电子数据取证中LED加密系统的积分故障分析

王 弈
(华东政法大学信息科学与技术系 上海 201620)

摘 要 在电子数据取证领域,取证与反取证技术的较量不断升级。数据加密技术是反取证技术的一个重要研究分支。为了在这场较量中占有先机,文中重点研究了物联网领域中所采用的LED轻量级密码算法,通过分析LED算法的加、解密过程,引入积分故障分析对其进行安全性分析,提出了一种破解LED密码算法的积分故障分析方法。积分故障分析主要利用同一明文正常加密输出的密文与注入故障后产生的密文之间的差异,通过在加密过程中注入随机故障获得故障密文;并通过一个积分故障识别器,恢复最后一轮的子密钥值,进而获得最后一轮的加密输入,它是倒数第二轮的输出。重复上述过程,直到加密密钥可以通过密钥生成算法获得。在上述推导的基础上进行实验仿真测试,从精确度、可靠性和时间复杂度3个方面证明了积分故障分析方法可以在有效时间内通过构造一个基于半字节故障模型的3轮故障识别器来实现破解过程。该方法可以为破解AES类轻量级加密算法提供参考与借鉴。

关键词 积分故障分析,电子数据取证,反取证

中图法分类号 TP393.09 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2019.08.031

Integral Fault Analysis on LED Cryptosystem in Digital Data Forensic

WANG Yi
(Department of Information Science and Technology, East China University of Political Science and Law, Shanghai 201620, China)

Abstract The competition between digital data forensic and anti-forensic is upgrading day by day. Data encryption is an important research field in anti-forensic technology. In order to have the lead in the competition, this paper mainly studied LED cryptosystem widely used in IoT field. Through analyzing encryption and decryption process of LED algorithm, integral fault analysis was introduced to test security attribute of LED algorithm, and a method of breaking LED cryptosystem was proposed by integral fault analysis attacking. Integral fault analysis mainly uses difference between ciphertext outputted by normal encryption of the same plaintext and ciphertext generated after injection failures. The attackers induce random errors in some rounds of the encryption, and thus obtain faulty ciphertexts. By constructing an integral distinguisher, the attackers can recover the value of the last subkey. Then they can decrypt the right ciphertext to obtain the input of the last round, which is the output of the penultimate round. At last, they repeat the above procedure to induce more faults until the secret key is obtained by the key schedule. Then through mathematical proof and experimental proof from accuracy, reliability and time latency, this paper drew the conclusion that integral fault analysis attacking can break LED cryptosystem by constructing a three-round fault distinguisher in a half byte-oriented fault model. This attacking method can provide more reference of AES-like lightweight cryptosystems.

Keywords Integral fault analysis, Digital data forensic, Anti-forensic

1 概述

随着电子数据取证技术的日新月异,反取证技术也在不断更新与升级,其中数据加密技术是反取证技术的一个重要研究分支。对通信数据、电子文档以及可能在呈堂时对自身不利的电子数据进行加密传输和存储,是犯罪分子对抗网络侦查、电子数据取证的利器之一。加密技术本身并没有好坏之分,但对其的不同利用动机会导致截然相反的结果。

在信息技术高速发展的今天,信息安全问题受到的关注程度越来越高,相应的反侦察、反取证手段也水涨船高。经验老道的信息犯罪者可以熟练采用数据擦除、粉碎、加密以及反追踪技术,来逃脱应有的惩罚。作为电子数据取证的工作者和研究人员,在飞速发展的科技环境下,需要不断更新取证技术和装备,只有保持科技领先优势,才能在取证与反取证的这场持久战中占领先机。

鉴于此,本文通过研究加密技术的破解方法,以期在取证与反取证的对抗中突破犯罪嫌疑人利用加密技术保护的重要电子数据,为及时侦破案件提供技术上的支持。本文重点研究了物联网领域中采用的LED轻量级密码算法[1]。该算法在2011年CHES会议上被提出,主要用于保护RFID标签和

到稿日期:2018-10-13 返修日期:2018-12-21 本文受国家社会科学基金项目(13CFX054)资助。

王 弈(1974—),女,教授,硕士生导师,主要研究方向为信息安全与信息法学,E-mail:wangyi@ecupl.edu.cn。

智能卡等嵌入式设备的通信安全。与传统密码算法相比，LED算法具有能耗低、实现简单、安全强度高的优点，更适合计算能力弱、存储空间受限以及能源储备有限的物联网组件。与其他轻量级密码算法相比，其实现效率更高，环境适应能力更强，是众多轻量级密码算法中的佼佼者，因而成为嵌入式、便携式等受限设备与终端的选择。

物联网作为互联网技术的延伸与发展，是目前信息化社会的典型代表之一，正逐步渗透到人们的社会生活与日常生活之中。攻击与破坏物联网的犯罪行为成为信息犯罪领域的一个新方向。目前，物联网技术在环境检测、食品安全、智能交通和现代化物流等领域中应用得较为普遍，而上述领域对于维持人们正常的生产生活有着重要的作用。

本文通过引入积分故障分析，干预LED密码变换的正常运行，从而恢复出密码所采用的全部或部分密钥，以达到破解密码系统的目的。故障攻击是旁路攻击的一种类型，它最早由Boneh等于1996年提出，首先应用于基于RSA加密过程的密码分析中[2-3]。此后，各种各样的故障分析技术被提出，主要有差分故障分析、碰撞故障分析、不可能故障分析、中间相遇故障分析等[4-8]。这些技术在数学分析的帮助下放大和估算泄露的信息，通过差分、碰撞、中间相遇等检测手段，基于正确操作和加密结果之间的关系以及故障操作和加密结果之间的关系来获得密钥信息[9-16]。

积分故障分析最先应用于AES算法，AES算法与LED算法采用了相同的SPN结构[17]，但是构造一个破解LED算法的积分故障分析器比构造破解AES算法的积分故障分析器更加困难。因为AES算法的最后一轮加密过程包括3部分变换：字节替换、行位移变换、轮密钥加。攻击者可以通过逆变换这一轮的字节替换、行位移变换和轮密钥加来减少最后一轮子密钥和故障之间的积分关系。根据故障的特征，倒数第二轮的列混淆(MixCloumnSerial)的输出值之和为零，攻击者可以独立地推导每一个字节的可能值，进而计算出最后一轮子密钥的所有可能值，来确定最后一轮的子密钥。然而，对于LED算法，每一轮加密过程都是由常数加(AddConstants)、子信元变换(Sublells)、行移位变换和列混淆4部分构成。为了获得最后一轮的子密钥，在积分关系中必须考虑计算最后一轮的列混淆。由于子信元变换和行移位变换的混淆与扩散作用，列混淆中每一列的值相互之间均有关系。因此，为了计算最后一轮的子密钥，采用上述类似AES算法的积分故障分析方法将变得更加复杂。

本文为破解LED算法构造了一个积分故障识别器，随机将错误引入到加密过程的轮数中。对于一个3轮的积分故障识别器，最后一轮的子密钥可以被恢复。之后，可以解密该轮的密文，获得最后一轮加密的输入，它是倒数第二轮的加密输出。上述过程可以重复进行，以恢复更多轮的子密钥，从而通过密钥生成算法获得密钥。

2 LED密码算法简介

LED算法是一个基于SPN结构的轻量级分组加密算法[1]。它支持64位和128位密钥长度，分别对应32轮和48轮加密过程。整个算法包括加密、解密和密钥生成3个部分，如图1所示。其中，X表示输入的明文；Y表示输出的密文；K_1和K_2是密钥K的子密钥。

加密过程可以表示为以4比特信元为单位的4×4的矩阵阵列的状态转移过程，矩阵阵列的转换结果称为状态。每一轮，状态转移矩阵会与这一轮的子密钥进行异或(XOR)操作，称之为轮密钥加(AddRoundKey)，然后执行这一轮的4个变换步骤，即常数加、子信元变换、行移位变换和列混淆。其中，常数加即将状态矩阵与常数相异或(XOR)；子信元变换即将状态矩阵中的半字节分别应用S盒操作，进行非线性变换；行移位变换即将状态矩阵的后三行分别进行不同偏移量的行位移；列混淆即对状态矩阵中所有列进行混合计算，生成新的列。

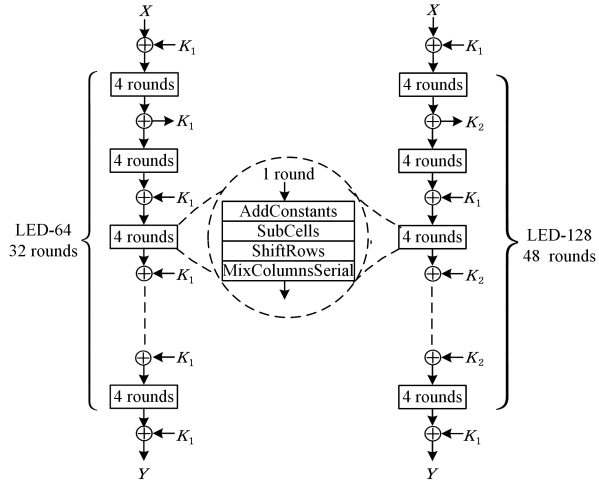

图1 LED算法的结构

Fig. 1 Structure of LED algorithm

为了后续论述的统一性，在此将本文中用到的符号及其含义一并说明如下：

A_r, B_r, C_r, D_r从左到右依次表示第r轮加密中常数加、子信元变换、行移位变换和列混淆的输出值，其中$1\leqslant r\leqslant 1$。

AC, SC, SR, MC从左到右依次表示常数加、子信元变换、行移位变换和列混淆操作。

$AC^{-1}, SC^{-1}, SR^{-1}, MC^{-1}$从左到右依次表示常数加、子信元变换、行移位变换和列混淆的逆变换。

LED密码算法的解密过程与加密过程相同，解密时子密钥的使用顺序也与加密过程相同。每一轮的子密钥由密钥输入到密钥生成器而获得。

在64位密钥的LED算法中，密钥与子密钥的关系如下：

$K_1=K_2$

在128位密钥的LED算法中，密钥与子密钥的关系为：

$K=K_1 \parallel K_2$

3 LED密码算法的积分故障分析

3.1 故障模型和基本假设

积分故障分析主要利用同一明文正常加密输出的密文与注入故障后产生的密文之间的差异。本文提出的故障模型基于以下两个假设：

1)攻击者能够选择明文加密，并能获得相应的正确加密后的密文以及故障密文(选择明文攻击CPA)。

2)攻击者可以将 4 位故障注入到加密变换的其中一层。攻击过程中可以控制故障,在同一故障位置注入故障的值可以控制在 $0\sim2^4-1$ 的取值范围之内。然而这一层的出错位置和每个故障注入点的具体错误值都是未知的。对于故障攻击而言,在加密接近完成的位置进行故障分析,并假设符合通用随机故障模型,即故障以随机方式修改加密过程中的数据。对轻量级密码算法进行攻击的一个直观方式是破坏它的密钥生成器。实际上,LED 算法采用了一种简单方式计算子密钥,对 64 位密钥而言,子密钥等于加密密钥,且子密钥只有一个。对 128 位密钥而言,加密密钥分解为两个子密钥,加密密钥的前半部分为子密钥 K_1,后半部分为子密钥 K_2。因此,本文的故障分析将重点放在对 LED 算法中加、解密部分的算法的安全性分析上。

3.2　破解基本思想

本文破解过程的主要思想如下:当明文用加密密钥加密时,要获得其对应的正确密文。攻击者在加密的一些轮中注入随机故障,获得故障密文。通过构造一个积分故障识别器,攻击者可以恢复最后一轮的子密钥值。于是可以解密正确的密文获得最后一轮的加密输入,它是倒数第二轮的输出。最后,攻击者重复上述过程,并将更多故障注入到加密过程中,直到加密密钥可以通过密钥生成算法获得。

3.3　LED 密码算法的积分故障分析

本节基于上述基本思想与观点提出了一个积分故障分析方法来破解 64 位和 128 位密钥长度的 LED 加密算法。对于 LED 密码系统而言,如果第一轮的输入只有 1 个 4 比特主动信元(active cell),其他 3 个都是 4 比特被动信元(passive-cell),那么到第三轮,加密输出的所有 4 比特信元都满足平衡等式。如图 2 所示,故障位置和子密钥的破解在 5 轮加密范围之内。

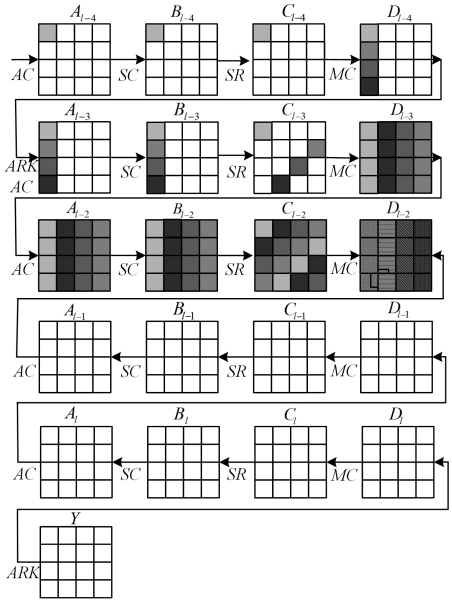

图 2　最后 5 轮加密中积分故障分析的攻击路径

Fig. 2　Attacking paths of integral fault analysis in the last 5 rounds

步骤 1　获得随机明文 X 用加密密钥加密后的密文 Y。

步骤 2　在这一阶段,攻击旨在破解最后一轮加密所使用的子密钥 K_1,分析加密过程可知:

$$D_l=Y\oplus K_1$$

$$\begin{aligned}D_{l-1}&=AC^{-1}(SC^{-1}(SR^{-1}(MC^{-1}(D_l))))\\&=AC^{-1}(SC^{-1}(SR^{-1}(MC^{-1}(Y\oplus K_1))))\\&=AC(SC^{-1}(SR^{-1}(MC^{-1}(Y\oplus K_1))))\\&=AC(SC^{-1}(Y'\oplus K_1'))\end{aligned}$$

其中:

$$Y'=SR^{-1}(MC^{-1}(Y))$$

$$K_1'=SR^{-1}(MC^{-1}(K_1))$$

攻击者在第 $l-4$ 轮中注入随机故障,并且获得相对应的错误密文。如图 2 所示,故障可以注入到 A_{l-4},B_{l-4} 或 C_{l-4} 中,在其他轮中,攻击方式也是一样的。对半字节信元信息的任何修改都会引发差分:ΔD_{l-4} 与 D_{l-4},ΔA_{l-3} 与 A_{l-3},ΔB_{l-3} 与 B_{l-3},ΔC_{l-3} 与 C_{l-3},ΔD_{l-3} 与 D_{l-3},ΔA_{l-2} 与 A_{l-2},ΔB_{l-2} 与 B_{l-2},ΔC_{l-2} 与 C_{l-2},ΔD_{l-2} 与 D_{l-2},ΔA_{l-1} 与 A_{l-1},ΔB_{l-1} 与 B_{l-1},ΔC_{l-1} 与 C_{l-1},ΔD_{l-1} 与 D_{l-1},ΔA_l 与 A_l,ΔB_l 与 B_l,ΔC_l 与 C_l。这将原始的正确密文修改成了注入故障后的错误密文。攻击者可以随机选取一个位置,通过激光、X 射线或微荧光检测等手段在 $0\sim15$ 取值范围内控制半字节故障值。对同一位置而言,只有一个正确密文,其他 15 个均为错误密文。因而对于每组 D_{l-2} 的取值而言,其满足以下等式:

$$\begin{aligned}\bigoplus_{u=0}^{15}D_{l-2}^{(u)}&=\bigoplus_{u=0}^{15}AC^{-1}(SC^{-1}(SR^{-1}(MC^{-1}(D_{l-1}^{(u)}))))\\&=\bigoplus_{u=0}^{15}AC(SC^{-1}(SR^{-1}(MC^{-1}(AC(SC^{-1}(Y'^{(u)}\oplus K_1'))))))\\&=0\end{aligned}$$

其中:

$$Y'^{(u)}=SR^{-1}(MC^{-1}(Y^{(u)}))$$

$$K_1'=SR^{-1}(MC^{-1}(K_1))$$

且 $0\leqslant u\leqslant15$。上述等式中的 MC^{-1} 操作通过穷举搜索 16 位 K_1' 所有可能的取值而获得。穷举搜索的值需要满足以下等式:

$$\begin{cases}\bigoplus_{u=0}^{15}AC(SC^{-1}(SR^{-1}(MC^{-1}|_i(AC(SC^{-1}(Y'^{(u)}_{4i}\oplus K'_{1,4i})))))=0\\\bigoplus_{u=0}^{15}AC(SC^{-1}(SR^{-1}(MC^{-1}|_i(AC(SC^{-1}(Y'^{(u)}_{4i+1}\oplus K'_{1,4i+1})))))=0\\\bigoplus_{u=0}^{15}AC(SC^{-1}(SR^{-1}(MC^{-1}|_i(AC(SC^{-1}(Y'^{(u)}_{4i+2}\oplus K'_{1,4i+2})))))=0\\\bigoplus_{u=0}^{15}AC(SC^{-1}(SR^{-1}(MC^{-1}|_i(AC(SC^{-1}(Y'^{(u)}_{4i+3}\oplus K'_{1,4i+3})))))=0\end{cases}$$

其中,i 表示状态矩阵的第 i 列,取值范围为 $0\leqslant i\leqslant3$。

攻击者穷举搜索每个 4 比特 K_1' 的可能值。可以通过重复上述方法获取由同一加密密钥生成的不同明文的正确和错误密文对来减少 K_1' 的穷举空间,直到 K_1' 的候选值只有一个。然后根据推测出的 K_1',子密钥 K_1 的值可以通过下式推演得到:

$$K_1=MC(SR(K_1'))$$

若加密密钥为 64 比特长，则跳转到步骤 4；否则（密钥长度为 128 比特），跳转到步骤 3。

步骤 3　在恢复了子密钥 K_1 之后，攻击者可以执行相似的步骤来破解子密钥 K_2。假设故障注入到第 $l-8$ 轮，攻击者可以通过 K_1 解密正确密文获得倒数第 4 轮的输入 $AC^{-1}(A_{l-3})\oplus K_2$，这是倒数第 5 轮的输出。

$$\begin{aligned}\bigoplus_{u=0}^{15} D_{l-6}^{(u)} &= \bigoplus_{u=0}^{15} AC^{-1}(SC^{-1}(SR^{-1}(MC^{-1}(D_{l-5}^{(u)}))))\\ &= \bigoplus_{u=0}^{15} AC(SC^{-1}(SR^{-1}(MC^{-1}(AC(SC^{-1}(A'^{(u)}_{l-3}\oplus K_2')))))))\\ &= 0\end{aligned}$$

其中，

$$A'^{(u)}_{l-3} = SR^{-1}(MC^{-1}(A^{(u)}_{l-3}))$$

$$K_2' = SR^{-1}(MC^{-1}(K_2))$$

且 $0\leqslant u\leqslant 15$。通过以下等式来穷举 K_2'：

$$\begin{cases}\bigoplus_{u=0}^{15} AC(SC^{-1}(SR^{-1}(MC^{-1}|_i(AC(SC^{-1}(A'^{(u)}_{l-3,4i}\oplus K'_{2,4i})))))) = 0\\ \bigoplus_{u=0}^{15} AC(SC^{-1}(SR^{-1}(MC^{-1}|_i(AC(SC^{-1}(A'^{(u)}_{l-3,4i+1}\oplus K'_{2,4i+1})))))) = 0\\ \bigoplus_{u=0}^{15} AC(SC^{-1}(SR^{-1}(MC^{-1}|_i(AC(SC^{-1}(A'^{(u)}_{l-3,4i+2}\oplus K'_{2,4i+2})))))) = 0\\ \bigoplus_{u=0}^{15} AC(SC^{-1}(SR^{-1}(MC^{-1}|_i(AC(SC^{-1}(K'_{2,4i+3}\oplus K'_{2,4i+3})))))) = 0\end{cases}$$

其中，$0\leqslant i\leqslant 3$。

攻击者可以计算列混淆变换 D_{l-6} 的和，并对 K_2' 的每 4 位进行穷举。根据上述等式穷举获得 K_2'，再通过下式推演出子密钥 K_2：

$$K_2 = MC(SR(K_2'))$$

步骤 4　根据密钥生成算法，64 比特密钥长的 LED 算法中 $K_1=K_2$，128 比特密钥长的 LED 算法中 $K=K_1\parallel K_2$，从而可以得到秘密密钥 K。

4　实验仿真

采用软件模拟故障注入，在一台具有 32 GB 内存、支持 JAVA 语言的 PC 机上运行攻击算法。在此环境下，运行 1000 次攻击算法。

在实践中，估算故障密文数量和攻击复杂度尤为重要，因为注入的故障数越少，攻击者的破解密码算法的成功概率越大。当故障分析攻击复杂度在实践中容易被实现时，例如在 PC 机上，则认为该攻击是一次成功的破解。在轻量级密码应用中，在攻击者获得正确密文和故障密文后，密钥恢复过程推荐在 PC 机环境下实现。

整个攻击过程中，破解子密钥或主密钥所需要的故障数取决于所采用的故障模型和故障注入的位置。为了计算平衡信元的总和，攻击者至少需要一组密文，其中包括 1 个正确密文和 15 个故障密文。本文将通过精度、可靠性和延时性 3 方面的特性来详细评价实验结果。图 3 表示不同的候选子密钥的交集示意图。

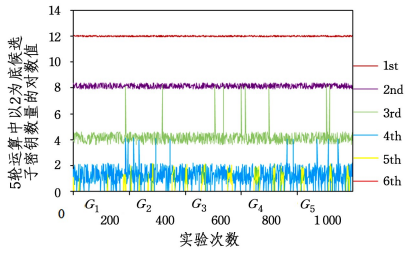

图 3　不同候选子密钥的交集

Fig. 3　Intersections of subkeys candidates

图 3 中，横轴表示实验的次数，纵轴表示以 2 为底候选密钥数的对数值，彩色的线条表示以 2 为底候选密钥数的对数值的 6 个交集。由实验数据可知，随着故障注入的次数增加，候选密钥集合的范围逐渐缩小，直到最终候选密钥可以被确定为止。

4.1　实验精确度

精确度（准确度）用于衡量候选密钥数与真实密钥数的接近程度。通常，候选密钥数越接近真实密钥数，实验结果越精确。因此，这里考虑采用均方根误差（Root Mean Squared Error，RMSE）来衡量实验精确度，RMSE 的定义如下：

$$RMSE = \sqrt{\frac{1}{m}\sum_{e=1}^{m}[\phi(e)-\phi']}$$

其中，m 为实验次数，e 是自然对数的底，$\phi(e)$ 是候选密钥的数量，ϕ' 是真实子密钥的数量。众所周知，这里只有一个真正的子密钥，因此 $RMSE$ 值越接近 0，说明实验越精确。1000 次实验被均分为 5 组，分别用 G_1，G_2，G_3，G_4 和 G_5 表示。表 1 列出了候选子密钥交集的 $RMSE$ 值。其中，$m=200$，$\phi=1$，$e\in\{1,\cdots,1000\}$。此外，精度值在每组的相同互操作是相同或相似的，因此恢复一个子密钥的最大密文数量为 6。

表 1　基于 RMSE 计算的子密钥恢复的精确度

Table 1　Accuracy of recovered subkey based on RMSE

组别	第 1 组	第 2 组	第 3 组	第 4 组	第 5 组	第 6 组
G_1	63.85	15.92	4.13	1.01	0.19	0
G_2	63.86	16.00	4.12	1.20	0.32	0
G_3	63.84	15.93	4.27	1.16	0.31	0
G_4	63.83	16.03	4.46	1.16	0.35	0
G_5	63.86	15.89	4.28	1.17	0.27	0

4.2　实验可靠性

可靠性是实验成功次数与所有实验次数的比值。若攻击者能获得一个密钥，那么实验就是成功的。根据表 2，第 1 组－第 6 组的候选子密钥交集中实验成功率的平均值分别为 0，0，0，36.7%，92.3%和 100%。

表 2　恢复子密钥的可靠性指标

Table 2　Reliability of subkey recovery

（单位：%）

组别	第 1 组	第 2 组	第 3 组	第 4 组	第 5 组	第 6 组
G_1	0	0	0	42.0	96.5	100
G_2	0	0	0	37.0	90.0	100
G_3	0	0	0	30.0	91.5	100
G_4	0	0	0	37.5	90.5	100
G_5	0	0	0	37.0	93.0	100

由此可知,如果攻击者想要 100%成功恢复出一个子密钥,则其需要引入 6 组随机故障才能确保万无一失。

4.3　时间复杂度

时间复杂度是指在软件模拟过程中,从注入第一个故障到恢复出子密钥所需的时间。图 4 展示了 1000 次实验的时间复杂度,所有实验均在 6s 内产生结果。

在第 5 轮攻击中,用于恢复 64 位和 128 位密钥的最大攻击时间复杂度分别为:

$$6 \cdot 2^{16} \cdot 2^{4} \cdot 4 \cdot 4 \approx 2^{26.59}$$

$$12 \cdot 2^{16} \cdot 2^{4} \cdot 4 \cdot 4 \approx 2^{27.59}$$

由时间复杂度可知积分故障分析在实际攻击中的可行性。即使遇到最坏情形,即攻击所需的时间为最长攻击时间,其所花费的时间也在可接受的范围之内。

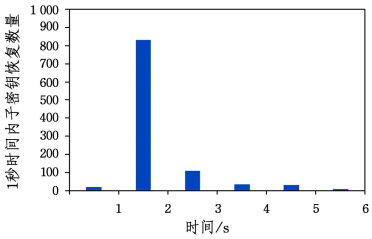

图 4　子密钥恢复的时间复杂度

Fig. 4　Complexity of subkey recovery

结束语　本文提出了一种破解 LED 轻量级加密算法的积分故障分析方法。根据数学分析和实验结果可知,积分故障分析可以通过构造一个基于半字节故障模型的 3 轮故障识别器完全破解 LED 密码系统。由此可见,LED 密码系统对于积分故障分析而言是脆弱的。此外,故障注入能够覆盖到 LED 加密算法的最后 5 轮中,它们是对 LED 算法进行故障分析至今所能达到的最深层次。

通过本文研究希望能为 AES 类轻量级加密系统的安全分析提供参考与借鉴。

参 考 文 献

[1] GUO J,PEYRIN T,POSCHMAN N A,et al. The LED Block Cipher[C]// International Workshop on Cryptographic Hardware and Embedded Systems. Springer,2011:326-341.

[2] BONEHD,DEMILLOR A,LIPTON R J,et al. On the Importance of Checking Cryptographic Protocols for Faults[C]// International Conference on the Theory and Applications of Cryptographic Techniques. 1997:37-51.

[3] BONEHD,DEMILLO R A,LIPTON R J. On the Importance of Eliminating Errors in Cryptographic Computations [J]. Journal of Cryptology,2001,14(2):101-119.

[4] JEONG K,LEE C. Differential Fault Analysis on Block Cipher LED-64 [J]. Future Information Technology, Application, and Service,2012,55(1/2):747-775.

[5] LI W,GU D,XIA X,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.

[6] JOVANOVIC P,KREUZER M,POLIAN I. A Fault Attack on the LED Block Cipher[C]// International Workshop on Constructive Side-Channel Analysis and Secure Design. 2012:120-134.

[7] ZHAO X,GUO S,ZHANG F,et al. Improving and Evaluating Differential Fault Analysis on LED with Algebraic Techniques [C]// Workshop on Fault Diagnosis and Tolerance in Cryptography. 2013:41-51.

[8] LI W,ZHANG W,GU D,et al. Impossible Differential Fault Analysis on the LED Lightweight Cryptosystem in The Vehicular Ad-hoc Networks [J]. IEEE Transactions on Dependable & Secure Computing,2016,13(1):84-92.

[9] YANG Y,CAI H,WEI Z,et al. Towards Lightweight Anonymous Entity Authentication for IoT Applications[C]// Proceedings of 21st Australasian Conference on Information Security and Privacy. 2016:265-280.

[10] BANIK S,BOGDANOV A,ISOBE T,et al. Regazzoni,Midori: ABlockCipher for Low Energy[C]// International Conference on the Theory and Application of Cryptology and Information Security. 2015:411-436.

[11] BEAULIEU R,SHORS D,SMITH J,et al. The SIMON and SPECK Lightweight Block Ciphers[C]// Design Automation Conference. 2015:1-6.

[12] CARLET C,GUILLEY S. Statistical properties of side-channel and fault injection attacks using coding theory [J]. Cryptography and Communications,2018,10(5):909-933.

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

[14] ZHAO X J,ZHANGF,GUO S Z,et al. Optimal model search for hardware-trojan-based bit-level fault attacks on block ciphers [J]. Science China Information Sciences,2018,61(3):039106:1-039106:3.

[15] ZHANG X J,FENG X T,LIN D D. Fault Attack on ACORN v3 [J]. The Computer Journal,2018,61(8):1166-1179.

[16] SALAM M I,SIMPSON L,BARTLE T T H,et al. Fault Attacks on the Authenticated Encryption Stream Cipher MORUS [J]. Cryptography,2018,2(1):4.

[17] WANG R Y,MENG X H,LI Y,et al. Towards Optimized DFA Attacks on AES under Multibyte Random Fault Model [J]. Security and Communication Networks,2018,3(5):15-23.