物理与工程 Vol.34 No.2 2024

用大学物理知识诠释前沿科技
——从光的偏振到量子通信

张 婷[1] 吴 伟[1] 孙仕海[2]
([1] 国防科技大学理学院量子信息研究所,湖南 长沙 410073;
[2]中山大学物理与天文学院,广东 珠海 519082)

摘 要 在大学物理教学中以科技前沿应用为牵引,用大学物理的语言解释前沿科技进展的原理,拉近基础课和前沿应用的距离,可以促进学生学习物理的兴趣,加深学生对于基础物理原理的理解。本文以量子密钥分配为例,仅用大学物理中偏振的内容就解释了经典的BB84方案的基本原理,并对该方案的实际实现进行了阐述,旨在表明任何理论方案和实际实现都存在相当的距离。本文还介绍了量子通信领域的最新研究进展和目前主要的研究方向,以激发学生主动探索和进一步研究的兴趣和热情。本文是为基础物理原理和高新尖技术之间搭建桥梁的一次有益尝试,相关思路值得在新工科背景下的大学物理教学中推广。

关键词 光的偏振;波片;量子密钥分配;BB84方案

ELABORATING FRONTIER TECHNOLOGIES USING COLLEGE PHYSICS KNOWLEDGES
—FROM POLARIZATION OF LIGHT TO QUANTUM CONMUNICATION

ZHANG Ting[1] WU Wei[1] SUN Shihai[2]
([1] Institute for Quantum Science and Technology, College of Science, National University of Defense Technology, Changsha, Hunan 410073;
[2]School of Physics and Astronomy, Sun Yat-sen University, Zhuhai, Guangdong 519082)

Abstract During the teaching process, if the teacher could take the frontier application of science and technology as the traction, explain the principles of cutting-edge scientific and technological progress in the language of college physics, and shorten the distance between basic courses and cutting-edge applications, the students' interest in learning physics will be promoted and their understanding of basic physics principles will be deepen. Taking quantum key distribution as an example, this paper explains the basic principle of the classical BB84 scheme with the polarization content in college physics, and expounds the actual implementation of this scheme, aiming to show that there is a considerable distance between the theoretical scheme and the actual implementation. In order to stimulate students' interest and enthusiasm for active exploration, the latest research progress and current main research directions in the

收稿日期:2019-12-03;**修回日期**:2020-05-21
通信作者:张婷,国防科技大学理学院量子信息研究所副教授,tingzhang@nudt.edu.cn
引文格式:张婷,吴伟,孙仕海. 用大学物理知识诠释前沿科技——从光的偏振到量子通信[J]. 物理与工程,2024,34(2):19-24.
Cite this article: ZHANG T, WU W, SUN S H. Elaborating frontier technologies using college physics knowledges—From polarization of light toquantum conmunication[J]. Physics and Engineering, 2024, 34(2): 19-24. (in Chinese)

field of quantum communication are also introduced. This is a pioneering attempt to bridge the fundamental physics theory and frontier technolies, which is worth promoting in college physics teaching in the context of emerging engineering education.

Key words polarization of light; wave plate; quantum key distribution; BB84 protocol

物理学是研究物质运动最一般规律和物质基本结构的学科，是推动当代高新技术发展的重要原动力[1]。然而，不少学生对大学物理课程的印象是“抽象”加“陈旧”，前者让学生觉得大学物理难学，后者则让学生觉得大学物理没意思，与后续专业课程脱节，这是大学物理教学中普遍存在的情况。如果教师在授课过程中能将大学物理中抽象的基本原理和实在的科技前沿联系起来，时刻注意以前沿应用为牵引，将一些高新尖内容落地到大学物理的教学范畴内，用尽可能简单的物理图像阐述前沿应用的基本原理，让学生认识到“基础”的大学物理知识也能直接应用于“高大上”的科研前线，把枯燥的基础理论和最新科研成果联系起来，这不仅能促进学生学习物理的兴趣，加深对物理基本原理的理解，而且有利于培养学生的科学素质，激发学生的创新意识。

本文以量子密钥分配(Quantum Key distribution, QKD)为例，首先简要回顾了大学物理中偏振的相关内容，然后在此基础上，解释了最经典的 QKD 方案——BB84 协议的基本原理，最后对 QKD 的实际实现展开讨论，希望以此示范如何跨越基本物理原理和高新尖科技前沿的距离，为新工科背景下大学物理的教学设计提供一个新思路。

1 光的偏振知识点的简要回顾[1,2]

光的偏振属于大学物理中波动光学部分。通过之前的学习，学生已经掌握了机械波等相关知识，了解“光是一种电磁波”。光的干涉与衍射现象是光的波动性的证明，而光的偏振特性则表明光的横波性。光的偏振这一章主要讨论光各种偏振状态的区别、不同偏振光的获得和检验方法等。这部分内容与前面讲的干涉及衍射相对独立，而且更为抽象，是教学的难点。因此在讲述过程中厘清思路，联系实际，特别是与高新尖技术前沿相联系，必将有助于学生建立清晰的物理图像，有意愿进一步主动探究学习。

光的偏振部分的内容可用“五二二”来概括，即“五”种偏振态、“二”个定律、“二”个器件。五种偏振态即：自然光、线偏光、圆偏光、椭圆偏振光和部分偏振光。二个定律即：马吕斯定律和布儒斯特定律。二个器件即：偏振片和波片。五种偏振光的产生和检验是贯穿本章教学的主线，利用偏振片和波片就可以实现。

具体来说，平面电磁波是横波，当光沿 z 方向传播时，电场只有 x，y 方向的分量。不失一般性，考虑单色简谐平面电磁波，其电场 x，y 分量的振幅比及其相位差就决定了光的偏振态。具体说来，有线偏光、圆偏光及椭偏光三种。再加上无偏的自然光和部自然光和线偏光的合成的部分偏振光，就是五种光的偏振态。

利用偏振片可以得到线偏光，而要改变光的偏振态，波片是最常用的器件。不考虑波片引起的损耗，光经过波片后光强不发生变化，仅偏振态有可能发生变化。具体说来，(1)线偏振光入射二分之一波片，出射光为偏振方向变化的线偏振光。(2)线偏振光入射四分之一波片，出射光为线偏光、圆振光、椭偏光都有可能。需要注意的是，这时得到的椭偏光并不是任意的椭偏光。要得到任意的椭偏光，需再用二分之一波片改变线偏振光的偏振方向实现。(3)圆偏光入射四分之一波片，出射光为线偏光。(4)椭偏光入射四分之一波片，出射光为一般还是椭偏光，若入射光长轴或短轴方向与光轴方向一致，则出射光是线偏振光。(5)(椭)圆偏光入射二分之一波片得到偏振旋转方向反转的(椭)圆偏光。偏振态的改变在 QKD 密钥生成过程中有重要的应用。

上述结论可概括为图 1。

2 基于光的偏振的量子通信

光的偏振虽然是大学物理的基础内容，但最知名、最经典的 QKD 的 BB84 方案，正是利用不同的偏振光来完成量子密钥分配，其基本原理仅用大学

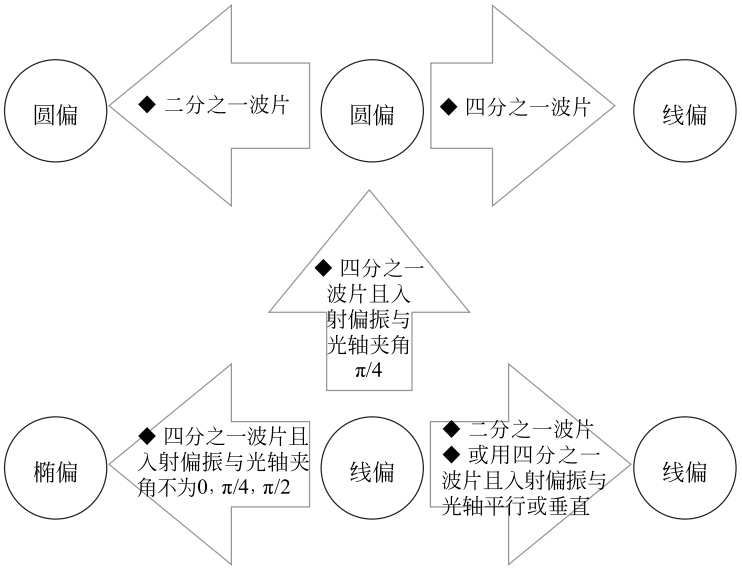

图 1 不同偏振态的互相转化

物理的知识就可以解释。该方案由查理斯·贝内特(Charles Bennett)与吉勒·布拉萨(Gilles Brassard)于 1984 年发表[3]。

首先我们先简要澄清三个概念:量子通信(Quantum Communication, QC)、量子保密通信(Quantum cryptography, QC)和 QKD。严格说来,这是三个不同的概念。基于量子态来进行信息传递的通信都可以称为量子通信,比如隐形传态(teleportation)[4]、稠密编码(dense coding)[5]、量子保密通信等。量子保密通信指的是采用量子的方法来确保信息安全的通信,不仅包含 QKD,还包括量子签名(quantum signature)[6]、量子安全直接通信(quantum secure direct communication)[7]、量子秘密共享(quantum secret sharing)[8-11]、量子比特承诺(quantum bit commitment)[12-14]等。QKD 特指利用量子态来实现安全的密钥分发,然后再结合经典的加密算法来保证信息的安全。可以看出,量子通信的概念最为广泛,指一般的通信过程,而量子保密通信的概念次之,仅包含通信中的保密通信部分,最后是量子密钥分发,它仅是保密通信中一种特殊的密钥分发方法。但是,也要指出在很多场景中人们会将这三个概念相互替代使用。

QKD 是目前发展最成熟的量子信息技术之一,在理论和实验上都有重要突破,已经逐渐开始步入实用阶段。各国都在积极布建基于量子密钥分发的量子通信网络。比如我国的京沪干线量子通信网络、日本的东京量子通信网络、美国的西海岸量子通信网络等。同时,这些量子通信网络已经在银行、政务、国防等领域得到了初步的应用。我国在此领域的研究处于世界领先地位。自 2009 年起,我国先后建成了若干个中小规模量子网络:2011 年安徽搭建了第一个广域 QKD 量子网络[15];2016 年 8 月 16 日,世界首颗量子科学实验卫星"墨子号"升空[16],并以其为中继,实现了中国和奥地利之间 7600km 的量子保密通信[17]。2017 年 9 月 29 日,从北京到上海的长达 2000km 的"京沪干线"量子通信骨干网正式开通[18]。总体而言,QKD 在网络化、实用化的进程中已经取得了丰硕的成果。

当前,量子通信有两个主要的研究方向。一是实际安全性问题。量子通信虽然具备协议的无条件安全,但受实际设备缺陷的影响,实现量子通信系统中存在潜在的安全性漏洞。为了解决这一问题,研究者提出设备无关、测量设备无关、半设备无关量子通信等高安全的协议。二是增加量子通信抗噪声的能力和密钥率,为此研究者提出了轮回差分相移、双场量子通信协议等。

2.1 QKD 的基本原理[19]

QKD 基于量子物理原理,生成一串随机的二进制数串作为密钥,配合香农信息论唯一可证明无条件安全的"一次一密"加密体系,可以实现由物理原理保证的理论上无条件安全的保密通信。所谓"一次一密"加密体系,是指加密的密钥长度

大于或等于明文的长度，每当使用与明文等长的密钥进行加密后，该密钥就被舍弃，下一次加密需要使用新的密钥。

在 BB84 方案中，发送者（Alice）和接收者（Bob）需要两条信道：一条量子信道用于发送偏振态不同的光子，另一条经典信道，譬如无线电或因特网，用于完成密钥协商过程。所谓光子，是光量子的简称，是电磁场不可再分的最小能量单元，光可以看成一束以光速运动的光子流。窃听者在量子信道和经典信道上均可以进行任何物理学所允许的操作，不需保证经典信道的安全性，只需保证其上所传递的信息具有可验证性即可。BB84 协议在设计时已经考虑到了两种信道都被第三方（Eve）窃听的可能。

BB84 方案中使用了两组处于不同线偏振态的光子，分别为直线组“＋”和对角组“×”。其中，直线组包含水平偏振（→）和竖直偏振（↑），分别记为 0 和 1；对角组包含 45°偏振（↗）和 135°偏振（↖），也分别记作 0 和 1，如图 2 所示。

	0	1
＋	→	↑
×	↗	↘

图 2 QKD 编码

量子密钥分配过程如下：首先，Alice 随机选择一组线偏振光（“＋”或“×”），然后再随机产生一个编码（0 或 1），以此来确定所发送的每一个光子的偏振态。如表 1 所示，选择“＋”组和编码 0 时发送水平线偏振态→，选择“＋”组和编码 1 时发送竖直线偏振态↑，选择“×”组和编码 0 时发送 45°方向的线偏振态↗，选择“×”组和编码 1 时发送 135°方向的线偏振态↖。Alice 不断重复此过程，向 Bob 发送一串线偏振光子。

其次，Bob 随机的从“＋”或“×”四个方向的检偏器中选择一个对接收到的光子进行检偏，并记录所选偏振片的通光方向及相应的测量结果。我们知道，当检偏器通光方向与待检光偏振方向一致时，光子通过检偏器后不发生变化；当检偏器通光方向与待检光偏振方向垂直时，光子无法通过；当检偏器通光方向与待检光偏振方向有一定夹角 α 时，光子通过后强度按马吕斯定律降低，即为原来的 $\cos^2\alpha$ 倍。因此，如果 Bob 选择了竖直方向通光的偏振片，且发现原光子无变化的通过，则可知原脉冲为竖直偏振，测量结果为 1，如果发生消光，则可知原脉冲为水平偏振，测量结果为 0。选择同属“＋”组的水平检偏器结果类似。但如果选择的检偏器组与待检光偏振状态组不匹配时，譬如选择了竖直方向的偏振片去检测“×”组偏振光子时，无论是 45°或是 135°方向的线偏振态，都会发现光子强度减半，即无法区分原脉冲编码的信息究竟是 0 还是 1。事实上，光子作为电磁场能量不可再分的最小单元，强度变或不变是无法区分的，这两种情况的区分要靠通信双方对照起偏组和检偏组来完成。也就是说，起偏器组与检偏器组不一致，将不能得到正确的编码信息。但这也正是我们利用线偏振光子进行安全密钥分配的物理基础，后文将会说明。

表 1 BB84 的 QKD 流程

Alice 的随机比特	0	1	1	0	1	0	0	1
Alice 随机选择的组	＋	＋	×	＋	×	×	×	＋
Alice 处的起偏过程	→	↑	↖	→	↖	↗	↗	↑
Bob 随机选择测量的组	＋	×	×	×	＋	×	＋	＋
Bob 处的检偏过程	→	↗	↖	↗	→	↗	→	↑
在公共信道中对比组	√		√			√		√
共有的密钥	0		1			0		1

再次，当 Bob 完成所有偏振光子检偏之后，利用经典信道与 Alice 联系。Alice 公布发送过程中所选择的起偏组，Bob 公布测量过程中所用的检偏组，双方通过经典信道进行比对，舍弃双方选择了不同组的测量结果，保留双方选择相同组的测量结果，这些就是双方共享的密钥。完全理想的情况下，通信误码率为零。

在此基础上，双方可以通过拿出共享密钥的一部分进行错误率对比来检查是否存在窃听者。

假设有第三方(Eve)在量子信道上进行窃听,为了获得 Alice 发送的偏振光信息,窃听者 Eve 仿照 Bob 进行检偏。若 Eve 选择了与 Alice 相同的组去测量,则不会影响 Bob 的测量结果,Alice 和 Bob 对比密钥时不会发现有 Eve 的存在。然而,Eve 还有 50%的概率会选择与 Alice 不同的检偏组去检偏,这会使光子偏振态改变,此时 Bob 再测量这个光子又有 50%的概率得到与 Alice 不同的结果。这样,如果假设 Eve 对 Alice 发送的所有光子进行截取测量后重发,则 Eve 的存在会给通信带来 25%的误码率,Alice 和 Bob 通过相互对比就可以发现有窃听者 Eve 的存在。

2.2 量子密钥分配的具体实现

以上是最理想的离散变量量子密钥分配方案的基本原理,但这仅仅是迈向完整 QKD 系统实际实现的第一步。正如大学物理在理工科高等教育的基础性地位一样,上述 QKD 协议也仅仅是 QKD 系统的基础。传统大学物理讲述的内容大都是纯粹的、完美的理论,目的是使学生获得完整的物质世界图像,认识物质世界运动变化的基本规律。但在新工科背景下的大学物理教学,除了给学生构筑完整理想的物理知识背景和结构外,还有必要在合适的情境下,让他们跳出完美但不实际的理论,去见识书本上的知识和实际世界的差距,建立开放的和发展的科学理念。因此,下文就实际 QKD 的实现补充说明几点。

第一,理想方案中信息的载体是单光子,实际中获得单光子的方法大致分为两类:单光子源和微弱激光源。单光子的不可再分性从物理原理上保证了量子密钥的安全性。单光子源最直观的一个例子就是原子从激发态跃迁至基态时会释放一个光子。实际中,这个过程是概率性的。单光子源显然更符合 QKD 安全性的理论要求,但受限于技术成熟度,其实际制备效率、使用条件等均尚不适合实用化系统的应用,因此目前实际 QKD 系统中采用的都是制作成本低、方便的微弱激光源。将激光秒冲衰减至每个脉冲的平均光子数小于 1,即一串连续的光脉冲中,只有一定比例的脉冲包含一个光子,大部分的脉冲是空的,还有很少比例的脉冲包含两个及以上的光子。微弱激光源中含有的多光子成分带来的安全性隐患已经有有效的方法可以高效的弥补[20-22]。

第二,实际激光器产生的光多是单一的线偏光,要产生四种不同线偏振光一般有两种方法。一是利用两个 50/50 的分束器将单一光束一分为四,然后再借助二分之一波片将其偏振方向转到需要的方向上。另一种方法则直接用四个同样的激光器结合二分之一波片来实现。墨子号量子通信卫星采用的是后一种方法[15]。

第三,实际中检偏多采用偏振分束器而不是偏振片。原因在于用偏振分束器简单且效率更高。顾名思义,偏振分束器把入射光分成两束偏振方向相互垂直的反射光和透射光。对于单光子入射,如果为线偏振,且偏振分束器通光方向与其偏振方向一致(垂直),则只有透射(反射)方向能检测到光子。如果偏振分束器的通光方向与入射线偏方向夹角为 45°或 135°,则在反射和透射方向上各有 50%的概率能够探测到光子。注意,并不是透射光和反射光强度各为入射光强的一半,因为单光子已是不可再分的最小单位。也就是说,单个光子 100%通过和 50%通过的情况仅用偏振分束器是不可区分的,通信双方需对照起偏组和检偏组来完成。

第四,前面讲到对于理想的 QKD 系统而言,如果没有窃听者 Eve 存在,则系统误码率为 0,如果存在窃听者 Eve,则系统误码率为 25%。但对于实际系统而言,即使没有窃听者存在也有一定的误码率,这主要是由于光学器件的非理想(比如起偏器的消光比有限)以及信道的噪声(比如信道的退偏)等因素的影响。而从安全性角度考虑,我们并不能区分噪声所引入的误码率和窃听者所引入的误码率。因此,实际系统中需要将所有的噪声都认为是窃听者引入的。此时就不能简单地通过误码率来判断系统中是否存在窃听者。事实上,随着理论的发展,当前的 QKD 系统中已经不是通过误码率来简单判断是否存在窃听者,而是通过误码率来估计窃听者所获取的信息量,然后通过严格的信息论分析和数学处理来擦除掉窃听者所获取的信息,从而保证即使存在窃听者时也可以建立无条件安全的密钥。这涉及较为复杂的理论分析,此处不展开说明,感兴趣的读者可以参考相关的书籍和文献。

3 结语

本文以光的偏振和 QKD 为例,对基础物理到

高新尖技术的跨越进行了一次有益的尝试。偏振是波动光学中最抽象的一章内容，光的不同偏振态及其相互转化连不少研究生也没有完全理清楚，但其应用又十分的广泛，相当一部分光学实验都会涉及光的偏振。本文在简要回顾大学物理偏振部分教学内容的基础上，简洁明了地解释了QKD的基本原理，并对实际实现进行了较为充分的讨论，旨在表明任何理论方案和实际实现都存在相当的距离，这对于激发学生见识基本物理原理与实际前沿应用的密切联系有很好的示范作用，有望激发学员进一步主动探索研究的兴趣和热情。

新工科是基于国家战略发展新需求、国际竞争新形势、立德树人新要求而提出的我国工程教育的改革方向[23]。新工科要求我们培养学生的探索精神和创新意识的学生。作为高等学校理工科学生通识教育必修课的“大学物理”课程，正是本着传授知识，培养能力和科学素质的宗旨为理工科创新性人才的培养服务的。新工科建设“新”字当头，在大一大二这培养学生自我学习兴趣和自我学习能力的关键时期，将经典物理原理与现代的高新尖技术无缝对接，利用大学物理教学内容解释高新尖技术的基本原理，同时也阐述理论和实际实现之间的距离，激起学生主动探索甚至是进一步研究的愿望，必将有益于大学生自我学习兴趣和能力的培养及提升，获得终身学习能力，从而进一步开发和培养创新能力，这正是新工科人才培养的新理念。

参 考 文 献

[1] 李承祖，曾交龙. 大学物理学[M]. 北京：科学出版社，2019.

[2] 廖延彪. 偏振光学[M]. 北京：科学出版社，2003.

[3] BENNETT C H, BRASSARD G. Quantum cryptography: Public key distribution and coin tossing[C]. Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, New York), 1984: 175.

[4] CHARLES H B, GILLES B, CLAUDE C, et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels[J]. Physics Review Letter, 1993(70): 1895.

[5] ADRIANO B, ARTUR E. Dense coding based on quantum entanglement[J]. Journal of Modern Optics, 1995(42): 1253.

[6] 温晓军，陈永志. 量子签名及应用[M]. 北京：航空工业出版社，2012.

[7] DENG F G, LONG G L. Secure direct communication with a quantum one-time pad[J]. Physics Review A, 1997(56): 1154-1162.

[8] HILLERY M, BUŽEK V, BERTHIAUME A. Quantum secret sharing[J]. Physics Review A, 2004(69): 052319.

[9] KARLSSON A, KOASHI M, IMOTO N. Quantum entanglement for secret sharing andsecret splitting[J]. Physics Review A, 1999(59): 162-168.

[10] CLEVE R, GOTTESMAN D, LO H-K. How to share a quantum secret[J]. Physics Review Letter, 1999(83): 648.

[11] CRÉ C, GOTTESMAN D, SMITH A. Approximate quantum error-correcting codesand secret sharing schemes [C]//Advances in Cryptology-EUROCRYPT 2005, Lecture Notes in Computer Science. Berlin, 2005: 285-301.

[12] LO H K. Insecurity of quantum secure computations[J]. Physics Review A, 1997(56): 1154-1162.

[13] LO H K, CHAU H F. Is quantum bit commitment really possible? [J]. Physics Review Letter, 1997(78): 3410-3413.

[14] MAYERS D. Unconditionally secure quantum bit commitment is impossible[J]. Physics Review Letter, 1997(78): 3414-3417.

[15] WANG S, CHEN W, YIN Z Q, et al. Field and long-term demonstration of a wide area quantum key distribution network[J]. Optical Express, 2014, 22(18): 21739-21756

[16] LIAO S K, CAI W Q, LIU W Y, et al. Satellite-to-ground quantum key distribution[J]. Nature, 2017(549): 43-47.

[17] LIAO S K, CAI W Q, HANDSTEINER J, et al. Satellite-relayed intercontinental quantum network[J]. Physics Review Letter, 2018(120): 030501.

[18] China's 2,000-km Quantum link is almostcomplete[EB/OL]. https://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete

[19] 李承祖. 量子通信和量子计算[M]. 长沙：国防科技大学出版社，2000.

[20] HWANG W Y. Quantum key distribution with high loss: Toward global secure communication[J]. Physics Review Letter, 2003, 91(5): 057901.

[21] WANG X B. Beating thephoton-number-splitting attack in practical quantum cryptography[J]. Physics Review Letter, 2005, 94(23): 230503.

[22] LO H K, MA X, CHEN K. Decoy state quantum key distribution[J]. Physics Review Letter, 2005, 94(23): 230504.

[23] 钟登华. 新工科建设的内涵与行动[J]. 高等工程教育研究，2017(3): 1-6.
ZHONG D H. Connotations and actions for establishing the emerging engineering education[J]. Research in Higher Education of Engineering, 2017(3): 1-6. (in Chinese)