

网络空间安全本科量子信息教学实践

陈巍, 银振强, 韩正甫, 俞能海

(中国科学技术大学, 安徽 合肥 230026)

摘要: 量子信息是量子物理和信息技术交叉融合产生的新兴学科。近年来, 量子信息技术得到了迅速发展, 并开始衍生相关产业。与此相对, 量子信息从业人员严重缺乏, 工程技术人员对量子信息的理解不够深入、实操能力不足, 这些已成为限制该技术应用和发展的严重瓶颈。人才的匮乏源于教育的缺失。当前, 我国的量子信息和新工科蓬勃发展, 已具备将量子信息相关课程渗透到工科专业本科阶段的基本条件。在新工科教学思想的指导下, 中国科学技术大学面向网络空间安全专业的本科生开设了量子信息相关的导论课程。课程基于我校在量子信息方面的研究和基础, 与网络空间安全专业的核心需求和特色结合, 在教学目标、课程结构和内容、授课方法和实践手段等方面进行了完整而创新的设计, 并取得了较好的教学效果。该课程的教学思路和实践方法为网络空间安全学科的量子信息教学提供了有价值的参考。

关键词: 网络空间安全; 量子信息; 教学实践

中图分类号: TN929.1, TP393.0

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019028

Quantum information course for the undergraduate students of cyber security

CHEN Wei, YIN Zhenqiang, HAN Zhengfu, YU Nenghai

University of Science and Technology of China, Hefei 230026, China

Abstract: Quantum information is a new discipline with the intersection of quantum physics and information technology, which has developed rapidly recently and has been on the road of industrialization. In contrast, the severe shortage of the practitioners, who can understand quantum information technology in depth, have become bottlenecks restricting the development of this technology. The lack of talent stems is from the lack of education, especially for the undergraduate students of engineering. Benefitting from the vigorous growth of quantum information in China, the fundamental of infiltrating the quantum information course in the undergraduate education of engineering can be performed, and some positive effects have been achieved. The course has carried out the teaching re-

收稿日期: 2019-05-16; 修回日期: 2019-06-03

通信作者: 俞能海, ynh@ustc.edu.cn

基金项目: 教育部2018年首批“新工科”研究与实践基金资助项目; 国家一流网络安全学院建设示范基金资助项目

Foundation Items: “Emerging Engineering” Research and Practice Project of 2018, National First-class Construction Project for School of Cyber Security

论文引用格式: 陈巍, 银振强, 韩正甫, 等. 网络空间安全本科量子信息教学实践[J]. 网络与信息安全学报, 2019, 5(3): 81-88.

CHEN W, YIN Z Q, HAN Z F, et al. Quantum information course for the undergraduate students of cyber security[J]. Chinese Journal of Network and Information Security, 2019, 5(3): 81-88.

forms, and practices in terms of teaching objectives, curriculum structure, practical methods, which have gained good teaching results. These teaching experiences and ideas provide a valuable reference for quantum information education in the cyberspace security discipline.

Key words: emerging engineering, cyber security, quantum information, teaching practice

1 背景

近年来,在第 4 次工业革命大潮下,人工智能、大数据和网络空间安全等新兴产业和学科得到了迅速的发展。特别是以量子信息为代表的许多理学研究成果以全新的形式完成了与工程技术的嫁接。这些经济源动力的产生和发展为“新工科”教育提供了土壤和契机。新工科教育的重点之一是促进传统学科和新兴学科的对接与延伸,以及理学背景与工科技术的交叉融合。这要求工科人才具备更宽广的视野、更灵活的思维模式和更扎实的技能,并且在学科交叉融合方面的创新能力更强^[1]。人才需求的变化对工科教育的理念和方法提出了变革的需求和挑战,也使我国的工科教育步入了新一轮的快速发展中。

网络空间安全是国务院学位委员会和教育部在 2015 年新设立的工学一级学科。它面向人在信息网络空间中的基本保障要求,相比传统的信息安全来说,其实际环境和要求更为复杂,问题的综合性也更强,对新兴技术的前瞻判断和跟踪能力的要求更高^[2]。因此,在新工科教育发展的背景下,网络空间安全的教育应当尽可能的覆盖新兴的产业和未来的技术发展方向。量子信息技术是量子物理和信息技术交叉融合的产物,也是我国着力发展的新一代信息技术。量子信息技术包含量子通信、量子计算和量子计量等多个方向。其中量子密码和量子计算与网络空间安全有较紧密的关联,也为该学科的发展提供了新的机遇和挑战。因此,网络空间安全的教育应尽早将量子信息的相关课程纳入教学体系,兼顾核心概念和技术实现,培养对量子信息有正确和深入理解的

工程技术人员,补全量子信息从理到工、从实验室到产业界的缺失环节。

2 网络空间安全学科量子信息教学的需求和特点

面向工科和物理类学生的量子信息教学在需求、特点和手段等多方面有较大的不同。以下重点阐述网络空间安全学科量子信息教学的需求和难点,并概述中国科学技术大学(以下简称“我校”)开展教学改革的基础。

2.1 网络空间安全量子信息教学的要求

工科学生和理科学生的培养目标不同,教学上的侧重点也不同,前者更侧重于原理应用、技术创新和工程实现,后者则更侧重于原理创新和验证。因此,两者在教学的知识体系和讲授重点等方面有明显的区别。例如,我校物理学院开设的光学和原子物理两门课各为 80 学时,而大多数工科院系和专业的光学和原子物理合并为一门课,或者作为《普通物理》课程中的一部分,总共只有 60 或 80 学时。两者在讲授内容和深度上差别较大。此外,工科专业的培养计划中通常未设置物理类的进阶课程。例如,大多数工科系并未将《量子力学》设置为必修课,这导致了如果按照理科的授课目标、要求和教学模式设计面向工科专业本科生的量子信息课程,难以取得良好的教学效果。另外,工科教学中的很多课程,如电子线路、信号处理等,一般需要在理论教学的基础上,通过实验来巩固知识点并形成解决实际问题的能力^[3-4]。在新工科尤其重视实践能力的指导精神下,在网络空间安全的教育中亦应加强实践环节。

量子信息是物理和信息学的交叉学科。与传统工科教育相比,当前量子信息技术的教学尚处于萌芽阶段,现有的课程和教材从思维模式和体系结构上,大多侧重讲述物理原理和基础方案的验证性实验。总体来看,现有的量子信息类课程和教材更适合理科学子的理解模式,能够直接用于工科专业教学的案例、教材和实验资源严重缺乏。因此,面向网络空间安全学科的本科学生开设量子信息方面的课程,需要在课程设计、授课思维、讲课方式和实践工具等多个方面,进行全方位的创新和探索。

2.2 网络空间安全量子信息教育的难点

总体上,我校网络空间安全等工科专业的量子信息教学面临着前置课程缺失、思维模式不匹配、学时少和实验条件缺乏等困难。课程设计和教学实践需要立足于实际情况,解决这些实际困难。具体来说,在进行课程设计时,针对我校的实际情况,重点考虑了以下实施难点。

1) 教学目标的差异:课程设时要尽可能契合网络空间安全的学科要求,并非大而全地介绍量子信息技术,而是要让学生在积累基本知识的前提下尽可能学以致用,开拓和发展量子信息在网络空间安全场景下的应用方法和技术,使教育出的学生有能力补全从基础到应用的过渡环节。

2) 学生知识体系与课程要求不匹配:学生的前导课程中物理类课程较少,讲述内容较浅,量子力学、非线性光学和量子光学等是物理类专业学生的必修前置课程,而工科专业大多没有设置相关的课程。这些课程的缺失将导致学生在理解量子信息的基本原理时,可能出现较大的困难。

3) 学生兴趣与思维模式的建立:从普遍情况来看,工科学生在思维模式和学习方法上与理科学生有着一定的差异。同时,在教学过程中也发现,尽管很多学生在课程开始时对量子信息显示了较高的兴趣,但是当进入课程的技术讲述阶

段时,往往会出现理解上的困难,进而产生畏难情绪。如果不能让学生迅速对技术核心产生认同感,则很难保证后续教学的质量和效果。

4) 建立实践平台的难度较大:目前量子信息的操控对象主要是光子。当前的大学物理实验中有光学实验的板块,但其内容以经典光学的几何和波动光学为主;而专业的量子光学实验平台通常成本较高,作为教学资源进行全面部署具有较大的难度。

2.3 我校的优势资源和基础

我校前期已经在多个方面积累了较好的基础,如能在教学设计中善用这些资源,可以有效提升教学质量。

1) 我校在量子信息领域具有优质的科研环境和研究团队,并且有多位工作在科研一线的教师同时承担着教学工作。因此,在基础教学和一线科研的衔接方面具有一定的优势。

2) 我校已开设了面向物理类专业研究生的《量子信息物理》和《量子信息导论》,以及面向全校的本硕贯通课程《量子信息技术》等选修课程。虽然这些课程在内容和侧重点上并非面向网络空间安全量身定制,但可作为本课程设计的基础和参考。

3) 目前国内已有多家从事量子信息相关产业的公司,其中多家公司与我校有着良好的产学研合作联系和基础,这为量子信息学科与产业的衔接创造了条件和基础。因此,我校面向工科学生的教学理应兼顾与实际产业的对接。

3 网络空间安全量子信息本科教学设计

我校网络空间安全学院以新工科思维为指导,结合已有的积累和特色,在本科第三学期开设了《量子信息与安全导论》,并将其设置为专业核心课程。考虑到培养计划总学时的安排,该课程设置为40学时理论授课+10学时实验。

课程难点和解决思路如图1所示。以下分为教学目标、结构与内容和实践方法几个方面,对教学的设计思路和操作模式进行阐述。

3.1 课程的目标设计

本课程面向本科生教学,以导论命名说明了其定位并非全面而深入地讲述量子信息的专业课程,而是更侧重于让学生了解量子信息的基本概念、基本命题和基本方法,对量子信息学科的全貌和发展脉络有初步的了解,在后续开展研究和对接产业时,可以有专业的理解和清晰的判断。课程以案例带动思维,使学生理解量子信息与传

统信息技术的关联和区别,初步形成网络空间安全与量子信息交叉融合的思维方式,并以此为出发点,思考将量子信息与现有网络安全体系进行有效融合的设计思路和技术手段。

总体来说,希望通过本课程的学习,学生可以了解量子信息的基本原理,消除其畏惧心理,并补齐交叉学科研究所需的知识和技能短板。最终使学生初步具备后续研究的愿望、基础和能力。

3.2 课程的结构和内容设计

在设计课程时,将课程划分为3个大的板块,如图2所示。

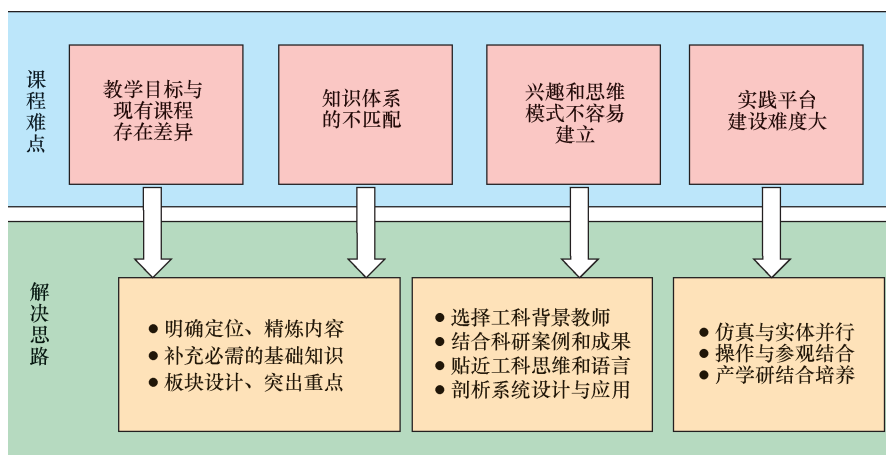


图1 课程难点和解决思路

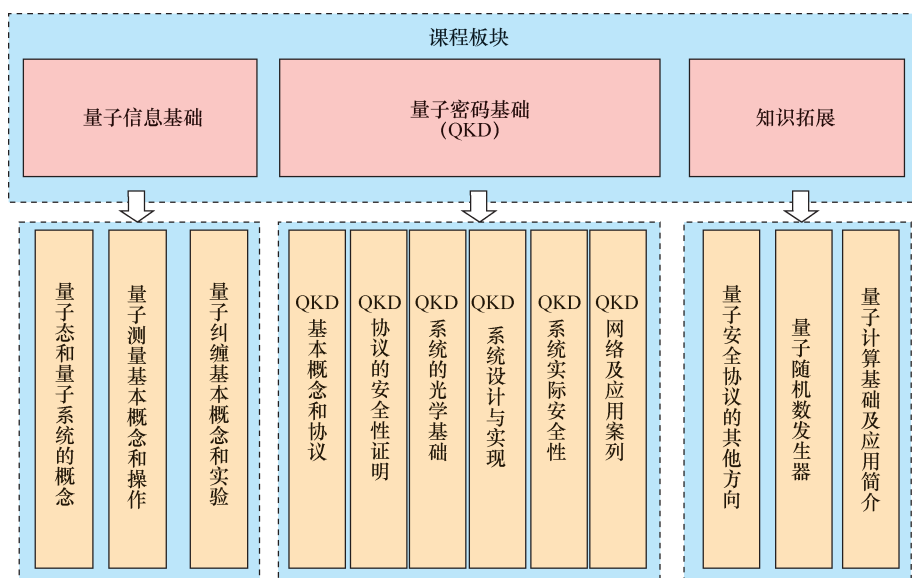


图2 课程的板块和内容设计

第一个板块是量子信息的基础知识，考虑为学生相对完整地介绍量子信息研究中所使用的基本语言、核心概念和描述方法（这一部分相对完整，但绝非事无巨细）。因此，需要精炼出量子力学中用于量子信息，特别是量子密码和量子计算的核心概念，如态矢、密度矩阵、变换和测量等。对量子密码等技术中不太常用的内容，如波函数及其计算则稍微弱化。

考虑到工科背景学生在光学方面的基础较为薄弱，课程也适度补充了理解后续内容所必备的光学知识，特别是重点讲授了量子密钥分发系统的实现技术，如光子偏振操控和相位干涉的原理、器件和实现方法等。

在这一板块中，我们也大致梳理学科的发展脉络，并对量子纠缠等基本概念进行了适度深度的讲授，为后续的安全性证明环节打下基础。总体来说，力求通过对概念和内容的适度取舍，在一定课时限制的条件下，让学生快速熟悉量子信息的专业语言并了解学科的概貌。

第二个板块是量子密码学基础。这一部分是量子信息与网络空间安全结合最直接和最紧密的内容之一，也是本课程讲授的重点。该板块集中讲述了量子密码的核心——量子密钥分发（QKD）。QKD是目前最成熟的量子密码技术，并且已经在实际场景中进行了试用。该板块是本课程的核心内容。从理论协议到工程实现，较全面地对QKD技术进行剖析和讲解，讲述的主要内容包括QKD协议介绍、协议理论安全性证明的基本方法、协议的系统实现、系统的实际安全性和网络化验证等。我们将量子保密通信作为一个大的案例，以目前安全性分析最完善和实际应用最广的BB84协议^[5]作为主要讲述对象，从原理到系统实现，从理论安全性到实际安全性逐层递进。通过理论和实际系统的对照，以及同一协议的不同实现方法之间的对比，使学生了解理工

融合的实际思维模式和实现技术；通过对实际应用案例的剖析，使学生了解量子密钥分发与现有信息安全体系结合的思路和方法。

第三个板块是对相关拓展内容的介绍。主要包括量子安全协议、量子随机数发生器和量子计算等前沿内容的概要介绍。量子安全协议包括量子比特承诺和量子数字签名等方向。对该方向的介绍可以使学生了解到量子密码不仅是QKD的一项内容，还包括与密码学其他领域相关的很多分支。随机数是密码学的另一项基础内容。我们希望在量子随机数部分，使学生初步了解利用量子过程产生高质量的真随机数的原理和技术途径。在量子计算部分，概要地介绍量子计算的基本概念、特点和潜在的优势。通过介绍Deutsch算法，使学生初步了解量子算法的特点。此后，介绍Shor算法的基本原理及其对现用密码算法的潜在影响。量子计算对于网络空间安全的发展来说，更像是矛，而量子密码则像是盾。以契合传统网安学科知识体系的视角，增加量子信息课程内容上的“矛和盾”，可以有效拓宽学生的视野，使学生更深刻地理解新技术对传统学科带来的机遇和挑战，提升其创新意愿和能力。

通过以上几个板块的讲授，我们力求以点带面，使学生对于量子信息有正确和较为全面的了解，强化其理工结合的思维模式、创新能力和执行手段，为开展后续研究打下良好的基础。由于课时的限制，在实际讲授时，对课程内容在范围和深度上有一定的取舍。我们将在今后的课程执行过程中，通过增加课时和精炼内容解决这一矛盾，并进一步结合网络空间安全的学科发展需求优化教学效果。

3.3 课程的理论授课和教案设计

课程在理论授课方面，在任课教师的选择、教学语言的运用和例证方法等方面尽可能贴近工科学生的知识体系和学科背景，以保证良好

的教学效果。

课程尽可能选择在科研一线从事量子信息研究、有本科基础课程教学经验以及具有工科专业背景的主讲教师,这对于提升工科学生对量子信息的接受程度非常有帮助。在教学方法上,授课教师从语言、描述习惯和公式体系等方面,尽可能贴近工科学生的背景和理解方法。例如,物理类专业在描述量子通信过程时,常用量子态制备、操控、传输和测量等专业用语。这些用词对于工科学生来说较为陌生,如果将其与经典通信系统中常用的信源、调制、信道和解调等语言进行对比阐述,则理解起来要容易很多。

在教材选择上, Nielsen 和 Chuang 合著的 Quantum Computation and Quantum Information^[6], Benenti 等合著的 Principles of Quantum Computation and Information I^[7]、张永德著《量子信息物理原理》^[8]等是目前物理专业常用的经典教材。但是在初期使用这些教材的过程中,发现大多数学生反映来说较为艰深,其主体内容也与网络空间安全的侧重点和实际需求存在着一定的差异。近年来新出现的一些优秀的专著,如郭弘等编著的《量子密码》^[9]具有较全面的量子密码知识背景介绍、清晰的逻辑框架和完整的参考文献索引,可以作为很好的教学参考资料。但是受到课时限制,仍需要进行节选整编并补充可用于布置作业的习题。此外,课程涉及的量子计算等其他方面内容在该专著中未涉及。其他如曾贵华编著的《量子密码学》^[10]和 Kollmitzer 等编著的《Applied Quantum Cryptography》^[11]等专著也有部分内容适合选作课程讲授内容。

综合来看,目前仍没有一部教材完全符合本课程体系架构和内容的需求。因此,本课程自编了教学课件。我们节选整编现有教材、专著和文献作为基本框架;引入最新的科研文献补充前沿知识;形成特色专题进一步丰富各板块的教学内

容,如安全性证明的基本方法和案例,高速系统设计与实现、实际安全性攻击与防御和量子密码应用案例等;通过节选、改编和自编结合的方式构建习题库,根据网络空间安全的特点,简化过于艰深的理论推导相关的习题内容,侧重于基础概念的理解和应用,加强对于系统设计和应用方面的练习内容。在完成每一个章节或大板块的讲授之后,通过课堂测验和作业,加深巩固学生的知识点。通过对教材和习题的整体设计,课程初步形成了较完整和具有一定特色的体系,为后续的丰富和优化打下了较好的基础。

3.4 课程的实验设计

目前量子信息有多种实验体系,但大多成本很高,无法实际部署供本科学生进行教学实验。因此,课程在实验设计上充分利用了计算机技术发展带来的工具和方法,采取了虚拟仿真^[12-13]与实体结合的方法来解决教学实验资源短缺的问题,尽可能在教学效果和教学成本之间取得平衡。

课程设计了量子密钥分发协议的仿真实验内容。授课教师布置了结合诱骗态^[14-16]的 BB84 协议成码率计算等仿真实验,让学生基于熟悉的 C 语言、Matlab 和 Python 等工具编写仿真程序,计算 QKD 的安全密钥生成率并绘制码率与传输距离的关系图,加深对协议的理解,同时通过调整仿真模型的系统参数,对照实际系统的结构,分析器件参数的变化对系统性能造成的影响,初步理解实际系统和理论模型之间的区别与联系,逐步具备对实际系统的安全性分析能力。

针对纠缠光子的产生、操控和测量等物理特性丰富但设备昂贵的实验,我们尝试校企合作,研发了 3D 虚拟仿真软件,其界面如图 3 所示。我们对纠缠光源系统进行 1:1 的 3D 建模,在物理特性和操控方式上尽可能贴近真实器件,从而使学生接近于操作真实的量子光学实验系统,对基本概念的具体实现产生直接鲜活的感性认识。这

有助于学生理解纠缠源制备和 Bell 不等式测量等量子信息的基础和核心内容^[17-18]。这一仿真工具在学生的小范围试用中取得了较好的实际效果,后续将根据反馈意见进一步完善和推广。



图3 纠缠光源三维仿真软件截图

课程还利用授课教师工作在科研一线的条件,安排了对实际量子通信系统、科研级量子光学实验平台等内容的参观演示实验,进一步提升学生的兴趣,丰富学生的认知。

课程仿真的技术手段有效克服了教学资源不足、实物成本过高的问题,并通过虚实结合、实际操作与参观演示结合的方法,较为有效地解决了实验效果和实验投入之间的矛盾。

4 结束语

经过几年的教学实践,《量子信息与安全导论》课程在理念、目标、体系、内容、授课方法和实践工具上做出了创新和有益的尝试,积累了有价值的经验和教学反馈,并有望在近期形成独立完整的特色教材和授课工具包。本课程的教学工作为量子信息融入网络空间安全的教学体系提供了一条行之有效的实施思路,也为新工科教学的创新实践提供了有价值的参考案例。未来,我们将进一步完善课件,丰富实验教学资源,并尝试通过网络公开课等多种教学方式,为推动网络空间安全学科的量子信息教学发展做出贡献。

参考文献:

- [1] 黎海生, 夏海英, 宋树祥. 基于新工科的电子信息类专业人才创新能力培养模式研究与实践[J]. 实验技术与管理, 2019, 36(4): 200-202.
LI H S, XIA H Y, SONG S X. Research and practice of innovative ability training model for electronic and information professionals based on new engineering[J]. Experimental Technology and Management, 2019, 36(4): 200-202.
- [2] 张焕国, 韩文报, 来学嘉, 等. 网络空间安全综述[J]. 中国科学: 信息科学, 2016, 46(2): 125-164.
ZHANG H G, HAN W B, LAI X J, et al. Survey on cyberspace security[J]. Scientia Sinica Information, 2016, 46(2): 125-164.
- [3] 董玉冰, 李明晶. 新工科背景下混合式创新教学在数字电子课程中的应用探索[J]. 长春大学学报, 2017, 27(10): 117-120.
DONG Y B, LI M J. Exploration on application of mixed innovative teaching in digital electronic course under the background of new engineering discipline[J]. Journal of Changchun University, 2017, 27(10): 117-120.
- [4] 王晓茜, 苟立丹, 冯玉玲, 等. 《量子信息物理》课程教学改革的研究[J]. 教育现代化, 2018, 8(32): 64-71.
WANG X X, GOU L D, FENG Y L, et al. Research on the teaching reform of the course "quantum information physics"[J]. Education Modernization, 2018, 8(32): 64-71.
- [5] BENNETT C H, BRASSARD G. Quantum cryptography: public key distribution and coin tossing[C]//IEEE International Conference on Computers, Systems and Signal Processing. 1984:175-179.
- [6] NIELSEN M A, CHUANG I L. Quantum computation and quantum information[M]. Beijing: Tsinghua University Press, 2015.
- [7] BENENTI G, CASATI G, STRINI G. 量子计算与量子信息原理[J]. 北京: 科学出版社, 2015.
BENENTI G, CASATI G, STRINI G. Principles of quantum computation and information[M]. Beijing: Science Press, 2015.
- [8] 张永德. 量子信息物理原理[M]. 北京: 科学出版社, 2006.
ZHANG Y D. Principles of quantum information physics[M]. Beijing: Science Press, 2006.
- [9] 郭弘, 李政宇, 彭翔. 量子密码[M]. 北京: 国防工业出版社, 2016.
GUO H, LI Z Y, PENG X. Quantum cryptography[M]. Beijing: National Defense Industry Press, 2016.
- [10] 曾贵华. 量子密码学[M]. 北京: 科学出版社, 2006.
ZENG G H. Quantum cryptography[M]. Beijing: Science Press, 2006.
- [11] KOLLMITZER C. 应用量子密码学[M]. 北京: 科学出版社, 2015.

KOLLMITZER C. Applied quantum cryptography[M]. Beijing: Science Press, 2015.

- [12] 杨阔, 郭娟, 雷晓蔚. 大学物理可视化仿真实验系统设计与实现[J]. 实验室研究与探索, 2019, 38(2): 81-84.

YANG K, GUO J, LEI X W. Design and study on the visualization simulation system for university general physics[J]. Research and Exploration in Laboratory, 2019, 38(2):81-84.

- [13] 崔来中, 陆楠. 新工科背景下面向虚拟仿真实验的计算机网络课程实验教学探索[J]. 计算机教育, 2019, 3: 146-150.

CUI L Z, LU N. Exploring the experimental teaching of computer network course using virtual simulation experiment under the background of new engineering[J]. Computer Education, 2019, 3: 146-150.

- [14] HWANG W Y. Quantum key distribution with high loss: toward global secure communication[J]. Physical Review Letters, 2003, 5(91): 057901.

- [15] WANG X B. Beating the photon-number-splitting attack in practical quantum cryptography[J]. Physical Review Letters, 2005, 91(5): 230503.

- [16] LO H K, MA X F, CHEN K. Decoy state quantum key distribution[J]. Physical Review Letters, 2005, 94(23).

- [17] 孔小琴, 李琴, 李远科, 等. 基于纠缠的量子密钥分配协议仿真[J]. 计算机工程与应用, 2017, 53(1): 113-117.

KONG X Q, LI QIN, LI Y K, et al. Simulation of quantum key distribution based on quantum entangled states[J]. Computer Engineering and Applications, 2017, 53(1): 113-117.

- [18] 曹锐. 仿真技术在量子通信教学中的研究与应用[D]. 重庆: 重庆师范大学, 2015.

CAO K. Research and application of simulation in quantum communication teaching[D]. Chongqing: Chongqing Normal University, 2015.

[作者简介]



陈巍(1977—), 男, 河北石家庄人, 博士, 中国科学技术大学副教授, 主要研究方向为量子密码和量子信息。



银振强(1983—), 男, 甘肃兰州人, 博士, 中国科学技术大学教授, 主要研究方向为量子密码和量子信息。



韩正甫(1962—), 男, 安徽寿县人, 中国科学技术大学教授、博士生导师, 主要研究方向为量子密码和量子信息。



俞能海(1964—), 男, 安徽无为人, 博士, 中国科学技术大学教授、博士生导师, 主要研究方向为网络空间安全、计算机视觉和多媒体信息处理。