PRESENT相关功耗分析攻击研究

刘会英 王 韬 赵新杰 周 林
(军械工程学院计算机工程系 石家庄 050003)

摘 要 对PRESENT分组密码抗相关功耗分析能力进行了研究。基于汉明距离功耗模型,提出了一种针对PRESENT S盒的相关功耗分析方法,并通过仿真实验进行了验证。结果表明,未加防护措施的PRESENT硬件实现易遭受相关功耗分析威胁,5个样本的功耗曲线经分析即可恢复64位第一轮扩展密钥,将80位主密钥搜索空间降低到2^{16},因此,PRESENT密码硬件实现需要对此类攻击进行防护。

关键词 PRESENT,旁路攻击,汉明距离,功耗模型,相关功耗分析
中图法分类号 TP393.08 **文献标识码** A

Research on Correlation Power Analysis Attack against PRESENT

LIU Hui-ying WANG Tao ZHAO Xin-jie ZHOU Lin
(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract The correlation power analysis attack against PRESENT was discussed in this paper. An correlation power attack method according to the sbox in PRESENT cipher was presented based on hamming distance power leakage model. The results of experiment indicate that hardware implementation of PRESENT without protection measure is vulnerable to correlation power analysis attacks. The 64-bit first round expanded key can be recovered with 5 power traces, and the 80-bit PRESENT master key searching space can be reduced to 2^{16}, so that cryptographic devices should be protected to prevent this kind of attack.

Keywords PRESENT, Side channel attacks, Hamming distance, Power consumption model, Correlation power analysis

1 引言

近年来,出现了一种新的利用密码设备电路泄漏的功耗、电磁辐射等信息进行密钥破解的方法,称之为旁路攻击[1]。同传统基于数学的密码分析方法相比,旁路攻击具有攻击成本低、攻击力强、难以防护等特点。功耗分析是旁路攻击的一种重要方法,主要通过分析密码设备操作时的功率消耗与加密中间状态的相关性,结合算法结构来实现密钥破解。自从Kocher在1999年首次提出功耗分析方法后[2],国内外的密码学者对其进行了广泛的研究,常见的功耗分析方法有简单功耗分析(Simple power analysis, SPA)、差分功耗分析(Differential power analysis, DPA)、相关功耗分析(Correlation Power Analysis, CPA)。

PRESENT是由A. Bogdanov等人[3]于2007年提出的一种超轻量级分组密码算法,具有良好的硬件实现效率,在0.18μm工艺下仅需的逻辑单元为1570GE,非常适合在RFID标签、传感器网络等资源受限的环境中使用。作者对PRESENT的抗线性分析、差分分析等能力进行了评估,声称该算法是安全的。本文则对PRESENT密码算法的抗功耗分析安全性进行了研究,提出了一种针对PRESENT的相关功耗分析方法,并进行了仿真实验。结果表明PRESENT易遭受差分功耗分析攻击的威胁,5个加密样本的功耗曲线即可成功获取第一轮64位扩展密钥。

本文第2节介绍了PRESENT算法结构;第3节给出了PRESENT相关功耗分析的过程;第4节给出了仿真实验及结果;最后为结束语。

2 相关知识

2.1 PRESENT加密算法结构

PRESENT分组密码算法[3]采用SPN结构,分组长度为64位,支持80位、128位两种密钥长度,其加密共需迭代31轮,每轮轮密钥为$K_i(1\leqslant i\leqslant 31)$。为提高算法安全性,PRESENT在第31轮运算结束后使用64位密钥K_{32}进行后期白化操作。PRESENT加密流程如图1所示。

PRESENT加密轮函数F由轮密钥加、S盒代换、P置换3部分组成。

轮密钥加:当前中间状态$b_{63}\cdots b_0$同64位轮密钥K_i按位进行异或;

S盒代换:首先将轮密钥加的64位结果划分为16个4位值$W_{15}\cdots W_0$,$W_i=b_{4*i+3}||b_{4*i+2}||b_{4*i+1}||b_{4*i}(1\leqslant i\leqslant 15)$,然后依次将$W_i$代入一个4进4出的$S$盒,得到$S[W_i]$;

P置换:通过置换表$P(i)$对S盒代换结果进行重新排

到稿日期:2010-12-22 返修日期:2011-03-03 本文受国家自然科学基金项目(60772082),河北省自然科学基金数学研究专项(08M010)资助。
刘会英(1984-),男,博士生,主要研究领域为密码旁路分析,E-mail:lhy_fengling@126.com;王 韬(1964-),男,博士,教授,博士生导师,主要研究领域为信息安全和密码学;赵新杰(1986-),男,博士生,主要研究领域为分组密码旁路分析和故障分析。

列。

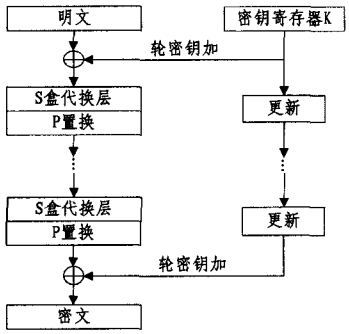

图1 PRESENT加密流程

密钥扩展算法为：首先将初始主密钥存储在寄存器 K 中，表示为 $k_{79}k_{78}\cdots k_0$。第 i 轮密钥 K_i 由寄存器 K 的左64位组成。当生成第 i 轮密钥 K_i 后，密钥寄存器 K 通过如下方法进行更新：

$$[k_{79}k_{78}\cdots k_1k_0]=[k_{18}k_{17}\cdots k_{20}k_{19}] \quad (1)$$

$$[k_{79}k_7k_{77}k_{76}]=S[k_{79}k_7k_{77}k_7] \quad (2)$$

$$[k_{19}k_{18}k_{17}k_{16}k_{15}]=[k_{19}k_{18}k_{17}k_{16}k_{15}]\oplus \text{round\_Counter} \quad (3)$$

式中，round_Counter为当前的加密轮数。易见，只需分析出第一轮的64位轮密钥 K_1，即可将80位PRESENT的初始主密钥搜索空间降低到 2^{16}。

2.2 相关功耗分析原理

密码算法在芯片或硬件系统的运行过程中会产生功率消耗。对于参与数据处理的某一寄存器中的一位触发器而言，功耗大小与所处理的数据直接相关。这种关系在CMOS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数据的汉明距离[4-6]。因此，可以用指令执行前后数据的汉明距离来分析密码芯片加密数据处理过程中的功耗情况。功耗分析攻击则主要利用硬件功耗与运算数据之间的相关性进行密钥分析。

相关功耗分析CPA通过计算加密功耗同预测加密中间数据汉明重或汉明距离的相关性来进行密钥破解。Pearson相关性系数是一种计算 X、Y 两个向量之间相关性的方法。Pearson相关性系数 $\rho_{X,Y}$ 定义如下[7]：

$$\rho_{X,Y}=\frac{Cov(X,Y)}{\sigma_X\sigma_Y}=\frac{E((X-\mu_X)(Y-\mu_Y))}{\sqrt{D(X)}\sqrt{D(Y)}} \quad (4)$$

式中，μ_X 和 μ_Y 分别是 X 和 Y 的数学期望值，σ_X 和 σ_Y 分别是 X 和 Y 的标准差，E 是数学期望值的操作符，Cov 表示协方差。$|\rho_{X,Y}|\leqslant 1$，$|\rho_{X,Y}|$ 值越大，X 和 Y 的线性相关性越强。

具体来说，相关功耗分析CPA主要根据已知明文或密文，预测一个子密钥块值 k_i，猜测 N 个样本执行同一操作时的汉明重或汉明距离 $HW\times[N]$，然后计算 $HW\times[N]$ 与实际采集的功耗值 $P[N][L]$（L 为每个样本的采集功耗点个数）中的每一个功耗点 $P[N][j]$ 列的Pearson相关性系数，得到 k_i 对应的功耗相关系数曲线，共 L 个点，正确的 k_i 预测值对应的相关功耗曲线中会出现较大尖峰，反之则比较平缓。

3 针对PRESENT的相关功耗分析

3.1 功耗模型的选取

常用的加密电路功耗泄露模型有汉明距离模型和汉明重量模型两种：

(1)汉明距离模型

如果加密算法运行过程中某一数据 X 经运算直接转换为 X'，那么该运算产生的功耗可以用 X 和 X' 之间的汉明距离表示，即 $P_{WH}=K.\ HW(X\oplus X')$。其中，$P_{WH}$ 表示运算产生的功耗值，HW 代表汉明重量函数，$H(X\oplus X')$ 即为 X 和 X' 之间的汉明距离，K 是一个常量因子。

(2)汉明重量模型

在某些情况下，汉明距离模型可以通过对系统实现细节的了解而被加以简化。例如，对于预置数据为全0的输入数据，经过某种运算操作后，功耗依赖于输出数据 X 的汉明重量，即 $P_{WH}=K.\ HW(X)$。

可以看出，汉明重模型仅是汉明距离模型的一个特例，汉明距离模型更能准确地体现功耗变化，因此本文主要利用汉明距离模型来模拟加密过程中产生的功耗。

3.2 PRESENT相关功耗分析

PRESENT算法由31次轮运算 F 构成。每一轮加密运算由1次轮密钥加、16次 S 盒代换以及1次 P 置换操作组成。本文选取第1到第5轮的 S 盒查找操作输入输出结果的汉明距离作为执行该点时的功耗值，这样对于一次的PRESENT加密过程可获取含有80个点的模拟功耗轨迹。对于密钥的分析，采用分而治之的策略：一次分析4位，恢复所有64位密钥需进行16次分析。

具体的相关功耗分析基本步骤如下：

(1) 对于 N 个随机明文 P，执行加密操作，采集PRESENT加密过程中的功耗曲线，每条曲线采集80个功耗点，共 $N\times 80$ 个功耗点，形成 $N\times 80$ 实际功耗矩阵 PO。

(2) 针对PRESENT第一轮的 S 盒代换操作，S 盒输入为 $p_i\oplus k_{1,i}$（p_i 和 $k_{1,i}$ 分别为明文 P 和第一轮密钥 K_1 的第 i 个4位值），输出为 $S[p_i\oplus k_1,i]$，则变化的汉明距离为 $p_i\oplus k_1,i\oplus S[p_i\oplus k_1,i]$。

(3) $k_{1,i}$ 为4位，共有16个可能值：假设 $k_{1,i}$ 为0x00，p_i 已知，代入上式得到预测的汉明距离 H，代入 N 个样本得到 N 个 H 值；依次将 $k_{1,i}$ 所有可能值代入上式，得到 $N\times 16$ 个 H 值；形成 $N\times 16$ 的预测功耗矩阵 HW。

(4) 计算 $k_{1,i}$ 为某预测值时对应的预测功耗矩阵 HW 的一列（N 个值）同实际功耗矩阵 PO 的每一列（N 个值）（共 L 列）的Pearson相关性系数向量 $r[]$，形成一条功耗相关性曲线。如果 $k_{1,i}$ 预测正确，对应相关曲线中会出现较大峰值，否则相关曲线比较平缓。

(5) 对 $k_{1,i}$ 的其它可能值进行相关分析，最终得到16条相关曲线。

(6) 观察曲线中存在最大尖峰的曲线，其对应的 $k_{1,i}$ 值就是正确的密钥值。

(7) 重复上述步骤，直到获得64位的第一轮扩展密钥 K_1，然后进行 2^{16} 次暴力破解获得完整的80bit的PRESENT密钥 K。

4 PRESENT硬件仿真实现及相关功耗攻击实验

基于ASIC流程对PRESENT进行了硬件仿真实现以及功耗采集实验。首先基于VHDL实现了PRESENT加密，经Synopsys Design Compiler综合仿真后生成PRESENT的门

级网表，并通过 ModelSim 进行仿真后生成 VCD 文件，最后利用 Synopsys 公司开发的门级仿真软件 PrimePower 建立功耗数据采集平台对网表和 VCD 文件进行功耗仿真。后端的数据分析包括功耗波形文件处理，相关系数计算均基于 Matlab 程序完成。

图 2 为 20 个样本条件下，PRESENT 加密第一轮密钥 K_1 的 16 个 4 位密钥块对应的 16 条相关性曲线。其中 X 轴表示 16 个 4 位密钥块，Y 轴表示每个 4 位密钥块的 16 个候选值，Z 轴表示每个 4 位密钥块的每个候选值对应的 Pearson 相关性系数。对于每一个 4 位密钥块来说，具有最大 Pearson 相关系数的相关性曲线对应的密钥候选值即为正确的密钥块值。从图中可看出 $k_{1,0}=1, k_{1,1}=7, k_{1,2}=1, k_{1,3}=0, k_{1,4}=0, k_{1,5}=6, k_{1,6}=3, k_{1,7}=e, k_{1,8}=0, k_{1,9}=2, k_{1,10}=3, k_{1,11}=9, k_{1,12}=4, k_{1,13}=9, k_{1,14}=5, k_{1,15}=7$。

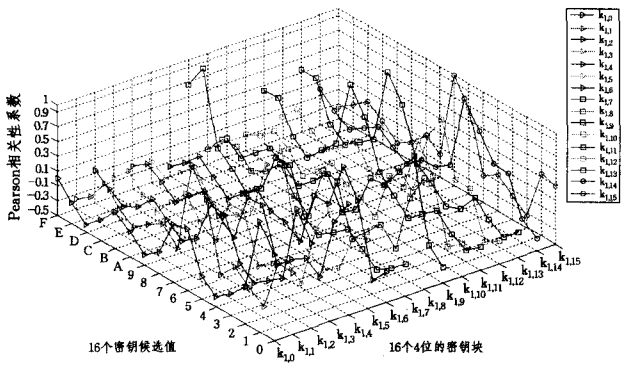

图 2　第一轮密钥 K_1 的 16 个密钥块对应的功耗相关性曲线

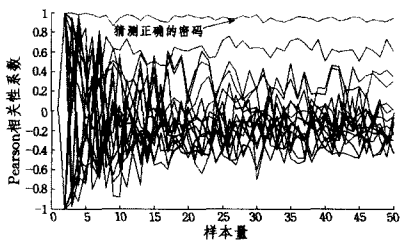

图 3　不同样本量某 4 位密钥块 16 个候选值对应的 Pearson 相关性系数

图 3 所示为不同样本量下猜测某 4 位密钥块值时，所有 16 个候选值对应相关功耗曲线的最大 Pearson 相关性系数图。其中，X 轴表示样本量大小，Y 轴表示 16 个候选值的 Pearson 相关性系数。可以看出在仿真环境下，当样本量大于 5 时，正确密钥块候选值对应相关功耗曲线的最大 Pearson 相关性系数在 16 个候选值中最大。

结束语　本文对 PRESENT 密码算法抗相关功耗分析能力进行了研究，提出了一种针对 PRESENT 分组密码的相关功耗分析方法，并通过仿真实验进行了验证。仿真实验表明，PRESENT 易遭受相关功耗分析威胁，通过对 5 个样本功耗曲线进行相关功耗分析，可恢复第一轮的 64 位密钥，结合密钥扩展方案得到 2^{16} 个 PRESENT 主密钥候选值，并进行暴力破解恢复 80 位 PRESENT 主密钥。为了避免这类攻击对密钥安全造成的威胁，需要对采用 PRESNET 的加密硬件及智能卡进行相应防护。因此，设计能够抵抗相关功耗分析的 PRESENT 密码算法电路是下一步的研究方向。

参 考 文 献

[1] ECRYPT. The Side Channel Cryptanalysis Lounge. http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html,2010-4-15

[2] Kocher P, Jaffe J, Jun B. Differential Power Analysis [C]// CRYPTO '99. LNCS 1666. Springer-Verlag,1999:388-397

[3] Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: An Ultra_lightweight BlockCipher[EB/OL]. http://www.ist_ubisecsens.org/publication/present_ches2007.pdf,2007-04-03

[4] Brier E, Clavier C, Olivier F. Correlation power analysis with a leakage model[A]// Joye M, Quisquater J J, eds. Cryptographic Hardware Embedded System-CHES 2004[C]. Volume 3156 of Lecture Notes in Computer Science. Springer-Verlag, 2004: 16-29

[5] 褚杰，丁国良，邓高明，等. DES 差分功耗分析攻击设计与实现[J]. 小型微型计算机系统，2007,11(11):2071-2073

[6] 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

[7] 邬可可，李慧云，于峰崎. 对同步流密码设备的相关性功耗分析(CPA)攻击[J]. 高技术通讯，2009,19(11):1142-1147

(上接第 11 页)

[27] Peng Pai, Ning Peng, Reeves D S. On the secrecy of timing-based active watermarking trace-back techniques[A]// Proceedings of the 2006 IEEE Symposium on Security and Privacy (SP'06), 2006[C]. Berkeley, California, USA: IEEE Computer Society, 2006:334-349

[28] 傅翀，钱伟中，赵明渊，等. 匿名通信系统时间攻击的时延规范化防御方法[J]. 东南大学学报：自然科学版，2009,39(4):738-741

[29] Jia Wei-jia, Tso F P, Ling Zhen, et al. Blind detection of spread spectrum flow watermarks[A]// Proceedings of the 28th IEEE International Conference on Computer Communications (Infocom'09), 2009[C]. Rio de Janeiro, Brazil: IEEE Computer Society, 2009:2195-2203

[30] Luo Xia-pu, Zhang Jun-jie, Perdisci R, et al. On the secrecy of spread-spectrum flow watermarks[A]// Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS'10), 2010[C]. Athens, Greece: Springer, 2010:232-248

[31] Houmansadr A, Kiyavash N, Borisov N. Multi-flow attack resistant watermarks for network flows[C] // Proceedings of IEEE International Conference on Acoustic, Speech, and Processing (ICASSP'09). Taipei, Taiwan: IEEE, 2009:1497-1500

[32] Zhang Lian-cheng, Wang Zhen-xing, Wang Qing-long, et al. Msac and multi-flow attacks resistant spread spectrum watermarks for network flows[A]// Proceedings of 2010 2nd IEEE International Conference on Information and Financial Engineering (ICIFE'10), 2010[C]. Chongqing, China: IEEE, 2010:438-441

[33] Paxson V, Floyd S. Wide-area traffic: the failure of poisson modeling[J]. IEEE/ACM Transactions on Networking, 1995, 3(3):226-244

[34] Abry P, Veitch D. Wavelet analysis of long range dependent traffic[J]. IEEE Transactions on Information Theory, 1998, 44(1):2-15

[35] 邵立松，窦文华. 自相似网络通信量模型研究综述[J]. 电子与信息学报，2005,27(10):1671-1676