Computer Science and Application 计算机科学与应用, 2019, 9(2), 188-204
Published Online February 2019 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2019.92023

Hans汉斯

A Modified Scheme of Quantum Secure Direct Communication Based on 4-Dimension Hilbert Space by Mixing Bell State Particles and Single Photons

Xinlong Wang[1], Hongxin Li[2,3], Yu Han[2,3], Huijie Jiang[2], Anping He[1], Caihong Li[1*]

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

Received: Jan. 12th, 2019; accepted: Jan. 23rd, 2019; published: Jan. 30th, 2019

Abstract

With the rapid development of quantum cryptography technology, quantum secure direct communication (QSDC) has achieved remarkable results as an important branch. We put forward a modified scheme based on 4-dimension Hilbert space, which mixes Bell state particles and single photons and loads 3 bits on a quantum state in order to improve the coding capacity, the information transmission efficiency and the security.

Keywords

Quantum Secure Direct Communication, Quantum Coding, 4-Dimension Hilbert Space, Eavesdropping Detection

一种基于4维Bell态粒子和单光子混合的量子安全直接通信改进方案

王欣龙[1]，李宏欣[2,3]，韩　宇[2,3]，姜慧杰[2]，何安平[1]，李彩虹[1*]

[1]兰州大学信息科学与工程学院，甘肃　兰州
[2]战略支援部队信息工程大学，河南　郑州
[3]数学工程与先进计算国家重点实验室，河南　郑州
Email: *lihongxin830@163.com

*通讯作者。

文章引用: 王欣龙, 李宏欣, 韩宇, 姜慧杰, 何安平, 李彩虹. 一种基于 4 维 Bell 态粒子和单光子混合的量子安全直接通信改进方案[J]. 计算机科学与应用, 2019, 9(2): 188-204. DOI: 10.12677/csa.2019.92023

收稿日期：2019年1月12日；录用日期：2019年1月23日；发布日期：2019年1月30日

摘　要

随着近年来量子密码技术的迅猛发展，作为其重要分支的量子安全直接通信(QSDC)技术也取得了令人瞩目的进展。本文提出了一种依托4维Hilbert空间的QSDC改进方案，该方案混合利用Bell态粒子和单光子并将3比特经典信息加载于1个量子态上以提高编码容量以及信息传输的效率和安全性。

关键词

量子安全直接通信，量子编码，4维Hilbert空间，窃听检测

1. 引言

1.1. 量子安全直接通信发展背景

量子密码技术是一种依托于量子物理基本理论来实现信息安全的新式保密技术，相较于经典加密系统基于数学计算复杂度的安全性描述，量子密码系统理论定义上的安全由量子纠缠效应、量子叠加等量子力学基本原理以及量子隐形传态、量子不可克隆等量子特性来保证。目前，量子密钥分发(Quantum Key Distribution, QKD)是使用最为广泛的一种量子密码技术，其商用产业化逐渐实现，实用性得到了很好的检验。1984 年，美国 IBM 公司的 Bennett、加拿大 Montreal 大学的 Brassard 首创了 BB84 量子密钥分发协议，该协议利用量子信道传输可用于经典密码体制的量子密钥[1]。因此量子密钥分发技术只是生成并传输密钥而无法直接传输机密信息。

考虑到量子密钥分发技术并不能直接作用于信息通信，科研工作者们便提出了量子安全直接通信的概念，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)借助不同量子态或量子操作加载信息，综合利用了量子特性以及量子力学基本原理，是一种可实现机密内容直接传输的量子密码技术[2]。通信双方利用量子安全直接通信技术交流机密信息，不需要生成密钥，只需要在系统安全性检测、传输错误率估计时交换少量经典信息。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。因此，量子安全直接通信也可以用于产生随机密钥来实现量子密钥分发的功能。

2000 年，清华大学龙贵鲁、刘晓曙首创了量子数据块传输与分步传输方法，提出了第一个利用 EPR 纠缠光子对实现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，提出了结构更完整、步骤更清晰的利用 EPR 纠缠光子对实现的两步 QSDC 方案[3]。2003 年，邓富国、龙贵鲁首次提出了利用单光子实现的 QSDC 方案，也称量子一次一密(quantum one-time pad)方案或 Deng-Long-04 (DL04)方案[4]，该方案在一次一密加密体系中利用了未知量子态的不可克隆特性，阐明了量子安全直接通信的物理机制以及需要满足的通信条件。早期的两个经典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 的深层次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功能的 QSDC 方案[8]。2012 年，北京邮电大学黄伟等人依据量子加密思想提出了一定程度上可抵抗集体噪声的容错 QSDC 方案[9]。2014 年，北京大学安辉耀等人研究了基于稳定子码的 QSDC 方案，该方案在噪声环境下可实现一定程度上的检错纠错，降低通信误码率[10]。2015 年，龙贵鲁对噪声环境中的 QSDC 方案进行了探究[11]。

在国内量子安全直接通信的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，因其在第一轮传输中没有安全性检测，后被证明是不安全的[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 等人提出了可验证通信方身份的 QSDC 方案，但该方案易受攻击[14]；意大利 Melbourne 大学的 Tombesi 等人实验证明了简化版的 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。随着技术条件的持续升级，其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运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，成功产生并传送、储存、编码了纠缠光子，成功检测了信道安全性，基本实验实现了基于纠缠的 QSDC 方案。基于此，下一步的 QSDC 实验在超过百公里的距离上进行，可成为支撑卫星与地球长距离通信以及全球化直接通信网络的研究基石[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 米环形光纤中实验验证了 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的两方通信可行性，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. 量子安全直接通信基本原理

经典密码通信系统中，可利用信息论相关知识唯一证明一次一密(one-time pad)保密体系是十分安全的。系统中，每次交互的通信密钥只能使用一次且长度应等于待加密明文的长度。窃听无法避免，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，窃听者对合法通信双方间的共享密钥只能进行

完全随机猜测，这样加密体系的安全性得以保证。

量子安全直接通信在物理原理上是可行的，其安全原理与一次一密加密体制相似。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，即编码加密信息，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只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加载于量子态上的机密难度会增大，这从物理原理上可保证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秘密，但必须具备在秘密泄露前就能判断出信道是否安全、有无窃听者存在的能力。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加密信息不会泄露。合法的接收者应具备直接读取加密信息的能力，不能依赖于任何经典辅助信息。

判断量子通信方案是否可实现真正的安全直接通信时，关注点应在于方案能否实现秘密信息的直接传输且没有泄露。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加密信息。

2) 窃听只能得到与加密信息无关的随机结果。

3) 通信双方在量子态加载秘密之前，就应判断出信道中是否存窃听。

数据应分块传输且应加载于量子态上。

1.3. 量子安全直接通信研究意义

量子安全直接通信的理论创新与实验应用融合发展，取得了一系列的成就。与经典密码体系和量子密钥分发技术相比，量子安全直接通信技术具有很多发展优势，研究意义颇深。

1) 量子安全直接通信没有电磁辐射，理论上窃听或探测易被发现，将其与经典加密体系结合利用，可使系统保密安全性较高，可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，信息传输率较高，可适用于某些紧急情况下的加密信息传输。同时，量子安全直接通信系统不依赖空间环境，无关传播媒介，通信具有较稳定的抗干扰能力和较强的传输能力，实际应用于环境条件恶劣复杂的区域时会有较好的适应能力，可增强密码体制的可靠性与稳定性。

3) 为了满足实际安全保密需求，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。量子安全直接通信可能成为未来量子密码研究的主攻方向，进而全球量子密码技术产业可实现实用化、网络化、商业化的综合发展。

2. 量子安全直接通信最新进展总结及对比

2.1. 端到端 QSDC 层面

2.1.1. QSDC 理论方案概述

除了在有噪情况或是在攻击条件下一些实用性较高的理论方案外，其余现有量子安全直接通信方案根据加载信息的量子载体不同，一般可分为利用单光子作载体的 QSDC 方案和利用纠缠粒子作载体的 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 DL04

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，得到了一定空间的发展。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。但单光子编码加密信息的容量较低，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。近三年的相关进展如下：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[24]，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[25]。2017 年，解放军电子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[26]；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[27]；2017 年，广东水利电力职业技术学院郑晓毅等人提出了基于 cluster 态的信道容量可控的 QSDC 方案，通过转变测量基规则和选用不同的编码粒子可将其进一步扩展为可控双向 QSDC [28]。基于纠缠态的 QSDC 方案不断创新进步，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、通过测量可简化加密信息在信道中的传输过程，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，方案无需建立量子信道，也不需传送经典辅助信息，其安全性得以保证是因为图灵机不能对 NP 完全问题进行有效求解[29]。2017 年，翁鹏飞等人提出了实际噪声背景条件下的一种基于量子纠错码的量子网络直接通信方案，系统需选择 w 态粒子作为控制比特才可通过量子纠缠实现完整的通信过程[30]。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。

2.1.2. QSDC 实验进展概述

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，具有实际利用价值，对下一阶段深入实验探索具有很强的指导作用。

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，依据频域内不同调制光子序列的统计特性实现信息编码，序列比特数不同，调制频率也会不同。以此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，从而读出加密信息。当时间块长度为 1 ms 时，数据传输率可达 4 kbps。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。此外，肖连团等人还提出了新的信息传输策略，可实现系统的无条件安全，为量子安全直接通信更深层次的实验实用化研究提供了

强有力的技术支撑。

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，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。

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实现了基于纠缠对的远距 QSDC 实验，实验是基于光纤光学技术完成的[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引入光纤萨格奈特环路中，利用好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。

2.2. 网络化 QSDC 理论方案层面

近年来针对量子安全直接通信的研究大多是端到端的双方单向或双向通信，研究中心聚焦于对新型通信方案的理论系统分析以及增强通信安全等方面，对基于 QSDC 的通信网络实验探索较少，仅停留在理论研究阶段。随着人们对量子密码技术可靠性、安全性、灵活性要求的日益提高，端到端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，必然是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发展的。

2007 年，邓富国等人利用单光子实现了经济型 QSDC 网络基本方案[31]。方案中存在发送端(Bob)、接受端(Charlie)以及制备并测量量子信号的服务器(Alice)。将量子服务器用于借助单光子实现的 QSDC 系统中可实现通信三方的信息交流。服务器 Alice 制备单光子序列，参与系统窃听检测，不会对原有两方通信系统的安全性产生影响。该方案中，因单光子源制备不完整，系统易受光子数分束攻击(Photon Number Splitting, PNS)的影响，2009 年，权东晓等人对其进行改进，提出了需利用诱骗态实现的广域量子 QSDC 网络方案。方案借助服务器方的设置可实现远距通信，且依据不同信道参数可估计不同距离的通过率[32]。2007 年，邓富国、李熙涵等人利用 EPR 纠缠粒子实现了 QSDC 网络化通信[33]。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[34]。2015 年，青岛理工大学马鸿洋等人讨论了噪声环境中的量子网络直接通信[35]。2016 年，曹正文等人提出了一种适用于星型网络的双向 QSDC 方案，方案能抵抗被动式攻击和截取重发攻击，通信效率较高[36]。

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 双方通信方

案的扩展，在端到端的 QSDC 通信系统中借助量子服务器可实现三方通信。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延长 QSDC 网络系统的通信距离，提高实用性能。在当前技术条件受制的情况下，量子安全直接通信网络的发展依面临严峻挑战。

2.3. 最新理论方案对比分析

通过对现有的多类理论方案进行深入探究，不仅可分析出当前主流研究趋势，从而预测未来理论方案研究的重点方向；还可在此基础上针对特定方向进行研究探讨，提出可保证通信安全、提高传输效率的改进建议，进一步完善理论功能内容。

此外由以上总结可看出，近年来量子安全直接通信实验研究虽然取得了一些进展，但始终处于起步阶段，实现的功能较初级单一。而理论研究发展却日益成熟，逐渐向系统化方向发展，体系较分明。因此，对近年来功能实现较齐全的理论研究方案进行分析对比，也可为实验验证的发展指明方向。

本文选择了近年来在功能实现方面较有特色的三个理论方案进行对比分析，其中两个方案可实现端到端通信，即 2017 年，翁鹏飞等人提出的 *w* 态的高维量子安全直接通信方案[27]、郑晓毅等人提出的基于 cluster 态的信道容量可控的可控 QSDC 方案[28]以及一个网络化通信方案，即 2016 年曹正文等人提出的一种星型网络中的双向 QSDC 方案[36]。最后，依据对比结果可对未来量子安全直接通信的理论研究进行预测展望。

2.3.1. 方案研究比较

1) *w* 态的高维量子安全直接通信

2017 年，翁鹏飞等人提出了 *w* 态的高维量子安全直接通信方案[27]。发送方 Alice 对需传输的秘密序列进行密集编码，接收方 Bob 通过联合测量读取相应的经典信息。通信双方将 *w* 态粒子作为检测粒子随机插入到多维 Bell 量子态序列中，利用其纠缠特性保证通信安全。

基于熵理论和窃听检测分析该方案的安全性，三粒子 *w* 态作为诱饵可得到每量子位 64%的窃听探测率，较扩展 GHZ 态提高了 6%的窃听率。同时，该方案为提高传输效率和量子比特效率，利用高维 Bell 态作为传输粒子。若方案应用于 4 维 Hilbert 空间，则效率可达 173. 9%，量子比特效率可达 43.8%。

本方案的一大意义是弥补了 2015 年昌燕等人提出的基于三粒子 *w* 态蜜罐的受控 QSDC 方案的缺陷，原方案利用信息序列中随机插入的三粒子 *w* 态可完成信道检测窃听，一旦窃听者 Eve 知道通信双方在受控通信中利用三粒子 *w* 态实现蜜罐粒子的作用，无需测量便可知窃听粒子的状态，此时窃听被探测到的概率为 0，会令通信双方误认为信道安全，从而造成信息泄露[37]。本方案在高维 Hilbert 空间中将纠缠态拆分开，利用 *w* 态纠缠特性可验证信道安全，使得窃听率有所提高。但相较于其他通信理论方案，量子比特效率并不是很高，方案也只能实现简单的双方通信。

2) 基于 cluster 态的信道容量可控的可控量子安全直接通信方案

2017 年，郑晓毅等人提出了基于 cluster 态的信道容量可控的可控 QSDC 方案[28]。通信三方将五粒子 cluster 态作为量子信道，借助其特殊的粒子分布结构以及诱饵光子和校验信息，可利用量子测量完成信道的第一次安全检测。在系统中，控制方 Cindy 随机选择测量基(*Z* 基或 *X* 基)来测量粒子序列以此完成对信道容量的调控。发送方 Alice 通过幺正操作编码待传输的机密和检测信息，并在插入诱骗光子后发送给接收方 Bob。Bob 依据 Alice、Cindy 告知的信息，进行 Bell 测量便可完成第二次安全检测并获/得机密信息。

方案采用基于两步 QSDC 方案的分步传输量子数据块的方法来保证通信安全，通过两次安全性检测判断信道是否安全。理论上在一定的噪声环境中可完成可控的量子安全直接通信，且根据方案结果可知，不同的测量基规则和不同的编码粒子可决定方案是否能够扩展为可控双向 QSDC。

该方案的一大特色在于利用了五粒子 cluster 态，cluster 态具有最大联通性，持续纠缠比 GHZ 和 w 态粒子要好，很难被局域操作破坏。在实际应用时，可通过多种方式完成 cluster 态的制备，操作性较强。方案中所采用的测量只限于常见的单光子测量、Bell 基测量，操作方便，相应的幺正操作也是简单的 Pauli 幺正操作。因此在实验条件成熟的情况下，安全直接通信利用五粒子 cluster 态控制信道容量是可以实现的。但与此同时，利用五粒子纠缠实现方案功能，通信过程较为复杂，传输效率与量子比特利用率并不高。

3) 一种星型网络中的双向量子安全直接通信方案

2016 年，曹正文等人提出了一种星型网络中的双向 QSDC 方案[36]。方案基于三粒子 GHZ 态，即通信双方需要在量子服务器的控制下，才可完成双向通信。利用不同的三粒子酉变换，双方双向通信中可实现一次 4bits 经典信息的传输，系统效率较高。研究方案的安全性可发现，利用特定的幺正变换再结合量子测量相关性可抵御被动式攻击和截获重发攻击，保证机密内容的安全传输。

该方案的一大优势在于可在网络化系统中实现通信方之间的双向通信，且通信效率也较高。但通过设计多种幺正变换才可实现信息编码，使得方案在实际执行操作时会较为复杂，不易控制，量子比特利用率不高。同时，方案在理论上基于星型网络，将其用于实际应用时还需推广成全网络端到端模式，这对每一通信方需要进行的量子存储操作具有很高要求，且通过量子信道分发粒子还应解决信道容量低及其安全性不稳定等问题。

2.3.2. 理论优化方向

在理论层面，以功能实现为主要指标对比分析上述三种方案，如表 1 所示：

Table 1. Function comparison of different schemes
表 1. 方案功能对比

主流方案 功能指标	w 态高维 QSDC	cluster 态 可控 QSDC	星型网络 双向 QSDC
安全性	理论安全	理论安全	理论安全
编码容量	一个态：4 bits	一个态：2 bits	一个态：2 bits
传输效率	1.739	暂无	2
量子比特利用率	0.438	不高	不高
容量控制	不可控	可控	不可控
通信方向	单向通信	可推广为双向通信	双向通信
通信模式	端到端通信	端到端通信	网络化通信

由以上主流方案可知，量子安全直接通信的理论研究虽然蓬勃发展，但方案安全性不高、传输速率低以及功能实现较单一等难题始终阻碍着科研工作的进一步深入探究，未来量子安全直接通信的理论方案研究重点可以有一些改进之处：

1) 通过将整个方案背景定义在高维 Hilbert 空间中，适当通过改进编码规则来提高通信编码容量。

2) 利用多粒子纠缠实现功能上的复杂性，例如实现信息的双向传递或是多方网络化的交流。

3) 通过定义冗余编码，降低噪声对通信的影响，提高通信系统稳定性，以此来提高系统的传输效率。

由以上三种方案推广可知，相关研究工作的深入探索需要注意编码方案的创新改进，从而可通过编码容量的适度提高一定程度上调高通信效率，或是进一步通过优化编码规则来增强抵御噪声的能力。在

此基础上，本文依据新的量子编码方案，提出了一种基于 4 维 Bell 纠缠态和单光子混合的 QSDC 方案，理论意义上通信容量较高并在一定程度上提高了通信效率和安全性。

3. 基于 4 维 Bell 态粒子和单光子混合的 QSDC 改进方案

3.1. 改进方案理论准备

3.1.1. 方案改进基础

2016 年，曹正文等人提出了基于 Bell 态粒子和单光子混合的 QSDC 方案，方案中发送方 Alice 首先制备一些 Bell 态粒子并将其划分为两个序列 S_A、S_B，将 S_B 发给接收方 Bob 以实现接下来的信道第一次窃听检测。在信道安全后，发送方 Alice 将加密信息编码在 S_A 和制备的单光子序列 S_S 上，最后通过顺序重排和添加单光子检测粒子等操作构成新序列 S 并发送给 Bob，Bob 可根据测量结果得到机密信息。该方案可避免复杂的 U 变换，简化实现过程，能抵抗测量重发攻击、截获重发攻击、辅助粒子攻击、拒绝服务攻击、木马攻击等多种攻击方法，同时 3 bits 经典信息编码在一个量子态上可提高编码容量，加快通信传输效率[24]。该方案的编码规则如表 2 所示：

Table 2. Coding rule of the scheme
表 2. 方案编码规则

信息序列	量子态	信息序列	量子态
000	$\|H\rangle$	100	$\|\varphi^+\rangle$
001	$\|V\rangle$	101	$\|\varphi^-\rangle$
010	$\|L\rangle$	110	$\|\psi^+\rangle$
011	$\|R\rangle$	111	$\|\psi^-\rangle$

2017 年，刘志昊等人研究了该方案的信息泄露问题。原方案中，为使接收方 Bob 可解码机密内容，发送方 Alice 在经典信道中要公布序列 S 原来的顺序、位置和测量基等辅助信息。当 Alice 公布哪些粒子需使用 X 基或 Z 基测量、哪些需使用 Bell 基联合测量时，窃听者 Eve 可读取到 Alice 发送的一部分机密消息。例如：当 Alice 公布编码粒子需使用 Z 基进行测量时，Eve 可得到该粒子状态为 $|H\rangle$ 或 $|V\rangle$，即编码的信息是 000 或 001，窃听者可确切得知该加密信息的前两位必为 00；当公布编码粒子需使用 Bell 基测量时，窃听者 Eve 可确定编码的加密信息是 100、101、110 或 111，即可得知对应的加密信息第一位必为 1 [25]。

为解决上述加密信息泄露的问题，刘志昊等人对编码方案进行了改进，如表 3 所示：

Table 3. Improved coding rule of the scheme
表 3. 改进的编码规则方案

信息序列	单量子态	信息序列	Bell 态
0	$\|H\rangle$	00	$\|\varphi^+\rangle$
1	$\|V\rangle$	01	$\|\varphi^-\rangle$
0	$\|L\rangle$	10	$\|\psi^+\rangle$
1	$\|R\rangle$	11	$\|\psi^-\rangle$

基于改进的编码方案，Alice 通过经典信道公布各粒子原来的顺序、位置和测量基信息时，窃听者即使成功截取也无法得到有关机密的任何信息。改进的方案中平均 1 量子比特编码 1 比特经典信息，解决

了信息泄露问题，可保证通信的高效、安全。本文借鉴上述两种方案的编码思想，提出了一种改进后的量子编码方案，可达到提高通信容量的目的。

3.1.2. *d* 维 Hilbert 空间定义

2017 年，翁鹏飞等人利用了 d 维 Hilbert 空间理论[26]。在 d 维 Hilbert 空间中，定义 Z_d 、 X_d 为 d 维单光子的两组非正交测量基，测量基 Z_d 的 d 个本征矢量可表示为 $|0\rangle,|1\rangle,|2\rangle,|3\rangle,\cdots,|d-1\rangle$，测量基 X_d 的 d 个本征矢量可表示为 $|\tilde{u}\rangle=\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\exp(2\pi ilu/d)|l\rangle$。$d$ 维 Bell 纠缠态可表示为 $|\varphi^{uv}\rangle=\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\exp(2\pi ilu/d)|l\rangle\otimes|l\otimes v\rangle$。

定义 d 维幺正操作 $U_{uv}=\sum_{l=0}^{d-1}\exp(2\pi ilu/d)|l\oplus v\rangle\otimes\langle l|$，则

$$\begin{aligned}U_{uv}|\varphi^{00}\rangle&=\sum_{l=0}^{d-1}\exp(2\pi ilu/d)|l\oplus v\rangle\otimes\langle l|\otimes\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}|l\rangle\otimes|l\rangle\\&=\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\exp(2\pi ilu/d)|l\oplus v\rangle\otimes|l\rangle\end{aligned}\tag{3-1}$$

令上式中 $l\oplus v=n$， $l=(n-v)\bmod d$，可得 $l=n\oplus v,(n=1,2,\cdots d-1)$，令 $l=n$，可得 $\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\exp(2\pi ilu/d)|l\rangle\otimes|l\oplus v\rangle=U_{uv}|\varphi^{00}\rangle=|\varphi^{uv}\rangle$，其中 $u,v=1,2,3,\cdots,d-1$。

3.1.3. 量子信道加密概念

2001 年，张永生等人提出了量子信道加密概念。量子密钥分发协议中，通信方将一对 Bell 纠缠粒子作为量子信道，发送方利用受控非(controlled-Not)操作将携带密钥信息的量子态纠缠入信道，接收方用 controlled-Not 操作解纠缠即可得到携带密钥信息的量子态[38]。

受控非门(CNOT 门)是两比特量子门，若控制比特 $|c\rangle$ 为 0，则目标比特 $|t\rangle$ 不变；若控制比特为 1，则目标比特翻转。即 $|c,t\rangle\to|c,c\otimes t\rangle$，具体实现为 $|00\rangle\to|00\rangle$ 、 $|01\rangle\to|01\rangle$ 、 $|10\rangle\to|11\rangle$ 、 $|11\rangle\to|10\rangle$。对应的酉算子为：

$$U_{CN}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\tag{3-2}$$

传输过程中，窃听者的截取测量攻击只能得到随机结果，但重点应保证量子信道是安全的，即通信双方共享 Bell 态的过程应是可靠有效的。本方案在利用单光子加载并传输机密信息时，利用已传输并确定安全的 Bell 态序列作为量子信道，既可提高通信信道可靠性，又可提高 Bell 态序列的利用率。

3.2. 改进方案描述

本方案定义在 4 维 Hilbert 空间中是为了实现特定的编码方案以提高通信容量。首先利用检测粒子可在通信双方间建立安全信道，从测量后复合系统的变化中可读取加密信息；接下来，在信道安全的前提下，借助量子信道加密的思想传递加载机密的单光子，操作简便的同时也会提高信道的利用率；最后，只需通过操作简便的单光子测量便可实现机密的安全传输。

3.2.1. 方案实施流程

方案设计 $d=4$，Alice 需发送 $3n$ 比特机密信息给 Bob。

1) 准备阶段

Alice 制备一串长为 $n-x+y$ 的 Bell 态序列，即 EPR 纠缠粒子对，其中 y 对用作检测粒子对，每对 Bell 态均处于状态 $\left|\varphi^{00}\right\rangle_{12}=\frac{1}{2}\left(\left|00\right\rangle+\left|11\right\rangle+\left|22\right\rangle+\left|33\right\rangle\right)_{12}$。

2) 加载机密

Alice 根据机密信息对 $n-x$ 对 $\left|\varphi^{00}\right\rangle$ 进行相应的幺正变换，双方约定 U_{00}、U_{01}、U_{02}、U_{03} 分别对应消息 010、101、100、011，其余消息 000、111、110、001 则分别由单光子进行编码。

当执行变换时，光子 1 和 2 构成的复合系统分别为：

$$U_{00}\left|\varphi^{00}\right\rangle_{12}=\frac{1}{2}\left(\left|00\right\rangle+\left|11\right\rangle+\left|22\right\rangle+\left|33\right\rangle\right)_{12},\quad U_{01}\left|\varphi^{00}\right\rangle_{12}=\frac{1}{2}\left(\left|01\right\rangle+\left|12\right\rangle+\left|23\right\rangle+\left|30\right\rangle\right)_{12}$$

$$U_{02}\left|\varphi^{00}\right\rangle_{12}=\frac{1}{2}\left(\left|02\right\rangle+\left|13\right\rangle+\left|20\right\rangle+\left|31\right\rangle\right)_{12},\quad U_{03}\left|\varphi^{00}\right\rangle_{12}=\frac{1}{2}\left(\left|03\right\rangle+\left|10\right\rangle+\left|21\right\rangle+\left|32\right\rangle\right)_{12}\tag{3-3}$$

3) 安全检测

Alice 将执行完幺正变换的 $n-x$ 对 Bell 纠缠粒子拆分成 $2(n-x)$ 个粒子，将所有纠缠粒子对的第一粒子组成序列 S_A，第二粒子组成序列 S_B。Alice 随机地将 y 对检测粒子中的第一粒子插入到序列 S_A 中，得到新序列 A^* 并保存；将第二粒子随机插入序列 S_B 中得到新序列 B^*，发送给 Bob。

Alice 选用 Z_d 基对 A^* 序列里的检测粒子进行测量并在经典信道公布检测粒子的位置及测量结果。Bob 在将对应检测粒子取出后进行 Z_d 基测量，若比较结果的误码率低于已设阈值，则认为信道中无窃听干扰，继续进行下一步的通信，否则放弃通信过程，再次重复以上步骤直至误码率低于阈值。

4) 机密传输

在保证信道安全后，Alice 根据剩余的机密信息制备 x 个单光子态 $\left|q\right\rangle_M$，$\left|q\right\rangle_M$ 为 4 维 Hilberrt 空间中四种单光子：$\left|H'\right\rangle$、$\left|V'\right\rangle$ (对应测量基 Z_d 基矢)，$\left|L'\right\rangle$、$\left|R'\right\rangle$，(对应测量基 X_d 基矢)，编码规则如表 4 所示：

Table 4. Single photon coding scheme
表 4. 单光子编码方案

加密信息	量子态	加密信息	量子态
000	$\left\|H'\right\rangle$	001	$\left\|L'\right\rangle$
111	$\left\|V'\right\rangle$	110	$\left\|R'\right\rangle$

Alice 以 S_A (从 A^* 中去除检测粒子后)中粒子为控制粒子，机密信息粒子为目标粒子，执行 C_{AM} 操作，对目标粒子依次执行后，Alice 便可将 S_M 发送给 Bob。

$\left|\varphi^{00}\right\rangle_{AB}\left|q\right\rangle_M\xrightarrow{C_{AM}}\frac{1}{2}\left(\left|00,q\right\rangle+\left|11,q+1\right\rangle+\left|22,q+2\right\rangle+\left|33,q+3\right\rangle\right)_{ABM}$。

Bob 收到 S_M 后，以 S_B 中粒子作为控制粒子，机密信息粒子作为目标粒子，执行 C_{BM} 操作，即 $\frac{1}{2}\left(\left|00,q\right\rangle+\left|11,q+1\right\rangle+\left|22,q+2\right\rangle+\left|33,q+3\right\rangle\right)_{ABM}\xrightarrow{C_{BM}}\left|\varphi^{00}\right\rangle_{AB}\left|q\right\rangle_M$，Bob 对所有执行完操作的粒子进行单光子测量便可得到机密信息。

5) 机密读取

Alice 对序列 S_A 进行单光子测量，公布测量结果以及单光子 $\left|q\right\rangle_M$ 的位置信息，Bob 对序列 S_B 进行单光子测量，根据 Alice 发送的测量结果以及单光子位置信息便可恢复出总机密。具体对应关系如表 5 所示，例如 Alice 公布的结果是 $\left|2\right\rangle$，Bob 经测量得到的结果是 $\left|1\right\rangle$，则传输的加密信息应为“001”。

Table 5. Information recovery
表 5. 信息恢复

加密信息	Alice 公布结果	Bob 测量结果	加密信息	Alice 公布结果	Bob 测量结果
010	$\|0\rangle$	$\|0\rangle$	100	$\|0\rangle$	$\|1\rangle$
	$\|1\rangle$	$\|1\rangle$		$\|1\rangle$	$\|2\rangle$
	$\|2\rangle$	$\|2\rangle$		$\|2\rangle$	$\|3\rangle$
	$\|3\rangle$	$\|3\rangle$		$\|3\rangle$	$\|0\rangle$
101	$\|0\rangle$	$\|2\rangle$	011	$\|0\rangle$	$\|3\rangle$
	$\|1\rangle$	$\|3\rangle$		$\|1\rangle$	$\|0\rangle$
	$\|2\rangle$	$\|0\rangle$		$\|2\rangle$	$\|1\rangle$
	$\|3\rangle$	$\|1\rangle$		$\|3\rangle$	$\|3\rangle$

3.2.2. 操作分析对比

研究上述所述编码规则不同的理论方案，对其操作流程进行对比分析如表 6 所示：

Table 6. Comparison of different operation procedures
表 6. 操作流程对比

理论方案 / 操作程序	Bell 态粒子和单光子混合 QSDC 方案(2016)	Bell 态粒子和单光子混合 QSDC 改进方案(2017)	本方案
单光子制备	随机处于四个量子态之一	随机处于四个量子态之一	可选择四个量子态
EPR 纠缠粒子对制备	随机处于四个量子态之一	随机处于四个量子态之一	均可处于同一量子态
单光子编码	3 bits	1 bit	3 bits
EPR 纠缠粒子对编码	3 bits	2 bits	3 bits
信道安全检测	对抽样粒子进行单光子测量	对抽样粒子进行单光子测量	幺正变换后插入检测粒子辅助测量
机密传输	编码后顺序重排再插入检测粒子	编码后顺序重排再插入检测粒子	通过量子信道加密传输
信息读取	单光子测量联合 Bell 基测量	单光子测量联合 Bell 基测量	单光子测量

由以上对比可得知，本方案子在粒子制备方面较简便且在信息读取时仅需要进行单光子测量，这使得方案实施更加简明高效，操作复杂性并不高。同时，本方案的编码容量较高，这会一定程度上提高传输效率。在进行信道安全性检测时，抽取已制备的检测粒子使得方案实施更加清晰有序，且通过量子信道加密传输信息可避免检测粒子顺序、位置以及测量基信息在经典信道上的传输，实现过程得以简化，也可降低对经典通信的依赖性。

3.3. 改进方案安全性描述

量子密码系统中会存在窃听干扰，针对整个系统较为有效的攻击方法主要有测量重发攻击、截取重发攻击以及辅助粒子攻击等，本文从这三种攻击手段出发，对方案的安全性进行了探讨分析。

3.3.1. 测量重发攻击

测量重发攻击是窃听者 Eve 捕获发送方 Alice 编码后要发送给接收方 Bob 的部分序列，随机选择测量基对其进行测量，由此可能会获得一些有用信息。随后窃听者 Eve 将测量后的序列依旧发送给接收方 Bob，若接下来的窃听检测中，通信双方没有察觉到窃听者的存在，则 Eve 的窃听攻击视为成功。

本方案中信息序列编码后又插入了部分检测粒子，即使 Eve 捕获了一部分光子并选择正确的测量基，但由于不清楚编码序列的顺序、位置，也无法得到有效信息。且在信道安全性检测过程中，攻击行为会

被发现。

假设窃听者 Eve 截取了发送方 Alice 编码的一部分含有 n 个粒子的信息序列，并采用 Z_d 基对其进行了测量。例如其中一个加载信息的粒子可表示为 $\left|\varphi^{00}\right\rangle_2$，由于不清楚发送方 Alice 的测量结果，窃听者 Eve 获得准确信息的概率就应为 $\frac{1}{4}$，若 n 个粒子全为信息粒子，则窃听者可获得正确信息的概率为 $(1/4)^n$。由此可见，n 越大，窃听获得正确信息的概率越小。此外，窃听者是无法区分测量的粒子中哪些是携带信息的粒子、哪些是检测粒子，因此窃听引起的错误很容易被检测到，攻击一般无效。

3.3.2. 截取重发攻击

截取重发攻击是窃听者 Eve 截获部分发送方 Alice 编码后的发送序列，并将自己提前制备好的一串序列伪造作为原发送序列，代发给接收方 Bob。在接下来的窃听检测中，作为合法双方中间人的窃听者 Eve 若没有被发现，则攻击很可能会获得有用信息。

在本方案中，窃听者 Eve 在攻击时由于不知原序列的顺序和检测粒子位置，攻击行为会被发现且毫无意义。此外，单光子传输机密信息时，S_M 与信道粒子 S_A、S_B 为最大纠缠态，Eve 的截取测量只能得到随机结果。

假设窃听者 Eve 截取了发送方 Alice 发送的含有 n 个粒子的信息序列，然后将已制备好的 n 个粒子发送给 Bob。截获并重发一个粒子引起的粒子错误率为 $\frac{3}{4}$，则 n 个截取粒子窃听被检测到的概率可达 $1-\left(\frac{1}{4}\right)^n$。窃听者 Eve 在不清楚原序列的粒子位置的情况下，想要成功伪造一条相似序列，难度很大。

3.3.3. 辅助粒子攻击

辅助粒子攻击是窃听者 Eve 先截获发送方 Alice 的粒子序列，再利用已制备的辅助粒子对其进行纠缠，即窃听者在发送的量子态和窃听系统所组成的一个更大的 Hilbert 空间中执行幺正变换。若窃听者通过在此空间中的操作获得了有用信息，则可视为攻击成功。

在本方案中，窃听者 Eve 可将制备的粒子与信道粒子进行纠缠，以期望获取机密信息，但在量子力学基本原理以及量子特性的保证下，窃听者 Eve 的窃听操作若获得了有用信息，则必然会引起检测错误。

信道安全性检测时，窃听者 Eve 在量子信号和检测粒子组成的 Hilbert 空间中进行幺正攻击操作，单粒子在攻击后变为 $\left|\varphi_1\right\rangle=E\left|my\right\rangle=a\left|0y_0\right\rangle+b\left|1y_1\right\rangle+c\left|2y_2\right\rangle+d\left|3y_3\right\rangle$（$\left|y_i\right\rangle$ 为攻击操作确定的纯态，且 $a^2+b^2+c^2+d^2=1$），此时密度算子为：

$$\begin{aligned}\rho&=\left|\varphi_1\right\rangle\left\langle\varphi_1\right|\\&=|a|^2\left|0y_0\right\rangle\left\langle 0y_{10}\right|+ab^*\left|0y_0\right\rangle\left\langle 1y_1\right|+ac^*\left|0y_0\right\rangle\left\langle 2y_2\right|+ad^*\left|0y_0\right\rangle\left\langle 3y_3\right|\\&\quad+ba^*\left|1y_1\right\rangle\left\langle 0y_0\right|+|b|^2\left|1y_1\right\rangle\left\langle 1y_1\right|+bc^*\left|1y_1\right\rangle\left\langle 2y_2\right|+bd^*\left|1y_1\right\rangle\left\langle 3y_3\right|\\&\quad+ca^*\left|2y_2\right\rangle\left\langle 0y_0\right|+cb^*\left|2y_2\right\rangle\left\langle 1y_1\right|+|c|^2\left|2y_2\right\rangle\left\langle 2y_2\right|+cd^*\left|2y_2\right\rangle\left\langle 3y_3\right|\\&\quad+da^*\left|3y_3\right\rangle\left\langle 0y_0\right|+db^*\left|3y_3\right\rangle\left\langle 1y_1\right|+dc^*\left|2y_3\right\rangle\left\langle 2y_2\right|+|d|^2\left|3y_3\right\rangle\left\langle 3y_3\right|\end{aligned}\tag{3-4}$$

以 $\left|0y_0\right\rangle$、$\left|1y_1\right\rangle$、$\left|2y_2\right\rangle$、$\left|3y_3\right\rangle$ 为基，矩阵表达式为：

$$\rho=\begin{bmatrix}|a|^2 & ba^* & ca^* & da^*\\ ab^* & |b|^2 & cb^* & db^*\\ ac^* & bc^* & |c|^2 & dc^*\\ ad^* & bd^* & cd^* & |d|^2\end{bmatrix}\tag{3-5}$$

当$|\varphi_1\rangle$处于最大纠缠态时，$a^2=b^2=c^2=d^2=1/4$，经计算ρ的特征值$\lambda_0,\lambda_1,\lambda_2,\lambda_3$分别为0、0、0、1，用冯·诺依曼熵表示窃听者Eve可获得的消息$\varepsilon=\sum_{i=0}^{3}-\lambda_i\log_2^{\lambda_i}=0$，即窃听不能得到任何有效信息。

Eve对整个系统进行酉攻击后，系统状态变为：

$$\begin{aligned}|\varphi_{Eve}\rangle&=U_{uv}\left(E\otimes I\otimes|\varphi^{00}\rangle\right)\\&=\frac{1}{2}\left(a|0y_0 0\rangle+b|1y_1 0\rangle+c|2y_2 0\rangle+d|3y_3 0\rangle\right)\\&+\frac{1}{2}\left(a|0y_0 1\rangle+b|1y_1 1\rangle+c|2y_2 1\rangle+d|3y_3 1\rangle\right)\\&+\frac{1}{2}\left(a|0y_0 2\rangle+b|1y_1 2\rangle+c|2y_2 2\rangle+d|3y_3 2\rangle\right)\\&+\frac{1}{2}\left(a|0y_0 3\rangle+b|1y_1 3\rangle+c|2y_2 3\rangle+d|3y_3 3\rangle\right)\end{aligned}\tag{3-6}$$

当Alice对处于4维Bell态的检测粒子做测量时，有窃听的概率为$p\left(|\varphi_{Eve}\rangle\right)=\left[1-\frac{1}{4}\left(a^2+b^2+c^2+d^2\right)\right]=\frac{3}{4}$，即Alice能以75%的概率检测出信道是否存在窃听。

3.4. 改进方案传输效率分析

本方案定义在4维Hilbert空间中，借助量子信道相关理论使得每传输1量子比特便可传输3比特的经典信息。依据信息论相关知识，可定义量子密码协议的效率公式为$\xi=\frac{b_s}{q_t+b_t}$，b_s是通信过程中需传输的机密信息比特数，q_t、b_t分别是通信时需交换的量子比特数、经典信息比特数[39]，计算传输效率时不考虑与窃听检测有关的经典比特、测量基以及位置信息。

方案利用n个量子态传输$3n$比特的经典信息，即$b_s=3n$、$q_t=n$，由2016年曹正文等人发表的基于Bell态粒子和单光子混合的QSDC方案中的效率计算方法可知$b_t\approx n/2$，因此本方案的传输效率约为2倍。

$$\xi=\frac{b_s}{q_t+b_t}\approx\frac{3n}{n+n/2}\approx 2\tag{3-7}$$

但协议的效率公式不能充分描述通信效率，因此引出量子比特效率的定义公式$\eta=q_u/q_t$，q_u、q_t分别为有效的量子比特、总量子比特[39]。对本方案而言，取$q_u=n$、$q_t\approx n$，则量子比特效率为$\eta=q_u/q_t\approx n/n\approx 1$。

按照效率公式的定义，对比分析一些文献中典型方案的安全性、量子通信传输效率、量子比特利用率，可发现本方案虽然有较高的编码容量，但兼顾了信息泄露问题且通信效率有所提高。结果如表7所示：

4. 结束语

本方案定义在4维Hilbert空间上，综合利用EPR纠缠粒子对、单光子加载机密信息，完成安全直接通信。理论上，所使用的量子编码方案一般不会因公布经典信息而造成机密泄露，方案的具体优势如下：

1) 高维Hilbert空间中，利用EPR纠缠对的幺正变换可对信息进行编码操作，多维Bell态粒子用作检测粒子可确保信道安全。

2) 单光子传输机密时，基于的是理论上已证明安全的量子信道，可提高通信的可靠度。

Table 7. Comparison of different efficiency parameters
表 7. 效率参数对比

理论方案	安全性	传输效率 ξ	量子比特率 η	编码容量
两步 QSDC 方案(2003)	理论安全	1	1	一个态：2 bits
DL04 方案(2004)	理论安全	1	1	一个态：1 bit
w 态高维 QSDC 方案(2017)	理论安全	1.739	0.438	一个态：4 bits
cluster 态可控 QSDC 方案(2017)	理论安全	暂无	暂无	一个态：2 bits
星型网络双向 QSDC 方案(2016)	理论安全	2	暂无	一个态：2 bits
Bell 态粒子和单光子混合 QSDC 方案(2016)	信息泄露	2	1	一个态：3 bits
Bell 态粒子和单光子混合 QSDC 改进方案(2017)	理论安全	1.5	1	一个态：1 bit
本方案	理论安全	约为 2	约为 1	一个态：3 bits

3) 混合利用单光子与 EPR 纠缠光子对，使得 1 量子比特可携带传输 3 比特经典信息，能够提高通信容量，从而提高量子比特传输率。

4) 通信双方利用经幺正变换后的粒子进行通信，可进一步完成系统双向交流，此外双方共享两个不对称信道，可有效避免量子编码攻击。

5) 方案在理论层面简明高效，量子比特利用率较高。

但本方案主要是理论研究，并没有进行过实际应用操作。方案不仅要制备并测量单光子、Bell 态，还需利用好量子存储技术进行安全存储。此外，如何综合利用好单光子与 Bell 态粒子还存在一定的现实难度，相信在量子安全直接通信实验研究取得了突破性进展的前提下，本方案所存在的技术难题会被逐一攻破，最终实现实验实用化验证。

基金项目

国家自然科学基金项目(No. 61402121)；国家自然科学基金项目(U1204602)；中央高校基本科研业务费专项资金(No. 861914)；国家高科技研究和发展项目(863 项目) (2011AA010803)；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.

[5] Man, X.Z. and Xia, Y.J. (2007) Improvement of Security of Three-Party Quantum Secure Direct Communication Based on GHZ States. *Chinese Physics Letters*, **24**, 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**, 942-947. https://doi.org/10.1007/s11433-011-4265-5

[9] Huang, W., Wen, Q.Y., Jia, H.Y., *et al*. (2012) Fault Tolerant Quantum Secure Direct Communication with Quantum Encryption against Collective Noise. *Chinese Physics B*, **21**, 101-109. https://doi.org/10.1088/1674-1056/21/10/100308

[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. (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. *EPL*, **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**, 1-12. 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.

[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] 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.

[25] 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.

[26] 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(5).

[27] 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.

[28] 郑晓毅, 龙银香. 基于 cluster 态的信道容量可控的可控量子安全直接通信方案[J]. 物理学报, 2017, 66(18): 55-61.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

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

[35] 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.

[36] 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.

[37] 昌燕, 张仕斌, 闫丽丽, 盛志伟. 基于三粒子 W 态蜜罐的受控量子安全直接通信协议[J]. 电子科技大学学报, 2015, 44(1): 39-42.

[38] 钱鹏, 李兴华. 基于信道加密的量子安全直接通信[J]. 量子电子学报, 2015, 32(6): 686-690.

[39] 王剑, 张盛, 张守林, 等. 基于纯纠缠态的量子安全直接通信协议[J]. 国防科技大学学报, 2009, 31(2): 51-54.