<<量子密码学>>

图书基本信息

书名：<<量子密码学>>

13位ISBN编号：9787030172761

10位ISBN编号：7030172760

出版时间：2006-6

出版时间：科学出版社

作者：曾贵华

页数：280

<<量子密码学>>

前言

人类的进步得益于科学研究的突破、生产力的发展和社会的进步。

计算机、通信、半导体科学技术的突破，形成了巨大的新型生产力。

数字化的生活方式席卷全球。

农业革命、工业革命、信息革命成为人类历史生产力发展的三座丰碑。

古老的中华大地，也正在以信息化带动工业化的国策下焕发着青春。

电子政务、电子商务的各种信息化应用之花，在华夏沃土上竞相开放，炎黄子孙们，在经历了几百年的苦难历程后，在国家崛起中又迎来了一个运用勤劳和智慧富国强民的新契机。

科学规律的掌握，非一朝一夕之功。

治水、驯火、利用核能都曾经经历了非常漫长的岁月。

不掌握好科学技术造福人类的一面，就会不经意地释放出它危害人类的一面。

生产力的发展，为社会创造出许多新的使用价值。

但是，工具的不完善，会限制这些使用价值的真正发挥。

信息化工具也和农业革命、工业革命中人们曾创造的许多工具一样，由于人类认识真理和实践真理的客观局限性而存在许多不完善的地方，从而形成信息系统的漏洞，造成系统的脆弱性，在人们驾驭技能不足的情况下损害着人们自身的利益。

世界未到大同时，社会上和国际间存在着竞争、斗争、战争和犯罪。

传统社会存在的不文明、暴力，在信息空间也同样存在。

在这个空间频频发生的和被有些人利用系统存在的脆弱性运用其“暴智”来散布计算机病毒，制造拒绝服务的事端，甚至侵入他人的系统，盗窃资源、资产，以达到其贪婪的目的。

人类运用智慧开拓的信息疆土正在被这些暴行蚕食破坏着。

随着信息化的发展，信息安全成为全社会的需求，信息安全保障成为国际社会关注的焦点。

因为信息安全不但关系国家的政治安全、经济安全、军事安全、社会稳定，也关系到社会中每一个人的数字化生存的质量。

信息革命给人类带来的高效率和高效益是否真正实现，取决于信息安全是否得以保障。

什么是信息安全？

怎样才能保障信息安全？

这些问题都是严肃的科学和技术问题。

面对人机结合和非线性、智能化的复杂信息巨系统，我们还有许多科学技术问题需要认真研究。

我们不能在研究尚处肤浅的时候，就盲目乐观地向世人宣称，我们拥有了全面的解决方案；我们也不能因为面对各种麻烦，就灰头土脸，自暴自弃，我们需要的是革命的乐观主义精神、坚忍不拔的奋勇攀登科学技术高峰的坚定信念。

<<量子密码学>>

内容概要

《量子密码学》是《信息安全国家重点实验室信息安全丛书》之一。
书中深入系统地论述了量子密码的基本概念、实现原理、物理基础和信息论基础、协议与算法、密码系统的实现技术以及与经典密码的关系，并探讨了量子密码的可能应用。
《量子密码学》共九章，构建了量子密码的整体框架体系。
主要内容包括密码学及量子密码的概况、量子比特的数学性质和物理性质、量子密钥、量子密码体制、量子认证、量子秘密共享、量子安全协议、量子密码分析、量子密码系统的实现技术及典型量子密码系统的介绍。
《量子密码学》可作为密码学、物理学、量子光学、计算机科学、通信和数学等学科的科研和工程技术人员的参考书，也可供相关专业的高校师生参考。

<<量子密码学>>

书籍目录

章节摘录

由于量子密码中存在具有信息安全的量子密码方案，也提出了基于计算复杂度的量子密码方案，因此，量子密码的安全性理论基础是量子信息理论和量子计算复杂性理论。
基于量子信息理论的信息系统以量子物理学为基础，而基于Shannon信息论的信息系统以经典物理学为基础。
众所周知，量子物理学和经典物理学遵循不同的法则，因此量子信息理论不能简单地套用Shannon信息论，必须在Shannon信息论的基础上建立新的理论体系。
针对量子密码的安全性而言，主要有两种信息论分析方法。
一方面，由于量子密码系统中的通信者和攻击者往往是通过测量而获取信息的，而测量结果只能反馈经典信息（测量后的比特是经典比特），因此可采用Shannon信息理论分析量子密码系统的安全性。由于这种方式可以给出确定的值，很多学者采用这种分析方式。
另一方面，量子比特携带了量子信息，可从量子信息理论的角度分析量子密码系统的安全性，一些学者（如A.Cabello等人）开展了这方面的研究。

量子计算机的概念提出后，量子计算复杂性理论随之被提出。
从1992年开始，Brassard，Bennett，Deutsch等人陆续分析了量子计算复杂性，发现量子图灵机不能解决所有的NP问题（这里著者强调，该结论还没有得到严格的证明），并提出了量子计算复杂性理论。以这套理论为基础，基于量子计算复杂性的密码体制成为量子密码的一个发展方向。

量子信号检测理论不同于经典信号检测理论，因为在量子信息系统中，任何扰动都会留下痕迹，为检测提供依据，这个特点为量子密码系统的安全性分析提供了基础。
事实上，量子密码协议或算法是否安全与对敌手的检测情况紧密结合在一起，因此，量子密码表现出来的对攻击者的可检测性应该有一个合适的检测标准。
例如，在量子密钥分配中对窃听者的检测标准对系统的安全性非常重要，如果没有合适的检测标准，量子密钥分配系统可能不安全，因为通信中合法通信者可能把有窃听的情况视为安全！
显然，如何检测敌手的存在与否是量子密码中的一个重要的技术问题。

……

版权说明