

针对基于中国剩余定理 RSA 算法的光故障攻击分析

王红胜, 宋 凯, 张 阳, 陈开颜

(军械工程学院 计算机工程系, 河北 石家庄 050003)

摘 要: 基于中国剩余定理的 RSA 算法在智能卡和密码系统中得到广泛的应用, 其安全性直接关系到人们的利益. 本文使用一种简单的方法对密码芯片进行光故障注入, 通过激光照射开封后的芯片, 影响密码系统加密过程, 获取芯片内部的秘密信息. 实验说明对运行基于中国剩余定理 RSA 算法的密码芯片存在安全隐患.

关键词: 故障注入; 旁路攻击; 中国剩余定理; 密码芯片

中图分类号: TN918

文献标识码: A

文章编号: 1000-7180(2012)01-0038-04

Optical Fault Attack on CRT-Based RSA

WANG Hong-sheng, SONG Kai, ZHANG Yang, CHEN Kai-yan

(Department of Computer Engineering, Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: The Chinese Remainder Theorem (CRT) based RSA algorithm is very suitable in smartcard and cryptosystem, however the security benefit people's interest. This paper showed a method to practice an optical injection in cryptographic device. The attack was used laser irradiation the depackaged device to impact cryptographic computation process, obtained the secret information from the inside of chip. This paper presented implementation CRT-RSA algorithm in cryptographic device existed security issue.

Key words: fault injection; side channel attack; CRT; cryptographic chip

1 引言

如今, 旁路攻击方法已经成为密码分析学中一种重要手段. 通过智能芯片或者密码设备运行时泄露的物理信息(如时间、功耗、电磁和光等), 获取芯片内部的秘密信息. 其中一个最为普遍的旁路攻击方式是通过测量芯片执行密码运算操作时的功耗. P. Kocher 等人首先提出了一种叫做差分功耗分析的方法^[1-2], 利用统计学原理提取芯片内部的密钥. 也可以使用电磁^[3-4]、时间^[5]甚至是光^[6]等旁路信息来恢复内部的敏感数据. 这些被动式的攻击方式不需要在攻击时干预设备的运算, 而主动攻击方式通过使用外部或内部(如温度和电压)的变化来影响密码系统正常运行, 通过反馈回来的故障信息来获取芯片内部的秘密参量. 故障注入攻击是一种典型的主动攻击方式, 如使用紫外线对开封后的芯片进行

照射, 更改存储器中的部分内容, 使芯片运行时产生一定的故障. 剑桥大学计算机实验室使用闪光灯和激光对智能卡注入光故障^[7]. 另一种有效的故障注入攻击方式是电磁故障注入. 这种故障注入不需要对芯片设备开封, 如使用涡电流进行电磁故障注入可影响密码设备的正常运行. 图 1 为旁路信息分析模型. 旁路攻击特别是这种主动的故障注入攻击方式对密码设备的安全构成了更严重的威胁, 而且这类攻击能够应用在攻击一些常用的密码算法如 AES、RSA 等.

2 RSA 算法及攻击原理

RSA 是由麻省理工学院的 Ron Rives、Adi Shamir 和 Len Adleman 提出的一种公钥加密算法. RSA 在消息加密, 数字签名和身份验证中得到广泛使用.

收稿日期: 2011-04-02; **修回日期:** 2011-05-30

基金项目: 国家自然科学基金项目(60940019); 军械工程学院原始创新基金(YSCX0903)

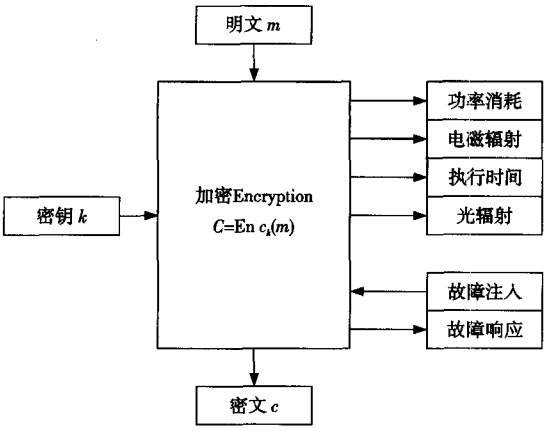


图 1 旁路信息分析模型

RSA 的安全性建立在大素数因子分解的困难性问题上,其数学安全性基础至今没有真正动摇.实践证明,在正确使用的前提下,RSA 被数学方法攻击破译的难度很大,或者说通常情况下在计算上是安全的.

2.1 标准 RSA 加密算法

表 1~表 3 简要概述了 RSA 算法的密钥生成过程以及加密解密过程.

表 1 RSA 算法密钥生成

1. 选取两个大素数 p 和 q , 其中 $p \neq q$
2. 计算 $n=pq$
3. 计算 $\phi(n)=(p-1)(q-1)$
4. 随机选择 $e: 1 < e < \phi(n), \gcd(e, \phi(n))=1$
5. 计算 $d: ed \equiv 1 \pmod{\phi(n)}$
6. 公钥为: $PU=\{e, n\}$
7. 私钥为: $PR=\{d, n\}$

表 2 RSA 算法加密过程

1. 明文: 选取任意明文 $M \in Z_n = \{0, 1, \dots, n-1\}$
2. 密文: $C=M^e \pmod{n}$

表 3 RSA 算法解密过程

1. 密文: $C \in Z_n$
2. 明文: $M=C^d \pmod{n}$

2.2 CRT-RSA 加密算法

使用中国剩余定理可以提高 RSA 加密算法的速度,这种方法使得 RSA 加密时间缩短到原来标准 RSA 算法的四分之一,这克服了传统 RSA 算法加密时间较长的问题,因此这种方法得到了广泛的使用.在确定 p, q 和 e 后,使用普通 RSA 算法为明文 M 加密为 $C=M^e \pmod{n}$,CRT-RSA 加密算法如

表 4 所示.

表 4 CRT-RSA 算法加密过程

1. $e_1=e \pmod{p}$
2. $e_2=e \pmod{q}$
3. $c_p=M^{e_1} \pmod{p}$
4. $c_q=M^{e_2} \pmod{q}$
5. $C=\text{CRT}(c_q, c_p)$
$=[c_p(q^{-1} \pmod{p})q+c_q(p^{-1} \pmod{q})p] \pmod{n}$

在这个算法中,假设 $p^{-1} \pmod{q}, q^{-1} \pmod{p}, e_1$ 和 e_2 都是事先计算好的,又由于计算中模数的变小,因此基于中国剩余定理的 RSA 算法在速度上具有一定的优势.

2.3 CRT-RSA 算法故障攻击原理

当使用中国剩余定理加速计算 RSA 系统时,如果密码设备在执行加密过程中出现了一定的故障,并且满足可以获得已知的密文和加密后的密文,那么就可以使参数 n 被分解. D. Boneh 和 R. A. De-Millo 等提出这种故障感应攻击理论^[8]. 即在 RSA 加密时,密码设备在计算 C_p (或 C_q , 但不能同时出错)过程中发生了错误,得到 $C'_p, C_p \neq C'_p$, 那么通过 C'_p 和 C_q 可以计算出一个错误的密文 $C'=\text{CRT}(C'_p, C_q)$, 图 2 为故障攻击模型. 可以计算出:

$$q = \gcd(((C')^e - M) \pmod{n}, n)$$

或者是已知正确的密文输出,可以计算出:
$$q = \gcd((C - C'), n)$$

所以这样的故障可以导致系数 n 被分解.

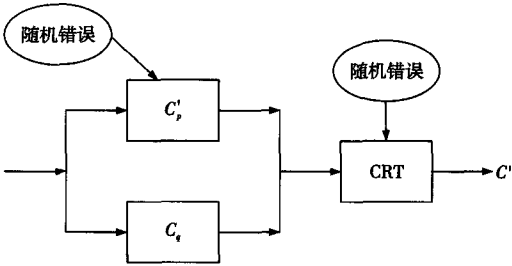


图 2 CRT-RSA 故障攻击模型

3 故障注入

3.1 激光对微控制器的影响

半导体晶体管对于电离辐射较容易受到损害.无论是核辐射、放射性同位素、X 光或者是宇宙射线都能使半导体晶体管受到影响.激光能够模拟电离辐射对半导体芯片的影响.其基本原理是当一个光子撞击金属时能够有如下的现象:如果光子的能量超过了 1.1eV,一个电子空穴碰撞偶就将生成.电子

吸收这个光子的能量,电子从原子键联中解放出来. 这样,电子逃离了金属的束缚,而且具有一定的动能形成电流. 这种诱导生成的电流能够引起随机存取数据存储器(SRAM)单元的翻转. 如果光子不具有足够的能量,电子就停留在金属中并且光子的能量再重新释放出来,称之为光电效应.

的实验目标是 SRAM 存储器,一个标准的六晶体管结构的 SRAM 单元如图 3 所示. 如果晶体管 T_3 被激光照射后短时间被打开,会引起由 T_1 和 T_3 构成的双稳态多谐振荡器其状态的改变. 通过对晶体管 T_4 的照射,单元将变成相反的状态. 然而本实验不需要精确的控制单元翻转的状态改变,只需要使 SRAM 某些状态改变或者影响程序流而使计算 C_p 或者 C_q 时出错.

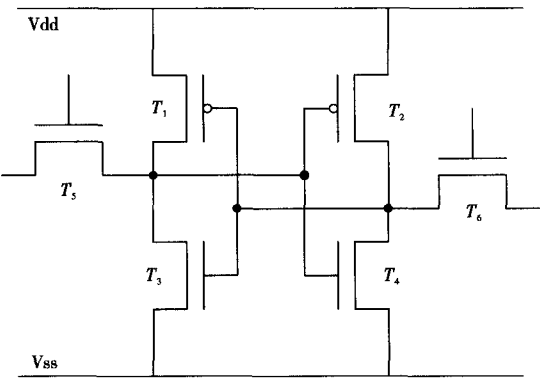


图 3 SRAM 单元六晶体管结构

3.2 光故障注入

对芯片注入光故障,需要使用激光照射芯片内部的晶圆,所以需要 对芯片进行解封. 激光能够改变芯片内部 SRAM 存储器单元的状态翻转. 使用的 AT89C52 微处理器,片内含有 8K 字节的 Flash 和 256 字节的 SRAM,其在晶圆上的位置可以使用放大镜或显微镜很容易的找到. 本实验并不需要十分精确的控制激光照射 SRAM 的位置进行故障注入,所以可以选择较为简单的激光设备进行实验. 为了达到故障注入的目的,我们选择了工业上用于定位操作的 200mW 的激光发生器,激光的波长为 650nm. 图 4 所示为使用激光对对开封后的微控制器进行光故障注入.

4 实验结果及分析

本实验使用的主要设备如表 5 所示. AT89C52 微控制器中运行基于中国剩余定理的 RSA 算法,密码系统没有任何的软件和硬件的防护措施,这样可以验证攻击的可行性. 微控制器系统与 PC 机通过

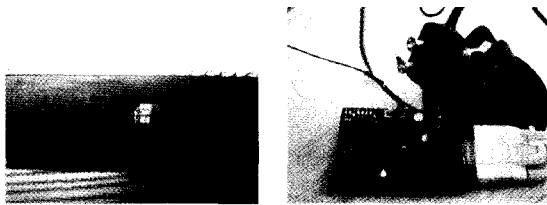


图 4 对微控制器进行光故障注入

串口连接,使用特定的通信协议收发明文密文. 使用示波器采集微控制器的功耗轨迹,观察故障注入时的功耗轨迹变化. 图 5 为本实验所使用的实验系统.

表 5 主要实验设备及参数

实验设备	参数
目标板	AT89C52,晶振 11.0592MHz
单路稳压稳流电源	DH1719A-3
数字存储示波器	Tektronix DPO4032,探头 P6139A
PC 机	P4 2.8G Hz,RS232 接口
激光器	650nm 红光点状激光器



图 5 实验系统

实验展示了 SRAM 存储器单元能够通过激光的照射被翻转,但是由于这种不是非常精确的攻击方法,不能控制 SRAM 具体某个位的改变. 攻击模型并不要求这种精确的攻击,只需要对 2.3 节中描述的过程注入故障即可. 实验结果如图 6 所示. 密码芯片计算 CRT-RSA 的 C_p 和 C_q 过程的功耗轨迹通过触发信号可以很清楚的辨认出来. 经过多次实

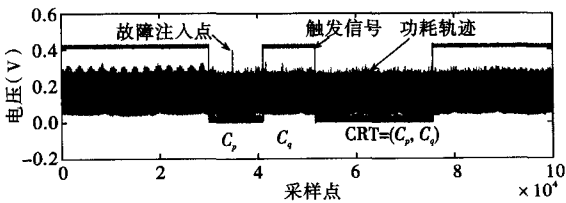


图 6 光故障注入功耗轨迹

验,故障注入到计算 C_p 过程,观察到在功耗轨迹上有一个明显的尖峰.这样计算 C_p 出现错误,而计算 C_q 正确,能够使用前面介绍的攻击模型对系数 n 进行分解.

5 结束语

实验证明了能够通过激光照射开封后的微控制器,针对运行 CRT-RSA 算法的密码系统达到故障注入攻击的目的.本实验不需要十分昂贵的设备,而且攻击模型对故障注入点的精确度要求不高,这对 CRT-RSA 算法的安全性构成了很大的威胁,这类算法的防护工作值得商榷.

参考文献:

- [1] Paul Ckocher, Joshua Jaffe, Benjamin Jun. Differential power analysis [C] // 19th Annual International Cryptology Conference. California: Advances in Cryptology, 1999.
- [2] 邹程,张鹏,邓高明,等.差分功率分析攻击中的信号对齐方法研究[J].微电子学与计算机,2009,26(7):227-229.
- [3] Dakshi Agrawal, Bruce Archambeault, Josyula R, et al.: Cryptographic hardware and embedded systems

[C]// The EM Side-channel(s). California: Springer, 2003.

- [4] 邓高明,张鹏,赵强,等.针对密码芯片的电磁模板分析攻击[J].微电子学与计算机,2010,27(1):1-4.
- [5] Paul C koher. Timing attacks on Implementations of diffie-hellman, RSA, DSS, and other systems [C] // 16th Annual International Cryptology Conference. California: Advances in Cryptology, 1996.
- [6] Korobogatov S. Semi-invasive attacks-a new approach to hardware security analysis[D]. London: University of Cambridge, Computer Laboratory, 2005.
- [7] Skorobogatov S, Anderson R. Cryptographic hardware and embedded systems workshop 2002 [C] // Optical fault Induction attacks. California, 2002.
- [8] Boneh D, Demill R A, Lipton RJ. On the importance of checking cryptographic protocols for faults [C] // Proc. of Advances in Cryptology - EUROCRYPT'97. Konstanz, Germany, 1997, LNCS 1233: 37-51.

作者简介:

王红胜 (1968—),博士,副教授.研究方向为军事信息安全.

宋凯 男,硕士.研究方向为军事信息安全.

张阳 男,硕士,助教.研究方向为军事信息安全.

陈开颜 女,博士,副教授.研究方向为军事信息安全.

(上接第37页)

- [3] Szeliski R, Kang S. Direct methods for visual scene reconstruction [C] // IEEE Workshop on Representations of Visual Scenes. Cambridge, Massachusetts, USA, 1995: 26-33.
- [4] 赵向阳,杜立民.一种全自动稳健的图像自动拼接融合算法[J].中国图象图形学报,2004,9(4):417-422.
- [5] David G Lowe. Object recognition from local scale invariant features [C] // International Conference on Computer Vision. Greece, Corfu, 1999:1150-1157.
- [6] David G. Lowe. Distinctive image features from scale-invariant key points[J]. International Journal of Computer Vision, 2004,60(2):91-110.
- [7] Herbert Bay, Andreas Ess, Tinne Tuytelaars, et al SURF: speeded up robust features[J]. Computer Vision and Image Understanding (CVIU), 2008, 110(3): 346-359.
- [8] Fishchler M A. Random sample consensus: a paradigm for model fitting with app location to image analysis and automated cartography [J]. Communication

Association Machine, 1981, 24(6): 381-395.

- [9] 张炜,刘伟,普杰信.一种基于 SIFT 和区域选择的图像拼接方法[J].微电子学与计算机,2010,27(6): 205-208.
- [10] 何小诚,黄凯,谭毅华,等.基于 Mean Shift 的自适应尺度变化跟踪算法研究[J].微电子学与计算机,2010,27(4):69-72.

作者简介:



王楠楠 女,(1980—),讲师.研究方向为图形图像处理技术.

王存睿 男,(1980—),讲师.研究方向为智能优化.

段晓东 男,(1963—),教授.研究方向为模式识别;

焉德军 男,(1965—),教授.研究方向为控制理论.