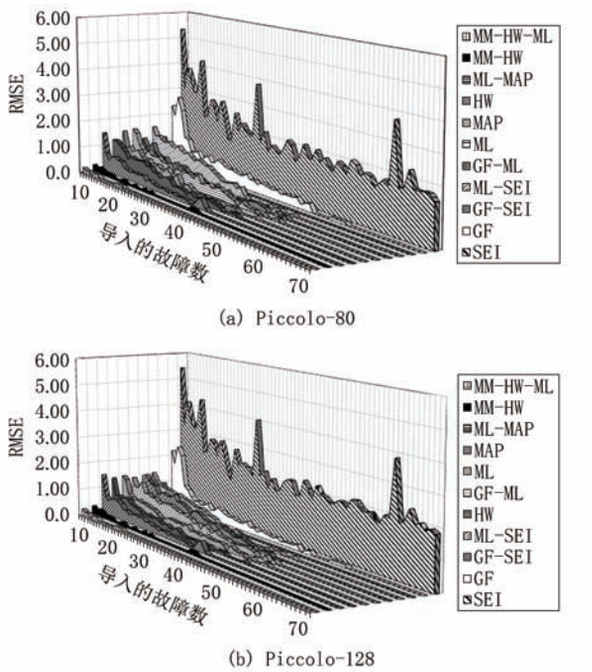

图4　各区分器破译Piccolo密码的准确度

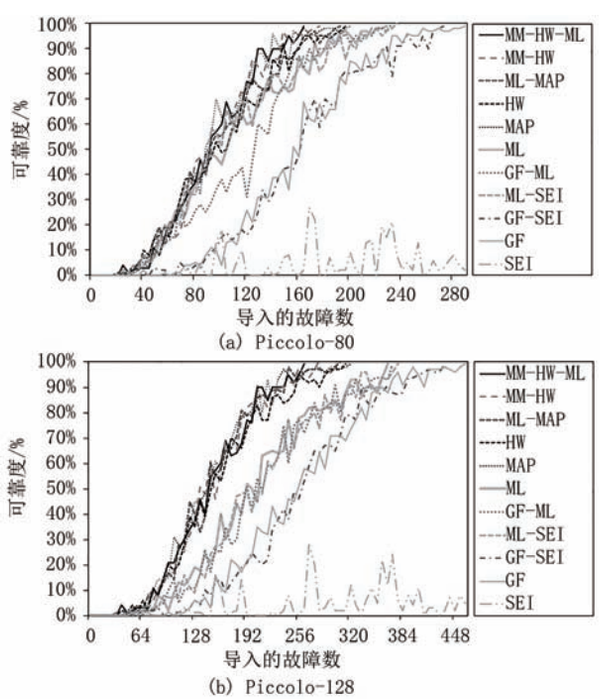

图5　各区分器破译Piccolo密码的可靠度

5.3　故障数

故障数是指区分器破译密码算法所需的故障数量. 在可靠度相同的情况下，故障数越少，表明攻击代价越小. 表4给出了可靠度达到最大值时，

表4 统计故障分析破译Piccolo密码的故障数比较

区分器	算法版本			
	Piccolo-80		Piccolo-128	
	故障数	可靠度	故障数	可靠度
SEI	168	27%	268	28%
HW	196	99%	313	99%
ML	228	99%	364	99%
GF	288	99%	460	99%
MAP	200	99%	320	99%
GF-SEI	272	99%	435	99%
GF-ML	232	99%	371	99%
ML-SEI	236	99%	377	99%
ML-MAP	192	99%	307	99%
MM-HW	176	99%	281	99%
MM-HW-ML	164	99%	262	99%

各区分器恢复Piccolo密码主密钥所需要的故障数.由图5可知,针对Piccolo-80版本和Piccolo-128版本,SEI区分器对应故障数分别为168和268,此时最大可靠度为27%和28%,其它区分器的可靠度均为99%及以上.针对Piccolo算法两个版本,本文提出的MM-HW-ML、MM-HW和ML-MAP区分器所需故障数164和262、192和307、176和281.与现有区分器相比,新型区分器所需故障数均较少.

5.4 耗时

耗时是指区分器在破译密码时所消耗的时间,包含故障导入、计算中间状态和搜索密钥等操作的时间.图6给出了故障导入数与恢复密钥所需的关系,其中,x轴为故障导入数,y轴为区分器在某一故障数的时间堆积.以Piccolo-128算法为例,SEI、HW、ML、MAP、GF、GF-SEI、GF-ML、ML-SEI、ML-MAP、MM-HW及MM-HW-ML区分器分别需要耗时161.90、190.18、327.44、208.70、297.11、270.99、242.09、243.93、248.06、198.37、170.62及170.28分钟,恢复出正确密钥.当可靠度达到99%及以上时,新型区分器MM-HW-ML、MM-HW以及ML-MAP耗时最少,如附录表A3所示.

5.5 复杂度分析

时间、数据和存储复杂度分别表示用于衡量破译密码时所需要的时间量、数据量和存储量.以MM-HW-ML区分器为例,破译Piccolo-80版本和Piccolo-128版本所需时间复杂度分别为

$$51\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1}),$$

和

$$51\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1}).$$

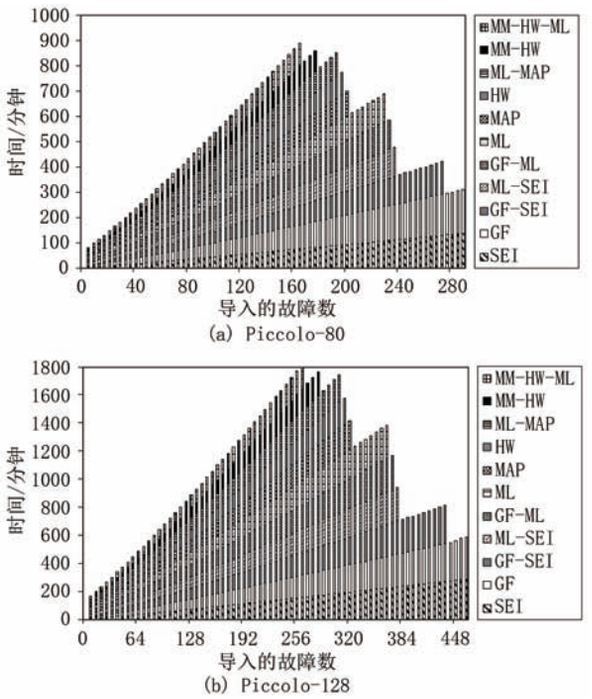

图6 各区分器破译Piccolo-80/128算法的时间堆积

其中,s_1和s_2为各区分器推导的白化密钥和轮密钥比特数,各区分器系数不同,如表5所示.

表5 各区分器破译Piccolo密码的时间复杂度公式

区分器	Piccolo-80	Piccolo-128
SEI	$16\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$16\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
HW	$17\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$17\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
ML	$17\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$17\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
GF	$16\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$16\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
MAP	$18\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$18\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
GF-SEI	$34\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$34\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
GF-ML	$35\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$35\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
ML-SEI	$35\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$35\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
ML-MAP	$37\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$37\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
MM-HW	$34\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$34\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$
MM-HW-ML	$51\cdot f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$	$51\cdot f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1})$

各区分器破译Piccolo-80版本和Piccolo-128版本所需数据复杂度均为

$$f\cdot(2^{s_1+1}+5\cdot 2^{s_2+1})$$

和

$$f\cdot(2^{s_1+1}+11\cdot 2^{s_2+1}),$$

所需的存储复杂度均为

$$768\cdot f+s_1+s_2+2^{32-s_1}+2^{16-s_2}$$

和

$$1536 \cdot f + s_1 + s_2 + 2^{32-s_1} + 2^{16-s_2},$$

其中，s_1和s_2为各区分器推导的白化密钥和轮密钥比特数. 表6总结了可靠度达到最大时，恢复Piccolo密码所需的复杂度. 与现有区分器相比，新型区分器MM-HW-ML、MM-HW以及ML-MAP的时间复杂度排名居中，数据和存储复杂度最少.

表6　各区分器破译Piccolo密码的复杂度总结

区分器	算法版本					
	Piccolo-80			Piccolo-128		
	时间	数据	存储	时间	数据	存储
SEI	$2^{31.31}$	$2^{27.31}$	$2^{16.31}$	$2^{31.31}$	$2^{27.31}$	$2^{16.31}$
HW	$2^{30.70}$	$2^{26.61}$	$2^{16.41}$	$2^{30.70}$	$2^{26.61}$	$2^{16.41}$
ML	$2^{30.92}$	$2^{26.83}$	$2^{16.51}$	$2^{30.92}$	$2^{26.83}$	$2^{16.51}$
GF	$2^{32.17}$	$2^{27.17}$	$2^{16.67}$	$2^{32.17}$	$2^{27.17}$	$2^{16.67}$
MAP	$2^{30.81}$	$2^{26.64}$	$2^{16.42}$	$2^{30.81}$	$2^{26.64}$	$2^{16.42}$
GF-SEI	$2^{32.67}$	$2^{27.09}$	$2^{16.63}$	$2^{32.67}$	$2^{27.09}$	$2^{16.63}$
GF-ML	$2^{32.47}$	$2^{26.86}$	$2^{16.52}$	$2^{32.47}$	$2^{26.86}$	$2^{16.52}$
ML-SEI	$2^{31.93}$	$2^{26.88}$	$2^{16.53}$	$2^{31.93}$	$2^{26.88}$	$2^{16.53}$
ML-MAP	$2^{31.71}$	$2^{26.59}$	$2^{16.39}$	$2^{31.71}$	$2^{26.59}$	$2^{16.39}$
MM-HW	$2^{31.55}$	$2^{26.46}$	$2^{16.34}$	$2^{31.55}$	$2^{26.46}$	$2^{16.34}$
MM-HW-ML	$2^{32.03}$	$2^{26.36}$	$2^{16.30}$	$2^{32.03}$	$2^{26.36}$	$2^{16.30}$

6　结束语

本文针对Piccolo密码抵抗唯密文故障分析的安全性进行了研究，提出了新型区分器MM-HW-ML、MM-HW和ML-MAP，不仅可以降低攻击所需的故障数，而且可以提高攻击效率和效果. 研究表明，Piccolo密码易受到统计故障分析的威胁，在物联网环境中实现时，设计人员需采取必要的有效措施用于抵御统计故障分析的攻击.

参考文献

[1] Izadi M, Sadeghiyan B, Sadeghian S, et al. MIBS: A new lightweight block cipher//Proceedings of the International Conference on Cryptology and Network Security. Kanazawa, Japan: 2009: 334-348

[2] Shibutani K, Isobe T, Hiwatari H, et al. Piccolo: An ultra-lightweight blockcipher//Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems. Nara, Japan: 2011: 342-357

[3] Guo Jian, Peyrin T, Poschmann A, et al. The LED block cipher//Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems. Nara, Japan: 2011: 326-341

[4] Wu Wen-Ling, Zhang Lei. LBlock: A lightweight block cipher//Proceedings of the International Conference on Applied Cryptography and Network Security. Nerja, Spain: 2011: 327-344

[5] Naito Y, Sugawara T. Lightweight authenticated encryption mode of operation for tweakable block ciphers. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019, 2020(1): 66-94

[6] Beaulieu R, Shors D, Smith J, et al. The SIMON and SPECK lightweight block ciphers//Proceedings of the Annual Design Automation Conference. San Francisco, USA: 2015: 1-6

[7] Banik S, Bogdanov A, Isobe T, et al. Midori: A block cipher for low energy//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Auckland, New Zealand: 2015: 411-436

[8] Guo Jian, Peyrin T, Poschmann A. The PHOTON family of lightweight hash functions//Proceedings of the Annual Cryptology Conference. Santa Barbara, USA: 2011: 222-239

[9] Boneh D, DeMillo R, Lipton R. On the Importance of Checking Cryptographic Protocols for Faults//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Konstanz, Germany: 1997: 37-51

[10] Biham E, Shamir A. Differential Fault Analysis of Secret Key Cryptosystems//Proceedings of the Annual International Cryptology Conference. Santa Barbara, USA: 1997: 513-525

[11] Courtois N, Ware D, Jackson K. Fault-algebraic attacks on inner rounds of DES//Proceedings of the Strategies Telecom and Multimedia. Montreuil, France: 2010: 22-24

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

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

[14] Azimi S A, Ahmadian Z, Mohajeri J, et al. Impossible differential cryptanalysis of Piccolo lightweight block cipher//Proceedings of the International Conference on Information Security and Cryptology. Tehran, Iran: 2014: 89-94

[15] Tolba M, Abdelkhalek A, Youssef A. Meet-in-the-middle attacks on reduced round Piccolo//Proceedings of the Lightweight Cryptography for Security and Privacy. Bochum, Germany: 2016, 9542: 3-20

[16] Fu Li-Shi, Jin Chen-Hui, Li Xin-Ran. Multidimensional zero-correlation linear cryptanalysis of lightweight block

cipher Piccolo-128. Security and Communication Networks, 2016, 9(17): 4520-4535

[17] Zhao Guang-Yao, Li Rui-Lin, Sun Bing, et al. Differential fault analysis on Piccolo. Chinese Journal of Computers, 2012, 35(9): 1918-1926(in Chinese)
(赵光耀,李瑞林,孙兵等. Piccolo算法的差分故障分析. 计算机学报, 2012, 35(9): 1918-1926)

[18] Zhao Xin-Jie, Guo Shi-Ze, Wang Tao, et al. Research of algebraic fault analysis on Piccolo. Chinese Journal of Computers, 2013, 36(4): 882-894(in Chinese)
(赵新杰,郭世泽,王韬等. Piccolo密码代数分析研究. 计算机学报, 2013, 36(4): 882-894)

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

[20] Li Wei, Liao Ling-Feng, Gu Da-Wu, et al. Ciphertext-only fault analysis on the LED lightweight cryptosystem in the Internet of Things. IEEE Transactions on Dependable and Secure Computing, 2019, 16(3): 454-461

[21] Li Wei, Wu Yi-Xin, Gu Da-Wu, et al. Ciphertext-only fault analysis of the LBlock lightweight cipher. Journal of Computer Research and Development, 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. 计算机研究与发展, 2018, 55(10): 2174-2184)

[22] Li Wei, Cao Shan, Gu Da-Wu, et al. Ciphertext-only fault analysis of the MIBS lightweight cryptosystem in the Internet of Things. Journal of Computer Research and Development, Journal of Computer Research and Development, 2019, 56(10): 2216-2228(in Chinese)
(李玮,曹珊,谷大武等. 物联网中MIBS轻量级密码的唯密文故障分析. 计算机研究与发展, 2019, 56(10): 2216-2228)

附录A. 实验数据

明文:随机生成

Piccolo-80版本主密钥:0011 2233 4455 6677 8899

Piccolo-128版本主密钥:0011 2233 4455 6677 8899 aabb ccdd eeff

表A1 各区分器恢复Piccolo-80/128算法密钥的RMSE值

故障数	SEI	HW	ML	GF	MAP	GF-SEI	GF-ML	ML-SEI	ML-MAP	MM-HW	MM-HW-ML
1	1024.00/1024.00	256.00/256.00	256.00/256.00	256.00/256.00	256.00/256.00	256.00/256.00	256.00/256.00	256.00/256.00	256.00/256.00	256.00/256.00	256.00/256.00
2	255.49/255.70	63.83/64.04	64.02/63.90	192.17/191.93	63.72/63.60	63.96/63.84	63.79/63.91	64.04/63.92	66.36/66.38	63.84/63.88	64.08/64.12
3	63.71/64.03	15.95/16.09	16.17/15.94	111.14/110.83	16.82/16.59	55.85/55.62	15.73/15.96	16.16/15.93	16.02/16.08	15.98/16.00	16.06/16.08
4	15.41/15.50	3.66/3.78	4.15/4.00	31.10/30.98	3.97/3.82	13.96/13.81	3.72/3.87	4.03/3.88	3.92/3.93	3.69/3.74	3.91/3.96
5	19.68/19.89	2.52/2.73	3.04/2.92	19.20/18.96	2.84/2.72	15.65/15.53	2.77/2.89	2.48/2.36	2.53/2.55	1.49/1.53	1.33/1.37
6	8.55/8.87	1.73/1.87	2.09/1.86	4.96/4.65	1.96/1.73	4.76/4.53	1.68/1.91	2.16/1.93	1.91/1.97	0.60/0.62	0.60/0.62
7	6.04/6.13	1.46/1.58	1.92/1.77	1.74/1.62	1.93/1.78	1.69/1.54	1.81/1.96	2.00/1.85	1.52/1.53	0.37/0.42	0.32/0.37
8	6.20/6.41	1.24/1.45	1.65/1.53	2.08/1.84	1.74/1.62	1.29/1.17	1.54/1.66	1.86/1.74	1.48/1.50	0.29/0.33	0.26/0.30
9	5.40/5.72	1.30/1.44	1.56/1.33	1.83/1.52	1.89/1.66	1.05/0.82	1.17/1.40	1.81/1.58	1.48/1.54	0.22/0.24	0.15/0.17
10	5.32/5.41	1.16/1.28	1.51/1.36	2.30/2.18	1.46/1.31	1.08/0.93	1.10/1.25	1.52/1.37	1.46/1.47	0.25/0.30	0.17/0.22
11	2.99/3.20	1.16/1.37	1.37/1.25	1.94/1.70	0.78/0.66	0.57/0.45	0.82/0.94	1.20/1.08	0.69/0.71	0.06/0.10	0.10/0.14
12	3.81/4.13	1.06/1.20	0.97/0.74	2.70/2.39	0.94/0.71	0.98/0.75	0.70/0.93	1.24/1.01	0.48/0.54	0.24/0.26	0.12/0.14
13	3.38/3.47	0.95/1.07	0.81/0.66	2.21/2.09	0.77/0.62	0.59/0.44	1.04/1.19	1.10/0.95	0.65/0.66	0.17/0.22	0.00/0.00
14	2.96/3.17	0.84/1.05	0.66/0.54	1.18/0.94	0.85/0.73	0.45/0.33	0.70/0.82	1.05/0.93	0.69/0.71	0.10/0.10	0.14/0.14
15	2.97/3.29	0.60/0.74	0.87/0.64	1.14/0.83	0.92/0.69	0.56/0.33	0.61/0.84	1.13/0.90	0.61/0.67	0.14/0.14	0.14/0.14
16	4.23/4.32	0.76/0.88	0.72/0.57	0.72/0.60	0.72/0.57	0.39/0.24	0.60/0.75	1.02/0.87	0.60/0.61	0.10/0.10	0.00/0.00

续表

故障数	SEI	HW	ML	GF	MAP	GF-SEI	GF-ML	ML-SEI	ML-MAP	MM-HW	MM-HW-ML
17	2.14/2.35	0.68/0.89	0.70/0.58	0.72/0.48	0.63/0.51	0.29/0.17	0.65/0.77	0.95/0.83	0.40/0.42	0.00/0.00	0.00/0.00
18	2.10/2.42	0.70/0.84	0.76/0.53	0.81/0.50	0.72/0.49	0.14/0.14	0.43/0.66	1.10/0.87	0.38/0.44	0.00/0.00	0.00/0.00
19	2.82/2.91	0.72/0.84	0.65/0.50	0.53/0.41	0.57/0.42	0.14/0.14	0.45/0.60	0.95/0.80	0.32/0.33	0.10/0.10	0.00/0.00
20	2.59/2.80	0.74/0.95	0.60/0.48	0.66/0.45	0.45/0.33	0.00/0.00	0.58/0.70	0.88/0.76	0.37/0.39	0.10/0.10	0.00/0.00
21	2.04/2.36	0.61/0.75	0.62/0.39	0.76/0.56	0.64/0.41	0.20/0.20	0.47/0.70	0.96/0.73	0.35/0.41	0.00/0.00	0.10/0.10
22	2.86/2.95	0.63/0.75	0.43/0.28	0.55/0.35	0.51/0.36	0.00/0.00	0.56/0.71	0.83/0.68	0.35/0.36	0.00/0.00	0.10/0.10
23	2.26/2.47	0.48/0.69	0.38/0.26	0.59/0.39	0.45/0.33	0.00/0.00	0.51/0.63	0.74/0.62	0.40/0.42	0.10/0.10	0.10/0.10
24	1.52/1.84	0.48/0.62	0.58/0.35	0.73/0.53	0.63/0.40	0.10/0.10	0.37/0.60	0.83/0.60	0.22/0.28	0.00/0.00	0.00/0.00
25	1.48/1.57	0.35/0.47	0.52/0.37	0.67/0.47	0.47/0.32	0.00/0.00	0.38/0.53	0.78/0.63	0.32/0.33	0.00/0.00	0.00/0.00
26	2.56/2.77	0.42/0.63	0.48/0.36	0.57/0.37	0.36/0.24	0.10/0.10	0.45/0.57	0.69/0.57	0.22/0.24	0.10/0.10	0.00/0.00
27	1.92/2.24	0.48/0.62	0.55/0.32	0.53/0.33	0.55/0.32	0.00/0.00	0.27/0.50	0.71/0.48	0.18/0.24	0.00/0.00	0.00/0.00
28	2.25/2.34	0.43/0.55	0.50/0.35	0.54/0.35	0.22/0.22	0.10/0.10	0.32/0.47	0.61/0.46	0.16/0.17	0.10/0.10	0.00/0.00
29	2.01/2.22	0.24/0.45	0.42/0.30	0.50/0.30	0.20/0.20	0.00/0.00	0.23/0.35	0.52/0.40	0.20/0.22	0.00/0.00	0.00/0.00
30	1.94/2.26	0.27/0.41	0.63/0.40	0.46/0.26	0.32/0.32	0.00/0.00	0.17/0.40	0.43/0.20	0.16/0.22	0.00/0.00	0.00/0.00
31	1.88/1.97	0.27/0.39	0.35/0.20	0.46/0.26	0.20/0.20	0.00/0.00	0.07/0.22	0.32/0.17	0.13/0.14	0.00/0.00	0.00/0.00
32	3.84/4.05	0.23/0.44	0.36/0.24	0.58/0.39	0.10/0.10	0.10/0.10	0.33/0.45	0.34/0.22	0.18/0.20	0.00/0.00	0.00/0.00
33	1.76/2.08	0.12/0.26	0.45/0.22	0.41/0.22	0.10/0.10	0.00/0.00	0.10/0.33	0.37/0.14	0.11/0.17	0.00/0.00	0.00/0.00
34	2.17/2.26	0.28/0.40	0.32/0.17	0.43/0.24	0.10/0.10	0.00/0.00	0.07/0.22	0.41/0.26	0.14/0.14	0.00/0.00	0.00/0.00
35	1.49/1.70	0.12/0.33	0.38/0.26	0.33/0.14	0.14/0.14	0.00/0.00	0.25/0.37	0.26/0.14	0.15/0.15	0.00/0.00	0.00/0.00
36	1.76/2.08	0.18/0.32	0.43/0.20	0.43/0.24	0.10/0.10	0.00/0.00	0.01/0.24	0.37/0.14	0.12/0.12	0.00/0.00	0.00/0.00
37	1.59/1.68	0.20/0.20	0.35/0.20	0.38/0.20	0.14/0.14	0.00/0.00	0.07/0.22	0.10/0.10	0.05/0.05	0.00/0.00	0.00/0.00
38	1.53/1.74	0.22/0.22	0.29/0.17	0.36/0.17	0.14/0.14	0.00/0.00	0.10/0.22	0.00/0.00	0.08/0.08	0.00/0.00	0.00/0.00
39	1.76/2.08	0.26/0.26	0.22/0.22	0.32/0.14	0.14/0.14	0.00/0.00	0.10/0.14	0.00/0.00	0.30/0.30	0.00/0.00	0.00/0.00
40	2.13/2.22	0.20/0.20	0.17/0.17	0.38/0.20	0.00/0.00	0.00/0.00	0.02/0.17	0.00/0.00	0.40/0.40	0.14/0.14	0.00/0.00
41	1.99/2.20	0.16/0.16	0.00/0.00	0.28/0.10	0.10/0.10	0.00/0.00	0.17/0.17	0.00/0.00	0.10/0.10	0.10/0.10	0.00/0.00
42	1.44/1.76	0.12/0.12	0.24/0.24	0.32/0.14	0.10/0.10	0.00/0.00	0.20/0.20	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00
43	1.67/1.76	0.00/0.00	0.14/0.14	0.32/0.14	0.10/0.10	0.00/0.00	0.22/0.22	0.10/0.10	0.00/0.00	0.00/0.00	-/-
44	2.14/2.35	0.10/0.10	0.10/0.10	0.31/0.14	0.00/0.00	0.00/0.00	0.17/0.17	0.00/0.00	0.00/0.00	0.00/0.00	-/-
45	1.78/2.10	0.10/0.10	0.10/0.10	0.37/0.20	0.00/0.00	0.00/0.00	0.14/0.14	0.10/0.10	0.00/0.00	-/-	-/-
46	1.70/1.79	0.10/0.10	0.00/0.00	0.17/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.10/0.10	0.00/0.00	-/-	-/-
47	2.08/2.29	0.00/0.00	0.10/0.10	0.27/0.10	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	-/-	-/-
48	1.70/2.02	0.00/0.00	0.00/0.00	0.31/0.14	0.10/0.10	0.00/0.00	0.17/0.17	0.00/0.00	0.00/0.00	-/-	-/-
49	1.88/1.97	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.00/0.00	0.10/0.10	-/-	-/-	-/-
50	1.63/1.84	-/-	0.10/0.10	0.00/0.00	0.00/0.00	0.00/0.00	0.14/0.14	0.00/0.00	-/-	-/-	-/-
51	1.52/1.84	-/-	0.10/0.10	0.00/0.00	-/-	0.00/0.00	0.00/0.00	0.00/0.00	-/-	-/-	-/-
52	1.90/1.99	-/-	0.00/0.00	0.00/0.00	-/-	0.00/0.00	0.00/0.00	0.00/0.00	-/-	-/-	-/-
53	1.78/1.99	-/-	0.00/0.00	0.10/0.10	-/-	0.00/0.00	0.00/0.00	0.00/0.00	-/-	-/-	-/-
54	1.54/1.86	-/-	0.00/0.00	0.10/0.10	-/-	0.00/0.00	0.00/0.00	0.00/0.00	-/-	-/-	-/-
55	2.08/2.17	-/-	0.00/0.00	0.10/0.10	-/-	0.00/0.00	0.00/0.00	0.00/0.00	-/-	-/-	-/-
56	1.97/2.18	-/-	0.00/0.00	0.10/0.10	-/-	0.00/0.00	0.00/0.00	0.00/0.00	-/-	-/-	-/-
57	1.64/1.96	-/-	0.00/0.00	0.00/0.00	-/-	0.00/0.00	0.00/0.00	0.00/0.00	-/-	-/-	-/-
58	1.79/1.88	-/-	-/-	0.00/0.00	-/-	0.00/0.00	0.00/0.00	0.00/0.00	-/-	-/-	-/-
59	1.73/1.94	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-
60	1.41/1.73	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-
61	1.59/1.68	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-

续表

故障数	SEI	HW	ML	GF	MAP	GF-SEI	GF-ML	ML-SEI	ML-MAP	MM-HW	MM-HW-ML
62	1.77/1.98	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-
63	1.62/1.94	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-
64	3.78/3.87	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-
65	1.64/1.85	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-
66	1.67/1.99	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-
67	2.31/2.40	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-
68	1.74/1.95	-/-	-/-	0.00/0.00	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-
69	1.73/2.05	-/-	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-	-/-	-/-
70	1.77/1.86	-/-	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-	-/-	-/-
71	1.75/1.96	-/-	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-	-/-	-/-
72	1.54/1.86	-/-	-/-	0.00/0.00	-/-	-/-	-/-	-/-	-/-	-/-	-/-

表A2 各区分器恢复Piccolo-80/128算法密钥的可靠度(%)

故障数	SEI	HW	ML	GF	MAP	GF-SEI	GF-ML	ML-SEI	ML-MAP	MM-HW	MM-HW-ML
1	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
2	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
3	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
4	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0
5	0/0	0/0	0/0	0/0	0/0	0/0	0/0	0/0	1/0	0/1	0/0
6	0/0	1/2	1/0	0/0	0/4	0/0	2/0	2/0	1/0	1/0	4/4
7	0/0	1/1	1/0	0/0	1/0	1/0	1/1	1/2	1/2	1/0	1/1
8	0/0	4/4	1/0	0/1	2/2	0/0	1/0	4/1	2/0	2/3	2/2
9	0/0	2/1	2/2	0/0	5/1	0/0	3/2	3/1	5/4	4/3	3/3
10	0/0	10/6	4/2	2/1	5/2	1/2	8/3	8/2	7/3	5/0	3/3
11	0/0	8/2	6/2	0/1	3/8	0/2	7/4	5/4	7/7	6/3	3/3
12	0/0	14/10	7/2	0/0	7/10	3/2	8/2	7/3	14/9	7/6	11/11
13	0/0	16/8	13/8	0/0	9/14	2/3	18/4	9/3	19/9	15/10	8/8
14	0/0	19/15	20/6	1/0	16/14	2/0	13/5	13/8	12/13	13/15	15/15
15	0/0	15/20	18/2	0/1	20/15	0/0	14/10	21/7	18/17	17/16	21/21
16	0/0	23/18	25/9	1/0	23/31	0/1	16/14	21/7	22/14	15/17	21/21
17	0/1	30/20	27/13	1/0	29/28	5/1	28/5	20/8	27/28	17/28	26/26
18	2/3	38/28	24/12	4/1	36/25	3/2	19/10	36/16	30/29	25/27	30/30
19	1/2	39/39	31/15	4/3	33/35	2/3	21/11	32/11	41/45	34/32	34/34
20	1/1	37/35	36/19	5/6	41/45	4/6	26/11	32/9	37/40	45/37	37/37
21	5/1	39/45	40/18	4/5	32/45	3/4	28/16	41/17	37/33	47/51	46/46
22	0/0	43/39	47/24	8/7	51/48	7/10	25/26	42/15	48/39	40/48	40/40
23	0/0	47/49	48/21	11/3	56/52	9/8	29/17	58/24	52/60	50/61	55/55
24	13/16	53/56	47/25	10/15	70/61	11/13	34/26	57/27	56/55	53/46	57/57
25	18/10	49/53	44/40	4/11	63/58	15/14	38/25	51/28	55/58	53/57	60/60
26	0/0	50/60	50/30	13/9	65/65	17/9	33/35	66/31	59/65	61/69	69/69
27	0/1	58/70	57/35	14/22	62/69	14/13	39/28	60/37	61/66	64/66	63/63
28	5/2	57/68	62/44	12/20	65/76	16/16	40/30	64/47	59/71	68/65	64/64
29	10/14	69/66	64/40	20/17	72/78	18/19	43/42	69/48	63/81	74/78	68/68
30	0/0	70/74	60/52	26/22	74/79	16/21	31/51	70/49	72/79	75/82	77/77
31	0/0	68/78	61/50	21/23	83/81	19/25	45/42	59/41	78/79	86/84	76/76
32	0/0	67/83	68/45	31/35	88/91	25/22	60/54	71/49	75/86	83/86	90/90

续表

故障数	SEI	HW	ML	GF	MAP	GF-SEI	GF-ML	ML-SEI	ML-MAP	MM-HW	MM-HW-ML
33	0/0	74/77	70/63	31/33	88/80	34/20	58/49	73/48	74/87	79/86	90/90
34	3/0	74/77	78/64	31/32	82/93	29/22	56/59	76/61	73/86	87/82	85/85
35	0/1	86/86	73/65	39/43	96/83	32/34	67/59	80/58	80/89	86/85	90/90
36	1/0	83/87	72/64	39/37	91/93	39/38	72/62	79/63	80/89	86/91	90/90
37	7/2	92/84	75/65	42/36	91/97	42/42	74/75	75/72	87/88	97/90	90/90
38	8/8	81/85	73/77	34/46	85/95	43/38	80/60	74/63	86/98	93/92	95/95
39	1/1	88/88	74/66	51/45	97/91	42/49	86/75	79/67	87/95	92/92	92/92
40	0/0	90/95	87/78	47/51	95/96	48/46	86/77	82/73	91/93	96/98	95/95
41	2/3	95/93	82/79	69/58	98/96	58/53	82/72	87/77	93/96	95/95	99/99
42	27/28	95/92	80/82	62/57	96/97	65/59	90/77	85/77	95/97	97/94	-/-
43	22/20	92/93	92/82	61/56	95/97	70/65	85/84	87/80	97/97	98/97	-/-
44	0/2	95/90	87/81	68/64	97/98	59/64	90/78	81/74	92/97	99/100	-/-
45	0/3	95/95	90/82	62/58	98/96	70/67	90/82	84/87	95/96	-/-	-/-
46	7/7	94/97	95/84	66/71	98/98	68/67	90/82	93/80	96/96	-/-	-/-
47	1/2	96/97	92/85	66/71	98/98	67/65	91/91	91/85	98/98	-/-	-/-
48	2/2	97/97	96/82	79/71	96/97	78/72	94/80	95/77	99/100	-/-	-/-
49	2/2	99/99	97/88	76/69	98/98	81/79	96/87	86/87	-/-	-/-	-/-
50	9/12	-/-	95/93	85/74	99/99	80/79	92/87	92/91	-/-	-/-	-/-
51	2/4	-/-	92/93	84/77	-/-	81/77	95/93	90/86	-/-	-/-	-/-
52	0/0	-/-	97/86	81/82	-/-	81/89	93/91	96/96	-/-	-/-	-/-
53	13/6	-/-	97/90	88/77	-/-	83/85	96/88	94/96	-/-	-/-	-/-
54	14/11	-/-	96/91	82/88	-/-	83/82	95/93	98/89	-/-	-/-	-/-
55	0/5	-/-	98/88	83/89	-/-	86/87	98/94	98/90	-/-	-/-	-/-
56	19/22	-/-	98/94	90/90	-/-	89/88	98/94	95/94	-/-	-/-	-/-
57	15/12	-/-	99/99	84/88	-/-	91/91	97/93	97/93	-/-	-/-	-/-
58	21/24	-/-	-/-	95/93	-/-	79/88	100/99	98/96	-/-	-/-	-/-
59	8/6	-/-	-/-	95/96	-/-	91/87	-/-	100/99	-/-	-/-	-/-
60	2/2	-/-	-/-	92/91	-/-	91/88	-/-	-/-	-/-	-/-	-/-
61	5/8	-/-	-/-	96/95	-/-	96/94	-/-	-/-	-/-	-/-	-/-
62	2/4	-/-	-/-	95/98	-/-	92/94	-/-	-/-	-/-	-/-	-/-
63	13/11	-/-	-/-	95/95	-/-	95/95	-/-	-/-	-/-	-/-	-/-
64	0/0	-/-	-/-	98/90	-/-	95/96	-/-	-/-	-/-	-/-	-/-
65	1/3	-/-	-/-	97/97	-/-	96/97	-/-	-/-	-/-	-/-	-/-
66	6/3	-/-	-/-	97/97	-/-	98/96	-/-	-/-	-/-	-/-	-/-
67	2/0	-/-	-/-	98/97	-/-	98/96	-/-	-/-	-/-	-/-	-/-
68	3/2	-/-	-/-	97/98	-/-	99/99	-/-	-/-	-/-	-/-	-/-
69	6/7	-/-	-/-	97/97	-/-	-/-	-/-	-/-	-/-	-/-	-/-
70	8/2	-/-	-/-	98/96	-/-	-/-	-/-	-/-	-/-	-/-	-/-
71	4/8	-/-	-/-	98/98	-/-	-/-	-/-	-/-	-/-	-/-	-/-
72	2/5	-/-	-/-	99/99	-/-	-/-	-/-	-/-	-/-	-/-	-/-

表A3　各区分器恢复Piccolo-80/128算法密钥所需的时间(分钟)

故障数	SEI	HW	ML	GF	MAP	GF-SEI	GF-ML	ML-SEI	ML-MAP	MM-HW	MM-HW-ML
1	0.60/0.75	0.56/0.71	2.27/3.01	0.77/0.80	2.28/3.06	0.73/0.89	2.58/3.17	2.40/2.99	2.38/2.94	0.69/0.81	2.88/3.24
2	0.95/1.18	0.90/1.13	2.61/3.41	1.21/1.25	2.61/3.47	1.05/1.33	2.87/3.58	2.68/3.38	2.68/3.35	0.99/1.21	3.17/3.57
3	1.25/1.57	1.21/1.53	2.91/3.82	1.63/1.63	2.90/3.87	1.35/1.70	3.17/3.98	2.96/3.75	2.97/3.75	1.30/1.65	3.50/3.93
4	1.59/2.00	1.54/1.94	3.23/4.23	2.07/2.05	3.22/4.29	1.68/2.12	3.49/4.38	3.29/4.15	3.29/4.16	1.62/2.05	3.91/4.40
5	1.93/2.42	1.88/2.36	3.54/4.59	2.52/2.49	3.53/4.65	2.03/2.53	3.79/4.76	3.60/4.52	3.59/4.52	1.96/2.46	4.27/4.80

续表

故障数	SEI	HW	ML	GF	MAP	GF-SEI	GF-ML	ML-SEI	ML-MAP	MM-HW	MM-HW-ML
6	2.30/2.89	2.25/2.80	3.90/5.04	2.95/2.96	3.88/5.08	2.38/2.99	4.13/5.19	3.93/4.96	3.93/4.96	2.32/2.93	4.59/5.16
7	2.64/3.31	2.58/3.26	4.20/5.49	3.40/3.37	4.20/5.52	2.75/3.46	4.47/5.63	4.28/5.40	4.28/5.39	2.69/3.39	4.88/5.49
8	3.00/3.76	2.95/3.69	4.54/5.90	3.87/3.85	4.54/5.93	3.11/3.93	4.80/6.05	4.61/5.81	4.60/5.81	3.05/3.83	5.27/5.93
9	3.40/4.26	3.34/4.18	4.89/6.36	4.37/4.33	4.88/6.39	3.48/4.38	5.17/6.50	4.94/6.24	4.97/6.26	3.43/4.32	5.64/6.35
10	3.76/4.74	3.70/4.65	5.23/6.74	4.79/4.78	5.23/6.80	3.86/4.88	5.48/6.90	5.30/6.69	5.29/6.66	3.78/4.77	6.04/6.79
11	4.14/5.21	4.07/5.13	5.58/7.20	5.29/5.28	5.57/7.25	4.24/5.35	5.83/7.35	5.65/7.12	5.64/7.10	4.17/5.27	6.42/7.22
12	4.53/5.70	4.47/5.62	5.94/7.69	5.77/5.78	5.95/7.73	4.64/5.86	6.22/7.83	6.02/7.59	6.03/7.60	4.56/5.75	6.83/7.68
13	4.91/6.17	4.86/6.10	6.30/8.11	6.27/6.23	6.29/8.16	5.01/6.31	6.56/8.25	6.36/8.02	6.36/8.02	4.93/6.22	7.23/8.14
14	5.31/6.68	5.25/6.61	6.67/8.61	6.78/6.76	6.67/8.63	5.42/6.84	6.93/8.74	6.73/8.50	6.74/8.49	5.35/6.74	7.66/8.61
15	5.70/7.21	5.64/7.12	7.04/9.07	7.27/7.26	7.03/9.13	5.83/7.36	7.31/9.22	7.12/8.98	7.12/8.98	5.74/7.24	8.10/9.11
16	6.08/7.64	6.01/7.58	7.42/9.55	7.77/7.75	7.42/9.57	6.20/7.84	7.66/9.66	7.47/9.43	7.47/9.44	6.12/7.72	8.50/9.56
17	6.50/8.20	6.44/8.12	7.77/10.02	8.30/8.28	7.79/10.07	6.62/8.37	8.07/10.18	7.86/9.94	7.88/9.92	6.55/8.27	8.94/10.06
18	6.91/8.71	6.84/8.63	8.18/10.55	8.83/8.78	8.18/10.57	7.04/8.87	8.45/10.67	8.27/10.42	8.26/10.46	6.96/8.80	9.37/10.54
19	7.30/9.22	7.22/9.12	8.56/10.97	9.28/9.26	8.56/11.05	7.40/9.35	8.81/11.13	8.65/10.91	8.62/10.88	7.34/9.29	9.80/11.03
20	7.72/9.75	7.65/9.65	8.98/11.52	9.84/9.82	8.98/11.59	7.85/9.90	9.25/11.68	9.03/11.40	9.06/11.44	7.75/9.79	10.25/11.53
21	8.13/10.26	8.07/10.17	9.36/12.01	10.37/10.32	9.37/12.05	8.28/10.42	9.62/12.14	9.43/11.92	9.44/11.92	8.18/10.34	10.70/12.04
22	8.54/10.80	8.49/10.67	9.75/12.48	10.86/10.85	9.74/12.56	8.64/10.92	10.01/12.65	9.82/12.43	9.81/12.42	8.57/10.81	11.16/12.56
23	8.98/11.35	8.90/11.26	10.17/13.05	11.43/11.41	10.15/13.12	9.09/11.49	10.45/13.21	10.25/12.92	10.28/12.98	8.99/11.37	11.61/13.06
24	9.37/11.80	9.30/11.71	10.56/13.53	11.94/11.91	10.57/13.60	9.54/12.04	10.82/13.67	10.66/13.46	10.66/13.45	9.44/11.92	12.03/13.53
25	9.80/12.36	9.73/12.25	10.98/14.06	12.46/12.70	10.98/14.13	9.94/12.55	11.26/14.19	11.06/13.97	11.09/13.96	9.86/12.42	12.53/14.10
26	10.24/12.90	10.14/12.81	11.38/14.59	13.01/13.01	11.39/14.65	10.37/13.09	11.68/14.75	11.47/14.48	11.49/14.53	10.27/12.96	13.00/14.62
27	10.66/13.44	10.54/13.30	11.82/15.08	13.52/13.51	11.80/15.16	10.79/13.62	12.07/15.24	11.88/15.03	11.88/14.99	10.70/13.49	13.41/15.09
28	11.09/13.99	11.02/13.92	12.23/15.66	14.07/14.08	12.23/15.73	11.21/14.15	12.54/15.81	12.31/15.55	12.33/15.58	11.10/14.01	13.93/15.67
29	11.48/14.46	11.40/14.41	12.66/16.16	14.62/14.57	12.64/16.22	11.65/14.71	12.94/16.33	12.72/16.04	12.74/16.07	11.57/14.60	14.38/16.18
30	11.92/15.02	11.84/14.92	13.06/16.69	15.14/15.13	13.08/16.78	12.07/15.21	13.35/16.87	13.16/16.62	13.16/16.63	11.95/15.08	14.86/16.71
31	12.37/15.61	12.28/15.52	13.49/17.27	15.70/15.69	13.51/17.32	12.49/15.78	13.81/17.41	13.58/17.14	13.63/17.17	12.40/15.63	15.33/17.25
32	12.75/16.09	12.71/16.03	13.94/17.80	16.28/16.21	13.94/17.81	12.95/16.34	14.21/17.91	13.97/17.65	14.05/17.70	12.85/16.20	15.83/17.81
33	13.22/16.69	13.13/16.56	14.37/18.31	16.83/16.77	14.36/18.40	13.35/16.85	14.63/18.48	14.46/18.23	14.45/18.23	13.28/16.75	16.31/18.35
34	13.64/17.22	13.60/17.07	14.81/18.84	17.35/17.29	14.78/18.92	13.77/17.39	15.08/19.00	14.85/18.77	14.84/18.76	13.69/17.27	16.80/18.90
35	14.08/17.72	13.96/17.63	15.25/19.37	17.89/17.82	15.23/19.47	14.21/17.92	15.50/19.57	15.31/19.30	15.30/19.30	14.12/17.82	17.25/19.40
36	14.52/18.31	14.43/18.24	15.67/19.98	18.47/18.41	15.66/20.03	14.64/18.48	15.95/20.13	15.73/19.86	15.74/19.87	14.56/18.37	17.75/19.96
37	14.96/18.85	14.87/18.71	16.12/20.45	18.99/18.93	16.11/20.53	15.10/19.03	16.36/20.67	16.15/20.38	16.16/20.38	15.01/18.91	18.20/20.48

续表

故障数	SEI	HW	ML	GF	MAP	GF-SEI	GF-ML	ML-SEI	ML-MAP	MM-HW	MM-HW-ML
38	15.39/19.42	15.31/19.32	16.54/21.01	19.59/19.50	16.53/21.12	15.51/19.58	16.83/21.19	16.60/20.95	16.58/20.95	15.40/19.47	18.72/21.05
39	15.81/19.95	15.76/19.87	16.97/21.60	20.15/20.04	16.99/21.67	15.97/20.09	17.24/21.76	17.04/21.46	17.00/21.47	15.86/19.99	19.21/21.61
40	16.25/20.47	16.17/20.39	17.42/22.13	20.68/20.61	17.44/22.24	16.38/20.68	17.67/22.28	17.48/22.08	17.42/22.05	16.28/20.55	19.68/22.13
41	16.71/21.07	16.59/20.94	17.87/22.66	21.24/21.15	17.86/22.78	16.80/21.20	18.14/22.87	17.92/22.61	17.83/22.57	16.71/21.10	20.18/22.70
42	17.13/21.59	17.07/21.48	18.30/23.30	21.77/21.70	18.30/23.34	17.28/21.76	18.60/23.39	18.34/23.16	18.25/23.10	17.18/21.68	-/-
43	17.60/22.16	17.48/22.02	18.77/23.80	22.36/22.25	18.76/23.87	17.70/22.31	19.07/23.98	18.82/23.73	18.67/23.68	17.60/22.19	-/-
44	18.00/22.72	17.90/22.59	19.20/24.35	22.89/22.78	19.20/24.44	18.15/22.86	19.54/24.43	19.25/24.24	19.09/24.22	18.05/22.75	-/-
45	18.44/23.24	18.31/23.11	19.65/24.89	23.46/23.32	19.66/25.02	18.59/23.43	20.01/25.00	19.67/24.81	19.51/24.75	-/-	-/-
46	18.87/23.81	18.72/23.70	20.10/25.47	23.99/23.91	20.08/25.57	19.01/23.97	20.47/25.53	20.10/25.33	19.93/25.29	-/-	-/-
47	19.29/24.33	19.14/24.27	20.54/26.03	24.56/24.43	20.53/26.11	19.48/24.55	20.94/26.11	20.52/25.89	20.35/25.88	-/-	-/-
48	19.75/24.93	19.55/24.80	20.98/26.61	25.12/25.02	21.00/26.66	19.91/25.09	21.41/26.69	20.95/26.50	20.77/26.45	-/-	-/-
49	20.19/25.48	19.96/25.36	21.42/27.15	25.68/25.56	21.43/27.24	20.33/25.61	21.87/27.22	21.37/26.99	-/-	-/-	-/-
50	20.61/26.00	-/-	21.86/27.71	26.20/26.11	21.86/27.83	20.77/26.17	22.34/27.76	21.80/27.54	-/-	-/-	-/-
51	21.08/26.59	-/-	22.30/28.26	26.80/26.66	-/-	21.24/26.75	22.81/28.35	22.22/28.10	-/-	-/-	-/-
52	21.53/27.12	-/-	22.74/28.84	27.36/27.22	-/-	21.68/27.28	23.27/28.94	22.65/28.70	-/-	-/-	-/-
53	21.98/27.67	-/-	23.18/29.37	27.90/27.78	-/-	22.11/27.86	23.74/29.48	23.07/29.19	-/-	-/-	-/-
54	22.38/28.20	-/-	23.62/29.97	28.47/28.32	-/-	22.56/28.43	24.21/30.02	23.50/29.73	-/-	-/-	-/-
55	22.84/28.77	-/-	24.07/30.50	29.06/28.87	-/-	23.00/28.95	24.67/30.58	23.92/30.26	-/-	-/-	-/-
56	23.28/29.32	-/-	24.51/31.14	29.61/29.44	-/-	23.46/29.52	25.14/31.17	24.35/30.91	-/-	-/-	-/-
57	23.71/29.87	-/-	24.95/31.66	30.13/29.97	-/-	23.84/30.04	25.61/31.72	24.77/31.39	-/-	-/-	-/-
58	24.17/30.41	-/-	-/-	30.69/30.55	-/-	24.30/30.59	26.08/32.28	25.20/31.97	-/-	-/-	-/-
59	24.59/30.98	-/-	-/-	31.28/31.09	-/-	24.74/31.16	-/-	25.62/32.52	-/-	-/-	-/-
60	25.04/31.54	-/-	-/-	31.83/31.65	-/-	25.19/31.74	-/-	-/-	-/-	-/-	-/-

续表

故障数	SEI	HW	ML	GF	MAP	GF-SEI	GF-ML	ML-SEI	ML-MAP	MM-HW	MM-HW-ML
61	25.48/32.08	-/-	-/-	32.40/32.19	-/-	25.63/32.26	-/-	-/-	-/-	-/-	-/-
62	25.95/32.64	-/-	-/-	32.95/32.78	-/-	26.04/32.82	-/-	-/-	-/-	-/-	-/-
63	26.36/33.19	-/-	-/-	33.52/33.32	-/-	26.46/33.36	-/-	-/-	-/-	-/-	-/-
64	26.80/33.75	-/-	-/-	34.11/33.89	-/-	26.87/33.94	-/-	-/-	-/-	-/-	-/-
65	27.24/34.30	-/-	-/-	34.62/34.42	-/-	27.29/34.46	-/-	-/-	-/-	-/-	-/-
66	27.70/34.89	-/-	-/-	35.21/34.98	-/-	27.70/35.03	-/-	-/-	-/-	-/-	-/-
67	28.14/35.42	-/-	-/-	35.76/35.52	-/-	28.11/35.55	-/-	-/-	-/-	-/-	-/-
68	28.57/35.98	-/-	-/-	36.34/36.10	-/-	28.53/36.13	-/-	-/-	-/-	-/-	-/-
69	29.06/36.53	-/-	-/-	36.90/36.64	-/-	-/-	-/-	-/-	-/-	-/-	-/-
70	29.49/37.08	-/-	-/-	37.46/37.20	-/-	-/-	-/-	-/-	-/-	-/-	-/-
71	29.95/37.90	-/-	-/-	38.02/39.27	-/-	-/-	-/-	-/-	-/-	-/-	-/-
72	30.35/38.18	-/-	-/-	38.58/39.61	-/-	-/-	-/-	-/-	-/-	-/-	-/-

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

LI Jia-Yao, Ph. D. candidate. His main research interests include fault analysis of block ciphers.

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

WANG Meng-Lin, M. S. candidate. Her main research interests include security analysis of lightweight ciphers.

CAI Tian-Pei, M. S. candidate. His main research interests include security analysis of block ciphers.

Background

Our work is supported by the National Natural Science Foundation of China under grand No. 61772129, 61932014, National Cryptography Development Fund under grant No. MMJJ20180101, Shanghai Natural Science Foundation of China under grand No. 19ZR1402000, the Opening Project of Shanghai Key Laboratory of Scalable Computing and Systems, the Opening Project of Shanghai Key Laboratory of Integrate Administration Technologies for Information Security and the Fundamental Research Funds for the Central Universities.

The lightweight Piccolo cryptosystem, proposed at CHES, can be implemented with low storage and power consumption in the Internet of Things. It provides a wide range of options among area, throughput and power consumption. The designers analyzed the security of Piccolo against differential analysis, linear analysis, impossible differential analysis, boomerang analysis and meet-in-the-middle analysis, etc.

In addition to the above classical cryptanalysis, fault analysis has been a competitive threat of a cryptosystem since 1997. It breaks the secret key of a cryptosystem by fault injections. Boneh et al. applied the fault analysis successfully

to break the RSA cryptosystem with the exploitation of Chinese Remainder Theorem. Later, more kinds of fault analysis are presented, such as differential fault analysis, algebraic fault analysis, meet-in-the-middle fault analysis and statistical fault analysis, etc. The attacking assumptions of most classical cryptanalysis and some fault analysis focus on the known-plaintext attack (KPA) or the chosen-plaintext attack (CPA).

However, the above assumptions are not suitable to apply in the Internet of Things, and the attackers cannot have so strong ability to get the corresponding ciphertexts from the known or designated plaintexts. In the real scenario, the attackers may only have the weakest capability of ciphertext-only attack (COA). In 2013, Fuhr et al. proposed the statistical fault analysis (SFA) of AES in the software implementation. Later, Dobraunig et al. successfully applied the SFA on some authenticated encryption schemas in 2016. Li et al. expanded the SFA with new distinguishers on the LED and other cryptosystems.

In the literature, no research has been published on the SFA analysis of Piccolo, which motivates us to investigate new distinguishers of SFA on Piccolo. Our study analyzes the SFA analysis of Piccolo with 11 different distinguishers in the software implementation. The experimental results show that the novel distinguishers of MM-HW-ML, MM-HW and ML-MAP can recover the secret key of Piccolo with the reliability of at least 99% in the SFA, respectively. The novel proposed distinguishers of SFA are able to reduce the faults and improve efficiency. It provides a significant reference for analyzing the security of lightweight ciphers in the Internet of Things.