<<分组密码的攻击方法与实例分析>>

图书基本信息

书名：<<分组密码的攻击方法与实例分析>>

13位ISBN编号：9787030266095

10位ISBN编号：7030266099

出版时间：2010-5

出版时间：科学出版社

作者：李超，孙兵，李瑞林　著

页数：234

前言

随着计算机网络和通信技术的飞速发展，人们对信息的安全存储、处理和传输的需要越来越迫切，信息的安全保护问题已经显得十分突出，人们正面临着信息安全的巨大挑战，作为信息安全理论和技术的基础，密码学扮演着十分重要的角色，分组密码作为对称密码学的重要分支，已经在信息安全领域中得到了广泛应用，分组密码的研究内容主要包括分组密码的设计与分析，两者相互作用，共同推动着分组密码理论的发展，对于从事密码学相关领域的研究人员来说，深刻理解分组密码的分析方法是从事分组密码理论与应用研究的前提，自20世纪90年代差分密码分析和线性密码分析提出以来，分组密码的分析理论有了长足的发展，但有关分组密码分析的理论成果大多散落在国内外与密码学相关的学术会议论文集上，专门讲述分组密码攻击方法的著作并不多见。

国防科技大学李超教授及其课题组多年来从事分组密码相关理论的研究，取得了一系列学术成果，这些成果相继发表在国内外重要期刊和学术会议论文集上，引起了国内外密码学者的高度关注，最近，他们结合自身在密码分析方面的工作体会，编写了《分组密码的攻击方法与实例分析》，通过对一些具体密码算法的实例分析，系统论述了分组密码攻击方法的基本原理与应用。

我相信，本书的出版对于从事分组密码的理论与应用研究将具有十分重要的参考价值。

内容概要

本书以美国AES计划和欧洲NESSIE计划等推出的著名分组密码算法为背景，系统地介绍分组密码的攻击方法和实例分析，包括差分密码攻击、线性密码攻击、高阶差分密码攻击、截断差分密码攻击、不可能差分密码攻击、积分攻击、插值攻击和相关密钥攻击等主要攻击方法的基本原理及其应用实例.
本书可以作为密码学专业和信息安全专业高年级本科生和研究生的选修课教材，也可以作为从事密码理论和方法研究的科技人员的参考书.

<<分组密码的攻击方法与实例分析>>

书籍目录

章节摘录

（10）插值攻击由Jakobsen和Knudsen提出，如果一个密码算法对于固定的密钥是低次多项式函数，或者这个多项式的项数较少，可以估算出来，则通过插值的方法可以得到其代数表达式，从而有可能恢复出密钥；孙兵等在FSE 2009上改进了插值攻击的方法，在改进的插值攻击中，多项式函数的某些项的系数可以精确计算出来，从而利用有限域上的Fourier变换也可以求出相应的密钥。
另外，如果密文可以写作两个多项式的商，且这两个多项式的项数可以估计出来，那么同样可以恢复出相应的密钥。
（11）非满射攻击首先由Rilmen，Preneel和Win给出，当Feisel结构密码的轮函数不是满射时，就可以利用其输出分布的不均匀性对算法实施攻击。
由于SPN结构密码采用的函数均是单射，因此非满射攻击对SPN结构密码一般无效。
针对n-Cell结构算法，李瑞林等提出了一种如何在各个组件都是满射的密码算法中构造非满射区分器的方法。
（12）代数攻击由Courtoi和Pieprzyk提出，该攻击方法主要通过求解一个多变元的代数方程组来恢复密钥。
尽管部分密码学者认为这可能是对。
AES算法最具威胁的攻击，但这一方法目前仍受到很多密码学者的质疑。
该攻击对序列密码比较有效，由此推动了密码学界对布尔函数的代数免疫度的研究。
（13）滑动攻击由Biryukov和Wagnei提出,该方法对分析轮函数比较弱且密钥扩展方案呈现某种周期性的迭代分组密码时较为有效，若将算法的轮变换向前或向后平移若干轮后，所得的算法与另一个算法几乎相同，则对该密码可实施滑动攻击。
这个攻击方法的最大特点就是攻击方法与密码加密轮数无关。
（14）相关密钥攻击由Biham和Knudsen研究LOKL法时分别独立提出，该方法与其他密码分析方法不同之处在于它更多地考虑了密钥扩展算法的性质，攻击的假设更加苛刻，该思想提出后，人们对一系列分组密码的密钥扩展算法进行了研究，并将其推广至相关密钥差分攻击。
一般而言，若密钥扩展算法的密码学性质强，如不同轮密钥之间不具有简单的递归性质、线性逼近，甚至相等的情况，算法可以抵抗相关密钥攻击。
（15）相关密码攻击是伍宏军提出的攻击方法，如果一个密码算法有不同轮数的输出，且采用相同的密钥扩展算法，则低轮密码的输出可以看作高轮密码的中间状态，据此攻击者可以获得密钥信息。

版权说明