计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170437
54(10):2205-2214, 2017

物联网环境中 LED 轻量级密码算法的统计故障分析研究

李 玮[1,2,3] 葛晨雨[1] 谷大武[2] 廖林峰[1] 高志勇[1] 郭 筝[4] 刘 亚[5] 刘志强[2] 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)

[4](上海交通大学微电子学院 上海 200240)

[5](上海理工大学计算机科学与工程系 上海 200093)

(liwei.cs.cn@gmail.com)

Research on the LED Lightweight Cipher Against the Statistical Fault Analysis in Internet of Things

Li Wei[1,2,3], Ge Chenyu[1], Gu Dawu[2], Liao Linfeng[1], Gao Zhiyong[1], Guo Zheng[4], Liu Ya[5], Liu Zhiqiang[2], 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 Integrate Administration Technologies for Information Security (Shanghai Jiao Tong University), Shanghai* 200240)

[4](*School of Microelectronics, Shanghai Jiao Tong University, Shanghai* 200240)

[5](*Department of Computer Science and Engineering, University of Shanghai for Science and Technology, Shanghai* 200093)

Abstract The typical lightweight cipher LED, proposed in CHES 2011, is applied in the Internet of things (IoT) to provide security for RFID tags and smart cards etc. Fault analysis has become an important method of cryptanalysis to evaluate the security of lightweight ciphers, depending on its fast speed, simple implementation, complex defense, etc. On the basis of the half byte-oriented fault model, we propose new statistical fault analysis on the LED cipher by inducing faults. Simulating experiment shows that our attack can recover its 64-bit and 128-bit secret keys with 99% probability using an SEI distinguisher, a GF distinguisher and a GF-SEI distinguisher, respectively. The attack can be implemented in the ciphertext-only attacking environment to improve the attacking efficiency and decrease the number of faults. It provides vital reference for security analysis of other lightweight ciphers in the Internet of things.

收稿日期:2017-06-11;**修回日期**:2017-07-31

基金项目:国家"九七三"重点基础研究发展计划基金项目(2013CB338004);国家自然科学基金项目(61672347,61772129,61402288,61402286,61402250,61572192);上海市自然科学基金项目(15ZR1400300,16ZR1401100);上海市教育委员会科研创新重点项目(14ZZ066);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);中央高校基本科研业务费专项资金项目(040)

This work was supported by the National Basic Research Program of China (973 Program) (2013CB338004), the National Natural Science Foundation of China (61672347, 61772129, 61402288, 61402286, 61402250, 61572192), the Shanghai Natural Science Foundation (15ZR1400300, 16ZR1401100), the Innovation Program of Shanghai Municipal Education Commission (14ZZ066), the Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (AGK201703), and the Fundamental Research Funds for the Central Universities (040).

通信作者:石秀金(sxj@dhu.edu.cn)

Key words Internet of things (IoT); lightweight cipher; LED; statistical fault analysis; cryptanalysis

摘 要 LED 算法是于 2011 年密码硬件与嵌入式系统国际会议(CHES)中提出的一种典型轻量级密码算法,用于在物联网环境下保护 RFID 标签以及智能卡等设备的通信安全.故障分析凭借其攻击速度快、实现简单和难以防御等特点,已成为评测轻量级密码算法安全性的一种重要手段.提出了针对 LED 算法的新型统计故障分析方法,采用面向半字节的故障模型,分别使用 SEI 区分器、GF 区分器和 GF-SEI 双重区分器对算法进行统计分析.实验结果表明:在较短时间内以 99%的成功概率恢复出 LED 算法的 64 b 和 128 b 原始密钥.该攻击方法不仅可以在唯密文攻击条件下实现,而且提升了故障攻击效率,降低了故障数,为物联网环境下其他轻量级密码的安全性分析提供了重要参考.

关键词 物联网;轻量级密码;LED;统计故障分析;密码分析

中图法分类号 TP309.7

物联网(Internet of things, IoT)是通过使用射频识别、传感器、红外感应器、全球定位系统、激光扫描器等信息采集设备,按照约定的协议把任何物品与互联网连接起来进行信息交换和通信,以实现智能化识别、定位、跟踪、监控和管理的一种网络[1].物联网代表了未来计算与通信技术的方向,被认为是继计算机、Internet 之后,信息产业领域的第三次发展浪潮.随着物联网建设的加快,物联网的安全问题必然成为制约物联网全面发展的重要因素[2].

与互联网安全技术相比,物联网安全技术更具大众性和平民性,与人类的日常生活密切相关,这就要求物联网安全技术采用低成本、简单、易用、轻量级的解决方案[3-4].在 2011 年召开的密码硬件与嵌入式系统国际会议(CHES)上,Guo 等人提出的 LED 算法就是一种典型的轻量级密码算法,相较于其他轻量级密码算法,它的软硬件执行效率更高、适应环境的能力更强,是应用于物联网安全中的算法佼佼者[5-13].

在物联网环境下,轻量级密码的许多硬件实现和以硬件为表现形式的软件实现环境中,譬如手机 SIM、IC 银行卡、物流 RFID、手持无线设备、数字无绳电话、NFC 近场通信设备、蓝牙、汽车遥控锁、各类交通卡、校园卡、门禁卡和高端身份卡等密码载体等,攻击者往往不仅具备传统密码攻击的条件,而且还可以通过电路剖析和软件逆向分析等手段获得算法的硬件结构和编码实现方法,并可以观察和测量密码变换等信息,"干预"密码变换的正常运行使其出错.攻击者利用这些额外的出错信息有可能实现比传统分析技术更有效地破译密码.这种环境下的攻击被称为"故障分析(fault analysis, FA)".由于其成功的攻击效果和潜在的发展前景,已经引起了国内外从事密码和微电子研究学者的极大关注,并成为密码分析和密码工程领域发展最为迅速的方向之一[14].

在故障分析的发展历程中,先后产生了差分故障分析(differential fault analysis, DFA)、代数故障分析(algebra fault analysis, AFA)、不可能故障分析(impossible differential fault analysis, IDFA)以及统计故障分析(statistical fault analysis, SFA)等多种方法.随着故障注入精度以及软硬件逆向技术的不断提高,对密码载体成功实施故障攻击所依赖的前提条件不断减弱,成本不断下降,故障分析环境已经在一定程度上可以控制,从而使这些故障分析在面向物联网环境中逐步发展为攻击密码体制的主要方法.

不同于其他故障分析方法,统计故障分析是唯一现有的可以在唯密文攻击(ciphertext-only attacks, COA)条件下进行攻击的技术,它在面向物联网等实际环境中更易实现且难以防御,攻击者只要统计故障密文的特性,就能以低的计算量和存储量推导出正确的密钥.目前,在 LED 算法抗统计故障攻击的安全性方面,国内外尚未发现有公开发表的结果.在深入分析 LED 算法后,本文提出了一种针对 LED 算法的新型统计故障分析方法,不仅提高故障导入的效率,而且使用较少的故障数即可恢复原始密钥,对于保护物联网的通信安全,对于增强密码装备的自主设计、开发和分析能力,无疑都具有重要意义和价值.

1 研究背景

1997 年 Boneh 等人利用随机故障成功破译 RSA

算法,此后故障分析在评测主流密码体制安全性的方法中占据了重要的位置[14-15].故障分析的成功实现必须具备了一个重要前提——故障假设,它表明了攻击者具备的能力,决定了攻击的可行性和难易度.一般情况下,攻击者可以任意选择明文进行处理,从而获得相对应的密文,通常为选择明文攻击(chosen plaintext attacks, CPA).

在 LED 算法密码的故障分析中,诸如差分故障分析、代数故障分析和不可能故障分析等方法,均采用了选择明文攻击的故障假设.攻击者可以选择任意明文获得相应的正确密文和错误密文.国内外研究学者针对 LED 算法于 2012 年相继提出了差分故障分析方法,Jeong 等人在随机半字节故障下破译了 LED 算法的 64 b 密钥;Li 等人在随机半字节和字节模型下,至少以 3 个故障和 6 个故障恢复了 64 b 和 128 b 密钥;Jovanovic 等人通过利用不同轮之间的线性关系将故障数降为 1 个和 2 个故障[16-20].2013 年,Zhao 等人利用代数关系,使用代数故障分析对 LED 算法进行了破译[21-22].2016 年,Li 等人利用不可能差分故障分析恢复了 LED 算法的 64 b 和 128 b 密钥[23].这些方法充分结合了传统密码分析技术以及软硬件实现,不仅扩大了攻击面,而且提升了威胁性.表 1 列出了针对 LED 算法的各种故障分析技术对比.

Table 1　Comparison of Fault Analysis on LED

表 1　针对 LED 算法的故障分析对比

Type	Assumption	Model	Rounds	References
DFA	CPA	Nibble,Byte	$l-2$	Ref[17-20]
AFA	CPA	Nibble	$l-2$	Ref[21-22]
IDFA	CPA	Nibble	$l-3$	Ref[23]
SFA	COA	Nibble	$l-1$	This paper

然而,在面向物联网等现实的运行环境下,如果攻击者不具备选择明文攻击的前提,即不能实现对同一明文必须至少加密 2 次,则上述故障分析方法难以实现.众所周知:唯密文攻击比选择明文攻击弱,攻击者在此模型下仅能使用密文,因而无法获得有效数据进行故障分析破译.

2013 年 Fuhr 等人首次提出了统计故障攻击方法[24],并用于破译了 AES 算法.该方法在唯密文攻击的假设下,在算法运行时引入故障,使算法执行某些错误的操作、过程,并产生错误的结果,再利用这些结果,结合统计分析方法,破译出该算法的密钥.在随机字节故障模型下,他们通过采用平方欧氏距离 SEI 作为区分器,将故障导入在倒数第二轮的指定位置,以 320 个故障且 99%的成功概率恢复出 AES 算法的唯一密钥.

由此,在统计故障分析中,区分器发挥了举足轻重的作用.因此,在 LED 算法的新型统计分析中,我们不仅给出了 SEI 的攻击结果,而且提出了拟合优度检验 GF 作为新型区分器.更为重要的是,在 SEI 和 GF 区分器的基础上,又构建了 GF-SEI 双重区分器.结果表明:可以以更少的故障且 99%的成功率恢复 LED 算法 64 b 和 128 b 原始密钥,不仅提升了故障攻击效率,而且降低了故障攻击数.

2　LED 算法简介

LED 算法是一种具有 SPN 结构的迭代型分组密码,分组长度为 64 b,密钥长度分别为 64 b 或 128 b.根据密钥长度的不同,加密算法对应的轮数分别为 32 轮和 48 轮,表示为 LED-64 和 LED-128,如表 2 所示.由于解密算法与加密算法的结构相同,并且子密钥的使用顺序相同,因此以下仅介绍加密算法和密钥编排方案.

Table 2　The Relationship Between Rounds and Key Sizes

表 2　LED 算法的轮数和密钥长度的关系

Version	Block Size/b	Key Size/b	Rounds
LED-64	64	64	32
LED-128	64	128	48

2.1　符号说明

本文记号如下所示:

设明文输入为 $X\in(Z_2^4)^{16}$,密文输出为 $Y,Y^*\in(Z_2^4)^{16}$,原始密钥 $K\in(Z_2^4)^{16}$,子密钥 $k_1\in(Z_2^4)^{16}$ 和 $k_2\in(Z_2^4)^{16}$,轮数 $l\in\{32,48\}$.

记 AC,SC,SR 和 MC 分别为轮常数加运算、信元代替运算、行移位运算和列混合运算.

记 AC^{-1},SC^{-1},SR^{-1} 和 MC^{-1} 分别为轮常数加运算、信元代替运算、行移位运算和列混合运算的逆运算.

记 A_r,B_r,C_r 和 D_r 分别为第 r 轮的轮常数加运算、信元代替运算、行移位运算和列混合运算的输出,其中,$1\leqslant r\leqslant l$.

2.2　算法描述

LED 算法的结构如图 1 所示.

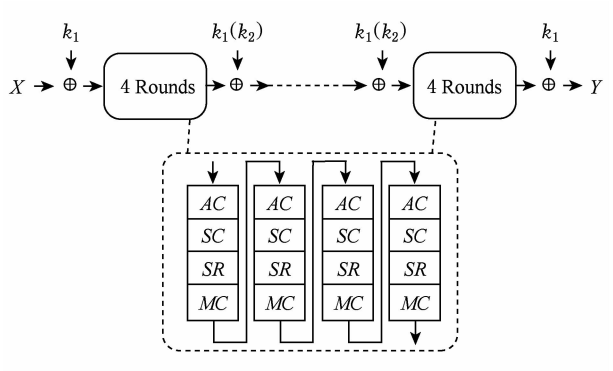


Fig. 1 The structure of LED

图 1 LED 算法的结构

加解密算法包含 5 个基本运算:

1) 子密钥加运算(AddRoundKey, ARK). 该运算对中间状态与子密钥进行异或.

2) 常数相加运算(AddConstants, AC). 该运算将中间状态与常数相加.

3) 信元代替运算(SubCells, SC). 该运算将中间状态中的每半字节通过 S 盒非线性地变换为另外一个半字节.

4) 行移位运算(ShiftRows, SR). 该运算对一个状态的每一行循环不同的位移量. 第 0 行移位保持不变,第 1 行循环左移 4 b,第 2 行循环左移 8 b,第 3 行循环左移 12 b.

5) 列混合运算(MixColumnsSerial, MC). 该运算对一个状态逐列进行变换,通过与矩阵

$$\begin{pmatrix} 4 & 2 & 1 & 1 \\ 8 & 6 & 5 & 6 \\ B & E & A & F \\ 2 & 2 & F & B \end{pmatrix}$$

相乘实现.

LED-64 和 LED-128 的加密变换分别如算法 1、算法 2 所示.

算法 1. LED-64 加密变换.

输入:明文 X、密钥 K;

输出:密文 Y.

① $T=X$; /* 将 X 赋值给中间状态 T */

② for $i=1$ to 8

③ $T=ARK(T,k_1)$;

④ for $j=1$ to 4

⑤ $T=MC(SR(SC(AC(T))))$;

⑥ end for

⑦ end for

⑧ $Y=ARK(T,k_1)$.

算法 2. LED-128 加密变换.

输入:明文 X、密钥 K;

输出:密文 Y.

① $T=X$; /* 将 X 赋值给中间状态 T */

② for $i=1$ to 6

③ $T=ARK(T,k_1)$;

④ for $j=1$ to 4

⑤ $T=MC(SR(SC(AC(T))))$;

⑥ end for

⑦ $T=ARK(T,k_2)$;

⑧ for $j=1$ to 4

⑨ $T=MC(SR(SC(AC(T))))$;

⑩ end for

⑪ end for

⑫ $Y=ARK(T,k_1)$.

2.3 密码编排方案

在 LED-64 算法中,K 通过密钥编排方案生成了 k_1,它们的关系为

$$K=k_1.$$

在 LED-128 算法中,K 通过密钥编排方案生成了 k_1 和 k_2,它们的关系为

$$K=k_1 \| k_2.$$

对于 LED-64 算法,攻击者仅需要恢复出任意一轮的子密钥 k_1,就能恢复出密钥 K;而对于 LED-128 算法,攻击者仅需要恢复任意一轮的子密钥 k_1 和 k_2,就能恢复出密钥 K.

3 LED 密码的统计故障攻击方法

3.1 故障假设和故障模型

故障假设为唯密文攻击,即攻击者仅能获得密码算法的任意密文进行攻击. 考虑到实际应用中的易操作性以及 LED 算法的设计特点,本文中使用随机半字节故障模型,以按位与的方式导入,故障大小为半字节.

3.2 主要过程

攻击者使用同一个密钥对随机明文进行加密,并在运行过程中的某一轮导入随机故障,获得一组错误密文. 故障导入的动作可以通过软件模拟的方式实现,也可以通过激光、电磁和电压干扰等技术手段对真实的密码实现硬件进行处理来实现. 由于受故障影响,加密过程中的一些中间状态值会呈现非均匀分布. 利用特定的区分器统计这些中间状态值的分布律,得到最后一轮的子密钥的部分比特. 重复上述步骤,可以恢复子密钥的全部比特,最终通过密钥编排方案求得原始密钥.

3.3　攻击步骤

针对 LED 算法,本文验证了 Fuhr 等人提出的 SEI 区分器,并提出了 2 种新型区分器用于统计故障分析,均可以破译 LED-64 和 LED-128 算法.具体有 5 个步骤:

步骤 1.随机生成一组明文,使用同一密钥加密,在加密过程中随机导入半字节故障,获得一组错误密文.故障导入的位置可以是 A_{r-1},B_{r-1} 或者 C_{r-1},导入在这 3 个位置时故障扩散路径是相同的.如图 2 所示,图 2 中阴影表示受故障影响的半字节,不同灰度的阴影表示不同比例的故障差分值.

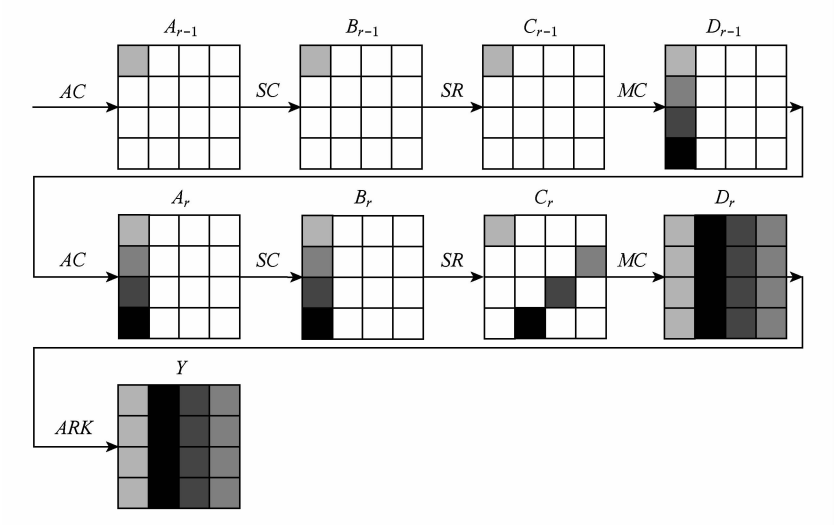


Fig. 2　Fault diffusion path in the penultimate round

图 2　故障导入在倒数第 2 轮后的扩散路径

步骤 2.经过列混合变换后,中间状态的每个半字节的分布律都受到上一个中间状态的 4 个半字节分布律的影响.攻击者需统计未经过 MC 且受到故障影响的半字节的分布,即 A_{r-1},B_{r-1} 或者 C_{r-1}.以 C_{r-1} 为例,通过加密算法可以得出,C_{r-1} 的每一个半字节都能用子密钥 k_1 和错误密文 Y^* 的 4 个半字节来表示:

$$C_{r-1}=MC^{-1}(AC^{-1}(SC^{-1}(SR^{-1}(MC^{-1}(Y^*\oplus k_1)))))=MC^{-1}(AC^{-1}(SC^{-1}(SR^{-1}(MC^{-1}(Y^*)\oplus MC^{-1}(k_1))))).$$

步骤 3.通过统计分析,计算出 k_1 的 16 b.对于每一个子密钥候选值,都能求出一组 C_{r-1}.选定一个区分器,将这组数据作为样本,求出每个候选值的区分器值,经过比较,选取区分器值最大(小)的候选值,即为正确子密钥.

本步骤中所使用的区分器有 3 种:

1) SEI 区分器

平方欧氏距离(square Euclidean imbalance, SEI)是由 Fuhr 等人提出的一种统计故障分析区分器,用于判断一组样本值是否服从均匀分布.攻击者计算出最不可能服从均匀分布的那一组样本值,即可求出子密钥的部分位.表达式为

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

其中,$\gamma[\varepsilon]$ 记录了样本值为 ε 的样本个数;N 为样本总个数;λ 表示计量值的分组组数.当求得的 SEI 越小,表示这组样本越服从均匀分布.

2) GF 区分器

拟合优度(goodness of fit, GF)作为统计故障分析新区分器之一,适用于已知样本分布率的情况下.攻击者通过计算一组样本是否满足该分布,从而求出子密钥的部分位.表达式为

$$GF=\sum_{\varepsilon=0}^{\lambda-1}\frac{(O_\varepsilon-\Phi_\varepsilon)^2}{\Phi_\varepsilon},$$

其中,λ 表示计量值的分组组数;O_ε 表示样本处于分组 ε 中的个数;Φ_ε 表示在相同的样本总数下,处于分组 ε 中的理论个数.与 SEI 区分器结果类似,若计算结果越小,则表示该组样本越服从该分布.

根据半字节随机故障模型,攻击者可以预先计算出 LED 算法的 C_{r-1} 分布情况,设 $V_1\in Z_2^4$ 为 4 b 中间值,$V_2\in Z_2^4$ 为随机 4 b 故障值,则故障以按位与的方式导入后的所有可能值如表 3 所示.攻击者推算出如表 4 所示的分布律,并在 GF 区分器中使用该分布律.

目前拟合优度检验标准已经发展成熟,攻击者可自定义精度 α,根据统计量的自由度 df 从 χ^2 分布上侧分位数表中查询临界值 χ_α^2,并与求得的区分器

值作比较,从而得出统计推断.即规定当 $\chi^2 \leqslant \chi_\alpha^2$ 时,样本服从该已知分布.结合 LED 算法和本文使用故障模型,计量值取值在[0,15]之间的任意整数,因而本文使用 GF 区分器的样本分组组数 $\lambda=16$,自由度 $df=\lambda-1=15$.拟合优度检验在样本总数 $N\geqslant 50$ 且理论数 $\Phi_\varepsilon \geqslant 5$ 的情况下,N 越大,恢复子密钥成功率越高,效果尤为显著;然而,在攻击效果评价中,故障个数越少则攻击方法越有效,这与拟合优度检验对 N 的要求矛盾,因而单纯的 GF 区分器在统计故障分析中不能发挥它的优势.

Table 3 The Overview of a Nibble After Fault Injections

表 3 半字节受故障影响后的结果总览

V_1	V_2															
	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
2	0	0	2	2	0	0	2	2	0	0	2	2	0	0	2	2
3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
4	0	0	0	0	4	4	4	4	0	0	0	0	4	4	4	4
5	0	1	0	1	4	5	4	5	0	1	0	1	4	5	4	5
6	0	0	2	2	4	4	6	6	0	0	2	2	4	4	6	6
7	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
8	0	0	0	0	0	0	0	0	8	8	8	8	8	8	8	8
9	0	1	0	1	0	1	0	1	8	9	8	9	8	9	8	9
a	0	0	2	2	0	0	2	2	8	8	a	a	8	8	a	a
b	0	1	2	3	0	1	2	3	8	9	a	b	8	9	a	b
c	0	0	0	0	4	4	4	4	8	8	8	8	c	c	c	c
d	0	1	0	1	4	5	4	5	8	9	8	9	c	d	c	d
e	0	0	2	2	4	4	6	6	8	8	a	a	c	c	e	e
f	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f

Table 4 The Distribution of a Nibble After Fault Injections

表 4 半字节被故障影响后的分布率

V_1	P/%	V_1	P/%
0	31.7	8	10.5
1	10.5	9	3.5
2	10.5	10	3.5
3	3.5	11	1.2
4	10.5	12	3.5
5	3.5	13	1.2
6	3.5	14	1.2
7	1.2	15	0.5

3) GF-SEI 双重区分器

为了进一步减少故障数并且解决以上问题,攻击者可以将上述 2 个区分器结合,构建一个新型 GF-SEI 双重区分器.使用方法为:先用拟合优度检验筛选出符合中间状态值分布的所有样本组;再用 SEI 区分器从中寻找最优样本,从而恢复一定的密钥比特.

步骤 4.上述过程重复 4 次,即可恢复出子密钥 k_1 的全部位.LED-64 的原始密钥 K 即可通过密钥编排算法求得.

步骤 5.在破译 LED-128 算法时,首先按上述过程恢复子密钥 k_1;然后利用 k_1 解密最后 4 轮,得到第 44 轮的输出,重复上述步骤,即恢复子密钥 k_2;最后根据密钥编排算法求得原始密钥 K,使用故障数为 LED-64 算法的 2 倍.

4 实验分析

实验采用使用 Eclipse 平台编写 Java 代码进行算法的加解密和攻击操作,利用计算机软件模拟故障产生,通过随机数生成器生成随机半字节值,以按位与的方式导入到加密过程中的中间变量中,进而改变了该半字节的分布率.本节以恢复 k_1 的 16 b 为例,分别考量 SEI 区分器、GF 区分器和 GF-SEI 双重区分器的故障数和耗费时间,所有数据均为实验 1 000 次后的平均值.图 3 表示在不同的区分器作用下恢复出子密钥的概率.其中,横坐标轴表示导入的故障数,纵坐标轴表示恢复出正确子密钥的成功率.3 种不同线段分别表示使用 SEI 区分器、GF 区分器和 GF-SEI 双重混合区分器进行统计分析的结果.实验结果表明,在半字节随机故障模型下,使用 SEI 区分器、GF 区分器和 GF-SEI 双重区分器时,分别需要 68,64 和 48 个故障,即可以 99%的概率恢复出步骤 3 中的子密钥.因而使用后 2 种区分器可以降低攻击所用故障数,并且使用 GF-SEI 双重区分器时故障数减少明显.

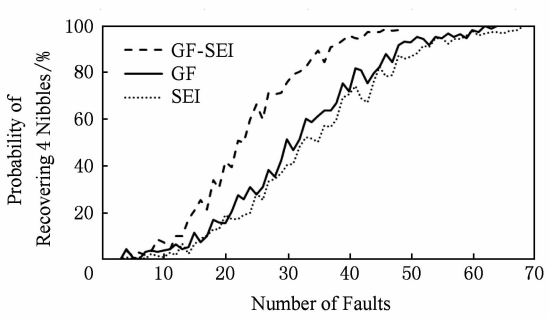


Fig. 3 The probability of recovering a partial subkey using different faults

图 3 使用不同故障数时恢复出部分子密钥的概率

图 4 表示使用 SEI 区分器、GF 区分器和 GF-SEI 双重混合区分器破译密钥的时间堆积图. 其中横坐标轴表示故障导入的个数,纵坐标轴表示以秒为单位的耗时. 实验结果表明,在半字节随机故障模型下,3 种区分器分别需要 2.5 s,2.4 s 和 1.7 s,即可以 99%的概率恢复出步骤 3 中的子密钥. 观察图 4 可知,对于同一个故障数,使用 3 种区分器进行统计分析所花费的时间比较接近. 特别值得一提的是,使用 GF-SEI 双重混合区分器不会增加攻击时间.

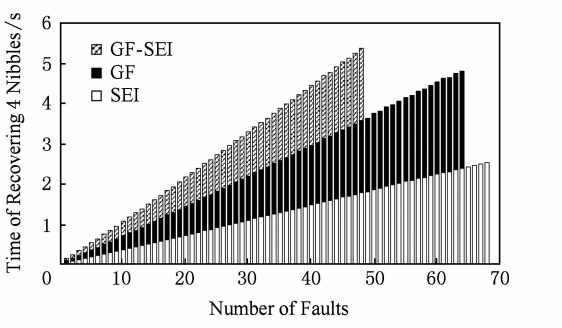


Fig. 4　The time shown with stacked charts of using different faults

图 4　使用不同故障数时耗费时间的堆积柱形图

结合图 3 和图 4 的实验结果,我们进一步对 SEI 区分器、GF 区分器和 GF-SEI 双重区分器的破译情况进行了比较,表 5 为统计故障分析 AES 算法和 LED 算法的攻击结果对比. 结果表明,使用 GF 区分器后的攻击效果比 SEI 区分器的攻击效果略佳,但效果不明显;而使用 GF-SEI 双重区分器所需要的故障数和耗费的时间比前两者均明显减少,是统计故障分析中目前已知的最佳区分器.

Table 5　Comparison of Statistical Fault Attacks on a Partial Subkey of AES and LED

表 5　AES 和 LED 算法统计故障分析部分子密钥结果对比

Cipher	Distinguisher	Fault Number	Latency Time/s	References
AES	SEI	80		Ref[24]
LED	SEI	68	2.5	This Paper
	GF	64	2.4	
	GF-SEI	48	1.7	

5　结束语

本文提出了针对 LED 轻量级密码算法的新型统计故障分析方法. 在半字节随机故障模型下,不仅将 Fuhr 等人的统计故障攻击思想应用于轻量级分组密码算法 LED 的安全性分析中,而且构建了 GF 区分器和 GF-SEI 双重区分器,通过 3 种区分器均可以恢复原始密钥. 相较于原有的 SEI 区分器,新型区分器从攻击效果和耗费时间上均具有较大优势. 结果表明:以 LED 为代表的轻量级密码算法易受到统计故障分析的威胁,在物联网环境实现时必须加以防护措施进行保护.

参　考　文　献

[1] Medaglia C M, Serbanati A. An overview of privacy and security issues in the Internet of things [C] //Proc of the Internet of Things. Berlin: Springer, 2010: 389-395

[2] Mayer C P. Security and privacy challenges in the Internet of things [J]. Electronic Communications of the Easst, 2009, 17(3): 11-22

[3] Ning Huangsheng, Liu Hong, Yang L T. Cyberentity security in the Internet of things [J]. Computer, 2013, 46(4): 46-53

[4] Suo Hui, Wan Jiefu, Zou Caifeng, et al. Security in the Internet of things: A review [C] //Proc of the 1st Int Conf on Computer Science and Electronics Engineering. Piscataway, NJ: IEEE, 2012: 648-651

[5] Guo J, Peyrin T, Poschmann A, et al. The LED block cipher [C] //Proc of the 13th Int Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2011: 326-341

[6] Ueno R, Homma N, Aoki T. Efficient DFA on SPN-based block ciphers and its application to the LED block cipher [J]. IEICE Trans on Fundamentals of Electronics Communications & Computer Sciences, 2015, 98(1): 182-191

[7] Liu Feng, Liu Xuan, Meng Shuai. Differential fault attack and meet-in-the-middle attack on block cipher LED [J]. Advanced Materials Research, 2013, 850(1): 529-532

[8] Shanmugam D, Selvam R, Annadurai S. Differential power analysis attack on SIMON and LED block ciphers [C] //Proc of the 4th Int Conf on Security, Privacy, and Applied Cryptography Engineering. Berlin: Springer, 2014: 110-125

[9] Isa H, Z'Aba M R. Randomness analysis on LED block ciphers [C] //Proc of the 5th Int Conf on Security of Information and Networks. New York: ACM, 2012: 60-66

[10] Fujishiro M, Yanagisawa M, Togawa N. Scan-based attack on the LED block cipher using scan signatures [C] //Proc of the 20th IEEE Int Symp on Circuits and Systems. Piscataway, NJ: IEEE, 2014: 1460-1463

[11] Isobe T, Shibutani K. Security analysis of the lightweight block ciphers XTEA, LED and Piccolo [C] //Proc of the 17th Australasian Conf on Information Security and Privacy. Berlin: Springer, 2012: 71-86

[12] Nikolić I, Wang Lei, Wu Shuang. Cryptanalysis of round-reduced LED [C] //Proc of the 20th Int Workshop on Fast Software Encryption. Berlin: Springer, 2014: 112-129

[13] Soleimany H. Probabilistic slide cryptanalysis and its applications to LED-64 and Zorro [C] //Proc of the 21st Int Workshop on Fast Software Encryption. Berlin: Springer, 2014: 373-389

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

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

[16] Mendel F, Rijmen V, Toz D, et al. Differential analysis of the LED block cipher [C] //Proc of the 18th Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2012: 190-207

[17] Jeong K, Lee C. Differential fault analysis on block cipher LED-64 [G] //Future Information Technology, Application, and Service. Berlin: Springer, 2012: 26-34

[18] Li Wei, Gu Dawu, Xia Xiaoling, et al. Single byte differential fault analysis on the LED lightweight cipher in the wireless sensor network [J]. International Journal of Computational Intelligence Systems, 2012, 5(5): 896-904

[19] Li Wei, Gu Dawu, Zhao Chen, et al. Security analysis of the LED lightweight cipher in the Internet of things [J]. Chinese Journal of Computers, 2012, 35(3): 434-445
(李玮, 谷大武, 赵辰, 等. 物联网环境下 LED 轻量级密码算法的安全性分析[J]. 计算机学报, 2012, 35(3): 434-445)

[20] Jovanovic P, Kreuzer M, Polian I. A fault attack on the LED block cipher [C] //Proc of the 3rd Int Conf on Constructive Side-Channel Analysis and Secure Design. Berlin: Springer, 2012: 120-134

[21] Zhao Xinjie, Guo Shize, Zhang Fan, et al. Improving and evaluating differential fault analysis on LED with algebraic techniques [C] //Proc of the 8th Workshop on Fault Diagnosis and Tolerance in Cryptography. Piscataway, NJ: IEEE, 2013: 41-51

[22] Ji Keke, Wang Tao, Zhao Xinjie, et al. Algebraic fault attack on LED light-weight block cipher [J]. Application Research of Computers, 2013, 30(4): 1183-1186
(冀可可, 王韬, 赵新杰, 等. 轻型分组密码 LED 代数故障攻击方法[J]. 计算机应用研究, 2013, 30(4): 1183-1186)

[23] Li Wei, Zhang Wenwen, Gu Dawu, et al. Impossible differential fault analysis on the LED lightweight cryptosystem in the vehicular ad-hoc networks [J]. IEEE Trans on Dependable & Secure Computing, 2016, 13(1): 84-92

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

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

Ge Chenyu, born in 1992. Master candidate. Her main research interests include security analysis of lightweight ciphers.

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

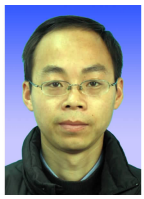
Liao Linfeng, born in 1993. Master candidate. His main research interests include security analysis of symmetric ciphers.

Gao Zhiyong, born in 1992. Master candidate. His main research interests include security analysis of symmetric ciphers.

Guo Zheng, born in 1980. PhD, lecturer. His main research interests include the design and analysis of smart cards and chips.

Liu Ya, born in 1983. PhD, lecturer. Her main research interests include the design and analysis of symmetric ciphers and computational number theory.

Liu Zhiqiang, born in 1977. PhD, associate professor. His main research interests include block chain, DAG-based distributed system, cryptanalysis and design of block ciphers and Hash functions.



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

附录 A. 实验数据及结果.

以 LED-64 算法为例.

明文:随机生成;

密钥:01 23 45 67 89 AB CD EF.

实验结果表明:通过 3 种区分器均可以恢复原始密钥,具体数据如表 A1 和表 A2 所示:

Table A1　Probability of Breaking LED Using Different Distinguishers

表 A1　不同区分器破译 LED 算法的概率

Faults	Breaking Probability/%		
	SEI	GF	GF-SEI
0	0.00	0.00	0.00
1	0.00	0.00	0.00
2	0.00	0.00	0.00
3	0.00	0.00	0.00
4	1.00	4.50	4.00
5	0.50	1.00	1.50
6	1.00	0.00	3.00
7	0.50	3.50	2.00
8	2.50	4.00	3.50
9	1.50	3.50	8.50
10	1.00	4.00	7.50
11	3.00	4.50	4.50
12	2.00	6.50	10.00
13	7.00	4.50	10.00
14	2.50	5.50	17.50
15	6.50	11.50	21.00
16	9.00	7.50	25.50
17	10.50	10.00	21.50
18	13.00	17.00	34.00
19	13.00	16.00	30.50
20	19.00	15.50	42.00
21	17.50	20.50	39.50
22	17.50	27.50	51.00
23	19.00	26.00	50.00
24	20.00	31.00	60.00
25	28.50	28.00	66.50
26	25.50	31.00	60.00
27	33.50	38.50	71.50
28	34.50	35.50	71.00
29	37.00	42.50	71.50

Continued (Table A1)

Faults	Breaking Probability/%		
	SEI	GF	GF-SEI
30	40.50	51.50	76.00
31	41.00	47.00	79.50
33	52.50	60.50	82.50
34	52.00	59.00	86.00
35	50.50	61.50	89.50
36	57.50	64.00	84.50
37	57.00	64.00	91.00
38	60.00	67.00	92.00
39	69.50	75.50	94.00
40	71.00	72.00	96.00
41	74.50	82.00	95.00
42	69.00	81.00	94.50
43	67.50	75.50	97.50
44	76.50	80.00	97.50
45	82.50	82.50	97.50
46	78.50	88.00	99.00
47	79.00	84.50	98.00
48	87.50	92.00	98.50
49	86.00	93.50	98.00
50	87.00	93.00	96.00
51	88.50	95.50	98.00
52	91.50	94.50	98.00
53	91.00	92.00	99.00
54	95.00	95.50	99.50
55	95.00	95.00	98.50
56	92.50	97.00	97.00
57	94.50	95.50	97.00
58	94.50	96.50	99.00
59	96.00	95.00	99.50
60	98.00	98.50	99.50
61	96.00	97.50	100.00
62	97.00	100.00	99.50
63	97.50	99.00	99.50
64	97.50	100.00	100.00
65	97.00	99.00	100.00
66	98.00	99.00	100.00
67	98.00	99.00	99.00
68	99.50	99.50	99.50
69	98.50	99.50	100.00
70	99.00	99.00	100.00

Table A2 Time of Breaking LED Using Different Distinguishers

表 A2 不同区分器破译 LED 算法的耗费时间

Faults	Latency Time/s		
	SEI	GF	GF-SEI
0	0	0	0
1	0.04	0.04	0.05
2	0.07	0.07	0.08
3	0.10	0.11	0.11
4	0.13	0.14	0.15
5	0.17	0.17	0.18
6	0.20	0.21	0.21
7	0.24	0.25	0.25
8	0.27	0.28	0.29
9	0.30	0.31	0.32
10	0.35	0.35	0.36
11	0.38	0.39	0.40
12	0.42	0.42	0.43
13	0.45	0.45	0.46
14	0.49	0.49	0.50
15	0.53	0.53	0.54
16	0.56	0.57	0.58
17	0.60	0.61	0.62
18	0.63	0.64	0.65
19	0.67	0.68	0.68
20	0.71	0.72	0.73
21	0.75	0.76	0.76
22	0.78	0.80	0.80
23	0.82	0.84	0.84
24	0.86	0.87	0.87
25	0.90	0.91	0.91
26	0.93	0.95	0.95
27	0.97	0.99	0.99
28	1.01	1.03	1.03
29	1.04	1.06	1.06
30	1.08	1.10	1.10
31	1.12	1.14	1.14
32	1.16	1.18	1.18
33	1.20	1.22	1.22
34	1.24	1.26	1.25

Continued (Table A2)

Faults	Latency Time/s		
	SEI	GF	GF-SEI
35	1.28	1.30	1.29
36	1.31	1.34	1.33
37	1.35	1.37	1.36
38	1.39	1.42	1.41
39	1.42	1.45	1.44
40	1.46	1.49	1.48
41	1.50	1.53	1.52
42	1.54	1.58	1.57
43	1.57	1.60	1.59
44	1.62	1.65	1.64
45	1.66	1.69	1.68
46	1.69	1.72	1.71
47	1.73	1.76	1.75
48	1.77	1.81	1.79
49	1.79	1.83	1.82
50	1.85	1.89	1.88
51	1.88	1.92	1.91
52	1.93	1.97	1.95
53	1.96	2.01	1.99
54	2.00	2.05	2.03
55	2.05	2.09	2.08
56	2.07	2.11	2.10
57	2.12	2.17	2.15
58	2.15	2.21	2.18
59	2.20	2.25	2.23
60	2.24	2.29	2.26
61	2.28	2.33	2.31
62	2.29	2.34	2.33
63	2.34	2.40	2.38
64	2.37	2.43	2.41
65	2.40	2.45	2.45
66	2.45	2.50	2.49
67	2.49	2.53	2.53
68	2.52	2.58	2.57
69	2.57	2.61	2.61
70	2.60	2.65	2.65