旁道攻击技术研究

曹云飞
（现代通信国家重点实验室）

摘　要：旁道攻击是一种针对密码设备的新型攻击技术。本文介绍旁道攻击技术，描述了旁道攻击技术的发展概括，给出和分析了一种可防旁道攻击的模指算法。

关键词：旁道攻击　能量攻击　时间攻击　错误攻击

引　言

在研究密码基本模块的时候，数学一个非常有用的工具。密码学家通常把密码模块作为一个数学函数来评估其安全性，可以如图1来说明。

在这个模式中，Alice和Bob试图使用密码在公开信道进行秘密通话。而窃听者Eve监听通话信道，想办法明白Alice和Bob的讲话内容。从传统角度来看，在此模式中能抵抗Eve的攻击的密码被认为是安全的。

然而，在现实世界中，在各种物理设备中实现密码会受具体实现环境的影响。电力设备(比如智能卡)消耗能量，产生电磁辐射，并且与周边环境温度相互反应等，这些物理效果将会被非法第三者所监控，并利用这些信息来进行密码分析。此类攻击技术称为旁道攻击(side channel attack)技术，研究表明此类攻击对很多密码的安全性产生巨大冲击。因此包含旁道攻击技术的密码模式应如图2表示。

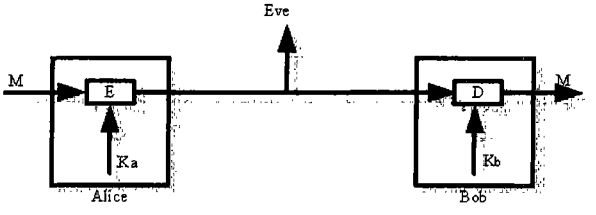

图1　传统的密码模式

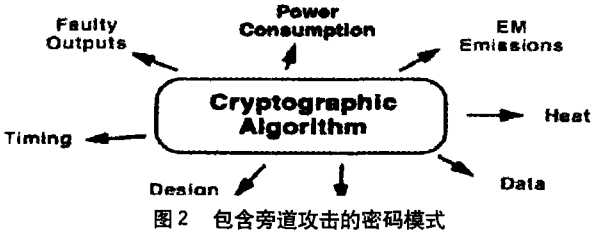

图2　包含旁道攻击的密码模式

旁道攻击是基于旁道信息的攻击，它利用密码分析技术，使用密码设备所泄漏的信息来恢复正在使用的密钥。旁道攻击类型很多种，我们只考虑最普通的，威胁最大的三种旁道攻击：时间攻击(timeing attack)，能量攻击(power attack)以及错误攻击(fault attack)。

由于旁道攻击技术发展迅猛，且攻击所需设备可行(硬件代价从几百到几千美元不等)，故旁道分析技术引起人们的广泛关注。攻击所需要的时间主要由攻击类型决定，一般而言，简单能量攻击只需要几秒钟可以破译一个智能卡，而差分能量攻击(differential Power analysis)需要几个小时。90年代后期，人们投入大量研究表明旁道所泄露的信息(比如运行时间，计算错误以及能量消耗等)对许多密码都是致命的。

研究现状

与旁道有关具有比较见解的观点是出现在文章《P. Wright. Spy Catcher: The Candid Autobiography of a Senior Intelligence》中，在1956年，British Intelligence (简称MI5)，试图破译埃及住伦敦大使馆的密码，当时受计算复杂度限制，无计可施。科学家Wright建议通过适当的放置一个扩音器，也许对破译有帮助。经反复测试后，使用一个Hagelin机器(一个基于密码的旋转圆筒)可以听见一个滴答声，于是通过监听这个声音所泄露的信息，使得MI5在以后几年内都窃取到这个大使馆的通话。

1995年10月29日，Paul Kocher[4]发现使用密码系统运行消耗的时间能够分析出密钥的值来。他进一步分析攻击者怎样利用密码系统运行的时间分析出(比如说RSA签名)签名的整个私钥。1999年，F. Koeune and J.J. Quisquater指出很多分组密码(比如Rijndael以及IDEA等)也存在此类风险。1998年A. Hevia and M. Kiwi研究表明：在类似RC5以及DES等中使用的比特滚动能泄露运行的Hamming重量。

1996年9月25日，Boneh，DeMillo and Lipton[2]宣布计算错误的出现将对密码系统的安全强度产生严重的影响。在某些的情况下，一个RSA签名错误危及签名者私钥的安全。由于智能卡小，可以被攻击者任意使用，可以人为的引起错误的出现，因此，此类攻击特别与智能卡的设计相关。此发现已引起广泛注意，密码学家迅速对其它密码系统的错误的影响进行研究。1997年Boneh，DeMillo and Lipton利用进行模指运算过程中引起的寄存器的错误对RSA(在实现中没有使用中国剩余定理，使用从右_左算法以及平方－乘法算法)进行有效的攻击，攻击时间为$O(n^3 \ln^2 n)$(其中n为RSA的模的比特长度)。

1997年E. Biham and A. Shamir[3]. 在文《Differential Fault Analysis of Secret Key Cryptosystems》中指出：错误分析可以运用到那些没有使用模乘的密码系统中去。具有比较典型的是，对称密码中使用比特或字节运算(比如：and，xor，rotate等运算)。研究表明了使用差分错误分析可以容易的破译DES密码。在个人PC机上Biham and A. Shamir使用50－200组密文就能破译DES的子密钥。

1996年，R. Anderson and M. Kuhn使用侵入错误(intrusive fault)模型能够分析出错误DES密码。

1998年6月22日，Kocher[5]将他的研究结果发表在纽约时代(New York Times)上，详细的概括了他最近的有关能量分析结果。其中一个令人吃惊的宣称是：对于一些密码系统，一个密码运行所消耗的能量痕迹完全可以揭露使用中的秘密密钥。更令人惊奇的声明是：通过检查大致1000条能量痕迹，Kocher和他的同仁能够破译许多智能卡，并给出数据(N =1，300，time ≈ 1 hour，equipment cost<$10K.)。

1999年，T. Messerges，E. Dabbish，and R. Sloan[6]. 在对RSA签名运算的SPA痕迹中进行分析中指出，平方和乘法运算可以通过能量痕迹进行区分，因而密钥比特很容易决定出来。

2000年，M.L. Akkar，R. Bevan，P. Dischamp，and D. Moyart[1] 指出差分能量分析很有力，攻击者研究来自不同输入的不同指令的多个能量消耗曲线，使用这些执行过程中的特定子集的统计差分，从而以自动的方式找到特定的密钥比特，2001年Kocher已经公开的声明：使用这个DPA技术，本质上可以破译金融系统使用的所有类型的智能卡。

2004年，Francois-Xavier Standaert，Siddika Berna等使用差分能量攻击对Rijndael的实现进行攻击。

可以看出国外对旁道攻击非常重视，许多密码学家在进行研究并取得显著的成功。

抗旁道攻击的模指算法

许多涉及到非对称密码算法(比如RSA或者Difffie－Hellman)都使用模指运算，攻击者往往可以利用模指运算所泄漏的信息来打破此方案。

计算模指运算$R=x^y \bmod n$的算法如下：

R=1

For i=k−1 down to 0; (k表示y的比特长度)

R=R × R mod n;

If(y_i=1) then R=R × x mod n (y_i表示y的第i比特)

从此算法可以看出用于y_i的比特值不同，所需运算也有很大差异。这导致较大的能量消耗差异，攻击者可以利用灵敏的设备在几分钟内破译该系统。

为了消除此算法所带来缺点，将此算法进行更改，算法实现如图3。

图3中k为n的最大字节数，步100是进行初始化，设置掩码值m_1的值为0。步105设置掩码值m_2，其值等于m_1比特取反，步115设置模乘寄存器Q的第j字节值。由于m1的值只能为0或255故，Q[j]的值也只能等于x[j]或R[j]，当

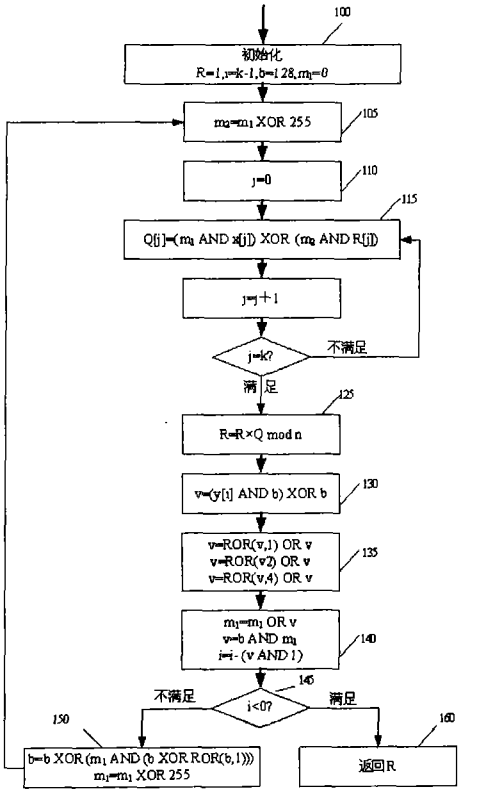

图3 修改的模指运算

m_i=0时Q[j]=R[j]；当m_i=255时，Q[j]=x[j]。步125更新R的值，为了提高运算速度，可以采用快速算法，不会影响到算法的实现安全性。步130通过加载y的第i字节值而得到v的值，由于b的值只可能为1，2，3，8，16，32，64或128，故v的值为0或b。步135三个比特滚动函数使得v的值为0或255，当步130中的v为非零时，步140中的v设置为255，否则v为0。步140，循环变量i以及字节计算器v更新，首先通过OR运算得到掩码值m_i(当v=0时，m_i为本身，否则m_i=255)，然后v临时存储b AND m_i的值，最后更新循环变量i的值(当v为奇数是i减去1，否则i不变)。步145，算法检测是否指数运算完成，如果i<0，处理步150，否则到步160返回最后的结果R。步150 对b的值进行更新，更新结果为b要么不变(当m_i = 0)，要么b向右滚动1比特。

在图3的算法中，消耗能量的地方为步125，其它地方为利于硬件实现的比特运算，其能力消耗可以忽略。此算法完全避开了因为模指的不同而进行的条件分支，从而不会泄漏任何有关模指的信息。也可推广到椭圆曲线实现，比如计算倍乘运算，还可应用于其它因为条件分支(非密钥依靠)而泄漏的关键信息算法上。

结 论

随着信息技术的大力发展，信息的安全性越来越重要，相应地出现了各种保密设备，如广泛使用的智能卡。它使用在移动电话，付费电视，计算机访问控制，身份卡，信用卡，电子商务等中。通常这些保密设备在通信时运行了存储在密码设备中的密码算法，攻击者的目标是从这些保密设备的运行中分析出正在使用的秘密密钥，从而得出一些关键内容，进行非授权的操作。设计安全的密码算法是密码算法设计者的主要任务，然而密码算法的最终实现总是依赖于电路实现，与算法设计的有效性、简单性准则相比较，在电路实现中的安全性还没有引起人们的足够重视。

一个密码算法从理论上是不可破的，然而，历史证明一个安全的密码算法往往屈从于它们实现中的弱点。旁道攻击涉及到保密设备的分发者和使用者以及密码算法的设计者，目前密码硬件的设计者以及密码算法设计者很少从算法实现上考虑抗击旁道攻击的技术，这必然为信息系统带来巨大潜在的安全隐患。因此，对旁道攻击的研究就显得特别重要和迫切，可以看出，开展旁道技术研究，有助于在密码系统中采取切实可行的措施来实现真正通信安全。

参考文献

[1] M.L. Akkar, R. Bevan, P. Dischamp, and D. Moyart. Power Analysis: What is now Possible. In T. Okamoto, editor, Advances in Cryptology — Proceedings of ASIACRYPT 2000, volume 1976 of LNCS, pages 489{502. Springer-Verlag, 2000.

[2] M. Bellare and P. Rogaway. The Exact Security of Digital Signatures { How to Sign with RSA. In U. Maurer, editor, Advances in Cryptology — Proceedings of EUROCRYPT 96, volume 1070 of LNCS, pages 399{416. Springer-Verlag, 1996. Available from http: //www-cse.ucsd.edu/users/mihir.

[3] E. Biham and A. Shamir. Differential Fault Analysis of Secret Key Cryptosys-tems. In B. Kaliski, editor, Advances in Cryptology - CRYPTO '97, volume 1294 of LNCS, pages 513{525. Springer-Verlag, 1997.

[4] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman,RSA,DSS and Other Systems. In N. Koblitz, editor, Advances in Cryptology -BIBLIOGRAPHY 89 CRYPTO '96, volume 1109 of LNCS, pages 104{113. Springer-Verlag, August 1996. An alternate version is available from http: //www.cryptography.com/timingattack/paper.html.

[5] P. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In M. Wiener, editor, Advances in Cryptology — CRYPTO '99, volume 1666 of LNCS, pages 388{397. Springer-Verlag, August 1999. Available from http: //www.cryptography.com/dpa/Dpa.pdf.

[6] T. Messerges,E. Dabbish,and R. Sloan. Investigations of Power Analysis Attacks on Smartcards. In USENIX Workshop on Smart-card Technology, pages 151{161, May 1999. Available from http: //www.eecs.uic.edu/~tmesserg/papers.html.