一种SMS4加密算法差分功耗攻击

李 浪[1,2] 李仁发[2] 李 静[2] 吴克寿[3]
(衡阳师范学院计算机系 衡阳 421008)[1] (湖南大学计算机与通信学院 长沙 410082)[2]
(厦门理工学院计算机系 厦门 361024)[3]

摘 要 针对SMS4加密电路,采用差分功耗分析攻击方式进行密钥破解。该攻击方法是一种典型的加密芯片旁路攻击方式,其理论基础为集成电路中门电路在实现加密算法时的物理特征、功耗模型及数据功耗相关性。结合中国第一个商用密码算法SMS4,详细介绍了针对SMS4加密系统进行差分功耗分析攻击的设计与实现。开发了相应的仿真实验验证平台,实验验证成功破解了SMS4加密算法的密钥,从而给SMS4加密算法研究者提供了有益的安全设计参考。实验表明,未加防护措施的SMS4加密系统难以抵御差分功耗分析的攻击。

关键词 SMS4,差分功耗攻击,汉明距离,功耗模型,仿真平台
中图法分类号 TP309 **文献标识码** A

Differential Power Analysis Attacks on SMS4

LI Lang[1,2] LI Ren-fa[2] LI Jing[2] WU Ke-shou[3]
(Department of Computer, Hengyang Normal University, Hengyang 421008, China)[1]
(School of Computer and Communication, Hunan University, Changsha 410082, China)[2]
(Department of Computer, Xiamen University of Technology, Xiamen 361024, China)[3]

Abstract The paper introduced Differential Power Analysis (DPA) attack of the decrypt encrypted circuits with SMS4, it is one particularly powerful type of Side Channel Attacks (SCA). All its theories are based upon the physical characters, power consumption models and data-dependent power consumption of CMOS logic gates which form the integrated circuits (ICs). The paper introduced the design and realization of DPA attacks of SMS4. Correct secret key of encryption algorithm is cracked successfully with experiments. It comes gradually and closely into ultimate target of the attack. The result indicates that SMS4 encrypted systems without some extra protective measures can't resist the attacks of DPA, because of the leakages from the physical signals and the difference of power consumption while processing the different data of ICs. The results can give the researchers to provide a useful reference for the safety design.

Keywords SMS4, Side channel attacks, Hamming distance, Power consumption model, Simulation platform

1 引言

2006年1月我国官方公布了第一个商用密码算法——SMS4密码算法[1,2]。该算法是一个迭代型分组算法,主要应用于无线局域网产品。SMS4算法的分组长度和密钥长度均为128bit,加密算法和密钥扩展算法都采用32轮非线性迭代结构。

加密算法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[3]。与其他攻击方法相比较,功耗攻击具有费用低廉、密钥搜索空间小等优点[4]。因此,功耗攻击及防护对策研究受到国内外相关领域的研究人员和业界的极大关注。

由于SMS4算法公布时间较短,SMS4分组密码算法的功耗分析攻击与防护方法的研究成果较少。这一方面是由于SMS4算法公布不久,另一方面则是由于SMS4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[5,6]。但是,SMS4算法作为我国公布的第一个商用密码算法和认证标准的组成部分,其功耗分析攻击与防护研究方面的空白亟待研究者填补。

本文主要研究了SMS4加密算法的功耗攻击流程、最佳功耗攻击点、攻击过程设计、SMS4加密算法功耗攻击仿真实验平台。

2 差分功耗攻击原理

目前,集成电路大都采用静态单轨的标准单元实现,其功耗与输入和输出的翻转状态密切相关。下面以反相器为例来

到稿日期:2009-09-29 返修日期:2009-11-09 本文受国家自然科学基金(60903203),湖南省科技计划项目(2009GK3023)资助。
李 浪(1971-),博士,副教授,CCF高级会员,主要研究方向为嵌入式系统安全,E-mail:lilang911@126.com;李仁发(1957-),教授,博士生导师,主要研究方向为嵌入式计算与安全;李 静(1986-),硕士生,主要研究方向为嵌入式系统安全;吴克寿(1975-),博士,副教授,主要研究方向为嵌入式系统安全与算法设计。

分析功耗特性，如图 1 所示。

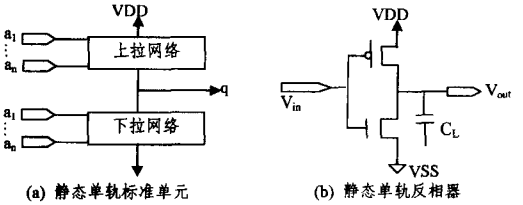

图 1　反相器电路示意图

文献[7]对单个 CMOS 门电路功耗模型表示为

$$P_D = C_L V_{DD}^2 P_{0\to1} f \tag{1}$$

式中，f 代表输入发生变化的最大可能速率，即时钟频率；$P_{0\to1}$ 是时钟变化时在该门的输出端引起 $P_{0\to1}$（即消耗功率）变化事件的概率；C_L 为等效电容，代表了每时钟周期发生开关的平均电容。

当输出信号发生 0－1 跳变时，反相器的功耗明显大于发生其它 3 种跳变时的功耗，因此功耗与密码模块中运算的数据具有一定的相关性。功耗分析的原理正是基于这种相关性，攻击者通过统计大量功耗样本即可分析密钥的值。

差分功耗分析(DPA)是一种对密码芯片的泄漏功耗进行统计分析而恢复密钥的攻击方法。DPA 的方法是对大量的曲线样点进行功耗统计测试，即根据大量功耗样本来分析密钥的值，具有比简单功耗攻击更高的强度。差分功耗攻击也称为一阶差分功耗攻击。高阶差分功耗分析与一阶差分功耗分析的不同是：对于同一个功耗曲线，一阶差分功耗分析只对其中一个单独时间点进行采样分析，而高阶则是对其 2 个或 2 个以上时间点进行联合采样统计分析，与之相应的区分函数和统计分析过程较一阶差分功耗攻击更加复杂，分析精度比一阶差分功耗分析高，但是数据采集量和计算复杂度远远大于一阶差分功耗分析。

3　SMS4 加密算法差分功耗攻击

3.1　SMS4 加密算法简介

SMS4 算法是一个分组算法，其分组长度为 128bit，密钥长度为 128bit。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，即解密轮密钥是加密轮密钥的逆序。轮运算比较简单，主要为 32bit 的异或运算、S 盒查表操作以及 32bit 的循环左移。

SMS4 加密算法流程如图 2 所示。

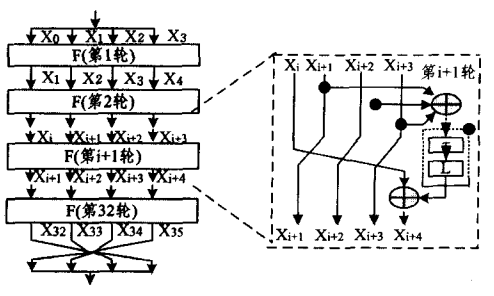

图 2　SMS4 算法加密流程

SMS4 加密算法采用非线性迭代结构，以字为单位进行加密运算。一次迭代运算为一轮变换，称作轮函数 F。非线性变换 S 由 4 个并行的 S 盒构成，每个 S 盒为固定的 8bit、输入 8bit 输出的置换，记为 $Sbox(.)$。轮函数 F 的运算流程如图 3 所示。

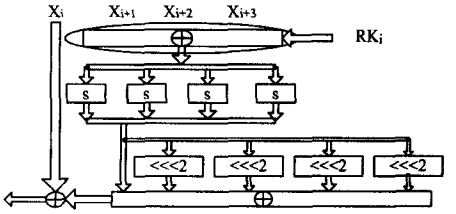

图 3　SMS4 算法 F 函数流程图

SMS4 算法中的轮密钥由加密密钥通过密钥扩展算法生成，运算流程如图 4 所示。

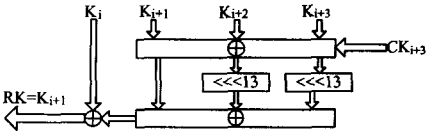

图 4　SMS4 算法密钥扩展流程图

3.2　SMS4 加密算法功耗攻击模型

加密芯片在运行 SMS4 加密程序时，在数据处理（系统中有数据变化，集成电路有负载电容充放电）中，电路有功耗消耗。对于系统中参与数据处理的某一寄存器其中的一位触发器而言，功耗的大小与所处理的数据是直接相关的。这种关系在门电路一级表现为负载电容充放电，在寄存器一级表现为寄存器中触发器的 0、1 翻转，在操作数一级表现为指令执行前后的数据的汉明距离。因此，可以用指令执行前后的数据的汉明距离来分析加密系统芯片中数据处理过程的功耗情况。

根据寄存器状态的前后变化来建立汉明距离功耗模型，将寄存器单元中的 0、1 翻转与功耗对应起来，上升到操作数一级。寄存器的功耗函数可表示为

$$W = aH(D \to R) + b \tag{2}$$

式中，W 表示功耗，H 表示数据的汉明重量，D 和 R 分别表示寄存器变化前后的状态，也就是原始操作数和结果。$H(D\to R)$ 表示 D 和 R 的汉明距离，a 和 b 是两个常量参数。

令 $a=1, b=0$，上述模型就可简化为

$$W = H(D \to R) \tag{3}$$

3.3　SMS4 加密算法差分功耗攻击点

根据前面对 SMS4 加密算法的加密流程介绍，可以选取 2 个时间点进行功耗分析攻击。第一个时间点是第一轮加密过程中的异或操作，第二个时间点是 S 盒的第一位输出。图 5 中黑色箭头指向且标示有(1)、(2)的为 2 个合适攻击点。

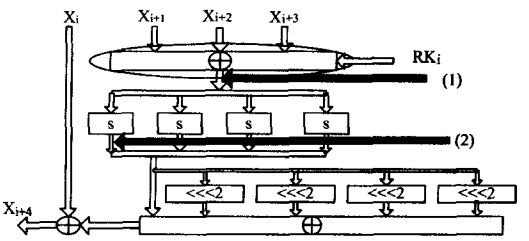

图 5　2 个攻击点标示

选取这 2 点为攻击点的主要原因分别描述如下：

1）选取第一轮加密过程中的异或操作[8]。

(1)对第一轮加密过程中能量消耗曲线的采集最为容易。在实践中，可以做到对加密芯片完整地运行一次能量消耗曲

线的测量与采集，而难以实现只采集其中特定某轮加密的能耗曲线。通过对整体的能量消耗曲线的观察与分析，选择较前端的曲线，此部分即可代表第一轮加密时的能耗曲线。该步操作在实际中易于实现。

(2)对于第1轮的明文输入可自行选取。对SMS4的能量分析攻击需要结合已知的明文输入才能实现。在SMS4算法中，只有第1轮的输入可直接控制，其他轮的输入都是由之前的若干轮迭代所产生，该值是未知的。

(3)当获取到第1轮加密子密钥(RK_0)时能够得到第2轮加密的输入。只有已知第1轮的加密子密钥才能实现对第2轮输入的控制，进而实现对第2轮的攻击。依此类推，当攻击到第4轮时，即可得到完整的加密密钥。

2)选取S盒的第一位输出点攻击的理由如下：

(1)S盒变换是算法唯一的非线性部件，其所耗资源在整个算法中占很大比重，其密码强度决定了整个算法的安全强度，运算量高、功耗相对较大、在功耗攻击中容易测量。

(2)S盒的第一位输出点易于进行时间点对齐，这点在功耗分析攻击中相当重要。

(3)我们也进行了实验，验证S盒的其它位，结果表明第一位在攻击实验结果上效果最好。

本文采用第二种方法进行SMS4差分功耗攻击。

4 SMS4加密算法差分功耗攻击实验

4.1 SMS4加密算法DPA基本思想

SMS4加密算法的一阶差分功耗攻击基本思想设计如下：

1)以首轮加密运算为功耗测试点，猜测k1中的8位密钥。

2)构造一个D函数。D为一位二进制0或1，D与明文或部分密钥有关，或者与密文和部分密钥有关。本实验令$D=R_{i-1}$，R_{i-1}代表SMS4算法中R_i的第一位。

3)执行一次SMS4加密算法，得到一个加密输出C和相应的功耗曲线。

4)将不同的明文输入所对应的功耗曲线利用D值分为两个集合：

$S_0=\{S_i[j]|D=0\}$

$S_1=\{S_i[j]|D=1\}$

5)分别计算两组的平均值$E(S_0)$和$E(S_1)$。

6)计算DPA偏差$\Delta[j]=E(S_0)-E(S_1)$。如果偏差为0，则猜测错误，表现在功耗曲线图上就是没有尖锋；如果为1，则有尖锋。

7)以此获得k1的第一个S盒的8位密钥。依次可以获得余下的密钥。

针对其它密钥段，分别构造D函数。注意D函数一定要与密钥、明文或密文具有相关性。余下的进行穷举，即可得到所有轮密钥位。

4.2 SMS4差分功耗攻击仿真平台设计

本文设计了一个软件模拟的功耗分析攻击的仿真实验平台。通过对加密算法IP核进行功耗模拟，提取出功耗曲线，进行功耗分析。另一方面，亦可以利用这一平台验证抗功耗分析攻击算法设计的有效性。功耗分析攻击的仿真实验平台架构流程如下：

1)完成硬件描述语言(如Verilog，VHDL等语言)对SMS4加密算法的描述，并编写合适的测试激励函数(testbench)。

2)经Modelsim逻辑仿真，验证正确后，在相应测试点设置测试函数(testbench)，生成所关心信号量的VCD(Value change dump)文件。VCD文件实质上是记录了相应时间测试点功耗波形的二进制形式的文件。

3)通过C语言编程读入VCD文件，把相应有效信息转换成文本文件txt。

4)通过项目组开发的功耗攻击仿真平台2.0软件进行数据处理(仿真平台开发原理如4.1节所述)，得到SMS4加密算法功耗分析攻击的功耗波形。

图6所示是SMS4加密算法在5000条明文下对第一个S盒的第一位进行功耗攻击成功的波形。余下的S盒可以用类似方法进行功耗攻击，最终用穷举法得到SMS4加密算法的剩余密钥。

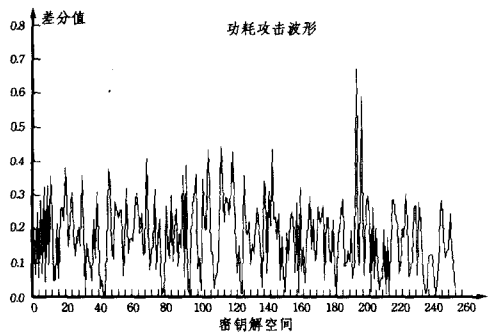

图6 功耗攻击密钥成功结果图

结束语 差分功耗分析攻击不同于常规的针对加密算法或安全系统的"穷举攻击"策略，其原理设计巧妙，攻击设备不贵且易于获取。而且功耗攻击方法为非入侵性攻击，不易察觉，不留痕迹，且无需对加密系统具有十分细致的了解。

SMS4加密算法是我国第一个自主制定的无线局域网加密标准算法，它的安全性是非常值得研究者重视的。本文中的理论和实验结果表明，未加防护的SMS4加密算法能够使一阶差分功耗攻击成功。

参考文献

[1] Office of State Commercial Cipher Administration. SMS4 cipher for WLAN products[EB/OL]. http: www. oscca. gov. cn/upFile 200621016423197990. pdf,2006

[2] 国家商用密码管理办公室. 无线局域网产品使用的SMS4密码算法[EB/OL]. http //: www. oscca. gov. cn/up-File 20062101642 3197990. pdf,2006

[3] Kocher P,Jaffe J,Jun B. Differential Power Analysis[C]// Proceedings of Advances in Cryptology-CRYPTO 99. Springer-Verlag,1999:388-397

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

[5] 白雪飞，郭立，等. SMS4密码算法的差分功耗分析攻击研究[J]. 小型微型计算机系统，2009,30(3):541-544

[6] 张蕾，张文玲. SMS4密码算法的差分故障攻击[J]. 计算机学报，2006,29(9):1596-1602

[7] Rabaey J M. Digital Integrated Circuits [M]. Englewood Cliffs, NJ:Prentice-Hall,1996

[8] 沈薇. SMS4算法的能量分析攻击及其防御研究[D]. 西安：西安电子科技大学，2009