# 量子通信研究进展与应用

龙桂鲁[1,2,3,†]　盛宇波[4]　殷柳国[3,5]

(1　清华大学物理系　低维量子物理国家重点实验室　北京　100084)

(2　量子物质科学协同创新中心　北京　100084)

(3　北京信息科学与技术国家研究中心　北京　100084)

(4　南京邮电大学通信与信息工程学院　南京　210003)

(5　清华大学信息科学技术学院　北京　100084)

2018－04－07收到

†　email：gllong@tsinghua.edu.cn

DOI：10.7693/wl20180701

# Progress and applications of quantum communications

LONG Gui-Lu[1,2,3,†]　SHENG Yu-Bo[4]　YIN Liu-Guo[3,5]

(1 State Key Laboratory of Low-Dimensional Quantum Physics，Department of Physics，Tsinghua University，Beijing 100084，China)

(2 Collaborative Innovation Center of Quantum Matter，Beijing 100084，China)

(3 Beijing National Research Center for Information Science and Technology，Beijing 100084，China)

(4 College of Telecommunications & Information Engineering，Nanjing University of Posts and Telecommunications，Nanjing 210003，China)

(5 School of Information Science and Technology，Tsinghua University，Beijing 100084，China)

**摘　要**　量子通信利用量子信道进行信息的编码、传输和处理，具有安全性高和信道容量高等特点。量子保密通信以信息安全为主要目的，包括量子密钥分发、量子安全直接通信和量子秘密共享等模式。利用量子纠缠，量子隐形传态根据事先已经分发的纠缠粒子对实现不传输实物粒子而传输未知粒子的状态，量子密集编码通过传输一个粒子而实现两个粒子信息的传输，这些是经典通信无法实现的任务。文章简单介绍量子通信的内容和进展情况。

**关键词**　量子通信，量子密钥分发，量子安全直接通信，量子秘密共享，量子隐形传态，量子密集编码，量子保密通信，量子密码学

**Abstract**　In quantum communication, information or signals are transmitted and processed quantum mechanically, with the advantages of high security and high capacity. The main objective of quantum secure communication is to protect the security of information. Quantum secure communication, or quantum cryptography, includes quantum key distribution, quantum secure direct communication, quantum secret sharing, and so on. With quantum entanglement, quantum teleportation can use prior distributed entangled pairs to transmit an unknown quantum state without transmitting the particle itself. Quantum dense coding can transmit the information encoded in two particles by just transmitting one particle. In classical communication, these tasks would be impossible. In this paper we briefly describe the current status of research in quantum communication.

**Keywords**　quantum communication, quantum key distribution, quantum secure direct communication, quantum secret sharing, quantum teleportation, quantum dense coding, quantum secure communication, quantum cryptography

## 1 引言

量子通信利用量子载体(一般称为量子信道)来传输信息或者信号。与经典通信方式相比，量子通信以量子不确定性原理、量子态不可克隆原理、量子态测量塌缩等为基础，具备原理上的可证安全性。量子保密通信自1984年诞生以来，取得了迅速的发展，朝着实用化迈进。

量子保密通信诞生于1984年，Bennett和Brassard提出首个量子密钥分发协议，即BB84协议[1]。该协议利用单光子的偏振量子态进行密钥分发，利用窃听测量会导致误码率显著上升的机制，现场发现窃听行为，从而保证分发的密钥的安全性。量子通信包括量子密钥分发[1]、量子安全直接通信[2]、量子秘密共享[3]、量子密集编码[4]和量子隐形传态[5]等主要模式，而量子密钥分发、量子安全直接通信和量子秘密共享是以保护信息(信号)的安全为主要目的，又叫做量子保密通信或者量子密码学。

## 2 量子密钥分发

量子密钥分发是指通信双方利用量子信道协商出安全的密钥(与密码学一致的名称应该是量子密钥协商，在经典密码学中密钥分发是指将已经确定好的密钥发送给其他用户，而量子密钥分发中的密钥是使用双方共同产生的，事先并没有确定)。要完成信息的传输，需要用协商得到的密钥将信息加密成密文，再通过经典通信将密文传输给接收方。基于量子密钥分发的保密通信的结构如图1所示。量子密钥分发解决了密钥的安全分发。密钥的存储和转移，以及密文的发送是采用经典方式的。由于敌人总是可以截获密文并保存，如果敌人窃取了密钥，则还是可以破译传输的秘密。当然这种事情发生的几率是非常小的。

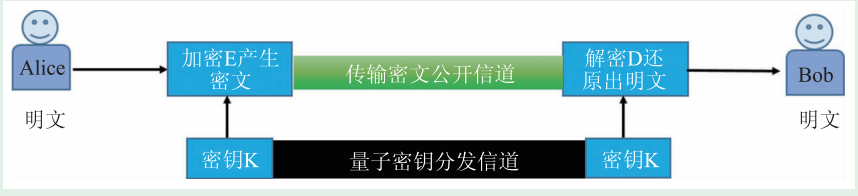


图1 基于量子密钥分发的保密通信结构

量子密钥分发提出后，长时间得不到学界的重视。在BB84协议提出5年后的1989年，方案提出人Bennett和Brassard自己组织了实验队伍，在美国IBM公司实现了32 cm自由空间信道的量子密钥分发实验，这是量子密钥分发的第一个实验[6]。1990年代初，英国国防部的实验室和瑞士日内瓦大学开始了实验研究。在中国，1994年应葛墨林先生的邀请，郭光灿先生在南开大学做了量子通信的第一个报告[7]，1995年中国科学院物理研究所吴令安研究员完成了第一个量子密钥分发实验[8]。

1994年以后，量子计算取得重大突破，Shor提出了大数分解算法[9]，Grover提出了量子搜索算法[10, 11]，充分显示了量子计算的强大计算功能。一旦量子计算机建成，将对现代保密通信产生重大影响，以大数分解为基础的公开密钥体系将会失效，而AES等对称密码体系的安全性也会降低。因此，能够抵御量子攻击的量子保密通信随着量子计算一起，成为世界前沿研究领域，提升到国家战略的高度，世界主要强国加大经费和人力的投入。在BB84协议提出12年之后，1997年量子密钥分发的安全性开始从理论上得以证明[12, 13]。量子密钥分发的距离及密钥产生速率得以不断提高。中国芜湖政务量子网[14]、合肥量子网[15]、济南量子网等量子通信试验网络的建设，意味着量子密钥分发正向网络和试验应用的方向发展。2016年中国发射了量子实验卫星，在国际上首次实现了星地量子密钥分发[16]。2017年京沪干线量子通信干线开通，标志着城域量子通信试验网络的诞生[17]。

## 3 量子安全直接通信

量子安全直接通信是一种在量子信道中直接传递秘密信息的技术[2]，它没有密

钥，没有密文，从根本上改变了保密通信的架构。通常保密通信架构中包含两个通道，如图1所示，一个通道用来分发密钥，一个通道用来传输加密后的密文。利用量子密钥分发进行保密通信时，密钥分发通道采用量子通道，而密文的传输还是在经典信道。图2是量子安全直接通信的结构，它没有密钥、没有密文，只有一条传输信息的量子信道，是一种新型的保密通信架构。在整体性能上，量子安全直接通信具有超越经典一次一密的安全性。经典一次一密加密方式被证明是完美安全的，但是要求绝对安全的保存密钥。因为窃听者可以很容易窃听获得传输的密文并加以保存，一旦获得密钥，就会破译截获的密文。密钥在使用以后一般会立即销毁，密钥丢失这种情形很难发生。但是由于各种原因，密钥有时也会丢失，历史上就有这样惨痛的教训，苏联在苏芬战争中将密码本丢失，造成其在西方的情报系统的溃败就是一个典型案例[18]。利用量子安全直接通信可在技术上避免这种问题的发生，因为量子直接通信没有密钥和密文，没有密钥丢失问题，同时窃听者也得不到密文。

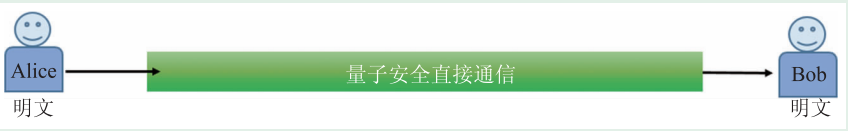

图2　量子安全直接通信结构

2000年龙桂鲁和博士生刘晓曙提出了国际上首个量子安全直接通信方案[2]，2003年龙桂鲁和博士生邓富国、刘晓曙提出了两步量子安全直接通信方案[19]，2004年龙桂鲁和邓富国提出了基于单光子的DL04量子安全直接通信方案[20]。近年来，量子安全直接通信得到了快速的发展，受到了广泛的重视。2016年龙桂鲁与山西大学肖连团教授合作，提出频率编码的单光子量子直接通信方案，并在实验上进行了原理验证，实现了噪声环境下的量子直接通信[21]。2017年中国科学技术大学郭光灿院士、史保森教授团队和南京邮电大学盛宇波教授团队合作，利用量子存储验证了龙桂鲁等提出的量子安全直接通信方案[22]，2017年清华大学张巍及其博士生朱峰、黄翊东教授与南京邮电大学盛宇波教授联合实验组首次在500 m光纤中实现了龙桂鲁等的量子安全直接通信方案[23]，量子安全直接通信走向实用化迈出了关键性一步。这些实验不仅引起了国际学术界对量子安全通信的关注，美国物理学会等众多科学媒体网站做了点评和报道[24]，麻省理工技术评论评价量子安全直接通信为新一代完美保密通信[25]，而且引起了美国情报专家和情报部门的重视，情报战专家Joel Harding[26]、曾就职于美国国防部长办公室的情报专家RC Porter两次撰文评述量子安全直接通信[27, 28]，美国国家安全网站以“中国在防间谍量子通信取得突破”为题报道了量子安全直接通信取得的进展[29]。

## 4　量子通信的其他模式

量子隐形传态是指通过通信双方共享的纠缠光子对，将发送方所持有的未知量子态在接收方重现的技术，即实现了不需要传递实物粒子而将粒子的状态传送给远方接受者。1993年，Bennett等人提出了量子隐形传态的首个理论方案[5]，该方案由Zeilinger教授、潘建伟院士等在1997年率先完成实验验证[30]。当前，量子隐形传态的技术研究主要集中在多光子纠缠的制备以及分发距离的提升上。重要的成果包括，2012年9月，奥地利等多国研究员实现了长达143 km的量子隐形传态[31]；2015年6月，潘建伟院士团队首次在实验上实现了多自由度量子隐形传态[32]，潘建伟、王建宇院士等实现地面和低轨道卫星之间的量子隐形传态[33]。量子隐形传态在分布式量子计算上有重要的应用。

量子秘密共享是Hillery等三位科学家在1999年提出的，将一个密钥在两个或者多个用户中共享[3]。量子密集编码是由Bennett和Wiesner在1992年提出的，利用量子纠缠可以实现通过传输一个粒子而传输两个粒子信息的密集编码功能[4]。

## 5 总结

经过30多年的努力，量子通信得到了快速发展，但仍存在以下技术难点亟待解决。一是单光子态的制备、探测技术。现有实验系统多采用相干态激光弱脉冲替代理想单光子源，其发出的脉冲很多是没有光子的空脉冲，效率低下。对于单光子的探测，传统半导体单光子探测器探测效率低、暗计数高，超导探测器的探测效率高，但需要低温装置，成本高。需要研制高效率、高速率、低噪声、低成本的单光子探测器。二是速率、抗干扰性能有局限性。量子通信技术在现有条件下，远比不上经典通信系统在通信速率、抗干扰等方面的性能。光纤量子密钥分发系统安全码率在50 km传输距离下可达1 Mbps。三是光子损耗及量子退相干问题。在量子通信过程中，应该尽量减小光子损耗，保持量子特性不被破坏，减少量子退相干效应。四是研制实用化量子存储，这是增加传输距离的关键器件，要构建大信息量、长距离的量子通信网络，需采用量子存储技术克服单光子信号在传输信道中的指数衰减问题。科学技术的进步并非是一蹴而就，这些问题将会随着技术的发展得到解决。

安徽芜湖量子政务网、合肥城域量子通信试验示范网络、济南量子通信试验网的建成，标志着大范围的城域量子通信网络技术的开始。国家发改委筹建的用于量子通信研究的“京沪干线”项目已经完成，“京沪干线”总长2000余千米，从北京出发，经过济南、合肥，到达上海。这一广域光纤量子通信网络，是大尺度量子通信技术验证、应用研究和示范平台。随着量子通信技术的应用，这一领域也面临着新的挑战。首先，需要制定相关行业标准，将目前的技术进行标准化，规范行业发展，防止不利因素破坏行业氛围。如近来各种公司、产品加上量子概念在资本市场套取好处，科普定义不严谨，以及媒体的大力渲染等现象，使得量子物理和量子通信在应用方面遭到了误解和质疑。其次，行业发展应注重量子通信领域人才培养和就业导向。习总书记指出：“创新的事业呼唤创新的人才，注重培养一线创新人才和青年科技人才”，推动量子通信的应用也应以人才建设为核心。

量子通信作为未来保障通信安全的关键技术之一，已经被各国广泛关注并大力发展，这一领域是我国在高新技术研究与应用领域与国际发展保持同步并且有望实现弯道超越、引领未来的突破口。今后，在工程技术、产业标准等方面取得进展和保障的前提下，量子通信在国家信息安全领域中将发挥重要作用。

## 参考文献


[1] Bennet C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. Proceedings of the International Conference on Computers, Systems and Signal Processing, 1984. Dec. 10-12

[2] Long G L, Liu X S. Physical Review A, 2002, 65: 032302

[3] Hillery M, Bužek V, Berthiaume A. Physical Review A, 1999, 59(3): 1829

[4] Bennett C H, Wiesner S J. Physical Review Letters, 1992, 69(20): 2881

[5] Bennett C H, Brassard G, Crépeau C *et al*. Physical Review Letters, 1993, 70(13): 1895

[6] Bennett C H, Bessette F, Brassard G *et al*. Journal of Cryptology, 1992, 5(1): 3

[7] 量子密码专委会学术年会在赤峰圆满召开. 中国密码学会通讯, 2014, (4): 03

[8] 邵进, 吴令安. 量子光学学报, 1995, 1(1): 41

[9] Shor P W. Algorithms for quantum computation: discrete logarithms and factoring. Proc. 35th annual symposium on foundations of computer science, 1994. 124-134

[10] Grover L K. A fast quantum mechanical algorithm for database search. Proceedings of the twenty-eighth annual ACM symposium on theory of computing. 1996. 212-219

[11] Long G L. Physical Review A, 2001, 64(2): 022307

[12] Lo H K, Chau H F. Science, 1999, 283(5410): 2050

[13] Mayers D. Unconditional security in quantum cryptography. arXive e-print quant-ph/9802025; preliminary version in: Mayers D. Quantum key distribution and string oblivious transfer in noisy channels. in Advances in Cryptology—Proceedings of Crypto '96, New York: Springer-Verlag, 1996. 343-357

[14] Xu F X, Chen W, Wang S *et al*. Chinese Science Bulletin, 2009,

54(17):2991
[15] Chen T Y, Wang J, Liang H *et al*. Optics Express, 2010, 18(26): 27217
[16] Liao S K, Cai W Q, Liu W Y *et al*. Nature, 2017, 549(7670): 43
[17] Courtland R. IEEE Spectrum, 2016, 53(11): 11
[18] 庞洪雷. 保密工作, 2014, (8): 62
[19] Deng F G, Long G L, Liu X S. Physical Review A, 2003, 68(4): 042317
[20] Deng F G, Long G L. Physical Review A, 2004, 69(5): 052319
[21] Hu J Y, Yu B, Jing M Y *et al*. Light: Science & Applications, 2016, 5(9): e16144
[22] Zhang W, Ding D S, Sheng Y B *et al*. Physical Review Letters, 2017, 118(22): 220501
[23] Zhu F, Zhang W, Sheng Y *et al*. Science Bulletin, 2017, 62(22): 1519
[24] Zyga L. Physicists use quantum memory to demonstrate quantum secure direct communication. https:// phys.org/news/2017-06-physicists-quantum-memory.html
[25] Quantum Breakthrough Heralds New Generation of Perfectly Secure Messaging. Mittechnology Review, November 1, 2017. https://www.technologyreview.com/s/609294/quantum-breakthrough-heralds-new-generation-of-perfectly-secure-messaging/
[26] Harding J. Two things struck me instantly. https://toinformistoinfluence.com/2017/06/14/physicists-use-quantum-memory-to-demonstrate-quantum-secure-direct-communication/
[27] Porter R C (Support CMShelplive). China has a breakthrough in spy-proof quantum communications. https://fortunascorner.com/2017/11/10/china-breakthrough-spy-proof-quantum-communications/
[28] Porter R C (Support CMShelplive). 'Unhackable' internet breakthrough as scientists develop new quantum teleportation tests to prevent 'eavesdropping'. China has a breakthrough in spy-proof quantum communications. https://fortunascorner.com/2018/01/06/unhackable-internet-breakthrough-scientists-develop-new-quantum-teleportation-tests-prevent-eavesdropping/
[29] Tucker P. China has a breakthrough in spy-proof quantum communications. Defenceone.com, November 9, 2017. http://www.defenseone.com/technology/2017/11/china-has-breakthrough-spy-proof-quantum-communications/142415/
[30] Bouwmeester D, Pan J W, Mattle K *et al*. Nature, 1997, 390 (6660): 575
[31] Herbst T, Scheidl T, Fink M *et al*. Teleportation of entanglement over 143 km. Proceedings of the National Academy of Sciences, 2015, 112(46): 14202
[32] Wang X L, Cai X D, Su Z E *et al*. Nature, 2015, 518(7540): 516
[33] Ren J G, Xu P, Yong H L *et al*. Nature, 2017, 549(7670): 70