轻量级 PRESENT 加密算法功耗攻击研究*

李 浪[1,2], 李仁发[2], 李肯立[2], 王 奕[2], 焦 铬[1], 邹 祎[1]
(1. 衡阳师范学院 计算机科学系, 湖南 衡阳 421002; 2. 湖南大学 信息科学与工程学院, 长沙 410082)

摘 要: PRESENT 密码算法是 2007 年提出来的一种轻量级分组密码算法,适合于物联网环境下的安全加密。对 PRESENT 加密算法结构进行了深入研究,提出了其适合功耗攻击的两个最佳攻击点,详细介绍了针对 PRESENT 加密系统进行功耗分析攻击的设计与实现过程,实验结果表明未加防护措施的 PRESENT 加密系统不能抵御一阶差分功耗分析攻击,从而给 PRESENT 加密算法的安全改进提供一定的设计参考。

关键词: PRESENT; 差分功耗分析攻击; 最佳攻击点
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2014)03-0843-03
doi:10.3969/j.issn.1001-3695.2014.03.049

Differential power analysis attacks on PRESENT

LI Lang[1,2], LI Ren-fa[2], LI Ken-li[2], WANG Yi[2], JIAO Ge[1], ZOU Yi[1]
(1. *Dept. of Computer Science, Hengyang Normal University, Hengyang* 421002, *China*; 2. *College of Information Science & Engineering, Hunan University, Changsha* 410082, *China*)

Abstract: PRESENT algorithm was designed as a lightweight block cipher algorithm in 2007. PRESENT is suitable for the security of encryption in the environment of the Internet of Things(IoT). This paper studied PRESENT algorithm in-depth, and proposed two power analysis attack points. It introduced power analysis attacks on PRESENT and its implementation process in detail. The experimental results show that unprotected PRESENT encryption system can not resist the first-order differential power analysis attack. The researches can improve the safety of the PRESENT encryption algorithm.

Key words: PRESENT; differential power analysis attack; the best point of attack

2007 年在 CHES 2007 国际会议上由 Bogdanov 等人[1]提出的轻量级密码算法,该算法是为资源受限环境下的加密而研究的,特别适合目前的物联网环境下安全应用,如 RFID、传感器节点加密等。加密算法自身的安全性是非常重要的,对密码算法的攻击与防御研究一直没有停止过。近年来出现了一种新的攻击方法——功耗攻击[2],与其他密码攻击方法相比较,功耗攻击这种方式具有成本不高、时间复杂度小等优点[3]。因此,目前这一攻击方法与防御对策相关研究在学术及工业界是热点问题,同时也促使了密码芯片安全标准进行了新的修订。目前相对来说 PRESENT 密码算法的功耗攻击与防护研究成果见诸发表的学术成果不多。一方面是由于 PRESENT 算法目前还没有进入广泛应用的阶段,相关的研究开展不多,另一方面是由于 PRESENT 算法公布时间较短[4]。但随着物联网的广泛应用,适合其加密应用的 PRESENT 算法安全问题也倍受关注,PRESENT 功耗分析攻击与防护研究方面的空白亟待相关研究者填补。

本文主要研究了 PRESENT 加密算法的功耗攻击流程,最佳功耗攻击点,攻击过程设计与实现。

1 PRESENT 算法

PRESENT 算法是一个轻量级分组算法,在 CHES 2007 国际会议上由 Bogdanov 等人提出的,主要为物联网中资源受限的智能卡或加密节点开发设计的,虽然是轻量级密码算法,但完全的 31 轮 PRESENT 密码算法可以抵抗现有的数学攻击。它的设计思路借鉴了 DES 加密算法,但具体实现还是有很大差别,PRESENT 的 S 盒是 4 位进 4 位出,位移和模 2 加运算,同时,PRESENT 的轮函数采用 SP 结构(替代—轮换),而 DES 采用 FEISTEL 结构;相比 DES、AES 等加密算法更适合资源受限的物联网安全应用。PRESENT 分组长度为 64 bit,密钥长度可以为 80 bit 或 128 bit;64 bit 明文经过 31 轮的迭代和最末轮白化运算后得到需要的 64 bit 密钥;PRESENT 算法加密运算流程如图 1 所示。算法 1 是 PRESENT 的伪代码描述。

算法 1 PRESENT 加密运算

```
generateRoundkeys( )
for i = 1 to 31 do
  addRoundkey(STATE, K_i)
  sBoxLayer(STATE)
  player(STATE)
end for
addRoundKey(STATE, K_32)
```

PRESENT 分组长度为 64 bit,即每次运算操作输入 64 bit,又由于是 4 进 4 出的方式,故推算共有 16 个 S 盒,其加密轮函数 F 主要操作有轮密钥加、S 盒置换、P 置换三个部分。31 轮中每一轮包括线性置换 P 和非线性置换 S,非线性置换 S 常称之为的 S 盒置换。在功耗攻击与防御研究中,本文主要关注轮

收稿日期: 2013-05-17; **修回日期**: 2013-06-27 **基金项目**: 国家自然科学基金资助项目(61173036); 湖南省教育厅青年项目资助(11B018); 湖南省博士后基金资助项目(897203005); 衡阳师范学院科学基金资助项目(12CXYZ01,11B43); 湖南省十二五重点建设学科资助项目

作者简介: 李浪(1971-),男,教授,博士,主要研究方向为嵌入式系统与信息安全(lilang911@126.com);李仁发(1957-),男,教授,博导,主要研究方向为嵌入式系统;李肯立(1971-),男,教授,博导,主要研究方向为高性能计算与信息安全.

密钥参与运算的详细过程,选取 PRESENT 密码算法的密钥长度为 80 bit 进行示例。

令 K 为用户选取的密钥,则

$$K = K_{79}K_{78}K_{77}\cdots K_2K_1K_0$$

定义 K_i 为 PRESENT 运算中第 i 轮密钥,则

$$K_i = K_{63}K_{62}K_{61}\cdots K_2K_1K_0 = K_{79}K_{78}K_{77}\cdots K_{18}K_{17}K_{16}$$

上式表明第 i 轮密钥是左移 64 bit 组成的,因为 PRESENT 算法分组长度为 64 bit。

在功耗攻击中只需分析一轮的密钥 64 bit,即可将密钥分析空间从 2^{80} 空间复杂度降低至 2^{16}。PRESENT 算法与 AES、DES 算法的实现性能特征比较如表 1 所示。

表 1 PRESENT 算法与 AES、DES 算法的实现比较

cipher	key bits	block bits	cycles per block	logic process/μm	area(GEs)
PRESENT	80	64	32	0.18	1570
DES	56	64	144	0.18	2309
AES	128	128	1032	0.35	3400

从表 1 可以很明显地看出 PRESENT 密码算法在实现面积上有较大优势,因此也特别适合于资源受限的物联网中的智能卡节点加密。正因为 PRESENT 算法作为一种超轻量级密码算法,主要应用在物联网环境中,因而一般具有以下几个易受功耗攻击的特点:a) PRESENT 一般是在 RFID、智能卡等嵌入式设备上以硬件方式实现;b)密钥一般是固定在硬件设备中,用户不能自行更换。

以上两点恰好是功耗攻击要求的攻击环境,所以 PRESENT 的功耗攻击防御技术研究迫在眉睫。

2 PRESENT 功耗攻击

2.1 PRESENT 功耗攻击分析模型

PRESENT 芯片在实际进行加密数据处理时,PRESENT 密码芯片集成电路中的负载电容会进行充放电动作,芯片电路就一定会有相应的能耗变化,相对于 PRESENT 密码芯片内部的数据寄存器中的某一位触发器,能耗变化的大小与密码芯片电路中数据处理是一一映射的,这种映射在间电路级别反映为电容的充电与放电行为,对应于寄存器则为相应的触发器的高低电平翻转(即 0、1 变化),在操作数级别则对应着 PRESENT 密码算法指令运算时前后数据的 Hamming distance。由于存在着这种对应映射关系,故可用 Hamming distance 来表示 PRESENT 密码芯片在加密运算时的相应功耗变化[5]。

将 PRESENT 密码芯片中寄存器中的 1、0 翻转变化与其能耗变化映射,对应操作数这一级别,并根据寄存器状态的前后变化来建立 Hamming distance 功耗模型。PRESENT 密码芯片加密运行时功耗模型可描述为

$$W = aH(D\rightarrow R) + b \tag{1}$$

其中:功耗用 W 表示;数据的 Hamming weight 用 H 表示;寄存器变化前后的状态用 D 和 R 表示,D 代表 RSENT 密码算法运算时输入的原始操作数;R 代表密码算法运算完成时的结果;D 和 R 的汉明距离则用 $H(D\rightarrow R)$ 表示;a 和 b 是根据运算时实际环境确定的常量。

对于式(1),在一定条件下可以取($a=1$,$b=0$),则式(1)可简化为

$$W = H(D\rightarrow R) \tag{2}$$

上述具体演算与实验验证可见文献[6]。

2.2 PRESENT 密码算法攻击点选取

PRESENT 密码算法是 16 个 S 盒变换,S 盒在 PRESENT 密码芯片中运算时消耗的功耗较大,另外一个是密钥与明文进行异或运算时,因此可以在这两个较好位置选取合适的时间点进行功耗攻击[7,8],如图 2 中用黑色箭头标明了两处合适的功耗攻击点。

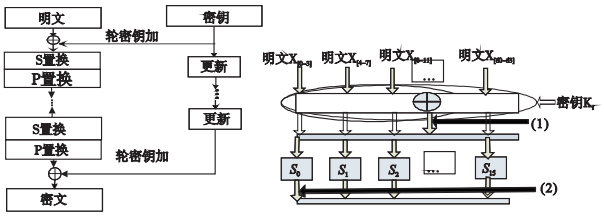

图1 PRESENT算法加密运算流程 图2 PRESENT算法最佳攻击点

选取这两点为最佳功耗攻击位置点主要理由说明如下:

1)对于明文与密钥异或后的攻击采样点

a) PRESENT 密码算法第一轮运算是由 64 bit 明文与 80 bit 密钥中的前 64 bit 密钥进行异或运算,然后再经寄存器进入后端的 S 盒置换进行操作运算。

b) 密钥已经在这一攻击点参与运算,在明文固定不变的情况下,随着密钥的不同,相应的 Hamming distance 也是不同的,在密码芯片电路上可以体现为密钥与功耗有关。

c) 根据功耗攻击可满足定义,在明文确定情况下,可以完整推测与之相对应的密钥位。

由此,选取这一点作为功耗攻击点是可行的,特别是在仿真实验中,选取这一点具有较好的优势,因为数据未作过多运算变化,在仿真攻击平台中易于获取所需数据(或者说对应的 Hamming distance)。但是如果是实际的物理攻击平台,即 PRESENT 加密算法已经进行了物理实现,通过示波器来获取相应的功耗曲线。但这一点不是整个密码芯片运算中产生最大功耗时刻点,故不是物理芯片最佳攻击触发点。

2)对于选取各 S 盒的第一位输出点

a)S 盒变换是 PRESENT 密码算法中唯一的非线性部件,因此在密码芯片加密运算时消耗功耗最大,在进行具体的功耗攻击中此点容易分析和测量。

b)攻击数据获取时,时间对齐非常重要,如果用在偏差的时间获取的数据进行统计分析,其猜测的密钥值自然不正确,而 S 盒的第一位输出点易于进行时间点对齐。

c)在功耗攻击实验中,对 PRESENT 密码算法 S 盒的其他位数据本文也进行了获取与统计分析,从实验效果证明第一位时间点在获取正确密钥最好。

根据分析,本文使用第二种方法进行 PRESENT 密码算法进行差分功耗攻击。

3 PRESENT 功耗攻击过程与实验结果

3.1 PRESENT 算法攻击流程

PRESENT 加密算法攻击过程如下:

a)取 PRESENT 加密算法第一轮为功耗攻击测试点,统计分析 K_1 中的 4 位密钥。

b)根据 PRESENT 加密算法的实际运行特点,相应构造的 D 函数,D 取值为 0 或 1,D 函数与 PRESENT 加密算法输入明文或其密钥相关。令 $D = R_{1-1}$,R_{1-1} 代表 PRESENT 算法中 R_1

的第一位。

c)执行一次 PRESENT 加密算法,由此可以获得 PRESENT 加密运算后输出 C 和对应的功耗曲线。

d)利用 D 值可以对不同的明文输入所对应的功耗消耗曲线分为两个相应集合:

$$S_0 = \{S_i[j] \mid D = 0\}$$
$$S_1 = \{S_i[j] \mid D = 1\}$$

e)分别计算两组的平均值 $E(S_0)$ 和 $E(S_1)$。

f)统计 DPA 偏差 $\Delta[j]$,其中 $\Delta[j] = E(S_0) - E(S_1)$,如果 $\Delta[j] = 0$,则说明实验进行的统计分析密钥错误,在统计分析数据图上则表示为没有相对尖锋,如果 $\Delta[j] = 1$,则在统计分析图上有相对尖锋。

g)通过上述统计,可以得到 K_1 的第一个 S 盒的 4 bit 密钥,同样采取类似方法,可以统计分析出 PRESENT 加密算法余下的 60 bit 密钥。

h)然后对最后 16 bit(80 - 64 = 16 bit)密钥进行 2^{16} 穷举,可以分析出 PRESENT 加密算法密钥。

3.2　PRESENT 差分功耗攻击实验及结果

对 PRESENT 加密算法进行了 C 语言实现,并通过工具导入到 AT89C51 芯片上,然后构建了如图 3 所示的攻击实验平台。

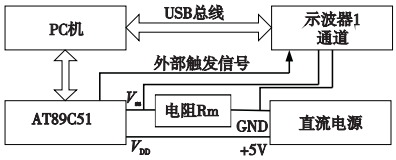

图3 PRESENT功耗攻击实验平台示意图

DPA 攻击实验过程如下:

a)明文由 PC 机产生经串口下载到 AT89C51;密钥事先在编程时设定好,并且在一次成功攻击前不得改变。

b)按攻击点 2 设置示波器采样触发点;其中示波器型号为绿扬 54500A。

c)电阻 R 上的瞬时电压实时由示波器记录并返回 PC 机。

d)按 3.1 节中的 DPA 流程对采集到的功耗曲线记录进行统计分析,统计分析工具为 MATLAB;也可以自行编程设计一个功耗处理软件平台进行统计分析。

DPA 攻击实验结果经统计分析后如图 4 所示。

3.3　实验结果分析

从图 4 的差分功耗攻击实验结果图可以看出,相比 DES、AES、SMS4,该方法的攻击效果更好,也就是说轻量级加密算法为了追求芯片实现的小面积低功耗而不得不在安全性有所降低。由于 PRESENT 加密算法是 SPN 结构,实现相对简单,在密钥参与运算后变换复杂度相对较小,因此,旁路攻击的难度也降低了许多。而且从实验结果图显示可以看出未加防护的 PRESENT 密码算法在攻击时噪声也少很多,正是因为这些原因,PRESENT 加密算法作为一种物联网准备大力推广使用的超轻量级算法,其旁路攻击安全性设计必须引起相关研究人员高度重视。

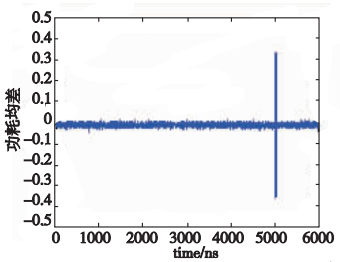

图4 未加防护的PRESENT差分攻击结果

4　结束语

PRESENT 加密算法在物联网大力发展的今天具有良好的应用前景,然而从本文的实验结果可以得出原始的 PRESENT 密码算法不能抗差分功耗攻击。因此,为了更好地保证 PRESENT密码算法的应用,研究人员应该对 PRESENT 密码算法的抗功耗攻击进行深入研究,从而保证 PRESENT 加密算法的抗旁路攻击能力。

参考文献:

[1] BOGDANOV A,KNUDSEN L R, LEANDER G,*et al*. PRESENT:an ultra-lightweight block cipher [C]//Proc of Cryptographic Hardware and Embedded Systems. Berlin:Springer-Verlag, 2007:450-466.

[2] KOCHER P, JAFFE J,JUN B. Differential power analysis[C]//Proc of Advances in Cryptology. Berlin:Springer-Verlag,1999:388-397.

[3] 李浪,李仁发. SEHM 安全 SoC 抗功耗攻击研究综述[J]. 计算机科学,2009,36(6):16-18.

[4] 刘会英,王韬,赵新杰,等. PRESENT 相关功耗分析攻击研究[J]. 计算机科学,2011,38(11): 40-42.

[5] GUILLRY S,HOOGVORST P,PACALET R. Differential power analysis model and some results[C]//Proc of the 18th IFIP World Computer Congress the 6th International Conference on Smart Card Research and Advanced Applications. 2004:127-142.

[6] 李浪,李仁发,徐雨明. 功耗攻击实验中一种高效功耗模型研究与应用[J]. 计算机应用研究, 2009, 26(12): 4722-4723.

[7] 李浪,李仁发,李静,等. 一种 SMS4 加密算法差分功耗攻击[J]. 计算机科学,2010,37(7):39-41.

[8] 李浪,李仁发,焦铬,等. 一种 ECC 加密芯片抗功耗攻击研究[J]. 微电子学与计算机, 2011,28(1):27-30.

(上接第 842 页)

参考文献:

[1] 沈昌祥,张焕国,冯登国,等. 信息安全综述[J]. 中国科学 E 辑:信息科学,2007,37 (2): 129-150.

[2] Kingsoft. Google 桌面搜索搜出隐私 [EB/OL]. [2011-10-22]. http://www. kingsoft. com/contentNDI4NTE = . shtml.

[3] 国际能源网. 日本电厂安全信息被个人电脑泄密[EB/OL]. [2011-12-18]. http://power. in-en. com/news/intl/2006/05/INEN_11780. html.

[4] 贺涛,李湘宁. 解密中国互联网史上规模最大的泄密事件[EB/OL]. [2012-07-10]. http://business. sohu. com/20120116/n332280135. shtml.

[5] 史茜. 最小侵入式数据隐藏系统的设计与实现[D]. 上海:上海交通大学,2007.

[6] 金晶. 一种 NTFS 文件隐藏方式研究[D]. 武汉:华中科技大学,2009.

[7] KHAN H,JAVED M,KHAYAM S A. Designing a cluster-based covert channel to evade disk investigation and forensics[J]. Computers & Security,2011,30(1): 35-49.

[8] ECKSTEIN K,JAHNKE M. Data hiding in journaling file systems [C]//Proc of Digital Forensic Research Workshop. 2005.

[9] 汤小丹,梁红兵,哲凤屏,等. 计算机操作系统[M]. 3 版. 西安:西安电子科技大学出版社,2007:203-208.

[10] 蔡风华. 基于 FAT32 文件系统的文件隐藏研究与实现[D]. 武汉:华中科技大学,2007.

[11] HUEBNER E,BEM D,WEE C K. Data hiding in the NTFS file system[J]. Digital Inverstigation:The Interational Journal of Digital Forensics & Incident Response,2006,3(4):211-226.