Computer Science and Application 计算机科学与应用, 2018, 8(7), 1102-1116
Published Online July 2018 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2018.87122

Hans汉斯

Development Analysis of Quantum Secure Direct Communication Technology

Yu Han[1,2], Huijie Jiang[1], Ning Tao[1], Shuyi Zhang[1], Qiang Li[1,2], Zongbo Zhang[1], Hongxin Li[1,2*]

[1]Strategic Support Force Information Engineering University, Luoyang Henan
[2]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Henan
Email: *lihongxin830@163.com

Received: Jul. 1st, 2018; accepted: Jul. 16th, 2018; published: Jul. 23rd, 2018

Abstract

Quantum secure direct communication technology has attracted lots of attentions since it can achieve direct sharing of secret information between two communication parties. This paper first introduces the basic theory of quantum secure direct communication technology and two classic scheme, and then analyzes the solutions to the existing theory and discusses the recent experimental progress and related communication network construction, finally through discussing noisy and practical problems, prospects the future development of quantum secure direct communication technology.

Keywords

Quantum Cryptography, Quantum Secure Direct Communication, Typical Scheme, Network Design, Future Prospect

量子安全直接通信技术发展研究

韩　宇[1,2]，姜慧杰[1]，陶　宁[1]，张书轶[1]，李　强[1,2]，张宗波[1]，李宏欣[1,2*]

[1]战略支援部队信息工程大学，河南　洛阳
[2]数学工程与先进计算国家重点实验室，河南　郑州
Email: *lihongxin830@163.com

收稿日期：2018年7月1日；录用日期：2018年7月16日；发布日期：2018年7月23日

摘　要

量子安全通信技术因其可以在通信双方安全的直接共享秘密消息而备受关注。本文首先介绍了量子安全

*通讯作者。

文章引用: 韩宇, 姜慧杰, 陶宁, 张书轶, 李强, 张宗波, 李宏欣. 量子安全直接通信技术发展研究[J]. 计算机科学与应用, 2018, 8(7): 1102-1116. DOI: 10.12677/csa.2018.87122

直接通信技术的基本理论和典型方案，然后对现有理论方案进行深入分析并研究了最新实验进展以及相关通信网络的建设，最后通过讨论噪声和实用性等问题，对量子安全直接通信技术的未来发展趋势进行了总结与展望。

关键词

量子密码，量子安全直接通信，典型方案，网络设计，未来展望

1. 引言

1.1. 发展现状

量子保密通信是以量子态为信息载体，利用量子纠缠效应、量子叠加等量子力学基本原理进行信息编解码、操纵控制和安全传输的一种新型通信方式。量子通信结合了量子论和信息论，在物理领域内利用量子力学基本原理进行高效率高安全的通信，具有区别于经典通信依赖数学计算复杂性的物理安全性；在通信领域内基于量子隐形传态、量子不可克隆等量子特性，利用量子测量等方法实现通信双方的信息交流。如图 1 所示，一个量子通信模型中量子信源产生信息，量子编码器将经典信息转化为量子比特，以量子态的形式加载信息，随后通过调制使量子信号能够适应量子信道传输。通信过程中，需要借助经典信道进行辅助信息的交换，接收方收到信号后，经过解调、译码等一系列操作使量子信宿能够接收信息。

目前，量子通信中应用最为广泛的技术便是量子密钥分发(Quantum Key Distribution, QKD)，以量子密钥分发为核心的量子保密通信技术逐步走向成熟，商用产业化得以实现，实用性得到了很好的检验。1984 年，美国 IBM 的 Bennett、加拿大 Montreal 大学的 Brassard 提出了 BB84 量子密钥分发协议，这是第一个量子通信协议，协议中量子信道传输量子密钥，经典信道传输用于基矢比对测量、窃听检测的大量辅助信息，最终通信双方可以 50%的概率成功获得随机共享的密钥[1]。量子密钥分发的安全性基于概率统计，通过抽样分析测量部分量子态来判断是否存在窃听，若有窃听，则放弃已有通信结果；若无窃听，则保留已传输的密钥。通信过程中，若窃听者进行拦截再发攻击就会有 75%的概率得到正确传输结果，通信双方间的错误率会达到 25%。量子密钥分发产生随机密钥后，可用于经典通信模式，即发送方利用共享的随机密钥加密信息，通过经典信道传输后由接收方解密读取，因此，量子密钥分发不能直接用来传输机密信息。

量子密钥分发无法突破经典通信模型，科研工作者们便提出了量子安全直接通信，以实现机密信息的直接安全传输。量子安全直接通信(Quantum Secure Direct Communication, QSDC)是用量子态加载信息，综合利用纠缠粒子的关联性和非定域性等量子特性以及海森堡测不准原理、不可克隆定理等量子力学基本原理，借助量子信道安全无泄漏地直接传输机密信息的一种量子通信技术。量子安全直接通信通过建立量子信道可直接传输机密信息，无需事先生成密钥，只在安全性检测、出错率估计时需要少量经典信息交换。机密信息加载于量子态前，通信方就应判断出是否存在窃听，若有窃听，则放弃此次通信过程；若无窃听，就开始传输机密信息。由此可见，量子安全直接通信也可产生随机密钥，实现量子密钥分发的功能，但量子密钥分发只能产生不涉及任何机密的随机密钥。

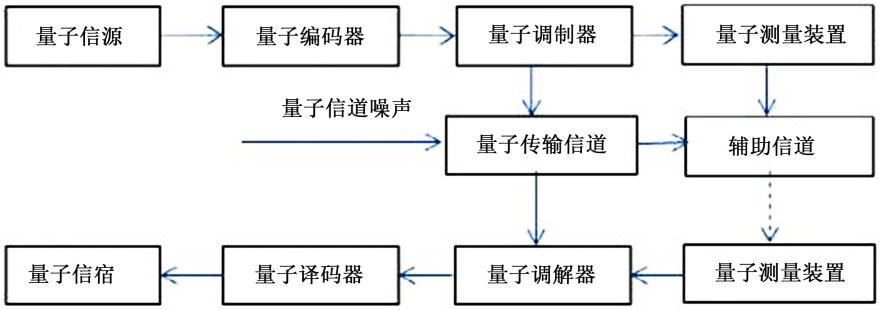

Figure 1. Quantum communication model
图 1. 量子通信模型

2000 年，清华大学龙贵鲁、刘晓曙将大数中心分布定理推广到量子体系，首创了量子数据块传输与分布传输方法，提出了第一个基于 EPR 纠缠光子对的两步高效量子通信方案，可解决通信过程中的信息泄漏难题[2]。2003 年，龙贵鲁、刘晓曙和北京师范大学的邓富国首次阐明了量子安全直接通信的定义、构造原理，提出了结构含义更完整的基于 EPR 纠缠光子对的两步 QSDC 方案[3]。2003 年，邓富国、龙贵鲁提出了基于单光子序列的量子一次一密直接通信方案，也称量子一次一密(quantum one-time pad)方案或 Deng-Long-04 (DL04)方案，该方案将未知量子态的不可克隆性融于一次一密加密体系，给出了 QSDC 需要满足的条件并阐明了其物理机制[4]。早期的两个典型方案给出了量子安全直接通信的构造原理和安全判据，为 QSDC 的进一步发展奠定了坚实的理论基础。

随后几年，QSDC 理论研究日益成熟完善，涌现出了很多基于单光子、纠缠粒子的新型 QSDC 方案，与此同时，QSDC 系统在有噪、攻击条件下的安全传输逐渐成为了其发展的关键制约点。2007 年，曲阜师范大学满忠晓等人分析了延边大学金星日等人提出的一种基于 GHZ 态的三方 QSDC 方案的安全性，发现窃听者依据公开信息可得到部分机密，因此给出了改进方案[5]。2008 年，北京邮电大学高飞等人研究分析了一种双向 QSDC 方案在不同攻击下系统的安全性问题，指出窃听者可利用公开的经典信息获取机密的部分内容[6]。2009 年，福建师范大学林崧等人提出了通过 PNS 攻击双向 QSDC 系统的方法并对方案进行了适当改进[7]。2011 年，南京大学顾斌等人首次研究了噪声条件下具有身份认证、基于密集编码的 QSDC 方案[8]。2012 年，北京邮电大学黄伟等人提出了基于量子加密的容错 QSDC 方案，方案在一定程度上可抵抗集体噪声[9]。2014 年，北京大学安辉耀等人研究了基于稳定子码的在噪声信道中的 QSDC 方案，该方案可对单量子的相位和比特错误进行检错纠错，降低通信误码率[10]。2015 年，龙贵鲁研究了噪声环境下的量子安全直接通信[11]。

在国内量子安全直接通信发展日趋成熟的同时，国外也逐步展开对量子安全直接通信的研究。2002 年，德国 Westfälische Wilhelms 大学的 K Bostrom、T Felbinger 提出了“乒乓”(ping-pong)通信方案，其在第一轮传输中没有安全性检测，但后来被证明是不安全的[12]。2004 年，韩国高等研究院 Nguyen 等人提出了一个可实现双向通信的 QSDC 方案[13]。2006 年，韩国信息安全技术中心 Lee 等人提出了一个可实现身份验证的 QSDC 方案，此方案后来被证明易受攻击，应通过阻止认证者获得信息的方法来增强安全性[14]；意大利 Melbourne 大学的 Tombesi 等人实验验证了简化版的 DL04 方案[15]。2008 年美国 Cornell 大学 Stefano Priandola，Samuel L. Braunstein 和 Stefano Manici、Seth Lioyd 提出了一个使用连续变量的 QSDC 方案[16]。2010 年，Cornell 大学 Ola M. Hegazy、Ayman M. Bahaa-eldin 和 Yasser H. Dakroury 提出了基于纠缠态和超密集编码的 QSDC 方案[17]。2015 年，乌克兰国际航空大学 Sergiy Gnatyuk、Tetyana Zhmurko 和波兰 Bielsko-Biała 大学的 Pawel Falat 为 QSDC 方案提供了一种效率加速思想，基于三元伪随机序列和有限域上的相关转换对 ping-pong 协议进行量子安全放大，既可增加方案安全性，又可提升通信

速率[18]。2016 年，巴西 Federal do Ceará 大学 AntoônioGeovan De Araújo Holanda Guerra、Francisco Franklin Sousa Rios 和 Rubens Ramos 提出了利用连续相干态的数字信号、模拟信号的 QSDC 方案[19]；同年，伊朗 Imam Reza 国际大学 Milad Nanvakenari、Monireh Houshmand 提出了基于四粒子群态的高效 QSDC 方案，方案可实现认证功能[20]。

此后，量子安全直接通信理论研究不断提升发展，思想理论极限得到突破，随着技术条件的持续升级，研发重点从理论研究逐步转向了实验验证。2016 年，山西大学肖连团等人利用简化频率编码的方法实验实现了 DL04 方案[21]。2017 年 6 月，中国科技大学和南京邮电大学联合实验，郭光灿等人首次利用量子存储，成功产生、传送、储存、编码了纠缠光子，检测了量子信道安全性，基本实验实现了基于纠缠的 QSDC 方案。以此为基础，可进一步开展百公里以上远距离的 QSDC 实验研究，为实现基于卫星的星地长距离通信和全球化量子安全直接通信网络奠定基础[22]。2017 年 11 月，清华大学与南京邮电大学合作，张巍、朱峰、盛宇波和黄翊东等人首次在 500 米环形光纤中实验实现了 QSDC，理论分析证明了凭借当前实验条件可验证相距几十公里双方通信的可行性，量子安全直接通信在实用化进程中取得了突破性进展[23]。

1.2. 通信原理

经典保密通信系统中，一次一密(one-time pad)加密体系是唯一用信息论相关理论被证明为绝对安全的。该体系中，每次通信密钥只能使用一次且长度应等于待加密的明文。系统中，窃听是无法避免的，但窃听只能获得加密后的操作结果，无法获取加密前的信息，窃听者不会同时拥有加密前后的结果，因此无法获得密钥，也就无法得到机密操作信息。通信过程中，合法通信双方间的共享密钥对窃听者而言是完全随机的，这可保证加密体系的安全性。

量子安全直接通信在物理原理上具有可行性，其安全原理类似经典一次一密加密体系。通信时，对系统的初始量子态进行不改变测量基矢的幺正操作，即编码机密信息，随后可进行信息传送。传输过程中窃听会得到操作后的量子态，但因不知系统初态，就无法读取量子幺正操作信息，机密就不会泄露。此外，用于量子通信的量子态不仅仅是一组基矢的本征态，在多组基矢的本征态综合排列后，窃听者准确读取操作后量子态信息的难度会增大，这从物理原理上保证了量子安全直接通信的安全性。

量子安全直接通信可直接传输机密信息，必须具备在信息泄露前就能判断出信道是否安全和有无窃听存在的能力。数据的块状传输保证通信双方可进行基于随机抽样统计的安全性分析，若存在窃听，窃听行为在分析结果中会有所体现，应放弃传输机密；若不存在窃听，则通过分布传输可保证量子幺正操作加载的机密信息不会泄露。合法的接收者应具备直接读取机密信息的能力，不能依赖于任何经典辅助信息。

判断一个量子通信方案是否是真正的量子安全直接通信时，关注点应落在方案是否能直接安全传输机密而不发生泄露上。因此，邓富国、龙贵鲁等人提出了 Deng-Long 判据[3] [4]用于进行辅助判断：

1) 借助量子信道传输量子态，只在安全性分析、出错率估计时需要少量经典信息交换，接收方可直接读取加载在量子态上的机密信息。

2) 窃听只能得到与机密信息无关的随机结果。

3) 通信双方在加载机密前就能判断出是否存在窃听。

4) 量子信息数据以量子态为载体，必须保证块状传输。

1.3. 研究意义

量子安全直接通信的理论研究与实验应用融合发展，取得了一系列成就。

与经典通信模式和量子密钥分发相比，量子安全直接通信具有很多发展优势，研究意义颇深。

1) 根据不可克隆定理，测量会造成量子态坍缩且量子通信没有电磁辐射，因此窃听或探测就无法进行，这使得量子安全直接通信具有高保密性、高安全性。将量子安全直接通信与经典加密相结合，可进一步提高通信安全，为保密需求极高的国防、军事等相关领域提供强有力的技术保证。

2) 量子安全直接通信线路时延低，信息传输率高，能很好地突破经典通信技术存在的物理极限，适合于某些紧急情况下的机密信息传输，可防止抵赖与造假行为。

3) 量子安全直接通信系统不依赖空间环境，也无关传播媒介，通信具有稳定的抗干扰能力和极强的传输能力，实际应用于条件恶劣、环境复杂的区域时会有较好的适应能力。

4) 目前光纤通信技术不断成熟扩大，量子安全直接通信可基于光纤系统实现实用化发展。为满足实际通信需求，量子安全直接通信必将成为未来量子通信研究的主攻方向，可带动全球量子通信产业化、网络化高速发展。

5) 相比于量子密钥分发，量子安全直接通信直接传输机密无需密钥生成，通过减少经典信息交换可降低复杂性，同时基于纠缠态的通信方案成倍地提高系统通信容量，现实通信速率会大大提升，这为未来进一步探索全球量子化通信技术的应用奠定了基础。

6) 国内外对量子安全直接通信的研究探索由浅渐深，由理论支撑逐步转向实验验证，进而可实现实用化、网络化、商业化的综合发展。

2. QSDC 典型方案分析

2.1. 两步量子直接通信方案

2003 年，邓富国、龙贵鲁和刘晓曙等人基于密集编码(quantum dense coding)提出了两步量子安全直接通信方案(two-step QSDC protocol) [3]，具体流程如图 2 所示。

信息发送方、接收方分别为 Alice、Bob。

1) 准备阶段

Alice 制备 N 个初始态都相同的 EPR 光子对，状态可处于 4 个 Bell 态之一，例如都处于量子态 $\left|\phi^{\pm}\right\rangle_{AB}$。Alice 选择每一个纠缠光子对中的 A 光子，按顺序构成序列 S_A，剩下的 B 光子按顺序构成检测序列 S_B。

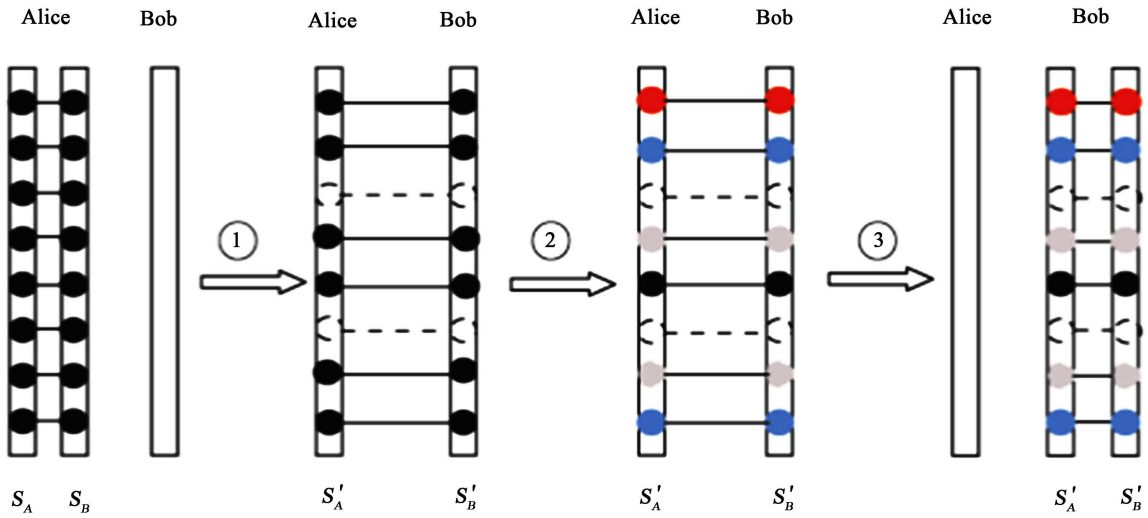

Figure 2. Theory of two-step scheme
图 2. 两步方案原理

2) 安全检测

Alice 将检测序列 S_B 发给 Bob，Bob 接受后随机抽取一些光子进行非对易基矢测量，随后将记录的抽样光子位置、基矢信息与测量结果告诉 Alice，由 Alice 进行测量比对。若出错率高于某一阈值，则 S_B 序列传输不安全，Alice 与 Bob 应放弃已有传输结果。若传输安全，用于安全检测的光子就被消耗掉了，两光子序列分别变为 S'_A 和 S'_B。

3) 机密编码

信道安全后，Alice 选用量子幺正操作 $U_i\left(i=0,1,2,3\right)$ 加载机密信息。窃听者 Eve 无法读取操作信息，监听跟随机猜测的结果完全一样，机密不会泄露。加载机密信息时，Alice 在 S'_A 序列中还要随机选取一些光子加载用于下一次安全检测的随机编码，具体规则如表 1 所示。

4) 机密收发

Alice 将编码后的信息序列发给 Bob，Bob 进行联合贝尔基测量可读取 Alice 加载的机密信息。此外，Bob 还应通过比对 Alice 的随机编码分析出错率，判断第 2 次传输的安全性以确定是否需要进行纠错等后续处理。

通信过程中，利用块状传输可保证检测序列的安全性，检测序列安全是机密信息安全的前提；分布传输可保证窃听者不能同时拥有携带信息的两部分，因此窃听不会导致机密泄露。系统安全性检测可用来判断是否存在窃听，检测过程中需要存储光子序列，对实验技术的要求很高，可用光学延迟技术代替，以防部分量子态未发送完而导致信息泄露。在噪声条件下，也可利用纠缠纯化或冗余编码等方法直接传输信息。

2.2. 一次一密——DL04 方案

2004 年，邓富国、龙贵鲁首次将块传输方法用于一次一密加密体系，提出了第一个基于单光子量子态序列的量子一次一密直接通信方案[4]，具体流程如图 3 所示。单光子态在实验上更易制备、更易测量，方案更具实用性。

1) 准备阶段

信息接收方 Bob 制备 N 个单光子态构成的序列 S，单光子随机处于 4 个量子态 $\{|H\rangle,|V\rangle,|R\rangle,|L\rangle\}$ 之一。

2) 安全检测

Bob 通过量子信道将光子序列 S 发给 Alice。Alice 随机选择两个基矢 $\{|H\rangle,|V\rangle\}$ 和 $\{|R\rangle,|L\rangle\}$ 对抽样选取的一些光子进行测量。随后通过经典信道将挑选的光子信息、测量基矢、测量结果告知 Bob，Bob 比对自己的光子制备情况进行安全性分析并将结果告知 Alice。若光子比对出错率高于某一阈值，则序列 S 的传输不安全，应放弃通信，否则表明传输安全。

Table 1. Encoding rule of secret information
表 1. 机密信息编码规则

量子幺正操作	机密信息
$U_0 = I = \|H\rangle\langle H\| + \|V\rangle\langle V\|$	“00”
$U_1 = \sigma_z = \|H\rangle\langle H\| - \|V\rangle\langle V\|$	“01”
$U_2 = \sigma_x = \|H\rangle\langle V\| + \|V\rangle\langle H\|$	“10”
$U_3 = -i\sigma_y = \|H\rangle\langle V\| - \|V\rangle\langle H\|$	“11”

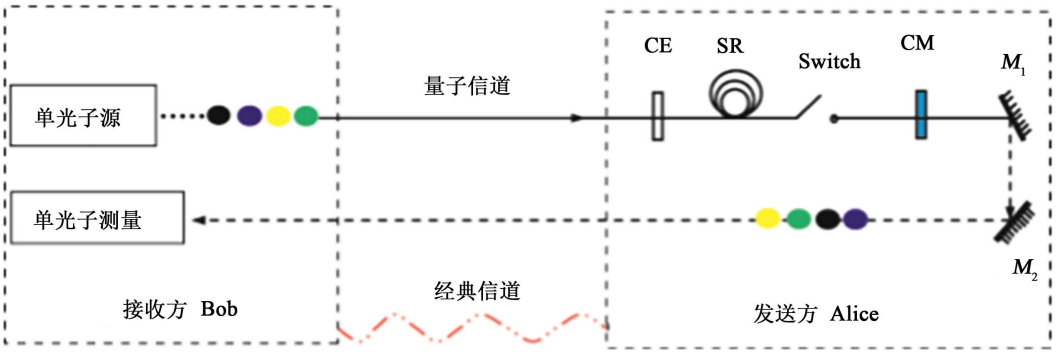

Figure 3. Theory of one-time-pad
图 3. 一次一密原理

3) 机密编码

Alice 对机密信息“0”采取单位操作 U_0，即光量子态保持不变；对机密信息“1”采取 U_3 操作，在一组正交基矢内反转量子态，即：

$$U_3|H\rangle=-|V\rangle,\quad U_3|V\rangle=|H\rangle,$$

$$U_3|R\rangle=|L\rangle,\quad U_3|L\rangle=|R\rangle。$$

幺正操作 U_0 和 U_3 可使基矢 $\{|H\rangle,|V\rangle\}$ 和 $\{|R\rangle,|L\rangle\}$ 中的两个本征态两两间转变或不变，具有操作不改变基矢的特点。编码时，Alice 还需随机选取一些位置的光子加载用于安全性检测的随机编码。

4) 机密收发

Alice 将编码后的序列发给 Bob，Bob 根据制备信息选择正确的基矢进行单光子测量，读取 Alice 传输的机密。Alice 公布随机编码的位置和操作信息，Bob 可通过比对分析出错率以判断第二次传输是否安全。

数据块状传输利于安全性检测，分布传输可确保机密不泄露。量子一次一密直接通信方案明确给出了基于单光子的量子安全直接通信设计要求：1) 加载机密信息前必须进行窃听检测，确保安全后才可传输信息。2) 信息数据必须块状传输，便于抽样进行窃听概率统计[4]。

3. QSDC 最新进展研究

3.1. QSDC 理论方案研究

现有量子安全直接通信方案根据加载信息的载体不同，可大致分为两类，一类是基于单光子的 QSDC 方案，另一类则是基于纠缠粒子的 QSDC 方案。信息载体不同使得方案的安全性、有效性、实用性均有一定程度的差异，引领着量子安全直接通信在不同方向的发展。

最早提出利用单光子作为信息载体的安全直接通信方案是 2003 年邓富国、龙贵鲁等人提出的一次一密 QSDC 方案，该方案可利用块传输、分布传输方法保证通信安全[4]；此后，有关单光子的 QSDC 理论方案逐步成熟完善，得到了一定程度的发展。2007 年，王剑等人利用单光子序列的顺序重排提出了多方控制的 QSDC 方案，在所有控制方都同意的情况下，接收方才可读取机密信息[23]；同年，邓富国等人提出了基于单光子的经济型 QSDC 网络方案[25]。2008 年，北京邮电大学王天银等人针对王剑等人提出的多方控制 QSDC 方案的缺陷，提出了改进方案并分析发现其能抵抗一种新的伪信号替换攻击[26]。2009 年，南京信息工程大学刘文杰等人提出了基于互认证的三维单光子 QSDC 方案，通过定义特定的酉算子与非正交测量基可使系统信息传输率很高[27]。2012 年，西安电子科技大学刘丹等人提出了利用极化单

光子和 EPR 纠缠对的 QSDC 方案，其中极化单光子用于身份认证、检测是否存在窃听，EPR 纠缠对用于传输机密信息[28]。2013 年，西安电子科技大学易运晖等人提出了基于单光子的随机多元基 QSDC 方案，利用单光子的随机多元基偏振校正方案，可完成各个偏振角度误差的补偿，通过延时可解决多态协议匹配率低的问题，方案保密性更好，通信距离更远[29]；北京邮电大学孙越等人提出了基于单光子态自避错传输的 QSDC 方案，可一定程度上抵抗信道中的联合噪声[30]。在基于单光子的量子安全直接通信方案兴起不久，方案逐步由简单利用单光子编码信息向利用单光子顺序重排、单光子高维度、高容量发展转变，这使系统中有关单光子的信息得到了最大化利用，在实现安全直接通信的基础上，还可实现复杂的身份认证，防止中间人攻击。但单光子编码机密信息的容量较低，会导致系统的通信效率低下，因此在 2010 年之后基于单光子的 QSDC 理论方案提出较少，研究逐步转向基于单光子的实验验证方面。

目前大多数 QSDC 方案是基于纠缠态的，这也是最早提出的完整的两步 QSDC 方案所采用的量子态。2005 年，北京师范大学王川等人提出了高维度系统超密集编码 QSDC 方案[31]和基于多粒子系统的多步 QSDC 模型[32]。2006 年，满忠晓等人提出了利用 GHZ 态和纠缠交换的 QSDC 方案[33]。2007 年，河北师范大学闫凤利等人提出了一种利用量子隐形传态技术实现的 QSDC 方案，通过 Controlled-NOT (CNOT) 门、本地测量和经典通信交换可安全地传输机密信息；满忠晓等人提出了基于量子纠缠转移技术的双向 QSDC 方案，两个合法通信方可同时交换机密信息[34]；王剑等人提出了利用 GHZ 纠缠态实现的多方控制的 QSDC 方案[35]。2008 年，林崧等人提出了基于 χ 型纠缠态的 QSDC 方案，方案利用密集编码技术可提高通信效率[7]。2011 年，北京师范大学王铁军等人首次提出了基于光子对两自由度超纠缠 Bell 态的高容量 QSDC 方案[36]。2013 年，江西师范大学徐越等人提出了基于 4 粒子纠缠态的 QSDC 方案，携带机密的粒子无需在公共信道上传输[37]。2014 年，北京邮电大学徐淑奖等人提出了基于二粒子的 Grover 搜索算法特性的 QSDC 方案，方案安全性较高[38]。2015 年，天津工业大学孔令浩等人提出了基于双向量子隐形传态的双向 QSDC 方案，方案无需传输携带机密的量子比特，系统安全性有所提高[39]。2016 年，西北大学曹正文等人提出了基于 Bell 态粒子和单光子混合的 QSDC 方案，方案的编码规则会导致部分信息泄露[40]，2017 年，南京信息工程大学刘志昊等人通过稍加改变编码规则提出了改进方案，可保证信息的高效安全传输[41]。2017 年，解放军理工工程学院翁鹏飞等人提出了基于 d 维 Bell 纠缠态的 QSDC 方案，传输效率高、窃听探测率也高[42]；同年，翁鹏飞等人弥补了昌燕等人于 2015 年提出的基于三粒子 w 态蜜罐的受控 QSDC 方案的缺陷，提出了 w 态高维 QSDC 改进方案[43]。基于纠缠态的 QSDC 方案不断突破创新，由最开始基于 EPR 光子对的两粒子纠缠逐步向三粒子 GHZ 态、四粒子、五粒子团簇态高维发展；同时利用纠缠粒子充当量子信道、通过测量可避免机密信息的传输，系统安全性得到加强；多粒子纠缠还可一定程度上提高编码容量，从而提高传输效率。基于纠缠态的 QSDC 理论方案成为了研究开发的重点，下一阶段在不断探索利用量子特性、量子力学基本原理的基础上，基于纠缠粒子的方案会进一步增多，逐步完善双向通信、多方可认证等功能，实现大跨越发展。

除上述两大类方案外，2006 年，国家信息中心吕欣等人提出了基于 CSS 纠错码的 QSDC 方案，无需建立量子信道，也不需传送经典辅助信息，安全性基于图灵机不能有效求解 NP 完全问题[44]。2017 年，翁鹏飞等人提出了实际噪声中基于量子纠错码的量子网络直接通信方案，但系统仍需选取 w 态粒子作为控制比特、传输机密信息的粒子作为目标比特，通过量子纠缠实现完整的通信过程[45]。QSDC 方案理论体系不断成熟完善，逐年创新发展，为进一步深入探索 QSDC 的实验实用化研究提供了必要的先决条件。

3.2. QSDC 实验进展研究

量子安全直接通信的理论研究是要为实验验证服务的。近几年，随着技术的不断创新，实验验证量

子安全直接通信相关理论取得了初步进展，效果明显，具有很好的实际应用价值，对下一阶段深入实验探索具有重要指导作用。

3.2.1. 基于单光子的实验方案

2016 年，肖连团等人实验实现了 DL04 方案[21]，该方案有别于理论方案，实验并没有利用幺正操作单独编码一比特信息，而是将光子序列分成不同长度的数据块，发送方依据周期函数对每一光子块进行相同的幺正操作，利用被调制的光子序列在频域内的统计特性将信息编码在光子序列的频谱上，不同调制频率对应不同比特数的序列块。完成单光子频率编码，便可抵抗一定强度的损耗和噪声、减少错误，弥补光纤损耗、单光子探测器并不完美等实验缺陷，增强系统的稳定性。第一次安全性检测后，接收方只要收到调制频谱，利用离散时间傅里叶变换便可准确计算出调制频率。依据调制频率中的频谱线，接收方就能得到被编码的频率，从而读出机密信息。

基于单光子频谱多自由度的特性，实验还实现了量子安全直接通信的多通道信息传输。对于给定的通信系统，利用公式 $N_c=\frac{f_{\max}-f_{\min}}{f_b}+1$，可得到最大信道数量 N_c，其中 $f_{\max}$、$f_{\min}$ 分别是最大、最小调制频率，f_b 是信道间隔。信息传输能力依赖于频率组成，假设发送方在一个单光子块上负载 r 个频率，有效自由度便是在 N_c 个频率信道上 r 个频率的不同组合数 $N_{\max}=\frac{N_c!}{r!(N_c-r)!}$，这意味着一个单光子块可携带 $b=\log_2 N_{\max}$ 比特的信息，信息传输率可扩展为 $I=\frac{b}{T_{span}}\log_2 N_{\max}$，其中 T_{span} 是时间间隔。实验选取 $N_c=16$，即选择 16 个调制信道，频率从 25 kHz 扩展至 400 kHz，信道间隔为 25 kHz。取单一的频率分量 $r=1$，即在一个时间间隔内 16 个频率信道中只有一个用于信息传输，因此通过传输一个数据块，接收者可得到 $\log_2 16=4$ 比特信息。当时间块长度为 1ms 时，数据传输率可达 4 kbps。

连续光脉冲服从泊松分布，导致实验所得频谱会受白噪声影响，但光子的损耗和错误仅改变频谱的信噪比。因此，白噪声背景下，接收方可利用基于频率调制的特征谱从编码中恢复出机密信息。实验还分析了通信系统可很好地抵抗截取重发攻击(intercept-resend attack)和光子数分束攻击(photon-number-splitting attack)。特征谱的信噪比是由正确探测到的被编码单光子数决定的。当信噪比小于 1 时，即使窃听者可得到被加密单光子块的部分光子，也不可能获取所有机密信息。系统的安全传输距离依赖于每脉冲的平均光子数，二者关系如图 4 所示，系统的最远传输距离大约可达 16 km，但实际信息比特数值在传输距离超过 1 km 后下降明显，如图 4 所示。此外，山西大学肖连团等人还提出了一种无条件安全的信息传输策略，为量子安全直接通信更深层次的实用化研究提供了坚实有力的技术支撑。

利用单光子实现安全直接通信，首要任务便是制备单光子。目前大多数单光子的制备方法较复杂，实验环境要求很严格，极大地限制了通信系统的建立，不理想的单光子甚至有可能导致窃听成功率增加；其次，实验中对光子操作控制的熟练程度也会影响实验结果，改善量子通信设备、加强科技实战化应用十分必要。科技力量只有不断革新，才能为量子安全直接通信实验的实用化研究提供坚实支撑，从而为未来基于单光子的 QSDC 实验验证拓宽发展空间。

3.2.2. 基于 EPR 光子对的实验方案一

2017 年 6 月，郭光灿等人利用量子存储技术实验验证了基于纠缠的 QSDC 方案，实现了光子纠缠的产生，量子信道安全性检测，纠缠态光子的传送、储存、编译码等方案的必要过程[22]。多数 QSDC 方案利用光学延迟技术储存编码后的光子，实验上是可行的，但光学延迟的固定时延会导致通信系统不够灵活。因此，本实验利用量子存储代替光学延迟技术，量子存储能很好地抵抗消相干作用，根据实际

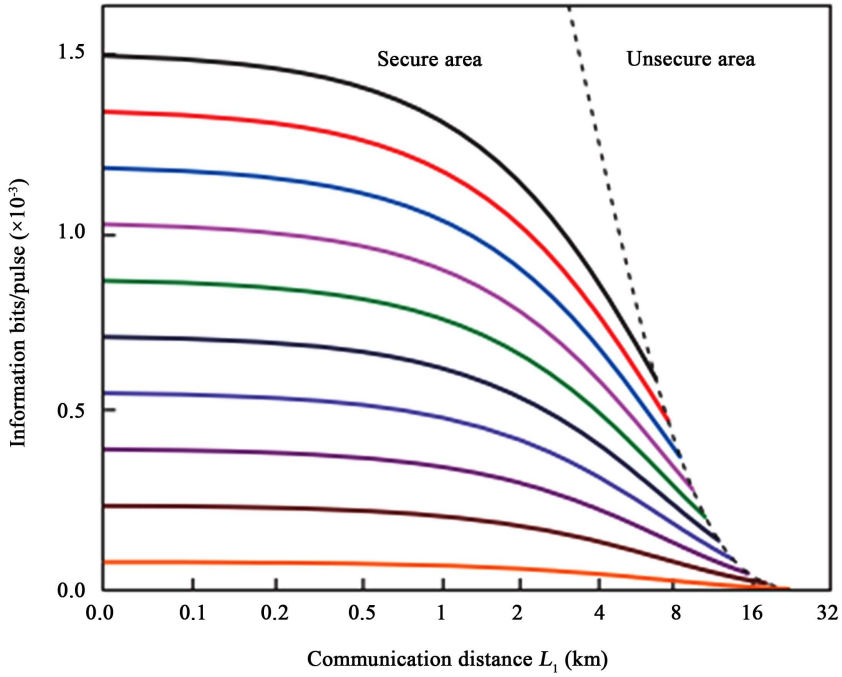

Figure 4. Relation between communication distance and every information bit pulse
图 4. 通信距离与每脉冲信息比特的关系

需求还可操作改变量子态，保证所控信息在一定时域内可高效传输，从而实现完整的通信过程，满足实际需求。实验成功实现了连续存储纠缠单光子、准确有效地控制量子态等极具挑战性的关键环节。

因 Bell 态难以区分，实验并没有完全按照理论方案所述进行，而是采用具有极化自由度的光子作为信息载体。发送方无需直接建立两光子纠缠 Bell 态，通过制备混合纠缠光子对，分发后储存于另一量子系统中，便可建立存储纠缠。机密传输时，对来自第一量子系统中的光子进行密集编码，在恢复来自第二量子系统中存储的光子后，通过密度矩阵的重建便可完成解码工作，解码时需实现完整确定的 Bell 态测量。实验利用密集编码可保证信息的高效传输，保真度大约可达 90%，系统的通信能力优于量子远程传态。

实验时，传送光子、编码操作均需一定时间，双方共享光子对的存储也需时间，存储时间大于 $T_0 + L/c$，T_0 是发送方的操作时间，L 是通信距离，c 是光速，L/c 是一个光子的传输时间。量子存储的时间是影响实验效率的关键因素，利用后向恢复技术，实验可保证量子存储的效率高于 90%，利用量子重复多元存储可较好地实现数据的块传输。

借助量子中继器，改善长距离通信时光纤中大部分光子丢失、失关联的情况，是未来实验必然面对的挑战。实验化的突破对未来基于卫星的超距、全球量子安全直接通信的实现以及量子安全网络的建立具有一定的启发价值。

3.2.3. 基于 EPR 光子对的实验方案二

2017 年 11 月，清华大学张巍、南京邮电大学盛宇波等人首次利用光纤光学技术实现了基于纠缠对的长距离 QSDC 实验[23]。光纤量子信道的长度可达 500 米，通信后两纠缠 Bell 态的保真度分别可达 91%、88%。

实验利用光纤量子光源方面的技术可制备出基于纠缠 Bell 态的量子光源，处于偏振纠缠 Bell 态的两光子既偏振纠缠又频率简并，这使得将两光子分离到两个不同光路时具有一定难度。实验将光纤中的自

发矢量四波混频效应双向地引入到光纤萨格奈特环路中，利用环路输出端的双光子量子干涉现象可解决分离难题。实验制备出的纠缠光子对存储于光纤圈中，性能高于量子存储。

实验还采用光纤光学器件构建偏振纠缠 Bell 态检测系统，使用的光纤既用作量子信道，又用作光子寄存器。与量子存储相比，光纤操作更简易，更具可靠性，当存储时间在几十微秒内时，系统的效率和保真度会很高。实验建立的完全基于光纤光学技术的 QSDC 系统，成功实现了纠缠安全检测、纠缠 Bell 态编解码等实验关键步骤，完整地论证了基于纠缠的 QSDC 在光纤传输条件下功能实现的可行性。未来实验中，通过使用较窄的光学滤波器或控制量子存储的温度可减缓光子的纠缠变换，以此可提高实验的可见度。以此为基础，利用与光纤通信兼容的成熟技术可实现面向光纤网络应用的 QSDC 系统，这是量子安全直接通信向实用化迈进的关键环节，具有巨大的发展潜力与现实价值。

对基于单光子以及两个基于 EPR 纠缠光子对的实验方案进行综合比较分析，对比实验结果如表 2 所示。

由表 2 可知，基于 EPR 纠缠光子对的实验相较基于单光子的实验在光纤衰减方面相差不大，在保真度、传输率、安全通信距离等方面存在一定优势，有利于直接远距离网络化通信。未来发展中，应着力研究基于纠缠对的量子安全直接通信。两个基于纠缠对的实验方案的编码保真度相差不大，但未来还应着重研究如何提高通信距离、改善存储性能、减缓光纤衰减等实验上的技术难题。此外，为深入探索发展 QSDC，还应寻找易制备纠缠态的新方法，发现并使用量子力学新性质来设计实现 QSDC 实验，突破传输效率、安全距离等实验极限，为量子远距通信、量子网络的建立提供完备的实验环境。

3.3. QSDC 网络设计研究

近年来量子安全直接通信的研究大多是基于点对点的双方单向或双向通信，主要集中在对不同新型通信方案的理论模型设计以及提高系统安全性等方面，对基于 QSDC 的量子通信网络实验探索较少，仅停留在理论研究阶段。随着人们对通信技术可靠性、安全性、灵活性要求的日益提高，点对点的传统通信模式无法满足多方用户需求，系统容量和灵活性都有待加强，量子安全直接通信实用便捷，必然要与经典通信网络相结合，综合发挥各自优势，向量子系统网络化方向迈进。

量子通信网络有自己特有的网络分层结构，主要分为物理链路层、网络层以及网络管理层。物理层实现量子信号的产生、探测、调制和编码，网络层负责为量子中继器寻找合适路由并进行路由控制、量子态交换、量子多址等操作，网路管理层实现密钥管理，降低误码率，保证系统安全性。

Table 2. Comparison of experimental results
表 2. 实验结果对比

实验结果 / 实验方案	肖连团组实验	郭光灿组实验	张巍组实验
实验时间	2016	2017	2017
使用的量子态	单光子	EPR 纠缠光子对	EPR 纠缠光子对
光脉冲重复频率	10 MHz	暂无	10 GHz
光纤衰减	0.2 dB/km	暂无	0.2 dB/km
编码保真度	暂无	90%	91%、88%
数据传输率	4 kbps	2.5 bit/s	暂无
实验距离	暂无	暂无	500 m
理论安全通信距离	16 km	暂无	25 km

2007 年，邓富国等人提出了基于单光子的经济型 QSDC 网络基本方案[25]。方案中有可以制备和测量量子信号的服务器(Alice)、发送端(Bob)和接受端(Charlie)。在利用单光子的 QSDC 系统基础上，引入量子服务器的概念可实现三方用户间的量子信息交换。服务器 Alice 是单光子序列的制备者，参与系统安全检测，不会破坏原有两用户系统的安全性。该方案中，因单光子信号源不完整，系统易受光子数分束攻击(Photon Number Splitting, PNS)，2009 年，权东晓等人对其进行改进，提出了基于诱骗态的广域量子 QSDC 网络方案。方案通过在局域网中设置服务器提高了通信距离，根据信道参量可估计不同通信距离的通过率，实现远距离的 QSDC [46]。2007 年，邓富国、李熙涵等人提出了基于纠缠态的 QSDC 网络方案，服务器 Alice 制备的是 EPR 纠缠对[47]。2014 年，华中科技大学葛华研究了 QSDC 相关的网络技术，提出了利用量子中继器连接的双通信环 QSDC 网络结构，可增加通信距离，提高系统的灵活性、实用性[48]。2015 年，青岛理工大学马鸿洋等人提出并讨论了噪声情况下的量子网络直接通信[49]。2016 年，曹正文等人提出了一种星型网络中的双向 QSDC 方案，方案具有较高的通信效率，可抵抗窃听者的被动式和截获重发攻击[50]。

从上述量子安全直接通信网络系统可看出，现有的 QSDC 网络化方案基本都是对 QSDC 具体通信方案的扩展，在点对点的 QSDC 通信系统中引入量子服务器实现三方通信。整体来看 QSDC 网络化模型结构相对简单，不够实用，忽略了网络系统中通信距离、通信质量等相关因素的影响，也没有考虑到真正量子通信网络化后路由寻址、信息交换等实际问题。随着传输距离要求的不断增加，信息在信道中传输时必然会损耗能量，由于量子态的不可克隆性，可采用基于纠缠交换的量子中继技术来扩大 QSDC 网络系统的通信距离，增强实用性能。受当前技术限制，量子安全直接通信的网络化发展依旧面临着严峻挑战。

4. QSDC 发展趋势展望

量子通信技术飞速发展，各国均斥资大力研发探究，我国在量子通信领域占据重要地位，理论与实验成果显著。量子通信具有高保密安全性，量子隐形传态不受材料空间限制，这些量子独有的优良特性使量子通信具有巨大的发展潜力与广阔的应用前景。随着信息网络技术的深层次发展，世界各国都大力追求机密传输安全与高速通信效率，量子通信技术必将成为未来通信技术中的主力，将其与现有信息网络格局相融合，在应用技术与实用效果层面取长补短、相互补充，必将引起新一轮的信息技术革命，引领未来通信发展主流趋势。目前，量子通信的基本理论和结构框架逐渐成熟，在制备单光子、测量量子态、量子存储等关键技术突破瓶颈、获得实验发展的条件下，量子通信工作重心开始由科研理论阶段向试点应用阶段转移。

我国在量子安全直接通信领域持续深入探索，理论方案与实验研究都取得了显著性进展，受到世界各国的广泛关注。量子安全直接通信基于单光子或纠缠粒子量子体系，巧妙运用块传输、分布传输思想，采用合适编码可保证信息传输的高机密性，通过安全检测可防止窃听造成的信息泄露。这种保密通信技术直接传输机密信息，保证系统通信可靠的同时，不失灵活可变性，进一步的发展实为必要，但逐步的深入探究依旧面临众多挑战：

1) 实际通信系统链路中必然存在噪声影响，噪声分为外部噪声和内部噪声。外部噪声是由外部环境、其它通信系统等外部干扰引起的，量子安全直接通信中制备所需量子态或进行量子测量等操作时，对实验环境要求较高，极易受到外界影响。外界环境对量子系统会产生耦合干扰，使量子系统的相干性随时间而衰减，即退相干或消相干现象，属于量子噪声。噪声越强，系统的消相干现象越明显。可采用量子编码等方法减缓退相干，特定的冗余编解码规则对量子噪声问题可起到一定的抑制效果。内部噪声是通信系统内部产生的噪声，不可避免，只能采取技术手段进行适度控制，在实验实现直接通信时也是无法

忽略的重要影响因素。采用机密放大、纠错等方法可保证信息的安全保真传输，量子态避错传输等方法可极大地克服信道噪声，利用纠缠纯化技术提高光量子态的纯度也可抑制信道噪声与环境噪声。但目前对量子安全直接通信系统受噪声影响的讨论仍较少，实验验证理论时存在困难，QSDC 系统离实用化的实现还存在较大差距。

2) 量子通信网络按照特定拓扑结构控制多方网络节点，利用量子特性、量子力学原理可进行基于光量子形式的经典机密信息传输。量子网络化的构建是下一阶段量子通信的研发重点，光纤通信技术的日常化应用不断成熟，为量子安全直接通信网络化的发展奠定了坚实的技术基础。但目前现有量子安全直接通信网络化方案还较为欠缺，理论研究不算成熟，结构体系也不太明确，受传输距离、传输质量的影响，通信会对精准传输控制量子态要求很高，对成熟使用具体量子仪器设备要求很严格，量子通信网络的实用化实现任重道远。实际实验时，可利用量子中继、量子态秘密放大、量子纠错等技术，或利用多自由度产生的高维度超纠缠量子态来实现量子安全直接通信的远程化与网络化。

3) 量子安全直接通信以光波为信息载体，在实验取得一定进展后，可继续探索研究通过量子复用提高系统通信容量、增加可靠性的技术手段，以满足商业化使用标准。但目前受实验技术限制，量子安全直接通信的实用化研究还存在很大缺陷，在复用技术领域的探索更是稀缺，这使得实验发展较为困难，但不可否认的是，深入探索研发空间是无限的。

量子安全直接通信的发展关系着我国信息安全领域的安全性、先进性，在现有成果基础之上，要进一步完善理论研究，多角度思考、多层面检验，提高系统的稳健性和高效性，同时需综合开发利用好量子的各种特性，大力投入相关领域的研究，着力推进量子通信技术的逐步完善，同时要注重研发精简实用的量子通信设备，多进行实验实用化探索，在通信理论、实现方法间实现完美转化，以保证我国量子安全直接通信领域的持续领先地位，最终带动全球实现量子安全直接通信的网络化、普及化。

基金项目

1) 国家高科技研究和发展项目(863 项目) (2011AA010803)；2) 国家自然科学基金项目(U1204602)；3) 数学工程与先进计算国家重点实验室开放课题项目(2013A14)。

参考文献

[1] Bennett, C.H. and Brassard, G. (1984) Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of IEEE International Conference on Computers*, *Systems and Signal Processing*, IEEE, Bangalore, 175-179.

[2] Long, G.L. and Liu, X.S. (2002) Theoretically Efficient High-Capacity Quantum-Key-Distribution Scheme. *Physical Review A*, **65**, 032302. https://doi.org/10.1103/PhysRevA.65.032302

[3] Deng, F.G., Long, G.L. and Liu, X.S. (2003) Two-Step Quantum Direct Communication Protocol Using the Einstein-Podolsky-Rosen Pair Block. *Physical Review A*, **68**, 113-114. https://doi.org/10.1103/PhysRevA.68.042317

[4] Deng, F.G. and Long, G.L. (2004) Secure Direct Communication with a Quantum One-Time Pad. *Physics*, **69**, 521-524. https://doi.org/10.1103/PhysRevA.69.052319

[5] 满忠晓, 夏云杰. Improvement of Security of Three-Party Quantum Secure Direct Communication Based on GHZ States [J]. 中国物理快报: 英文版, 2007, 24(1): 15-18.

[6] Gao, F., Wen, Q.Y. and Zhu, F.C. (2008) Teleportation Attack on the QSDC Protocol with a Random Basis and Order. *Chinese Physics B*, **17**, 1838-1842.

[7] 林崧. 量子密码的理论研究及其计算机仿真[D]: [博士学位论文]. 北京: 北京邮电大学, 2009.

[8] Gu, B., Zhang, C.Y., Cheng, G.S. and Huang, Y.G. (2011) Robust Quantum Secure Direct Communication with a Quantum One-Time Pad over a Collective-Noise Channel. *Science China Physics*, *Mechanics and Astronomy*, **54**, 942. https://doi.org/10.1007/s11433-011-4265-5

[9] 黄伟, 温巧燕, 贾恒越, 等. Fault Tolerant Quantum Secure Direct Communication with Quantum Encryption against Collective Noise [J]. 中国物理 b: 英文版, 2012, 21(10): 101-109.

[10] 安辉耀, 于涛, 刘敦伟, 等. 基于稳定子码的在噪声信道的量子安全直接通信方案研究[J]. 量子光学学报, 2014, 20(3): 187-191.

[11] 龙桂鲁. 噪声环境下的量子安全直接通信[C]//全国光学前沿问题讨论会会议. 2015.

[12] Boström, K. and Felbinger, T. (2002) Deterministic Secure Direct Communication Using Entanglement. *Physical Review Letters*, **89**, 187902. https://doi.org/10.1103/PhysRevLett.89.187902

[13] Nguyen, B.A. (2004) Quantum Dialogue. *Physics Letters A*, **328**, 6-10. https://doi.org/10.1016/j.physleta.2004.06.009

[14] Lee, H., Lim, J. and Yang, H.J. (2005) Quantum Direct Communication with Authentication. *Physical Review A*, **73**, 543-543.

[15] Cerè, A., Lucamarini, M., Giuseppe, G.D., *et al*. (2006) Experimental Test of Two-Way Quantum Key Distribution in the Presence of Controlled Noise. *Physical Review Letters*, **96**, 200501. https://doi.org/10.1103/PhysRevLett.96.200501

[16] Pirandola, S., Braunstein, S.L., Mancini, S., *et al*. (2008) Quantum Direct Communication with Continuous Variables. *Europhysics Letters*, **84**, 548-551. https://doi.org/10.1209/0295-5075/84/20013

[17] Hegazy, O.M., Bahaaeldin, A.M. and Dakroury, Y.H. (2010) Quantum Secure Direct Communication Using Entanglement and Super Dense Coding.

[18] Gnatyuk, S., Zhmurko, T. and Falat, P. (2015) Efficiency Increasing Method for Quantum Secure Direct Communication Protocols. *International Conference on Intelligent Data Acquisition and Advanced Computing Systems*: *Technology and Applications*, Warsaw, 24-26 September 2015, 468-472.

[19] Guerra, A.G.D.A.H., Rios, F.F.S. and Ramos, R.V. (2016) Quantum Secure Direct Communication of Digital and Analog Signals Using Continuum Coherent States. *Quantum Information Processing*, **15**, 4747-4758. https://doi.org/10.1007/s11128-016-1410-0

[20] Nanvakenari, M. and Houshmand, M. (2016) An Efficient Controlled Quantum Secure Direct Communication and Authentication by Using Four Particle Cluster States. *International Journal of Quantum Information*, **15**, 124.

[21] Hu, J.Y., Yu, B., Jing, M.Y., *et al*. (2016) Experimental Quantum Secure Direct Communication with Single Photons. *Light Science & Applications*, **5**, e16144. https://doi.org/10.1038/lsa.2016.144

[22] Zhang, W., Ding, D.S., Sheng, Y.B., *et al*. (2017) Quantum Secure Direct Communication with Quantum Memory. *Physical Review Letters*, **118**, Article ID: 220501. https://doi.org/10.1103/PhysRevLett.118.220501

[23] Zhu, F., Zhang, W., Sheng, Y. and Huang, Y. (2017) Experimental Long-Distance Quantum Secure Direct Communication. *Science Bulletin*, **62**, 1519-1524. https://doi.org/10.1016/j.scib.2017.10.023

[24] 王剑, 陈皇卿, 张权, 等. 多方控制的量子安全直接通信协议[J]. 物理学报, 2007, 56(2): 673-677.

[25] Deng, F.G., Li, X.H., Li, C.Y., *et al*. (2006) Quantum Secure Direct Communication Network with Einstein-Podolsky-Rosen Pairs. *Physics Letters A*, **359**, 359-365. https://doi.org/10.1016/j.physleta.2006.06.054

[26] 王天银, 秦素娟, 温巧燕, 等. 多方控制的量子安全直接通信协议的分析及改进[J]. 物理学报, 2008, 57(12): 7452-7456.

[27] 刘文杰, 陈汉武, 刘景发, 等. 基于互认证的三维单光子量子安全直接通信[J]. 中南大学学报(自然科学版), 2009(s1): 309-314.

[28] 刘丹. 量子通信协议与安全策略研究[D]: [博士学位论文]. 西安: 西安电子科技大学, 2011.

[29] 易运晖, 权东晓, 裴昌幸, 等. 随机多元基量子安全直接通信[J]. 吉林大学学报(工), 2013, 43(2): 515-519.

[30] 孙越. 基于单光子态自避错传输的量子安全直接通信协议[J]. 量子光学学报, 2013, 19(2): 122-128.

[31] Wang, C., Deng, F.G., Li, Y.S., *et al*. (2005) Quantum Secure Direct Communication with High-Dimension Quantum Superdense Coding. *Physical Review A*, **71**, Article ID: 044305. https://doi.org/10.1103/PhysRevA.71.044305

[32] Wang, C., Deng, G.F. and Long, G.L. (2005) Mufti-Step Quantum Mufti-Particle Green-Horne-Zeilinger State. *Optics*, **53**, 15-20.

[33] 满忠晓, 夏云杰. 利用 GHZ 态和纠缠交换的量子安全直接通讯[J]. 量子光学学报, 2006(b08): 10.

[34] Chen, Y., Man, Z.-X. and Xia, Y.-J. (2007) Quantum Bidirectional Secure Direct Communication via Entanglement Swapping. *Chinese Physics Letters*, **24**, 19-22. https://doi.org/10.1088/0256-307X/24/1/006

[35] Wang, J., Zhang, Q. and Tang, C.J. (2006) Multiparty Controlled Quantum Secure Direct Communication Using Greenberger-Horne-Zeilinger State. *Optics Communications*, **266**, 732-737. https://doi.org/10.1016/j.optcom.2006.05.035

[36] 王铁军. 基于腔量子电动力学的量子通信与量子门研究[D]: [博士学位论文]. 北京: 北京师范大学, 2011.

[37] 徐越, 李渊华, 桑明煌, 等. 基于 4 粒子纠缠态的量子安全直接通信[J]. 江西师范大学学报(自然版), 2013, 37(3):

253-256.

[38] 徐淑奖, 钮心忻, 陈秀波, 等. 两个基于 Grover 搜索算法的量子直接通信协议[J]. 2014.

[39] 孔令浩, 胡占宁. 基于双向量子隐形传态上的双向量子安全直接通信[J]. 重庆工商大学学报(自然科学版), 2015, 32(10): 54-57.

[40] 曹正文, 赵光, 张爽浩, 等. 基于 Bell 态粒子和单光子混合的量子安全直接通信方案[J]. 物理学报, 2016, 65(23): 37-43.

[41] 刘志昊, 陈汉武. 基于 Bell 态粒子和单光子混合的量子安全直接通信方案的信息泄露问题[J]. 物理学报, 2017, 66(13): 37-41.

[42] 翁鹏飞, 陈红, 蔡晓霞. 基于 d 维 Bell 纠缠态的量子安全直接通信方案[J]. 量子电子学报, 2017, 34(5).

[43] 翁鹏飞, 陈红, 蔡晓霞, 等. W 态的高维量子安全直接通信[J]. 激光杂志, 2017, 38(6): 21-24.

[44] 吕欣, 马智, 冯登国. 基于量子 Calderbank-Shor-Steane 纠错码的量子安全直接通信(英文)[J]. 软件学报, 2006, 17(3): 509-515.

[45] 翁鹏飞, 陈红, 蔡晓霞, 等. 量子纠错码在噪声信道中的量子网络通信方案[J]. 激光杂志, 2017, 38(10): 16-19.

[46] 权东晓, 裴昌幸, 刘丹, 等. 一种基于诱骗态的广域量子安全直接通信网络方案[J]. 光子学报, 2009, 38(12): 3283-3287.

[47] Deng, F.-G., Li, X.-H., Li, C.-Y., *et al*. (2007) Quantum Secure Direct Communication Network with Superdense Coding and Decoy Photons. *Physica Scripta*, **76**, 25-30. https://doi.org/10.1088/0031-8949/76/1/005

[48] 葛华. 量子安全直接通信及网络技术研究[D]: [博士学位论文]. 武汉: 华中科技大学, 2014.

[49] 马鸿洋, 秦国卿, 范兴奎, 等. 噪声情况下的量子网络直接通信[J]. 物理学报, 2015, 64(16): 32-38.

[50] 曹正文, 冯晓毅, 彭进业, 等. 一种星型网络中的双向量子安全直接通信方案[J]. 西北大学学报: 自然科学版, 2016, 46(4): 507-511.