DOI 10.15302/J-SSCAE-2018.06.014

量子通信的前沿、理论与实践

王向斌 [1, 2]

（1. 清华大学物理系，北京 100084；2. 济南量子技术研究院，济南 370102）

摘要：量子通信是量子信息科学的重要分支，其中最重要的两个应用是量子密钥分发和量子隐形传态。量子密钥分发可为通信双方提供无条件安全的密钥分发方式，其理论安全性由量子力学规律保证。量子密钥分发因其无条件安全的特点受到广泛关注。本文通过对量子密钥分发的广泛调研，系统地介绍了量子密钥分发的主要内容、理论安全性证明现状和实际安全性证明现状，着重介绍了诱骗态方法和测量装置无关的量子密钥分发方案；同时针对量子密钥分发在信道衰减严重时面临的问题做了系统调研，介绍了目前学术界对该问题的主流解决方法，即量子中继或卫星中继；最后指出量子密钥分发已经由理论模型发展到实际系统，为后续开展量子密钥分发相关研究提供了有益参考。

关键词：量子密钥分发；无条件安全性；现实条件安全性；纠缠分发；量子中继

中图分类号：TN915　　**文献标识码：**A

The Front, Theory and Practice of Quantum Communication

Wang Xiangbin [1, 2]

(1. Physics Department of Tsinghua University, Beijing 100084, China; 2. Jinan Institute of Quantum Technology, Jinan 370102, China)

Abstract: Quantum communication is an important branch of quantum information, where the two most important applications are quantum key distribution (QKD) and quantum teleportation. QKD can provide unconditionally secure key distribution methods between two remotely separated parties, and its information theoretical security is guaranteed by the laws of quantum mechanics. QKD has received much attention due to its unconditional security. Through extensive research on QKD, this paper systematically introduces the main content of QKD, the status of theoretical security proof and real-life security proof, and mainly focuses on the decoy state method and measurement-device-independent QKD. Besides, this paper systematically investigates the problems faced by QKD in the case of severe channel attenuation, and introduces the mainstream solution to the problem, i.e., quantum repeaters or satellite relay. This paper points out that the QKD has been developed from the theoretical model to the actual system, and provides a useful guidance for the subsequent research on QKD.

Keywords: quantum key distribution; unconditional security; practical security; entanglement distribution; quantum repeaters

收稿日期：2018-10-25；**修回日期：**2018-11-26

通讯作者：王向斌，清华大学物理系，教授，主要研究方向为量子信息科学；E-mail: xbwang@mail.tsinghua.edu.cn

资助项目：中国工程院咨询项目“工程科技颠覆性技术战略研究”(2017-ZD-10)

本刊网址：www.enginsci.cn

一、前言

“量子通信”一词来自于 Quantum Communication 的直译。作为量子信息科学的重要分支，量子通信是利用量子比特作为信息载体来进行信息交互的通信技术，可在确保信息安全、增大信息传输容量等方面突破经典信息技术的极限。正如郭光灿等 [1] 在其论文《两种典型的量子通信技术》中所指出的那样，量子通信有两种最典型的应用，一种是量子密钥分发，另一种是量子隐形传态。

量子隐形传态是分布式量子信息处理网络的基本单元，比如，未来量子计算机之间的通信，很可能就是基于量子隐形传态。从其一般形式来看，被传的态也可以是纠缠态，因此量子隐形传态也包含了量子纠缠转移，它是量子中继的基础。清华大学姚期智院士和中国科学技术大学潘建伟院士进一步指出，除了上述两个最典型的应用之外，量子通信还包括量子密集编码、量子通信复杂度等方向 [2,3]。受篇幅所限，下文着重介绍量子密钥分发（量子密码）。

二、量子密钥分发简介

量子密钥分发可以让空间分离的用户共享无条件安全的密钥，这是经典通信无法完成的任务，因此量子密钥分发始终是量子通信的重要方向。正因为这一国际学术界的广泛共识，包括 2010 年沃尔夫物理学奖获得者 Anton Zeilinger 教授等在内的众多国际学者就将量子密钥分发称为量子通信 [4]；美国物理学会的学科分类系统 PhySH 将量子密码作为量子通信条目下的一个子条目；欧盟最新发布的量子技术旗舰计划《量子宣言》，更是将以量子密钥分发为核心的量子保密通信作为量子通信领域未来的主要发展方向。特别地，由于量子密钥分发是最先实用化的量子信息技术，因此人们提到量子通信时往往特指量子密钥分发。

现有实际量子密码（量子密钥分发）系统主要采用 BB84 协议，由 Bennett 和 Brassard 于 1984 年提出 [5]。与经典密码体制不同，量子密钥分发的安全性基于量子力学的基本原理。即便窃听者控制了通道线路，只要窃听者不能攻入合法用户实验室内部，量子密钥分发技术就能让空间分离的用户共享安全的密钥。学界将这种安全性称之为“无条件安全”或者“绝对安全”，它指的是有严格数学证明的安全性，但是有下列假设前提：①窃听者不能攻入用户实验室内部；②依赖的基础是量子物理学原理，即要求窃听者不能拥有违反量子物理学原理的技术，但是可以拥有任何不违反量子物理学原理的技术，例如计算能力任意强大的计算机，包括量子计算机。量子密码的这种安全性，与计算复杂度无关，因此不论对手拥有多大的计算能力，其安全性都不会受到影响。

BB84 协议需要 4 种不同的单光子态，例如水平、竖直、45° 和 135° 的单光子偏振状态。在协议提出时，并没有安全性证明，只有直观的量子力学依据。例如一个未知的单量子态不可克隆，对量子态的观测原则上必然带来扰动等。简单地说，当时的直观依据就是：任何窃听者无法做到既能观测合法用户发射的量子态又不留下任何痕迹。但是，在很长一段时间内都没有严格的基于定量分析的安全性证明。例如许多人建议使用 BB84 协议建立安全密钥，若噪声太大就放弃（噪声可能是窃听行为的痕迹），若噪声太小就保留或使用，但是却给不出“大”和“小”的标准。

三、严格安全性证明

20 世纪 90 年代后期至 2000 年，安全性证明获得突破，BB84 协议的严格安全性证明被 Lo、Shor、Mayers 等人完成 [6~8]。他们的证明结果，大体可以表述为：BB84 协议，如果按照其所述的方法提炼最终码（final key），获得的最终码总是安全的。这个安全性证明要求在协议执行过程中，用户需要检验误码率，而误码率数据仅仅是用户自己对量子态的检测结果，无需监控通道链路。他们给出了最终码的成码率公式。根据这个公式，误码率高于一定值时就自动没有最终码产出。有了这个结论后，生成安全密钥只需要按照规定的程序提炼最终码，若能提炼出则总是安全的，而无需单独进行安全性判断决定是否放弃实验。这个安全性证明需要的条件就是 BB84 协议自身的条件：假定用户能生成 BB84 协议所要求的单量子态，假定窃听者不能攻入用户实验室内部并且只能拥有量子物理学原理允许的技术手段。在这些前提下，Mayers 等人的安

全性证明是完全成立的。严格证明的安全性究竟有多安全呢？其结论大体上可以表述为：我们有很大的概率（例如 $(1–2^{–50})\times100\%$ 这么大的概率）确定，按规定程序提炼出的最终码可能的信息泄露量小于一个很小值（例如 $2^{–50}\times100\%$）。当然，这里的“很大概率”和“很小值”，用户可以自行设定，设定的级别越高，则提炼出最终码的成码率也就越低。

后来，量子密钥分发逐步走向实用化研究，出现了一些威胁安全的攻击 [9,10]，这并不表示上述安全性证明有问题，而是因为实际量子密钥分发系统并不完全符合上述（理想）BB84 协议条件。2000 年后，又有多项直接面向实际系统的安全性证明理论突破 [11~21]，实际系统量子密钥分发的安全性已经在越来越广泛的条件下得以实现。

四、现实条件安全性证明

（一）现实条件下的安全性一：非理想单光子源与光子数分离攻击

实际 BB84 系统面临的一个特别严重的问题是光子数分离攻击（photon number splitting attack，简称 PNS attack）[9]。产生 BB84 态需要理想单光子源，然而，适用于量子密钥分发的理想单光子源至今仍不存在。实际应用中使用的是非理想单光子源，最典型的是弱相干态光源。虽然弱相干态光源大多数情况下发射的是单光子，但仍然存在一定的概率，每次会发射两个甚至多个相同量子态的光子。而通道存在损耗，距离越远损耗越大。假设窃听者拥有物理学原理所允许的一切能力，例如拥有无损耗或低损耗通道。窃听者可以将单光子事件全部阻隔，而在光源同时发射出两个光子的时候保留其中一个，将另一个（以无损耗或低损耗通道）发送给接收方，从而完全掌握通信双方的密钥，这就是“光子数分离攻击”。只要通道损耗达到一定程度，窃听者便不会因其实施光子数分离攻击而暴露自己的存在，因为其总可以用通道损耗掩盖自己的攻击行为。有人估算过，以当时最好的技术，考虑到光子数分离攻击，实际安全距离最多不超过 20 km，而且这还只是上界值，是指超过了完全不安全，未超过也不一定安全。光子数分离攻击无需窃听者攻击实验室内部。窃听者的光子数分离攻击原则上可以在实验室外部通道链路上的任何地方实施。若不采用新的理论方法，用户将不得不监控整个通道链路以防止光子数分离攻击，而这将使量子密钥分发失去其原本最大的优势卖点。换句话说，那其实就不是量子密钥分发了。事实上，在这个问题解决之前，一些知名量子通信实验小组甚至不做量子密钥分发实验。由韩国学者黄元瑛、清华大学王向斌和多伦多大学罗开广等人提出的诱骗态方法，终于解决了这个问题 —— 即利用非理想单光子源，例如弱相干光源，同样可以获得与理想单光子源等价的安全性，从理论方法创新上把量子通信的安全距离大幅度提高到百千米以上 [11~13]。2006 年，潘建伟率领的中国科技大学等单位的联合团队以及美国 Los-Alamos 国家实验室 –NIST 联合实验组同时利用诱骗态方案，将光纤量子通信的安全距离首次提高到 100 km，解决了光源不完美带来的安全隐患。当时《Physical Review Letters》杂志罕见地在同一期上，发表了 3 篇关于同一主题的独立实验论文 [14~16]：采用诱骗态方法实施量子密钥分发。后来，中国科技大学等单位的科研团队甚至把其安全距离拓展到 200 km 以上。

（二）现实条件下的安全性二：探测器攻击

实际系统量子密钥分发另一个可能存在的安全隐患集中在终端上。终端攻击本质上不属于 BB84 协议的安全性定义范围。如同所有经典密码体制一样，用户需要对终端设备进行有效管理和监控。量子密钥分发中对终端的攻击，主要是指探测器攻击，假定窃听者能控制实验室内部探测器效率。代表性的具体攻击办法是，如同 Lydersen 等 [10] 的实验那样，输入强光将探测器“致盲”，即改变探测器的工作状态，使得探测器只对他想要探测到的状态有响应，或者完全控制每台探测器的瞬时效率，从而完全掌握密钥而不被察觉。当然，针对这个攻击，可以采用监控方法防止。因为窃听者需要改变实验室内部探测器的属性，用户在这里的监控范围只限于实验室内部的探测器，而无需监控整个通道链路。

尽管如此，研究者还是会担心由于探测器缺陷而引发更深层的安全性问题。例如如何完全确保监控成功，如何确保使用进口探测器的安全性等。2012 年，Lo 等 [17] 提出了“测量器件无关的（MDI）”量子密钥分发方案，彻底解决了探测器攻击问题。

可以证明，该方法可以抵御任何针对探测器的攻击，包括所有已知的和未知的针对探测器的攻击。该方法无需监控探测器。甚至，类似于量子中继那样，即便让敌人控制探测器也不影响结果的安全性。另外，该方法本身也建议结合诱骗态方法，使得量子密钥方法在既不使用理想单光子源又不使用理想探测器的情况下其安全性同使用了理想器件等价。2013 年，潘建伟团队首次实现了（带诱骗态方法的）MDI 量子密钥分发，后又实现了 200 km 量子 MDI 量子密钥分发 [22,23]。至此，该方法面临的主要科学问题变成了如何获得有实际意义的成码率。清华大学王向斌小组提出了 4 强度优化理论方法，大幅提高了 MDI 方法的实际工作效率 [20]。采用此方法，中国科学家联合团队将 MDI 量子密钥分发的距离突破至 404 km [21]，并将成码率提高两个数量级，大大推动了 MDI 量子密钥分发的实用化。此项结果还表明，在通道损耗高达 63 dB 的情况下，仍然可以得到安全的量子密钥。这表明，这一方法只用现有的非理想光源在已经超越了原始 BB84 协议使用理想光源的距离 [21]。计算表明，在 63 dB 损耗下，原始 BB84 协议即便采用理想单光子源也不能生成密钥。

实际系统虽存在各类缺陷，但是在理论和实验科学家的努力之下，其安全性正在逼近理想系统。这种逼近，只要能达到一个合理的程度，实际量子密钥分发系统就能体现出其独特的安全价值。

五、Ekert91 协议及其安全性

一直以来，量子密钥分发的主流方法就是 BB84 协议 + 诱骗态方法，或者 BB84 协议 + 诱骗态方法 +MDI 方法。中国科学家量子密钥分发的实践活动也多采用这样的主流方法。当然，在此方法之外，还存在别的方法，例如 1991 年 Ekert [22] 提出的基于贝尔不等式验证的协议（后被称之为 Ekert91 协议）。此方法建议在纠缠分发的基础上通过验证贝尔不等式的破坏来确认量子密钥分发的安全性。如果实验损耗小于一定值 , 则可以无漏洞地证实贝尔不等式是否被打破，从而获得安全密钥。考虑到探测器攻击，例如 Lyderson 等人的探测器攻击方法 [10]，或者后来的各类变种方法，例如 Gerhardt 等人在文献 [23] 中提出的攻击方法。若只用 Ekert91 原协议而不辅以其他手段，则需要总损耗（含通道链路损耗和探测器件损耗）小于 17% 即 1 dB 才能确保密钥的安全性。但这种安全性条件只是 Ekert91 原协议的安全性条件，不是其他协议，比如 BB84 协议的安全性条件。中国科技大学等单位的实验基于 BB84 协议，诱骗态方法和 MDI 方法，所得到的量子密钥分发结果的安全性无需遵守 Ekert91 协议所要求的条件。事实上，404 km MDI 量子密钥分发实验本身已经证明了其所用的协议和方法在总损耗大于 60 dB 的情况下仍然可以安全成码。MDI 方法可以抵御任何针对探测器的攻击，也就是说，已有的 MDI 量子密钥分发实验，可以抵御所有类型的探测器攻击，不但包括 Lyderson 等人的探测器攻击方法 [10]，也包括后来的各类变种方法，例如 Gerhardt 等人的那种攻击。其实 Gerhardt 等人的攻击方法 [23] 只是这类探测器攻击方法中的一个，但是它既不是第一个，也不是影响力最大的一个。在量子通信领域人所共知的最早的也是最有代表性的是早在 2010 年就已经发表的 Lyderson 等人的探测器攻击方法 [10]。而 MDI 量子密钥分发正是在这个背景下产生的能抵御任何针对探测器攻击的方法。

BB84 协议与 Ekert91 协议的安全性对损耗的要求差别看似很大，其实差别并没有那么大。我们的实验并非孤立使用 BB84 协议，还使用了诱骗态方法和 MDI 方法。同样，如果对 Ekert91 协议辅以其他方法，例如，在接收端实验室入口实施光子数无损检测，能够判断具体哪些时间窗口有光子打入，那就可以只计入那些有光子打入的事件对应的测量数据从而使安全性条件从总损耗小于 1 dB 变成只需要探测器损耗小于 1 dB 而不论外部通道链路损耗有多大。这样的条件改变对安全距离其实已经基本没有限制了。同 BB84+MDI 量子密钥分发相比，执行远距离 Ekert91 协议要用到极高难度的实验技术（例如无损光子检测）。这是因为对于 Ekert91 协议，获得安全密钥也同时意味着完成了无漏洞贝尔不等式实验，而对于 BB84+MDI 量子密钥分发，获得安全密钥并不能给出对贝尔不等式的任何结果。

尽管 Ekert91 协议在量子信息领域以及后来在此基础上形成的“器件无关的（DI）”量子密钥分发 [24,25] 有其独到之处，但目前此方法对实验条件要求极为苛刻。而事实上，现有的主流方法，

BB84 协议 + 诱骗态和 MDI 方法，已在现实条件下有效地保证了量子通信的安全性。当然，这个方法只能用来生成安全密钥，却不能用来证实贝尔不等式破坏，因为它从不需要纠缠态。

六、安全距离的不受限拓展

由于量子通信信号无法放大，前述各种方法在实用化中安全距离受到限制 [26~29]。要突破这个瓶颈，需要有新的技术突破。一种方法是卫星量子通信。中国科学院团队利用墨子号科学实验卫星，于 2016 年采用诱骗态方法，成功实现了星地量子密钥分发，实现了上千千米量子密钥分发 [30~32]。另一种方法是基于量子中继，原则上距离不受限制。量子中继只负责远距离量子通道的建立，本身并不涉及密钥的任何信息，因此中继站点的安全也不需要人为保护（如果以量子中继的观点看 MDI 量子密钥分发的测量中间站，就很容易理解为什么这个方法能够抵御对探测器的任意攻击，甚至探测器有敌人控制也不影响密钥安全性）。原则上，即使量子中继器被敌方控制，只要能够在遥远两地建立起量子纠缠或者建立起适当的关联数据（虚纠缠），就可以实现安全的量子密钥分发。如同量子密码理论的奠基人 Gilles Brassard 和 Artur Ekert 所指出的：这将最终实现所有密码学者梦想数千年之久的“圣杯”。中国科学家已经在量子中继的核心——量子存储器上获得了世界上综合性能最好的效果 [26] 。

七、结语

正如诸多国际评论所述，事实表明，过去的十多年里，中国科学家已经在量子通信方面取得了巨大成就。在实用化量子保密通信研发上创造了大批世界首次突破和世界记录，逐渐逼近理想系统，建立了真实系统的安全性，也无可争议地处于世界领先地位。

参考文献

[1] 苏晓琴, 郭光灿. 两种典型的量子通信技术 [J]. 广西大学学报(自然科学版), 2005, 30(1): 30–39.
Su X Q, Guo G C. Two typical quantum communication technology [J]. Journal of Guangxi University (Natural Science Edition), 2005, 30(1): 30–39.

[2] Yao A C C. Quantum circuit complexity[C]. Palo Alto: IEEE 34th Annual Foundations of Computer Science, 1993.

[3] Yuan Z S, Bao X H, Lu C Y, et al. Entangled photons and quantum communication [J]. Physics Reports, 2010, 497(1): 1–40.

[4] Ursin R, Tiefenbacher F, Schmitt-Manderbach T, et al. Entanglement-based quantum communication over 144 km [J]. Nature Physics, 2007, 3(7): 481–486.

[5] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [C]. Bangalore: IEEE International Conference on Computers, Systems and Signal Processing, 1984.

[6] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances [J]. Science, 1999, 283(5410): 2050–2056.

[7] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. Physical Review Letters, 2000, 85(2): 441–444.

[8] Mayers D. Unconditional security in quantum cryptography [J]. Journal of the ACM (JACM), 2001, 48(3): 351–406.

[9] Brassard G, Lütkenhaus N, Mor T, et al. Limitations on practical quantum cryptography [J]. Physical Review Letters, 2000, 85(6): 1330–1333.

[10] Lydersen L, Wiechers C, Wittmann C, et al. Hacking commercial quantum cryptography systems by tailored bright illumination [J]. Nature Photonics, 2010, 4(10): 686–689.

[11] Hwang W Y. Quantum key distribution with high loss: Toward global secure communication [J]. Physical Review Letters, 2003, 91(5): 057901.

[12] Wang X B. Beating the photon-number-splitting attack in practical quantum cryptography [J]. Physical Review Letters, 2005, 94(23): 230503.

[13] Lo H K, Ma X, Chen K. Decoy state quantum key distribution [J]. Physical Review Letters, 2005, 94(23): 230504.

[14] Peng C Z, Zhang J, Yang D, et al. Experimental long-distance decoy-state quantum key distribution based on polarization encoding [J]. Physical Review Letters, 2007, 98(1): 010505.

[15] Rosenberg D, Harrington J W, Rice P R, et al. Long-distance decoy-state quantum key distribution in optical fiber [J]. Physical Review Letters, 2007, 98(1): 010503.

[16] Schmitt-Manderbach T, Weier H, Fürst M, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km [J]. Physical Review Letters, 2007, 98(1): 010504.

[17] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution [J]. Physical Review Letters, 2012, 108(13): 130503.

[18] Liu Y, Chen T Y, Wang L J, et al. Experimental measurement-device-independent quantum key distribution [J]. Physical Review Letters, 2013, 111(13): 130502.

[19] Tang Y L, Yin H L, Chen S J, et al. Measurement-device-independent quantum key distribution over 200 km [J]. Physical Review Letters, 2014, 113(19): 190501.

[20] Zhou Y H, Yu Z W, Wang X B. Making the decoy-state measurement-device-independent quantum key distribution practically useful [J]. Physical Review A, 2016, 93(4): 042324.

[21] Yin H L, Chen T Y, Yu Z W, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber [J]. Physical Review Letters, 2016, 117(19): 190501.

[22] Ekert A K. Quantum cryptography based on Bell's theorem [J]. Physical Review Letters, 1991, 67(6): 661–663.

[23] Gerhardt I, Liu Q, Lamaslinares A, et al. Experimentally faking the violation of Bell's inequalities [J]. Physical Review Letters, 2011, 107(17): 170404.

[24] Mayers D, Yao A. Quantum cryptography with imperfect apparatus [C]. Palo Alto: IEEE Symposium on Foundations of Computer Science, 1998.

[25] Vazirani U, Vidick T. Fully device-independent quantum key distribution [J]. Physical Review Letters, 2014, 113(14): 140501.

[26] Yang S J, Wang X J, Bao X H, et al. An efficient quantum light–matter interface with sub-second lifetime [J]. Nature Photonics, 2016, 10(6): 381–384.

[27] Liao S K, Yong H L, Liu C, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication [J]. Nature Photonics, 2017, 11(8): 509–513.

[28] Chen T Y, Liang H, Liu Y, et al. Field test of a practical secure communication network with decoy-state quantum cryptography [J]. Optics Express, 2009, 17(8): 6540–6549.

[29] Chen T Y, Wang J, Liang H, et al. Metropolitan all-pass and inter-city quantum communication network [J]. Optics Express, 2010, 18(26): 27217–27225.

[30] Liao S K, Cai W Q, Liu W Y, et al. Satellite-to-ground quantum key distribution [J]. Nature, 2017, 549(7670): 43–47.

[31] Yin J, Cao Y, Li Y H, et al. Satellite-based entanglement distribution over 1200 kilometers [J]. Science, 2017, 356(6343): 1140–1144.

[32] Ren J G, Xu P, Yong H L, et al. Ground-to-satellite quantum teleportation [J]. Nature, 2017, 549(7670): 70–73.