Security of Continuous-Variable Quantum Cryptography

连续变量量子密码安全

马祥春 王明阳 宋震 盖新貌 著

国防工业出版社
National Defense Industry Press

连续变量量子密码安全

Security of Continuous – Variable Quantum Cryptography

马祥春　王明阳　宋震　盖新貌　著

国防工业出版社

·北京·

内容简介

量子密码和量子保密通信是密码前沿领域研究最为活跃的热点之一，它可为我们的信息传输和隐私保护提供最理想的安全保障。本书针对连续变量量子密码实际系统可能存在的缺陷或非完美性，提出了若干种量子黑客攻击手段，研究分析了实际系统的安全性，给出了相应的安全防御措施，同时提供了测量设备无关协议的安全性理论分析及实验实现方案，这将有望使实际系统一次性关闭所有的探测端漏洞，免疫所有的探测端攻击。

本书内容专业性强、理论推导严谨，具有一定的启发性和实用性，适合相关专业研究生阅读和学习，也可作为密码领域研究人员的参考书。

图书在版编目(CIP)数据

连续变量量子密码安全 / 马祥春等著. —北京：国防工业出版社，2018.5

ISBN 978-7-118-11575-8

Ⅰ. ①连… Ⅱ. ①马… Ⅲ. ①量子-密码-研究 Ⅳ. ①TN918.1

中国版本图书馆 CIP 数据核字(2018)第 111773 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号　邮政编码 100048)

天津嘉恒印务有限公司印刷

新华书店经售

*

开本 710×1000　1/16　**印张** 8½　**字数** 146 千字

2018 年 5 月第 1 版第 1 次印刷　**印数** 1—2000 册　**定价** 32.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)88540777　　发行邮购：(010)88540776

发行传真：(010)88540755　　发行业务：(010)88540717

前　言

在信息和网络时代，量子密码不仅可以允许合法的通信方进行安全通信，还能够为我们日常生活中所处理的个人信息、隐私及重要数据提供无条件安全保护。相比于传统的经典密码，量子密码的安全性是由量子力学法则所保证的，可以实现信息论安全。

然而，由于实际系统中存在一些非完美性等因素，量子密码系统的安全性可能会受到一定程度上的损害。因此，在当前的密码应用中，研究实际系统的安全性具有非常重要的现实意义。本书正是聚焦连续变量量子密钥分发（CVQKD）的现实安全性研究，力图增强实际系统的安全性和可靠性。

首先，针对 Bob 端分束器的分束比依赖于波长的缺陷，本书完整提出了 CVQKD 波长攻击方案，攻击差分探测协议系统。攻击策略显示，Eve 发送给 Bob 的两束光经过平衡零拍探测器（BHD）后引入的散粒噪声，是 Bob 的探测结果偏离 Eve 的窃取结果的主要原因，因此需要仔细考虑。在这种情况下，本书首先具体分析了波长攻击下必须满足的方程的解，然后精确计算了 BHD 的散粒噪声，从而得出结论，在某些参数范围内波长攻击才能够被成功实施。

进一步，本书还分析了本底光随时间波动的 CVQKD 实际系统的安全性，该波动为窃听者窃取密钥打开了后门。窃听者通过降低本底光的强度可以模拟这种波动，从而隐藏高斯集体攻击留下的痕迹。数值模拟显示，如果 Bob 不监控本底光的强度，且不使用本底光强度的瞬时值对其探测结果进行归一化，则密钥率将会被严重高估。

另外，本书同时还发现本底光的强度波动不仅使 Bob 端探测结果的归一化变得困难，还可以改变非理想 BHD 的信噪比，从而可能会严重损害 CVQKD 实际系统的安全性。但进一步研究发现本底光的强度也可以被合法的通信方操控，即被调节稳定在一个预定的常数值上，以消除本底光的波动影响，从而避免 Eve 对本底光的可能攻击。而且，针对噪声信道，特别是城域 QKD 网络信道，通过调节本底光的强度，改变实际 BHD 的信噪比使其达到最优值，还可以提高实际系统的密钥率。在这种情况下，BHD 的高探测效率、低电子学噪声的设计要求也可以被降低。为了实现这种操作，本书给出了相应的实验方案，以此来增强

实际 CVQKD 系统的安全性。

通过分析单向 CVQKD 实际系统的现实安全性，除了克服实际系统中具体的非完美性或安全性漏洞外，本书还独立提出了连续变量测量设备无关（MDI）QKD 方案，即使用高斯调制相干态源来实现，从而可以一次性关闭所有的探测漏洞。该方案不仅可以将探测过程交给非可信的第三方，从而免疫所有的探测器侧信道攻击，相比于离散变量 MDI－QKD 协议，该方案还可以具有很高的密钥率。因此，非常适合高安全量子信息网络的构建。

针对 CV MDI－QKD，本书分别证明了其在单模攻击和双模攻击下的安全性。基于高斯集体攻击的最优性及纠缠的单配性（非共享性）结果显示，双模相干攻击，即两量子信道被潜在的窃听者 Eve 反关联，是次优的，而单模攻击，如每个信道上独立的纠缠克隆攻击，在渐近情况下是最优的。在这种情况下，密钥率的下界值可以被计算出来。而且，对于这样的基于中继的协议，由于中继是非可信的，所有这种破坏中继测量的多模攻击都应该被约化成单模攻击来进行安全性分析，从而简化分析过程。因此，向信道中注入纠缠或相关噪声并不能为 Eve 进行窃听带来更多的优势。

最后，为了使 CV MDI－QKD 能够应用于安全通信，基于局域制备本底光的测量原理，本书探索性地提出了真正实现该协议的实验方案。该方案不仅解决了 Alice、Bob 和 Charlie（Bell 中继）之间参考系的校准和同步问题，还极大地简化了发送方和接收方的光学布局，因此很容易进行芯片级集成。

另外，本书还探讨了平衡零拍探测器和大功率脉冲激光器的制备，弄清楚了它们的内部结构，这对高安全 CVQKD 系统的构建具有重要的意义。

本书从攻击的角度研究了连续变量量子密码实际系统的安全性，内容新颖，思路清晰，条理性强，可为相关专业领域的研究人员提供借鉴和参考。

本书编写过程中得到了梁林梅教授、孙仕海讲师、江木生博士等人的极大鼓励和支持，他们对本书的波长攻击、本底光强度攻击等相关章节内容提出了许多重要的建议，在此表示深深的感谢！本书的若干研究成果是在与国防科技大学的李春燕博士、周艳丽博士、唐光召、陈欢、单雨竹、徐耀坤、王灿、刘苹、桂明、石惟旭等人交流讨论的基础上得到的，在此一并表示衷心的感谢！

感谢国防工业出版社的工作人员为本书的出版所付出的辛勤劳动！

由于作者水平有限，前沿发展太快，时间仓促，书中的不足和疏忽之处恳请各位专家和广大读者批评指正。

目　录

第1章 绪 论

随着时代的发展、科技的进步，密码目前已经广泛应用于我们日常的生产、生活等各类活动中，如银行卡、信用卡、网上账户等都需要进行密码的设置和认证。特别是政治、军事以及商业，为保证高度机密的信息或数据安全传输和使用，密码的重要性无可置疑，其安全性更是极其关键。密码的发明和使用已逐渐成为一门完善的、博大精深的科学和技术，称为密码术（Cryptography）[1]。近年来，密码与量子力学结合形成量子密码（Quantum Cryptography）[2]，以极其迅猛的速度发展，掀起了一场密码界的风暴，引起了学术界、商业界，甚至包括政府、公司等各大机构或团体的广泛关注和研究。

1948 年，美国 Bell 实验室 Claude E. Shannon 发表了著名论文《通信的数学理论》（*A Mathematical Theory of communication*）[3]，奠定了现代信息理论的基础，标志着经典信息论与编码理论学科的诞生[4]。从此，数字通信领域飞速蓬勃发展，科技创新日新月异。伴随着计算机科学的发展，我们所处的信息社会以前所未有的态势大跨步前进。

经典信息论的深入发展，必然会涉足量子领域。事实上，从信息论的角度研究量子物理，这一思想在 20 世纪后期迅速发展起来，并逐渐发展成量子信息科学（Quantum Information Science），信息的终极支撑是量子的而非经典的观念也逐渐被人们所接受。其中，信息存储和信息传输极限的研究催生出了量子通信（Quantum Communication）领域，而计算能力极限的研究则产生了量子计算（Quantum Computation）领域或量子信息处理（Quantum Information Processing）领域。早在 20 世纪 70 年代，Stephen Wiesner 便提出了量子货币（Quantum Money）的概念，量子密码术的概念也由此产生[5]。几年后，Charles Bennett 和 Gilles Brassard 提出了两种密码类原型：密钥分发（Distribution of Secret Keys）和比特承诺（Bit Commitment）[6,7]。从此，量子密码迅猛发展，掀起了理论研究和实验探索的热潮。

量子密码的发展，也带动了量子纠缠的研究。量子密码和量子纠缠是密不可分的，量子密码制备和测量协议与基于纠缠的协议（或称密钥提取协议），安全性证明是等价的[8]。因此，量子密码与量子纠缠，二者相互促进，共同发展，

不断揭示新的物理现象和物理规律。1997 年，Dik Bouwmeester 实验实现了基于光子量子比特的量子隐形传态（Quantum Teleportation）[9]，使得 Charles Bennett 在 1993 年提出的该概念变成了现实[10]。随后，基于各种物理载体的量子隐形传态相继被实验实现，关于此领域的详细介绍可参考综述性文献[11，12]。这其中就包括纠缠态的隐形传输（Teleportation of Entanglement）[13]，或称为纠缠交换（Entanglement Swapping）[10,14]，为后来测量设备无关协议（参考第 6 章的介绍）的提出奠定了基础。近年来，远距离的量子纠缠分发或量子隐形传态，包括纠缠交换[15]，在自由空间中都得到了实验演示或验证，其中就包括远距离量子密码协议的应用实现[16,17]，大大促进了远距离量子密码的发展。因此，纠缠的研究和发展必将会使量子密码或量子通信发展更加成熟，应用更加广泛。

量子密码的发展也同时促进了 Bell 不等式[18]的实验验证。Bell 不等式的实验验证是为了证明量子力学的正确性。这种正确性是指量子力学所预测的结果不能用局域实在论进行解释。因此，利用 Bell 不等式有可能从实验上来解决 EPR 佯谬问题[19]。但遗憾的是，直到今天，真正的无漏洞的 Bell 不等式的实验验证仍然没能实现（但已取得实质性进展[20]，详细细节可参考综述性文献[21]）。因此，这激励着科学家不断挑战极限，持续研究，寻找突破。特别是，Bell 不等式的背离预示着非局域相关性的存在，或者说量子纠缠的存在，而这又可以应用于量子密码，即后来提出的全设备无关量子密钥分发协议（见后续章节相关介绍）。量子密码关于 Bell 不等式的理论研究又迫使其实验验证不断向前迈进，二者共同发展，相互促进。量子密码为 Bell 不等式的研究提供了应用平台，而后者又大大丰富了量子密码的内容和思想，特别是 Bell 不等式的背离还应用到了随机数的产生等更加广泛的领域。

随机数是量子密码不可或缺的组成部分，量子密码的实现涉及真随机数的使用，因此这又极大地促进了量子随机数的研究。量子随机数产生于量子真随机过程，该随机过程无法用经典力学进行解释和确定，因此具备自然随机性或真随机性。但量子随机过程总是与经典随机过程相混合，或量子随机性总是存在经典噪声，怎样从这种混合随机过程中提取出真正的量子真随机数，成为该领域研究的主要内容。然而，量子密码的不断发展，促使了更多种类的量子随机过程的发现及各类新思想的类比应用。例如，量子密钥分发中的设备无关思想应用于可验证的随机数产生[22]。利用 Bell 不等式的背离可以验证随机数的量子真随机性，并可去除设备可信假设条件。因此，量子密码促进了量子随机数的研究，量子随机数的深入发展也为量子密码提供了足够的安全保障。

量子密码的快速发展，也迫使量子计算领域快速发展。1994 年，美国 AT&T 公司的研究员 Peter Shor 提出大数质因子分解量子算法[23,24]，摧毁了经典密码

的安全性基础——经典算法的计算复杂度，从此量子密码引起了各界广泛的关注和深入研究。时至今日，量子密码率先进入商用化、实用化阶段，而量子计算机的成型和广泛使用仍尚需时日。虽然 D - wave 公司制造的 D - wave 计算机[25]仍引领该领域不断向前发展，但真正的通用量子计算机的诞生还需要技术的进步、科学的发展。在这种情况下，量子密码的发展不断刺激并带动着量子计算领域进行突破和创新，量子密码的研究也为量子计算[26,27]注入了活力，不断使量子信息领域朝着高、精、尖方向深入发展。另外，同时掌握量子密码和量子计算机技术对大国信息安全体系来说也显得尤为重要，二者犹如矛和盾的关系，两者结合起来才能在未来信息争夺中占居有利位置。

量子密码作为量子信息科学最重要的一个分支，其研究极大地促进了量子技术的发展。量子信息资源的制备和量子态的操控技术构成了量子技术的主体框架。量子技术的发展使得量子光学、集成光子学[28]等都有了长足的进步和发展。量子芯片、微纳波导等新型的片上系统及其片上操作[29]，使得量子密码应用更加广泛。通信设备的集成化、小型化使得两地通信更加方便、快捷，量子密码也将会很快应用到星地通信、全球网络。可以预见，在未来信息全覆盖的地球村，量子网络将会使通信变得更加安全、可靠。

量子技术的进步将毫无疑问地促进量子信息的发展，而量子信息的进一步深入研究也将会加深人们对量子力学的认识和理解，促使人们从信息论的角度来重新认识量子力学，甚至重构量子力学，使得量子力学有可能建立在人们可以普遍接受的、直观的物理基础之上，而不是一系列数学公理之上。例如，ChristopherA. Fuchs 和 Gilles Brassard 提出自然界允许密钥分发而禁止比特承诺的原理可以导出量子力学[30,31]，但该结论还不够完善，很快被反例推翻[32,33]。然而，这足够启示人们，量子力学的深刻理解离不开信息学的深入发展，二者相辅相成，相互促进，极有可能催生出新的物理现象，发现新的物理规律，产生新的物理认识和理解，有待我们去进一步探索和挖掘。

1.1 量子密码研究背景

量子密码的核心是量子密钥分发（Quantum Key Distribution，QKD），通常量子密码也称为量子密钥分发，但实际上量子密码的概念更加广泛，包含所有可能与秘密性有关的工作。然而本书所研究的量子密码范畴仅局限于量子密钥分发，因此在后续章节的叙述中，若非特别说明，二者指代同一个意思。下面我们就量子密码的发展历程来简要介绍本书工作的研究背景和研究现状，以此指明本书工作的研究动机和研究目标。

量子密钥分发允许远距离的通信双方，通常称为 Alice 和 Bob，建立一串无条件安全的密钥。这里的无条件安全（Unconditional Security）是指，安全性的证明不需要对窃听者（Eve）的计算资源和计算能力，以及作用在信号上的操控技术强加任何限制。因此，无条件安全的概念不同于通常所说的绝对安全，严格来说，绝对安全是不存在的。实际上，任何密码机制的产生都需要建立在一些预先假设的条件基础之上的。量子密码的建立同样需要一些假设性条件或强制性要求[34]，比如：

（1）通信双方的物理空间是安全的。即窃听者不能够侵入他们的实验室或设备直接获取产生的密钥或测量背景的选择等其他有用的信息，且通信双方的实验室或设备没有多余的信息经侧信道（Side Channel，又称旁路信道）或后门泄漏出去。

（2）通信双方所使用的随机数发生器是可信的。即量子态的发送选择和测量选择等是真正随机的，且不被窃听者所知道。因此，QKD 实验所使用的随机数发生器一般是量子真随机数发生器，以保证其可信度。

（3）通信双方的 QKD 设备是可信的。即双方的量子态制备设备和测量设备几乎处在完美的控制之下，双方完全清楚相关性的建立过程，包括希尔伯特空间的维度等。

（4）通信双方的存储器、计算机等经典设备是可信的。即保证量子设备所产生的经典数据的存储和处理是安全的。

（5）通信双方拥有可靠的不可篡改的公共经典信道。即保证双方的经典交互信息可以无误地传输而不被任意篡改。

（6）量子物理理论是正确的。通信双方和窃听者都服从量子力学法则。

这些假设性条件主要是针对合法通信双方的，而不是针对窃听者的窃听能力，所以与先前所提到的无条件安全并不矛盾。一般来说，大多数 QKD 协议所申明的无条件安全几乎都要建立在以上假设条件基础之上，只有少部分 QKD 协议可以放宽或不需要其中的某些限制性要求，例如，全设备无关协议（Fully Device - Independent QKD）[35-44]可以去除第 3 条要求。因此，如果没有上述条件或要求预先成立，合法通信双方将不可能建立无条件安全的密钥，任一条件的失败都将会损害密码的安全性，密码的建立也将无从谈起（DIQKD 协议第 3 条除外，有些安全性证明第 6 条也可以去除[37,42]，如基于无信号传输原理，No - Signaling Principle，其安全性证明并不要求量子力学是正确的）。

QKD 的安全性研究正是基于上述条件来分析窃听者的窃听行为对量子信号传输的影响，从而准确界定窃听者所窃取的粗密钥（Raw Key）信息。因为，量子密码的建立需要远距离通信双方通过量子信道交换量子信号，而量子信道却

不可避免地处在 Eve 的控制之下，因此量子信号可以被 Eve 窃听或干扰。这与经典密码分发中经典信道能够被 Eve 窃听或篡改是一致的。但有所不同的是，Eve 对量子信道的窃听会改变量子信号的状态并对其产生扰动，而从量子信道所观测出的扰动可以准确计算出 Eve 所获取的信息量。经典信道却不存在这样的特性，这也是量子密码能够实现无条件安全并因此备受关注的主要原因。早期的 QKD 安全性研究所关注的重点也正是针对不同的协议怎样准确界定或计算 Eve 所窃取的信息量。但直到今天，QKD 的无条件安全性也仅局限于几个成熟的 QKD 协议完成了证明，如 BB84 协议、连续变量相干态高斯调制协议、测量设备无关协议及全设备无关协议等。这些协议的安全性证明针对的都是最一般的窃听行为，即相干攻击下的安全性，或通过对称化处理操作约化成集体攻击下的安全性。然而，幸运的是，实践证明这些具体的协议也是实际实验中最容易实现且应用也最广泛的一类协议，有的甚至都推出了商用系统，建立起了量子网络。

理论的发展也相应地推动了实验的进步，实验的开展也进一步深化了理论的研究，二者不断相互促进，走向成熟。然而，在 QKD 实验实施过程中或在 QKD 系统的搭建过程中，人们发现实际系统总是存在一些诸如器件缺陷等非完美性，这些非完美性有时会带来一些严重的安全性漏洞（通常称为侧信道）。利用这些漏洞，窃听者可以窃取部分密钥甚至全部而不被合法通信方发现，从而破坏 QKD 的安全性。也就是说，尽管 QKD 理论上被证明是安全的，但在实验实施过程中其安全性可能会被大打折扣，甚至遭到破坏。因此，QKD 实际系统的攻击与防御研究也被广泛开展起来[45,46]，十分活跃，备受关注。

这其中，影响较大、意义深远的要属光子数分流攻击（Photon - Number - Splitting Attack）[47,48]与探测器致盲攻击（Detector - Blinding Attack）[49]。光子数分流攻击针对发送方光源缺陷（非完美单光子源，一般用衰减激光或弱相干脉冲代替），窃听者分离出编码在同一量子态上的多光子脉冲中的多余光子进行测量，从而获取编码在多光子脉冲上的全部信息而不被发现。由于完美的单光子源很难实现，该攻击在一定程度上影响了 QKD 实验实现的安全性。幸运的是，该漏洞后来被诱骗态（Decoy State）方案[50,51]完美地解决，且性能可与完美的单光子源相媲美。探测器致盲攻击针对单光子探测器的工作原理对其致盲，即窃听者向其发送强光使其工作在线性模式，从而探测器只能探测到强光脉冲而不能感应到单光子脉冲。这样，窃听者可以通过发送附加的强光来有效地控制探测器的响应，从而获取全部密钥。由于该攻击针对商用系统成功地实施了攻击，因而受到了业界的广泛关注，实际系统的非完美性也得到了大家的高度重视，越来越多的攻击方式和非完美性分析也相继被提出，表 1.1 列举了目前较受关注的针对商用或研究等实际系统的各种量子黑客攻击方式。

表 1.1　实际系统的量子黑客攻击[52]。针对商用或研究等实际系统的各种量子黑客攻击测试或理论分析

黑客攻击	攻击目标	测试系统
时序平移(Time shift)	探测器	商用系统
时序信息(Time information)	探测器	研究系统
探测器控制(Detector control)	探测器	商用系统
探测器控制(Detector control)[53]	探测器	研究系统
探测器死时间(Detector dead time)	探测器	研究系统
探测器饱和(Detector saturation)[54]	探测器	研究系统
信道校准(Channel calibration)	探测器	商用系统
相位重映射(Phase remapping)	相位调制器	商用系统
频移(Frequency shift)[55]	强度调制器	理论
法拉第镜(Faraday mirror)[56]	法拉第镜	理论
波长(Wavelength)[57-60]	分束器	理论
相位信息(Phase information)	光源	研究系统
设备校准(Device calibration)[58, 61, 62]	本底光	研究系统①
① 文献[58, 61]仅局限于理论分析		

在研究攻击与防御的过程中，人们渐渐发现这些攻击之所以能够成功，大多是因为 QKD 的实施过程违背了前文所提到的量子密码预先假设条件，包括主动的和被动的违背。如实际系统中器件的缺陷有可能导致第 1 条和第 3 条要求得不到满足。实际上这两点要求在一般的 QKD 协议的实施过程中也是很难得到保证的。有些协议的理论模型甚至不得不因此进行修改，从而将器件非完美性等其他已知漏洞纳入到模型的描述中，或者对实际系统打上补丁、采取防御措施来保证安全性。攻击与防御的研究还促使新的 QKD 协议被提出，这些新的协议大多规避了一些严重的安全性漏洞，例如测量设备无关协议去除了探测漏洞等，从而使协议的物理实现过程变得更加安全。

然而，量子黑客攻击的研究或实际系统的安全性研究，不应该引起人们的过度紧张，更不应该产生某些诸如“量子密码也不安全，所以没有研究的必要”等悲观性言论。因为，当前量子密码的实现仍然处在“斗争—测试”阶段，最初所出现的商用系统，存在的安全性缺陷也在这个斗争—测试过程中逐步得到发现并进行补救。因此，现在的 QKD 系统的安全性也变得越来越强，结合经典数据的加解密过程，QKD 将会使整个密码系统最终的安全性得到本质的增强，而且这种安全性是永久的。因为，通过 QKD 建立的密钥，相比于基于计算复杂度的

经典密钥分发，不会因将来量子计算机的诞生而使当前所存储的安全通信在未来得到破译。

1.2 连续变量量子密码研究现状

当前，量子密码的研究已经处于理论相对成熟、工程上积极推广应用的阶段。QKD 协议安全性得到严格的数学证明是量子密码取得巨大成就的主要标志之一。目前，远距离稳定的 QKD 已经在光纤和自由空间中分别得到了实现，商用系统也有了市场销售，QKD 网络的现场测试演示也在积极开展和部署。简言之，目前 QKD 已经发展得相对足够成熟，可以推广到现实生活，满足人们的日常需求和应用。

那么，研究人员现在都在做些什么呢？正如前文背景所介绍，目前，一部分人致力于缩小理论和实际的差距，以真正确保 QKD 实际实施的无条件安全性。一部分人在发展高速 QKD 系统，并极力实现强经典信号与弱量子信号在同一根光纤传输的复用技术，换言之，即挑战和攻克该领域的技术极限和技术瓶颈。另一部分人在研究可信和非可信中继节点 QKD 网络的实现和部署，包括星地通信的实现，即拓展 QKD 的覆盖范围。本书所研究的内容正是 QKD 实验实现的现实安全性，特别是连续变量量子密码实际系统的安全性，以缩小理论与实际的差距。下面就该领域的研究现状进行简要介绍，给出本书的研究动机和研究目标。

连续变量（Continuous Variable，CV）QKD，是基于高斯态调制编码与高斯测量或译码（如零拍测量和差分测量）的量子技术，信息编码在光场的两正交分量上。其无条件安全由连续变量系统两正交分量满足不确定性关系所保证，即基于 Heisenberg 不确定性原理。早期 CV QKD 协议基于高斯态离散调制而提出[63-65]，类似于 BB84 协议，并没有展现太多连续变量的优势。随后 Cerf、Levy 和 van Assche 于 2001 年提出了高斯态连续调制协议[66]。该协议利用压缩态进行安全编码，并很快被相干态编码取代。2002 年，Grosshans 和 Grangier 提出了第一个基于相干态高斯调制与零拍测量的 CVQKD 协议，此后被称为 GG02 协议[67]，并于 2003 年由 Grosshans、van Assche 等人进行了实验演示[68]。该协议充分展现了连续变量码率高、测量设备简单、易于集成当前标准的电信器件等优势，并很快得到了广泛的应用和推广。随后，基于差分测量（Heterodyne Detection）的无开关协议被提出[69,70]，并进行了实验演示[71]。该协议中的零拍探测由差分探测所取代，使得合法通信方可以同时使用两正交分量进行密钥分发。目前，相干态编码已经成为连续变量 QKD 协议实验演示的主流编码方式[72-77]，并出现了商用系统。

然而，CVQKD 协议对信道衰减比较敏感，传输距离严重受限。为了实现远距离传输，即突破 3dB 衰减极限，随后两种重要的技术被广泛使用，即 2002 年 Silberhorn 等人提出的后选择技术（Post Selection Technique）[78]，和 2003 年 Grosshans、van Assche 等人提出的反向协调技术（Reverse Reconciliation）[68]，两者都是针对密钥分发后的经典数据而提出的经典后处理技术。此外，2008 年 Pirandola 等人提出的双路 CVQKD 协议[79]，与 2009 年 Leverrier、Grangier 等人提出的离散调制协议[80]也展示了在传输距离上进一步拓展的可能性。近来，Weedbrook 等人将 CVQKD 由光频段理论上拓展到了红外频段，甚至可以延伸到微波频段，为噪声可容忍的短距离 QKD 通信提供了潜在的可实现平台[81,82]。关于 CVQKD 的安全性证明，2001 年，Gottesman 和 Preskill 基于离散变量量子纠错码，首先证明了一类压缩态离散调制协议，并给出协议安全性条件：压缩度超过 2.51dB[83]。随后，2004 年 Grosshans 和 Cerf 证明了 CVQKD 个体攻击下的安全性，2006 年集体高斯攻击下的安全性也得到了证明[84,85]。这样，根据 2009 年 Renner 和 Cirac 给出的将相干攻击约化为集体攻击的无条件安全性证明方法[86]，大多数 CVQKD 协议都可以在更简单的集体高斯攻击下进行安全性分析，2008 年 Pirandola 等人对此又给出了一个更完备的描述[87]。2010 年 Leverrier 等人还证明了对称相空间下高斯攻击的最优性[88]，接着，他们还分析了 CVQKD 协议有限密钥长度效应[89]，评估了当合法通信方交换有限数目量子系统时协议的安全性。在这种交换有限系统情况下，Leverrier 在 2013 年，基于多数 CVQKD 协议在相空间中的对称性特征，应用后选择技术（由 Christandl、Koenig 和 Renner 在 2009 年引入[90]，不同于数据后处理中的后选择技术）证明了有限尺度下 CVQKD 针对任意攻击下的无条件安全性[91]，并最终在 2015 年完成了 GG02 协议的组合安全性证明[92]。

尽管理论上 CVQKD 协议是无条件安全的，然而，在实际系统中由于存在像噪声或损耗等非完美性因素，协议的无条件安全仍会受到一定影响。正如前文所说，在单光子 QKD 中，像光子分束攻击[47,48]、被动法拉第镜攻击[56]、相位随机化攻击[93,94]等攻击方式得到了广泛而深入的研究，但在 CVQKD 中实际量子系统的安全性研究却才开始起步。这是因为连续变量系统是单向系统，相对于双向系统所需器件更少，攻击目标和攻击手段相对较少。而且，窃听者对 CVQKD 系统的大多数干预都可以通过经典后处理的参数估计步骤被探测出来。目前，CVQKD 协议实际系统安全性分析研究，主要是从对实际系统各器件非完美性的分析入手，如信号发送端由调制器引入的非完美性对实际系统的影响[95-98]，接收端实际分束器分束比依赖于波长等非完美性对信号测量的影响[59,60,99]，来提高 CVQKD 实际系统的可行性与密钥分发的有效性，并进行一定的安全性分析。

其发展趋势将会是针对实际系统的安全性漏洞提出量子黑客攻击方案和防御措施，引发人们对 CVQKD 实际系统的安全性的深入思考，从而发展量子侦听技术及防御技术，增强 CVQKD 实际系统的安全性，为其接入量子通信网络提供安全保障。另外，通过实际系统的攻防研究，新的 CVQKD 协议也将会被发现和提出，从而促进 CVQKD 的进一步发展。本书正是顺应这种发展趋势，开展了连续变量量子密码的安全性研究。

1.3 本书内容与结构

正如前文提到，本书主要研究连续变量量子密码（Continuous - Variable Quantum Cryptography）的安全性，特别是 CVQKD 实验实施的安全性，即现实安全性。实际系统中器件的非完美性可能会存在潜在的安全性漏洞，易被窃听者利用，从而使窃听者在不被发现的情况下有可能窃取部分密钥甚至攻破整个系统。另外，实际系统运行过程中也会不可避免地产生不易被察觉的安全性漏洞，因此找出这些漏洞并采取有效的应对措施显得迫切需要。本书将按照上述两条路线具体展开，详细介绍这方面的主要研究成果。下面给出各章节的内容概述及叙述结构，方便读者弄清写作思路，把握本书主旨。

第 2 章主要介绍本书研究的理论基础。首先介绍什么是连续变量量子密钥分发（CVQKD），包括分发协议的分类和介绍、协议的安全性分析及其理论证明，并简要分析 CVQKD 实际系统的非完美性及现实安全性。

第 3 章具体分析分束器的缺陷对 CVQKD 实际系统安全性的影响。实际分束器存在分束比依赖于波长的缺陷，利用该缺陷窃听者可以结合“截取—重发”攻击对使用差分探测协议的 CVQKD 系统实施所谓的“波长攻击”。但攻击过程中分束器的端口会引入额外的散粒噪声（Shot Noise），从而可能会被合法通信方发现。本章就此具体研究了窃听者成功实施波长攻击所需要的条件，以及针对这种缺陷合法通信方所应采取的防御措施，从而保证实际系统的安全性。

第 4 章针对光源问题揭示并分析 CVQKD 实验实施过程中本底光强度随时间波动对实际密钥分发系统安全性的影响。该波动为窃听者窃取密钥打开了后门，窃听者通过降低本底光的强度可以模拟这种波动并隐藏攻击痕迹。数值模拟显示，如果 Bob 不监控本底光的强度且不使用本底光强度的瞬时值对其探测结果进行归一化，密钥率将会被严重高估，安全性将会被大大降低。

第 5 章分析实际平衡零拍探测器（Balanced Homodyne Detector，BHD）的非完美性，提出非理想 BHD 攻击方案及其防御措施。非理想 BHD 具有探测效率和电子学噪声等非完美性，在实际的探测过程中，这些非完美性依赖于本底光强