基于碰撞模型的 LED 代数旁路攻击*

冀可可, 王 韬, 赵新杰, 刘会英
(军械工程学院 信息工程系, 石家庄 050003)

摘 要: 针对轻型分组密码 LED 提出了一种基于碰撞模型的代数旁路攻击。利用代数攻击方法建立密码算法等效布尔代数方程组,采集算法运行中泄露的功耗信息并转换为碰撞信息,并将碰撞信息转换成额外方程组,从而利用 CryptoMiniSAT 解析器求解密钥。实验结果表明:旁路碰撞信息可有效降低方程组求解的复杂度;已知明文条件下,利用 2 轮最少 50% 的随机碰撞信息,即可在 158.5 s 内恢复 64 bit LED 完整密钥。此外,该方法也可用于其他分组密码功耗碰撞分析。

关键词: 代数旁路攻击; 碰撞模型; LED; 可满足性解析器
中图分类号: TP309.08 **文献标志码**: A **文章编号**: 1001-3695(2013)01-0270-03
doi:10.3969/j.issn.1001-3695.2013.01.069

Collision model-based algebraic side-channel attack on LED

JI Ke-ke, WANG Tao, ZHAO Xin-jie, LIU Hui-ying
(*Dept. of Information Engineering, Ordnance Engineering College, Shijiazhuang* 050003, *China*)

Abstract: This paper proposed a collision model-based algebraic side-channel attack on lightweight block cipher LED. Firstly, it described the algebraic representations of LED. Secondly, it measured the power leakages of LED on ATMEGA324P microcontroller by a digital oscilloscope, and transformed to deduce collision. Finally, the collision was expressed as algebraic equations, and it applied the CryptoMiniSAT solver to solve for the key. Experiments demonstrate that the collision of side-channel information can introduce new algebraic equations into attack, reduce the complexity of solving equations; in the known-plaintext scenario, 2 rounds collision information is enough to recover the 64 bit LED master key in 158.5 s. The proposed method can be applied into the collision-based power attack of other block ciphers.

Key words: algebraic side-channel attack; collision model; LED; satisfiability solver

分组密码作为现代密码学的一个重要组成部分,对于保障信息安全有重要意义。随着信息技术和电子元器件的发展,密码设备逐渐轻型化,如何在 RFID 标签等轻型的密码设备上实现密码算法成为分组密码研究的新热点。轻型分组密码由于其在资源受限的应用环境下的特殊性,其安全性研究不容忽视。本文以 LED 轻型分组密码[1]为研究对象。

代数旁路攻击[2,3]将代数攻击[4]和旁路攻击[5]相结合,利用代数攻击建立密码算法明文和密钥的联立代数方程组,再将通过旁路攻击手段获取到的泄露信息代入方程组帮助求解。这种结合克服了代数攻击求解方程组复杂度高的缺陷,弥补了旁路攻击所需样本量大、旁路信息利用率低、分析轮数少、适用性较差等不足,是数学分析方法与旁路攻击发展的必然结果。代数旁路攻击可以在未知明密文的情况下恢复密钥,有时只需一个样本就能恢复密钥,对于一些加入防御措施的密码实现也能成功实现攻击,给分组密码特别是轻型分组密码造成了严重的安全威胁。如何基于代数旁路攻击进行高效的密钥恢复具有重要的理论价值及现实意义。功耗碰撞信息作为旁路信息的一种用于密码分析,最早由 Wiemers 等人[6]在 2001 年针对硬件实现的 ECC 进行攻击时使用,Schramm 于 2003 年首次将基于碰撞模型的功耗攻击应用于分组密码[7,8]。

本文以 LED 轻型分组密码为攻击对象,基于碰撞模型,通过采集微控制器上 LED 算法执行过程中的功耗泄露,使用 Pearson 相关系数[9]方法将加密中间状态的功耗值进行匹配并转换为代数方程组,在此基础上使用 CryptoMiniSAT 可满足性解析器[10]进行密钥求解。

1 基于碰撞模型的代数旁路攻击原理

1.1 碰撞模型

碰撞本义指两个或多个不同的东西在某点相遇,引申为某些性质相同。在分组密码代数旁路攻击中,如果算法运行时任意两个或多个中间状态的值相同,即为发生一次碰撞。将该碰撞信息转换为等式后可扩充算法的代数方程组,降低密钥的求解复杂度。

实际攻击中中间值的碰撞可以通过旁路信息的泄露表现出来,如功耗。密码设备运行时的功耗不仅与密码设备相关,还与处理的数据紧密相关。给定一条密码算法运行时的功耗曲线,通过对多轮 S 盒输出的某两个中间值(LED 为半字节)对应的功耗轨迹进行相关性匹配,计算功耗轨迹之间的相关性系数,从而推断这两个中间值是否发生碰撞。

图 1 所示的碰撞模型给出了对算法运行中的任意两个中间状态进行碰撞捕获和利用的过程。其中,m 为状态矩阵, i j

收稿日期: 2012-05-15; **修回日期**: 2012-06-25 **基金项目**: 国家自然科学基金资助项目(61173191)

作者简介:冀可可(1988-),女,河南上蔡人,硕士,主要研究方向为分组密码代数旁路分析(jackqui@163.com);王韬(1964-),男,教授,博导,博士,主要研究方向为信息安全和密码学;赵新杰(1986-),男,博士,主要研究方向为网络安全和密码分析学;刘会英(1984-),男,博士,主要研究方向为图像加密和密码旁路分析.

表示轮数。以相邻两轮的 S 盒输出为例,对功耗曲线中的相应部分进行相关性匹配,匹配成功后可以获取碰撞信息,捕获到的碰撞信息可以转换为代数方程。

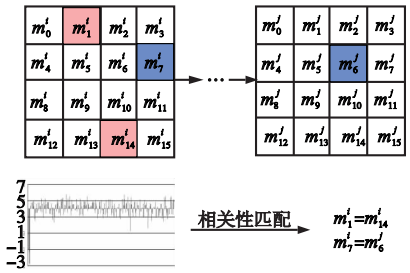

图1　基于功耗的碰撞模型

1.2　攻击原理

代数旁路攻击一般可分为三个步骤:

a)密码算法方程组表示。将密码算法表示为关于明文、密钥、中间变量、密文的代数方程组。在 LED 算法代数方程组构造过程中,最为关键的部分是如何构造非线性部件 S 盒的代数方程组。

b)旁路泄露采集及利用。给定一个密码算法的代数方程组,密钥恢复等价于代数方程组求解。直接进行代数方程组求解是一个 NP 难题,故需要利用旁路泄露信息降低方程组复杂度。攻击者可以根据待攻击密码的实现平台和自身的测量能力来选取一个旁路泄露模型 M,然后采集旁路泄露信息 L,根据泄露模型 M 将 L 转换为加密中间状态 D,最后将 D 使用额外的代数方程组表示出来。本文 LED 代数旁路攻击基于碰撞模型,采集的旁路泄露信息为功耗信息。

c)代数方程组求解。将前面建立的密码算法方程组与旁路泄露代数方程组联立起来进行方程组求解。目前,典型的代数方程组求解主要包括基于可满足性问题求解、线性化以及 Gröbner 基等方法。本文基于可满足性(SAT)问题求解方法进行代数方程组求解,首先将方程组转换为 SAT 问题,然后利用 SAT 解析器进行密钥求解。本文选用 CryptoMiniSAT 解析器作为求解代数方程组的工具。

2　LED 代数方程组构建

2.1　算法分析

LED 轻型分组密码采用了 SPN 结构,其实现只需 966 个门电路,是同类分组密码中最少的。由于它的结构特点可以导出很多类似 AES 的定理,其抗差分、线性、代数攻击能力极强,但在算法设计时并没有考虑抗代数旁路攻击的能力,对其进行代数旁路攻击对安全性评估及防护有重要的意义。

LED 算法分组长度为 64 bit,支持 64/128 bit 的密钥长度,加密轮数为 32 轮。本文中 LED 分组密码均指 64 bit 密钥的算法。算法第 1 轮前进行一次轮密钥加,以后每 4 轮进行一次,即全轮共有九次轮密钥加操作。为了提高加密速度及减小硬件实现规模,采取无密钥生成的策略,轮密钥即为初始密钥。算法的状态矩阵为 GF(2^4)上的 4 × 4 的矩阵,每个元素为 4 bit。每轮有轮常量加、S 盒、行移位和列混淆四个步骤。具体参数如文献[1], 图 2 为算法的流程。

a)轮常量加 AC。6 bit 的轮常量参数(rc_5, rc_4, rc_3, rc_2, rc_1, rc_0)的初始值为 0,在每一轮使用前依次左移,新的 rc_0 用 $rc_5 \oplus rc_4 \oplus 1$ 更新。

b)S 盒代换 SB。算法采用了 16 个 4 进 4 出的 S 盒,S 盒沿用 PRESENT 密码 S 盒。

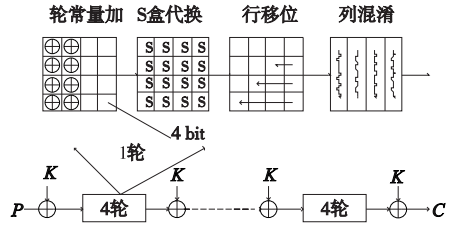

图2　LED算法流程

c)行移位 SR。状态矩阵的第 i 行向左移 i 位,i =0,1,2,3。

d)列混淆 MC。状态矩阵的每一列由混淆矩阵和该列向量相乘所得的新向量替换更新。

2.2　代数方程组构建

为建立 LED 算法加密代数方程组,本文结合算法结构,引入了 9 种类型的 64 bit 中间状态变量,对应标记及含义如表 1 所示。

表 1　通增变元及说明

变元	说明	变元	说明
P	明文	$X5$	MC 输出
$X1$	AK 输出	RC	轮常量
$X3$	SB 输出	$X2$	AC 输出
$X4$	SR 输出	K	密钥
C	密文		

引入变元之后,根据 LED 具体算法结构,可建立其对应的布尔方程组,如下:

$X1^0 = P \oplus K$;
for i =0 to 8 do{
　for j =0 to 4 do{
　　$X2^{4i+j} = AC(X1^{4i+j}, RC^{4i+j})$;
　　$X3^{4i+j} = SB(X2^{4i+j})$;
　　$X4^{4i+j} = SR(X3^{4i+j})$;
　　$X5^{4i+j} = MC(X4^{4i+j})$
　　$X1^{4i+j+1} = X5^{4i+j}$;}
　　$X1^{4i+j+1} = X1^{4i+j+1} \oplus K$;}
　　$C = X5^{31} \oplus K$;

S 盒代换是 LED 密码唯一的非线性变换,参考文献[11]中的 S 盒构建方法,将 LED 的每个 S 盒用 4 个方程表示出来,方程最高次数为 3,共有 22 个变量,如式(1)所示。每轮 LED 加密可引入 512 个变量、816 个 ANF 等式。最后加入轮密钥加操作后,全部 32 轮 LED 算法共引入 17 089 个变量、26 689 个 ANF 等式。

$$\begin{aligned} &1 + x_0 + x_2 + x_3 + x_1x_2 + x_0x_1x_3 + x_1x_2x_3 + x_0x_2x_3 + y_0 = 0\\ &1 + x_0 + x_1 + x_0x_2 + x_0x_3 + x_2x_3 + x_0x_1x_3 + x_0x_2x_3 + y_1 = 0\\ &x_0 + x_2 + x_0x_1 + x_0x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2x_3 + y_2 = 0\\ &x_0 + x_1 + x_3 + x_1x_2 + y_3 = 0 \end{aligned} \tag{1}$$

基于 SAT 问题的方程组求解包括线性化方程组、将线性化方程组转换为 CNF 两个步骤。由于 CryptoMiniSAT 可以自动将布尔方程组转换为 CNF 求解,所以线性化方程组之后不需要再进行切割及转换为 CNF 操作。方程组的线性化问题通过降幂来完成。以非线性多元布尔方程组(式(2))为例,对于其中的高次单项式 $x_1x_2x_3$,为了达到降幂的目的,需要引进一个未知变量 q,使得 $q = x_1x_2x_3$,降幂方法如式(3)所示。

$$x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_2x_3 = 0 \tag{2}$$

$$x_1x_2x_3 = q \Rightarrow \begin{cases} x_1 \vee \bar{q} = 1\\ x_2 \vee \bar{q} = 1\\ x_3 \vee \bar{q} = 1\\ \bar{x_1} \vee \bar{x_2} \vee \bar{x_3} \vee q = 1 \end{cases} \tag{3}$$

3 基于功耗信息的碰撞分析

3.1 基于功耗的碰撞捕获

碰撞的捕获包括功耗采集、相关性匹配两步。实验中功耗信息采集环境如图 3 所示。以 8 位 AVR 微控制器 ATMEGA324P 为攻击对象,系统晶振为 20 MHz。为测量 LED 加密在某一时刻的能量功耗,在微控制器和稳压电源 GND 端之间串联了一个阻值为 18.2 Ω 的电阻。加密过程中适时提供触发信号以便示波器采集电阻两端电压,并通过 USB 数据线将采集到的功耗轨迹传到 PC 机。实验中,电压设置为 5 V,微控制器工作频率为 8 MHz,数字示波器采样频率为 100 MS/s。

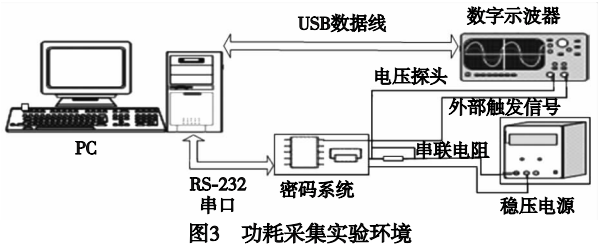

图3 功耗采集实验环境

采集到 LED 加密的功耗信息后,从中选取功耗泄露较为明显的算法操作对保证碰撞捕获的准确率十分重要。实验中选取每轮 S 盒代换输出的功耗泄露,用数组 $S[n][m](0<n\leqslant 32,\ 0\leqslant m\leqslant 15)$ 储存每轮每个半字节的功耗值。

在相关性匹配阶段,将数组 S 中的任意两个元素 $U=S[n_1][m_1]$,$V=S[n_2][m_2]$ 基于 Pearson 相关性系数公式(4)进行匹配,若相关系数 ρ 大于参考阈值则说明两个元素发生碰撞。若对 n 轮的 S 盒输出进行碰撞捕获,共需要进行 C_{16n}^2 次匹配。

$$\rho\langle U,V\rangle=\frac{\sum_{m=0}^{m}(U_m-\overline{U})(V_m-\overline{V})}{\sqrt{\sum_{m=0}^{m}(U_m-\overline{U})^2}\sqrt{\sum_{m=0}^{m}(V_m-\overline{V})^2}} \tag{4}$$

3.2 碰撞表示

捕获到碰撞后需要将其用方程组表示出来。若 $S[n_1][m_1]$ 和 $S[n_2][m_2]$ 发生碰撞,根据 2.2 节中 LED 代数方程组的建立方法,有

$$X3_{m_1}^{n_1}=X3_{m_2}^{n_2}\Rightarrow X3_{m_1}^{n_1}\oplus X3_{m_2}^{n_2}=0 \tag{5}$$

每发生一次碰撞增加一个代数方程,将新增的方程组和 LED 代数方程组联立之后,有助于降低 LED 的密钥求解复杂度。当碰撞达到一定数量则可以利用解析器解出全部密钥。

4 实验结果与分析

利用 3.1 节中的碰撞捕获方法对采集的功耗进行分析,推断出 S 盒输出的碰撞信息,然后利用 3.2 节方法将其转换为额外方程组,同 LED 加密方程组联立,最后利用 CryptoMiniSAT 进行密钥求解。基于 SAT 问题求解方程组的基本思想为:给出满足所有代数方程组的一个解,因此当碰撞信息足够多时才能锁定唯一解。

在理想情况下,加密过程中发生的所有碰撞都能通过相关性匹配捕获到,此时仅需 2 轮 S 盒的输出功耗信息,碰撞捕获次数平均为 33 次,即可在 3.5 s 内获取全部密钥。但在实际攻击中,受测试计量仪器精度、被测平台噪声等因素的影响,功耗信息的采集存在一定误差,在功耗分析中达不到 Pearson 相关性的阈值,并不能捕获全部碰撞信息。捕获率和密钥求解时间如表 2 所示,随着碰撞捕获率的升高,新加入的方程数量不断增加,降低了解析器求解密钥的复杂度,使求解时间减少。

表2 2 轮碰撞捕获率和密钥求解时间

碰撞捕获率/%	50	60	70	80	90	100
求解时间/s	158.5	57.6	19.8	6.9	4.1	3.5

3 轮 S 盒功耗信息的碰撞次数平均为 70 个,在最少 30% 的碰撞捕获率下可以在 27.8 s 内恢复密钥。4 轮 S 盒功耗信息的碰撞次数平均为 123 个,在最少 20% 的碰撞捕获率下可以在 159.7 s 内恢复密钥。图4 给出了不同求解轮数时碰撞捕获率和求解时间之间的关系。从图 4 中曲线总体趋势可以看出,功耗信息采集轮数越少,碰撞数量越少,求解方程组复杂度越大,求解时间越长。单个时间曲线的趋势显示,随着捕获的碰撞数量比例的增加,求解时间越来越短,当捕获的碰撞数量达到一定规模时,求解时间会急剧减少,最终趋于稳定。

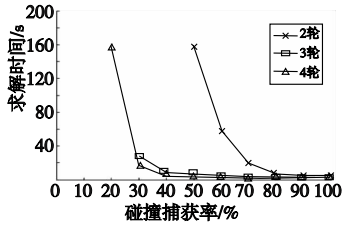

图4 不同求解轮数时碰撞捕获率和求解时间的关系

5 结束语

本文针对 LED 密码提出了一种基于碰撞模型的代数旁路攻击方法,并通过功耗物理实验成功对 8 位 ATMEGA324P 微控制器上的 LED 进行了攻击。结果表明:LED 易遭受此类攻击,利用 LED 加密部分轮功耗泄露的碰撞信息即可恢复 64 bit 初始密钥,耗时不超过 160 s。

参考文献:

[1] GUO Jian, PEYRIN T, POSCHMANN A, *et al*. The LED bock cipher[C]//Lecture Notes in Computer Science, Vol6917. Berlin: Springer,2011:326-341.

[2] BOGDANOV A, PYSHKIN A. Algebraic side-channel collision attacks on AES[EB/OL]. http:// eprint. iacr. org/2007/477. pdf.

[3] BOGDANOV A, KIZHVATOV I, PYSHKIN A. Algebraic methods in side-channel collision attacks and practical collision detection[C]//Lecture Notes in Computer Science, Vol5365. Berlin: Springer,2008: 251-265.

[4] COURTOIS N T, PIEPRZYK J. Cryptanalysis of block ciphers with over-defined systems of equations[C]//Lecture Notes in Computer Science, vol 2501. Berlin: Springer,2002:267-287.

[5] PAUL C K. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C]//Lecture Notes in Computer Science, vol 1109. Berlin:Springer,1996:104-113.

[6] WIEMERS A. Collision attacks for comp128 on smartcards[C]// Proc of ECC-Brainpool Workshop on Side-Channel Attacks on Cryptographic Algorithms. 2001.

[7] SCHRAMM K, WOLLINGER T, PAAR C. A new class of collision attacks and its application to DES[C]//Lecture Notes in Computer Science, vol 2887. Berlin: Springer,2003:206-222.

[8] SCHRAMM K, LEANDER G, FELKE P, *et al*. A collision-attack on AES: combining side-channel and diferential attack[C]//Lecture Notes in Computer Science, vol 3156. Berlin: Springer,2004:163-175.

[9] BRIER E, CLAVIER C, OLIVIER F. Correlation power analysis with a leakage model[C]//Lecture Notes in Computer Science, vol 3156. Berlin:Springer,2004:16-29.

[10] SOOS M, NOHL K, CASTELLUCCIA C. Extrending SAT solvers to cryptographic problems[C]//Lecture Notes in Computer Science, vol 5584. Berlin:Springer,2009:244-257.

[11] KNUDSEN L R, MIOLANE C V. Counting equations in algebraic attacks on block ciphers[J]. International Journal of Information Security,2010,9(2):127-135.