

EDU-QCRY1

EDU-QCRY1/M

量子密码学

演示工具包

手册



目录



第一章警告符号.....	1
第二章安全.....	2
第三章描述.....	3
第四章零部件清单.....	5
第五章量子密码学的基础.....	9
. 1. 5介绍.....	9
. 2. 5一次性垫.....	9
5. 3. 密钥分配.....	11
5. 3. 1. 入/2板和数据传输.....	11
5. 3. 2. 密钥分配.....	13
. 4. 5. 发现了一个窃听器.....	15
. 5. 5. “随机”是什么意思?	17
. 6. 5是什么阻止了一个人简单地复制这些信息?	17
. 7. 5实验程序.....	18
5. 8. 经典光与单光子.....	19
5. 9. 缠结.....	19
. 10. 5. 狄拉克符号中的数学描述.....	20
第六章实例.....	25
. 1. 6没有Eve的加密协议（两个字母）	25
. 2. 6与Eve的加密协议.....	27
第七章系统的设置和调整.....	30
. 1. 7组件组件.....	30
. 2. 7电子产品.....	32
7. 2. 1. 电源.....	32
. 2. 2. 7激光电子.....	32
. 2. 3. 7传感器电子.....	33

7. 3. 调整激光器和入/2型板.....	33
------------------------	----

7. 4. 设置为Alice和Bob.....	36
7. 5. 添加Eve.....	38
第八章实验.....	39
. 1. 8密钥生成.....	39
. 2. 8. 一个四个字母Word的加密和传输.....	40
. 3. 8. 添加Eve和窃听检测.....	40
第九章测量方案.....	42
第十章教学技巧.....	46
第十一章故障排除.....	47
第十二章确认.....	48
第十三条监管.....	49
第14章索尔拉布斯的全球联系方式.....	50

第一章警告符号

以下是您在本手册或设备上可能遇到的警告符号列表。

符号	描述
	直流电
	交流电流
	同时包括直流电和交流电
	接地端子
	保护导体端子
	机架或底盘端子
	等效性
	开启（供应）
	关闭（供应）
	处于双稳定推控制的位置
	双稳推控制的输出位置
	注意事项：有触电事故的风险
	注意：热表面
	注意：危险风险
	警告：激光辐射
	注意事项：ESD敏感部件

Chapter 2 Safety



WARNING



The laser module is a class 2 laser. Although no protective eyewear is required around class 2 lasers, you should not look directly into the beam or into scattered light.



ATTENTION



To avoid contamination and damage, never touch the $\lambda/2$ plates with bare fingers. Wear protective gloves.

第三章描述

密码学，即信息和数据的加密，一直是通信领域的一个基本课题。几个世纪以来，为了防止第三方解密，人们发展出了各种各样不同的方法。然而，所有的加密方法都有弱点：没有一种方法被认为是完全安全的。利用量子物理提出了加密方法，可以保证安全的安全性。本工具包讨论了将一次性的垫式加密方法与量子密钥分发方法相结合的BB84协议。

一次性pad方法使用0和1的随机二进制序列，构成了一个完美的数据传输密钥。将此密钥添加到预期的二进制消息中，加密消息也成为0和1的随机序列。使用密钥解码加密的消息，在解密前返回原始消息。只有当发送方（“Alice”）和收件人（“Bob”）知道密钥时，加密的消息才能被安全地公开传输。如果没有缺少的键，拦截是没有意义的，因为该键背后没有方法或模式。

这种加密方法的基本挑战是确保只有Alice和Bob知道加密密钥。BB84加密协议是专门为此目的而开发的。本协议描述了如何生成只有Alice和Bob才知道的加密密钥。这种方法的一个主要优点是，BB84协议本质上能够检测到第三方的拦截攻击，这被称为“Eve”（用于窃听）。

BB84协议的功能是定义两个基，每个基包含两个光偏振：+基由 0° 和 90° 偏振组成，x基由 -45° 和 45° 偏振组成。在这个方案中，任何一个基都可以用来表示一个二进制0（ 0° 或 -45° ）和一个二进制1（ 90° 或 45° ）。Alice以随机基础发送一个随机位，Bob以随机基础测量。然后，他们通过一个公共渠道来交换基础。如果它们各自使用了不同的基值，则测量将被丢弃；如果基值相同，则两者现在都生成了一个关键位。由于公开交换只包含基础，所以其他人不知道这个比特。如果伊芙试图干预爱丽丝和鲍勃之间，她也只能猜测每一点的基础。因为基础猜测是随机的，所以在50%的情况下会选择错误的基础，这会自动导致Alice和Bob可以通过交换一些测试位检测到错误。

该协议的量子物理方面依赖于使用单个光子光源来携带信息，这样，单个信息位只由一个处于特定状态的光子携带，因此不能被复制。量子光学过程也可以用来产生随机数。由于量子物理学在密钥生成中“只”起作用，因此“量子密码学”这个术语不如“量子密钥分配（QKD）”常用。

这个教育实验模拟了量子密码学中使用的关键原理。还进行了一次拦截攻击，并证明了它可以被探测到。实验从Alice和Bob开始，他们随机选择碱基，然后通过比较碱基生成一个密钥。Alice编码并发送消息，Bob接收并解码它。然后Eve加入到装置中，实验

反复的爱丽丝发送了一点，伊芙试图拦截它，然后伊芙发送了一点给鲍勃，在她选择了她的测量的基础上。在实验结束时，Alice和Bob通过公开交流和一些测试位来比较他们的基础。如果他们发现大约25%的测试位现在是不正确的(由发送的位中的错误造成的)

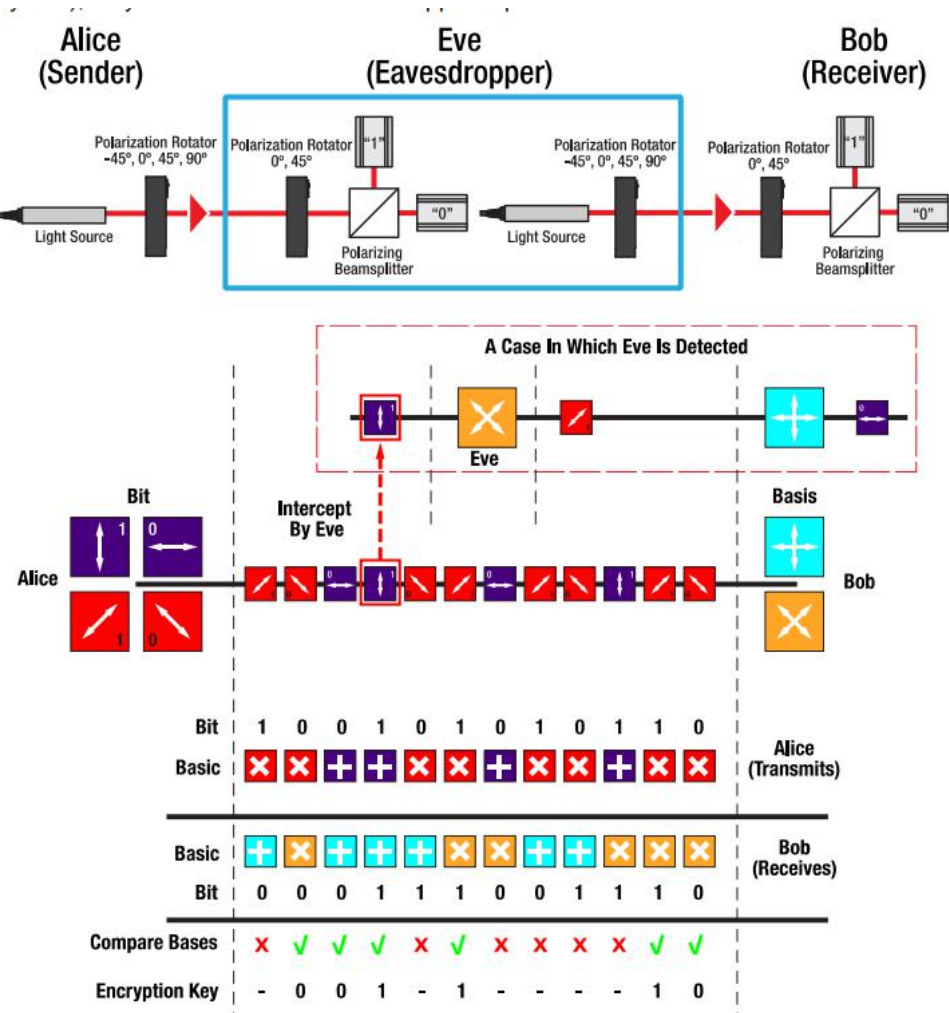


Figure 1量子密码学的建立与实验概述

这个实验使用的是脉冲激光器，而不是单个的光子。因此，所有的结果都可以纯粹通过经典的物理学来描述。量子物理装置可以与单个光子一起工作，但它的功能是完全相同的。因此，这种设置非常适合进行类似的实验。

第四章零部件清单


如果公制和英制套件包含具有不同项目编号的零件，除非另有说明，否则公制零件编号和测量值将用括号表示。

 <p>1 x MB8 (MB2020/M) 铝制面包板8 “x8” (20 cm x 20 cm)</p>	 <p>1 x MB810 (MB2020/M) 铝板 8” x 10” (20 cm x 25 cm)</p>	 <p>1 x MB1218 (MB3045/M) 铝板 12” x 18” (30 cm x 45 cm)</p>
 <p>3 x RDF1 橡胶阻尼脚 (4包)</p>	 <p>10 x BA1 (/M) 底座, 1英寸x3英寸x3/8英寸 (25 mm x 75 mm x 10 mm)</p>	 <p>5x PH2 (PH50/M) Ø1/2英寸 (Ø12.7mm) 柱架, 2英寸 (50 mm) 长</p>
 <p>6 x PH1.5 (PH40/M) Ø1/2 “ (Ø12.7mm) 柱架, 1.5英寸 (40毫米) 长</p>	 <p>UPH2 (UPH50/M) .7Ø1/2 “ (Ø12 mm) 通用撑柱架, 2英寸 (50 mm) 长</p>	 <p>帝国: 6 x TR1.5 公制: 4 x TR30/M, 2 x TR40/M Ø1/2 “ (Ø12.7mm) 柱, 长1.5” (30 mm, 40mm) 长</p>


 <p>7 x TR2 (TR50/M) 0 1/2英寸 (12.7mm) 阀柱 ， 2英寸 (50 mm) 长</p>		 <p>2xRSP1X225 (/M) -爱丽丝 01 “索引旋转 安装, 22.5° 步</p>	 <p>2 x RSP1X225 (/M) -BOB 01 “索引旋转 安装, 22.5° 步骤</p>
 <p>4 x WPH10E-633入 /2板, 零阶</p>		 <p>2x运动学安装修改后的 KM100PM (/M)</p>	 <p>2 x PM3 (/M) 夹臂</p>
 <p>2 x PBS201 偏振振幅器立方体, 20 mm x 20 mm</p>		 <p>2 x KM100运动 学安装装置, 01 “</p>	 <p>2 x AD11NT 01 “适配器 组件</p>

 <p>2 x CPS635R-C2 635 nm激光二极管模块，2级</p>	 <p>1 x BA1S(/M) 基础 1" x 2.3" x 3/8" (25 mm x 58 mm x 10 mm)</p>	 <p>1 x AT1(/M) 对齐工具 1.18" x 1.18" (30.0 mm x 30 mm).0</p>
 <p>2 x CL3/M 夹住</p>	 <p>1个BBH和1个面 包板把手</p>	 <p>1 x SPW606 SM1扳手， 长度=1"</p>
 <p>4个传感器</p>	 <p>2x传感器电子</p>	 <p>2倍激光电子</p>

帝国套件螺丝钉，球驱动器，和六角键

类型	数量	类型	数量
1/4英寸-20x3/8英寸帽螺钉	11	1/4英寸垫圈	19
1/4英寸-20x1/2英寸帽螺钉	12	 1个BD-3/16L球刀， 用于1/4" -20个螺钉	
1/4英寸-20x5/8英寸的帽螺钉	17		
1/4英寸-20x1.25英寸的螺帽螺钉	2		
1/4英寸-20x2英寸的帽螺钉	2		
十六进制键：9/64” ， 5月64” 和1月16”			
4 x AS4M8E： 螺纹适配器（内部M4 x 0.7，外部8-32螺纹螺柱）			

公制套件螺丝钉，球驱动器，和十六角键

类型	数量	类型	数量
M6 x 10 mm螺帽螺钉	11	M6垫圈	19
M6 x 12 mm螺帽螺钉	12	 1 x BD-5ML 用于M6螺钉的滚轴驱动器	
M6 x 16 mm带帽螺钉	17		
M6 x 30 mm带帽螺钉	2		
M6 x 45 mm的阀盖螺钉	2		
十六角制键：3毫米，2毫米和1.5毫米			

第五章量子密码学的基础

本节解释量子密码学是如何工作的以及执行它所需的步骤。它以一个简短的介绍开始，然后解释了将消息和密钥转换为加密消息的一次性记事本。接下来是密钥的生成，这构成了量子密码学的基本要素。

量子密码学的价值在于其不被拦截的安全性。第5.4节讨论了如何使用这种方法来检测到窃听者。

. 1. 5介绍

密码学描述了数据的加密：也就是说，使消息无法识别，理想情况下，使它只对发送者和收件人可读。这意味着加密的消息只有在要解码它的密钥已知时才有意义。密钥的安全性要么基于复杂的底层算法，要么基于实际的约束条件，如大量数字的因数分解。

所有经典的密码学方法都有一个缺点，即人们永远不能确定密钥最终不会被“破解”。然而，这个基本问题可以用量子物理学来解决。控制量子物理学的核心规则之一是，同时观察一个光子或粒子的状态会导致状态的变化。这一原则，以及真正的随机数生成，允许用户生成只有发送者和接收人知道的随机密钥。作为一个附加的特性，任何试图进行拦截的尝试在理论上都可以被识别出来。

目前已经有一些使用量子密码学的加密系统的例子。这些系统现在已经上市了，例如在<http://www.idquantique.com/量子安全加密/>

5. 2. 一次性垫

一次性垫，也称为一次性密钥，是一种加密方法，只要完全满足所有要求，原则上是100%安全。量子物理学仅仅是帮助满足这些要求，而该方法本身是一种经典的加密技术。

想象一个加密密钥，它完全由一个完全随机的0和1序列组成，称为“位”。现在想象一下，这个信息也由0和1组成。可以对消息和加密密钥进行二进制加法，得到另一个0和1也是完全随机的链。这将导致被加密的消息。

适用于二元加法的“计算规则”如下：

- 0 + 0 = 0
- 1 + 0 = 1
- 0 + 1 = 1
- 1 + 1 = 0

当预期的收件人获得加密消息时，他们将在加密消息和加密密钥上使用二进制添加。然后，这将生成原始消息。

通过一个例子，我们可以对单词“Test”进行编码。每个字母都可以翻译成一个五位数的二进制代码，如下表所示（参见第9章，了解一个将字母字母转换为二进制代码的表）：

Word	T					E					S					T				
<div>↓</div>																				
Binary word	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
<div>+</div>																				
Key (random)	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
<div>↓</div>																				
Encrypted message	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0
<div>+</div>																				
Key (as above)	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
<div>↓</div>																				
Binary word	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
<div>↓</div>																				
Word	T					E					S					T				

如果加密的消息被截获，窃听者就需要该密钥来解码它。如果没有这个键，零和1的随机序列在转换为一个单词时就会产生完整的“胡言乱语”。这使得消息完全安全，不被拦截。

总结一下这些基本要求:

1. 关键必须至少和消息一样长。
2. 该密钥只能使用一次。
3. 钥匙必须是完全随机的。
4. 必须只有发件人和收件人知道该密钥。

发送方很容易满足要求1, 他们只能加密小于或等于可用密钥比特数的比特数。

要求2是发送者和接收方的责任, 也很容易实现。

要求3很难经过进一步的检查才能满足, 因为每个随机数生成器最终都是基于一个算法的。这意味着由计算机生成的随机数总是仅仅是“伪随机的”。然而, 量子物理学可以用来解决这个问题, 因为它使真正的随机性成为可能。这将在第5.5节中进行更详细的讨论。

需求4也有问题, 因为密钥的经典传输打开了拦截它的可能性。这个问题也可以用量子物理学来解决。下一小节将讨论该密钥的秘密分配的方法。

5.3.5 密钥分配

5.3.1. 入/2板和数据传输

本小节旨在通过以一个基础简要地运行传输数据的过程, 来促进更好地理解实验设置。实际的量子密码学(在现实世界中和在这个类比实验中)与两个基础一起工作, 这将在下一个小节中描述。

光子被用来传输“0”或“1”。在本例中, 使用偏振方向作为位: 具有水平偏振的光子被解释为“0”, 具有垂直偏振的光子被解释为“1”。

那么, 什么样的实验装置可以以这种方式传输数据呢? 图2中显示了一个示例。

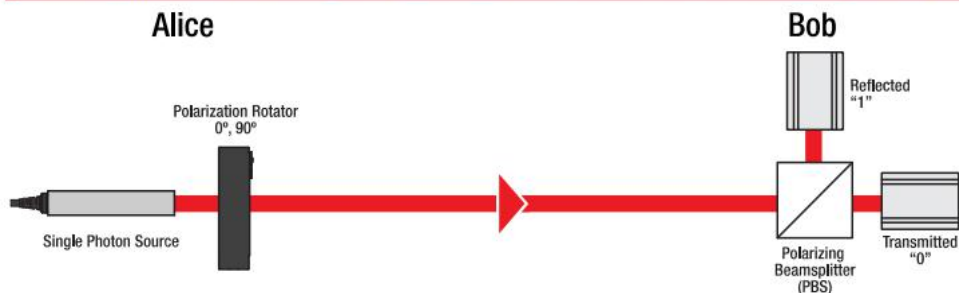


图2具有单极化基的数据传输

发送单元“Alice”由一个水平偏振的单个光子源和一个入/2板组成。

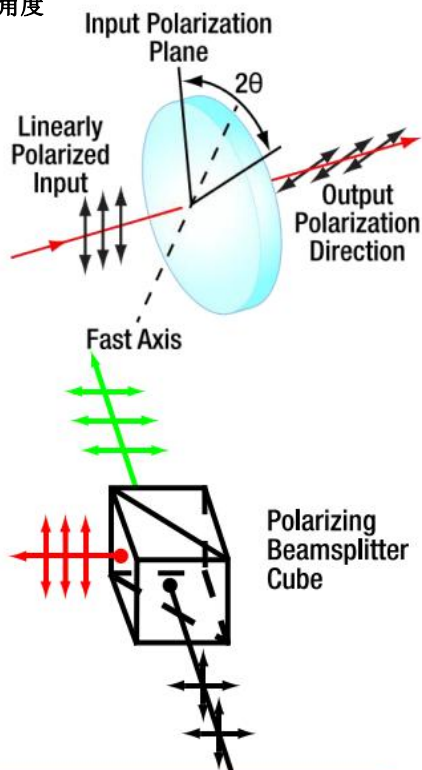
入/2板使入射光的偏振旋转加倍波板的物理旋转角。例如，当波板相对于入射偏振被物理旋转了 45° 时，光的偏振实际上被旋转了 90° 。这就是为什么入/2板也被称为“极化旋转器”。

当我们谈到“ 0° ”和“ 90° ”的设置时
从现在开始（后来的“ -45° ”和“ 45° ”），这个角度
总是指物体的旋转角度
极化和从不旋转的角度
入/2板。

一个描述入/2板如何操作的草图是
如图中的右侧所示。灯入射
波板被改变成极化
未与的快轴对齐的组件
双折射晶体是延迟的。线性
偏振光，结果是偏振光是
旋转的值是旋转的两倍
入/2板。

接收单元“Bob”由一个偏振器组成
分束器立方体和两个探测器。极化
分束器立方体反映了垂直极化
(90°)入射光的组件，而通过
水平极化(0°)分量，如图所示
在右边的图表中。

如果爱丽丝发送的光的偏振状态是
设置为 0° ，光子将通过
分束器（指定为事件“0”）。如果波
板被设置为旋转极化 90° ，该板
光子将被分束器反射
（指定为事件“1”）。



5.3.2. 密钥分配

虽然有一个基 (0° 或 90°) 的方法足以将数据从Alice传输到Bob, 但它不能保证不被拦截的安全。第二个基础是为了实现这一点。除了 0° 和 90° 的基础, 我们现在称之为“+基”之外, 还使用了 -45° 和 45° 的第二个基。从这里开始, 我们将称之为“x基”。

现在的设置如图3所示。这也是用于量子密码学 and 这个实验包的设置。

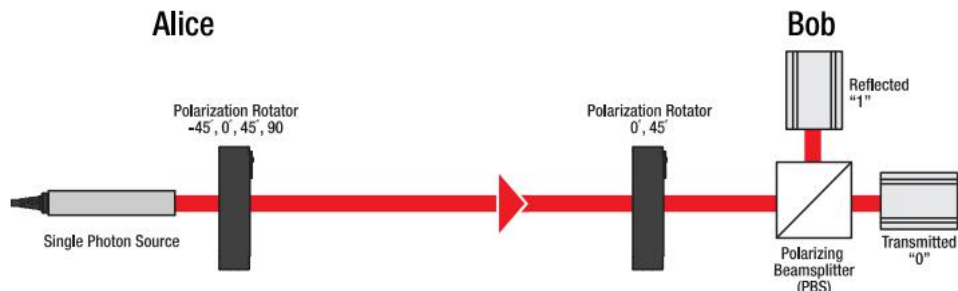


图3使用碱基+ (0° 和 90°) 和x (-45° 和 45°) 进行的量子密码学设置

现在, 爱丽丝必须为密钥的生成做出两个随机的决定:

爱丽丝必须随机选择她的碱基线, +或x

Alice必须选择一个随机位, 0或1

- o 使用+基选择0表示设置为 0°
- o 用+基选择1表示设置为 90°
- o 用x基选择0表示设置为 -45°
- o 用x基选择1表示设置为 45°

Bob设置他的偏振旋转器来区分+和x基。因此, Bob只需要设置 0° 和 45° 。

如果Bob选择了+基, Alice发送了+基, Bob得到一个明确的结果; 如果两者都选择x基, 这就适用。但如果鲍勃选择了一个和爱丽丝不同的基础呢? 选择一个不同于Alice的基的结果是, 45° 的偏振光将被发送到分束器。对于一个连续的光束, 一半被传输, 一半被反射。然而, 假设只有一个光子被发送, 两个探测器中只有一个可以响应。响应的探测器就有运气了。如果两个基不匹配, Bob将在两个探测器中的一个上测量信号。在两个探测器上探测到光子的概率分别为50%。

在下面的表中，不同的情况再次显示为概述：¹

艾丽斯			鲍勃				相同的 基础？
基础	比特	角度	基础	角度	探测器“0”	探测器“1”	
+	0	0°	+	0°	100%	0%	是
+	1	90°	+	0°	0%	100%	是
x	1	45°	+	0°	50%	50%	不
x	0	-45°	+	0°	50%	50%	不
+	0	0°	x	45°	50%	50%	不
+	1	90°	x	45°	50%	50%	不
x	1	45°	x	45°	0%	100%	是
x	0	-45°	x	45°	100%	0%	是

如果Alice发送一个由随机基中的随机比特组成的信号，而Bob使用随机基来分析信号——这又如何成为数据传输的关键呢？

答案是，Alice和Bob都会告诉对方以后使用哪个基来传输每个位。在表的最后三列中，只有当基数相同时，结果才会明确（100%）。

实际上，Alice和Bob将进行每个测量，并且只交流“+”或“x”。当两者不同时，两者都放弃了测量值。但如果两个碱基是相同的，那么两者都根据Bob’s探测器得到的结果知道传输了哪个比特。基础，而不是比特，总是被公开交流的。因此，加密密钥来自于Alice和Bob选择相同基础的测量。

一旦爱丽丝和Bob以这种方式完成了所有的测量，他们都拥有了（随机的）键。现在，Alice可以加密消息并在+的基础上发送它。Bob在+基础上接收消息，然后能够将其解密。

第5.4节扩展了该协议，并在该过程中引入了一个窃听者。同一练习的结果有很大不同的结果，这使得Alice和Bob可以检测到这个窃听者的存在。

¹ 如果在这个实验的其他实现中可以发现该表的轻微变化，这可能是由入射激光器的不同偏振引起的。如果它是垂直的，那么0°（Alice）和0°（Bob）构成一个数字1。

4. 5. 发现了一个窃听器

让我们来研究一下窃听器在爱丽丝和鲍勃之间的情况。Eve由与Alice和Bob相同的组件组成，只是在相反的顺序中。这一点如图4所示。

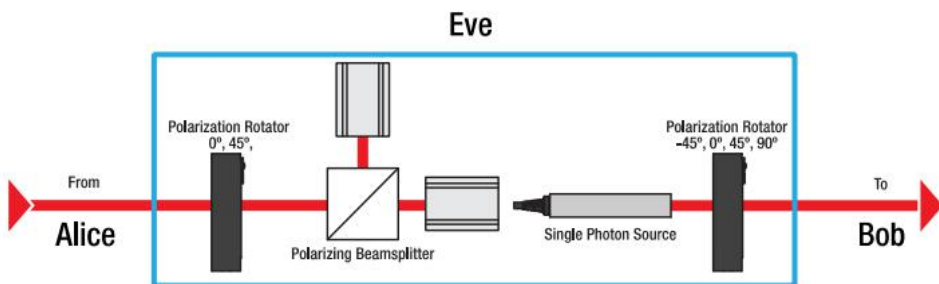


Figure 4在爱丽丝和鲍勃之间的窃听器夏娃

伊芙被放置在一个位置上，来测量来自爱丽丝的光，然后试图将相同的信息传递给鲍勃。请考虑以下两种可能性：

- 夏娃 挑选 那 同一的 基础 作为 爱丽丝：在这种情况下，Eve测量了爱丽丝正确发送的信号。因此，Eve将以最初由Alice发送的相同的基础，将正确的结果传递给Bob。现在鲍勃随机选择了他的基础，再次有两种可能性：
 - 鲍勃 挑选 那 同一的 基础 作为 爱丽丝：伊芙用同样的基础正确地传输了信号。因此，鲍勃在没有检测到Eve的存在的情况下，得到了爱丽丝发送的极化状态是准确的。
 - 鲍勃 挑选 那 其他的 基础：接收信号的基础与Eve传输的信号的基础不同。因此，他的一个探测器会随机响应。然而，当Alice和Bob现在比较他们的基时（结果与前面的小节相同），由于Alice和Bob使用的基不同，这种测量还是被丢弃了。
- 夏娃 挑选 那 错误的 基础：在这种情况下，夏娃选择了一个不同于爱丽丝使用的基础，并且夏娃的一个探测器会随机响应。因此，伊芙无法判断她是否选择了正确的依据。当伊芙向鲍勃发送她的信号时，她会以与她收到爱丽丝的信号相同的方式发送这个比特。

因为鲍勃也在随机选择他的基础，所以有两种可能性：

- 鲍勃 挑选 a 有差别的 基础 比 Alice：在Alice和Bob比较了基础之后，这个测量值就被丢弃了。

- o 鲍勃 挑选 那 同一的 基础 作为 爱丽丝：这个案例产生了一个错误，它允许爱丽丝和鲍勃检测到夏娃的窃听。请记住，Alice和Bob已经确认他们使用相同的基础发送和接收信号，所以测量不会被丢弃。然而，伊芙的窃听方式是不同的。这意味着发生了两次随机检测：伊芙拦截到爱丽丝的信号（因为她的基础与爱丽丝的不匹配），鲍勃接收到拦截到的信号（因为他的基础与伊芙的不匹配）。

在一半的情况下，正确的检测器会响应Bob，以便他接收到Alice发送的相同位。但在另一半的情况下，另一个探测器将探测到光子。因此，Bob获得的位与Alice发送的位不同。

总而言之：这意味着Alice和Bob用相同的基获得不同的位（如果没有第三方干扰就不可能发生）。因此，对间谍的测试很简单。在Alice和Bob比较了基之后，他们选择了一定数量的具有匹配基的位来进行公开比较。如果这些测试位是相同的，那么在系统中就没有窃听者。²但是，如果在大约25%的比较位中发现了错误，那么通信就会被拦截。

虽然Eve似乎只有在窃听后才发现，但事实并非如此，因为到目前为止只生成了一个测试加密密钥。即使Eve在窃听（因此拦截了一定数量的比特而未被检测到），这也是无关紧要的，因为没有任何实际消息的一部分已经被编码或传输。

个别案例再次在表格中简要进行概述。这里只考虑了Alice和Bob使用相同的碱基的情况。其余的测量值在基础比较过程中被丢弃。³

使用基础 爱丽丝和鲍勃	夏娃使用的 基础	错误？	爱丽丝和鲍勃 的匹配
+ +	+	不	100%
+ +	x	部分	50%
x x	+	部分	50%
x x	x	不	100%

² 从统计学上讲，所有的测试位都有可能是随机正确的。因此，比特的样本大小必须足够大，以确保结果具有统计学意义。

³ ~~25%的错误率可以从表中计算出来。如果Alice和Bob选择了+基，那么Eve也在50%的情况下选择了+基，这是无法检测到的。但在50%的情况下，她选择了x基。此外，在50%的情况下，正确的检测器由于与错误的信号传输相关的随机机会而作出响应。因此，总错误率为50% x 50% = 25%。~~

. 5. 5. “随机”是什么意思？

如第5.2节所述，一次性衬垫需要完全随机地选择加密密钥。这意味着计算机生成的伪随机数并不是一个具有100%安全性的解决方案。然而，量子物理学为真正的随机性提供了许多可能性。例如，一个光子击中一个50：50的非偏振分光器，就会被完全随机地传输或反射。一半被透射，另一半被平均反射，但单个光子的“决定”是完全随机的。虽然这一特殊的原理适用于光子，但许多其他过程，如放射性衰变也是完全随机的。

在实践中，我们可以将由分束器反射的光子解释为二进制0，将通过分束器传输的光子解释为二进制1。在传统的光在一个分束器后入射到两个单个光电探测器上的情况下，如果探测器上的强度相同，那么探测器上的撞击分布也可以被认为是完全随机的。

特别是，量子物理随机数生成器是量子密码学数据网络的一个关键组成部分。一些商业上可用的选择已经存在：<http://www.idquantique>. 随机数生成.

. 6. 5是什么阻止了一个人简单地复制这些信息？

考虑一下Eve可以简单地复制携带信息的光子的场景。在这种情况下，量子密码学的安全性将被消灭，因为她可以将原始光子发送给Bob，并对复制的光子进行测量。然后，伊芙可以在没有爱丽丝和鲍勃检测到窃听的情况下拦截关键部分。

然而，对量子物理状态的确切复制实际上是不可能的。这个原理被称为“无克隆定理”，在1982年提出并证明。一般来说，这个定理表明，量子态不能不改变其状态就被精确地复制。因此，Eve不能在不改变爱丽丝的情况下从它身上复制一个光子，也不能将一个未改变的光子发送给Bob，同时保留一个副本以供分析。

. 7. 5实验程序

本实验的步骤序列来自于BB84协议。你可以在这里找到最初的出版物：

[http://researcher.沃森.ibm.com/researcher/files/us-bennetc/BB84highest.pdf](http://researcher.ibm.com/researcher/files/us-bennetc/BB84highest.pdf)BB84协议实验的顺序为：

1. 密钥传输	<p>Alice选择一个随机的基（x或+）和一点（0或1）。然后Bob随机选择他的碱基（x或+）。两者都相应地设置了波板。然后光子通过装置发送（与我们一起，激光脉冲）。</p> <p>鲍勃注意到他测量的是0还是1。</p> <p>请多次重复此步骤。</p>
2. 擦除错误的基础	<p>爱丽丝和鲍勃检查了他们的测量，并告诉对方他们选择了哪些基地。当爱丽丝和鲍勃使用的碱基相同时，它们保持位的测量。序列中任何其他的全将被丢弃。</p> <p>注意：只有基础在Alice和Bob之间进行交流（这甚至可以公开完成）。</p> <p>经过比较后，剩下的比特就成为了Alice和Bob之间的秘密加密密钥。</p>
3. 测试间谍	<p>Alice和Bob在第2步中公开比较了传输位的一个样本。如果存在错误，这将确认间谍的存在，并且密钥将被删除。</p> <p>但是，如果没有检测到窃听器，则测试位将被删除，其余的位是最终的加密密钥。</p>
4. 加密消息	<p>使用步骤3中生成的密钥，Alice可以对消息进行加密。</p>
5. 发送消息	<p>Alice将加密的消息发送给Bob。这是公开的。</p>
6. 解密消息	<p>Bob在生成的加密密钥的帮助下解密消息。</p>

协议中还有其他步骤，在本实验中没有实现：

身份验证：在通信开始时，根据Alice和Bob预先建立的密钥交换一些位。这一步允许Alice验证她是在与Bob交流，而不是其他人。

如果没有任何错误发生，那么这将确认在一开始的这一行中没有窃听者。完成这一步的一种方法是从以前的通信中保存几位，以便在下次通信中进行身份验证。

纠错：由于没有一个系统是完美的，测量误差总是发生，因此使用某些算法进行纠错。这些算法在这里不被讨论，因为它不在实验的范围之内。

5.8. 经典光与单光子

这个类似的实验和真正的量子密码学设置之间的一个主要区别是，只有使用单一光子源，才能保证真正的拦截安全。这意味着一个比特的信息必须只通过一个光子来传输，因为根据第5.6节，它不能在不改变的情况下被复制或测量。

如果使用任何经典的光源（即使是减弱的激光器）来代替单一的光子源，那么Eve就无法被探测到。窃听所需要的只是Eve分离透射光的一部分进行检测/分析，同时将其余的部分发送给Bob。

因为这个工具包中详细的实验使用脉冲光源（仍然不是单一的光子源），它不能真正作为一个完美的加密系统。然而，该协议的序列与真正的量子加密系统完全相同。

5.9. 纠缠

关于量子密码学和量子纠缠之间的关系，经常会出现一个问题。值得注意的是，BB84协议并不需要偏振纠缠光子。在认识到1984年之后发表的第一批关于具有纠缠光子的量子密码学的论文后，这一点就变得清晰起来了。供参考：

- A. K. Ekert, 物理学。发动机的旋转拉脱维亚的67, 661 (1991)
- C. H. 贝内特, G. 布拉萨德, N. D. Mermin, 物理学。发动机的旋转拉脱维亚的68, 557 (1992)

此外，量子密码学的领域是非常动态的，并且已经看到了实质性的改进和引入了新的协议。这些都更复杂，但不需要单个光子。这些就是所谓的“诱饵状态”。以供参考：

- W. -Y. 黄, 物理学家。发动机的旋转拉脱维亚的91, 057901 (2003)
- H. -K. Lo, X. 妈妈. K. 陈, 物理学家。发动机的旋转拉脱维亚的94, 230504 (2005)

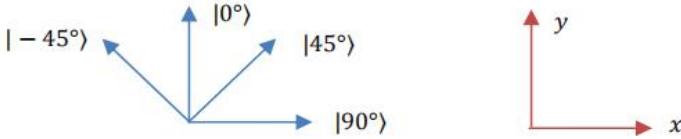
. 10. 5. 狄拉克符号中的数学描述

在这里，我们定性地描述了实验。Bob（和Eve）对偏振态的制备和测量是实验实现的综合部分。然而，每个物理理论都需要一个数学描述。下面，我们将实验转换为公式。

首先必须找到一个合适的符号。对于极化态，狄拉克的胸罩符号是一个优雅的选择。本实验中的四种极化态被表示为

$$|-45^\circ\rangle, |0^\circ\rangle, |45^\circ\rangle, |90^\circ\rangle \quad (1)$$

其中， $|0^\circ\rangle$ 和 $|90^\circ\rangle$ 为z基的基态， $|-45^\circ\rangle$ 和 $|45^\circ\rangle$ 为x基的基态。狄拉克符号的优雅之处在于，即使没有选择任何明显的坐标系，一种状态也可以被表示和处理。



当选择了一个坐标系时（在右边， Xy ），状态可以用向量形式写为

$$|0^\circ\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |90^\circ\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (2)$$

一个重要的数学工具是标量积，它以以下方法执行⁴

$$\langle 90^\circ | 0^\circ \rangle = (1 \ 0) \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = 0 \quad (3)$$

标量积的平方绝对值 $|\langle 90^\circ | 0^\circ \rangle|^2$ 是一个描述性的量，它表示一个 0° 的偏振光子通过一个面向 90° 方向的偏振器的概率。当然，这个概率为0，这与方程(3)一致。

这些状态也可以表示为线性组合，例如，

$$|45^\circ\rangle = a \cdot |0^\circ\rangle + F \cdot |90^\circ\rangle \quad (4)$$

由于标量积必须被归一化，所以它表明

$$1 \stackrel{!}{=} |\langle 45^\circ | 45^\circ \rangle|^2 = \alpha^* \alpha \underbrace{\langle 0^\circ | 0^\circ \rangle}_{=1} + \alpha^* \beta \underbrace{\langle 0^\circ | 90^\circ \rangle}_{=0} + \alpha \beta^* \underbrace{\langle 90^\circ | 0^\circ \rangle}_{=0} + \beta \beta^* \underbrace{\langle 90^\circ | 90^\circ \rangle}_{=1} = |\alpha|^2 + |\beta|^2 \quad (5)$$

⁴ 确切地说： $\langle a | b \rangle = \langle a | b \rangle^* = \langle b | a \rangle$ 是 a 的复共轭物。

由于对称性，它可以得出一个 $F=1/\sqrt{2}$ 。因此，所有这四种状态都可以表示为：

$$\begin{aligned} |45^\circ\rangle &= \frac{1}{\sqrt{2}} |0^\circ\rangle + \frac{1}{\sqrt{2}} |90^\circ\rangle \\ |-45^\circ\rangle &= \frac{1}{\sqrt{2}} |0^\circ\rangle - \frac{1}{\sqrt{2}} |90^\circ\rangle \\ |0^\circ\rangle &= \frac{1}{\sqrt{2}} |45^\circ\rangle + \frac{1}{\sqrt{2}} |-45^\circ\rangle \\ |90^\circ\rangle &= \frac{1}{\sqrt{2}} |45^\circ\rangle - \frac{1}{\sqrt{2}} |-45^\circ\rangle \end{aligned} \quad (6)$$

也可以选择一个向量表示法，e. g., $|\pm 45^\circ\rangle = (\pm 1/\sqrt{2}, \mp 1/\sqrt{2})^T$ 。现在可以计算出一个 0° 偏振光子通过一个 45° 定向偏振器的概率：

$$|\langle 45^\circ | 0^\circ \rangle|^2 = \left| \frac{1}{\sqrt{2}} \underbrace{\langle 45^\circ | 45^\circ \rangle}_{=1} + \frac{1}{\sqrt{2}} \underbrace{\langle 45^\circ | -45^\circ \rangle}_{=0} \right|^2 = \frac{1}{2} \quad (7)$$

这意味着一个 0° 偏振光子通过一个 45° 定向偏振器的概率为50%。

然而，在实验中，Bob和Eve只决定作为一个基础来测量（+或x），并观察哪个探测器的反应。问题是如何用数学方法来表达这一点。为了做到这一点，操作员 \hat{M}_+ 和 \hat{M}_x 在一个或另一个基础上描述一个测量。

$$\begin{aligned} \hat{M}_+ &= |0^\circ\rangle\langle 0^\circ| - |90^\circ\rangle\langle 90^\circ| \\ \hat{M}_x &= |45^\circ\rangle\langle 45^\circ| - |-45^\circ\rangle\langle -45^\circ| \end{aligned} \quad (8)$$

首先，+基的算符作用于垂直和水平极化状态：

$$\begin{aligned} \hat{M}_+ |0^\circ\rangle &= |0^\circ\rangle\langle 0^\circ|0^\circ\rangle - |90^\circ\rangle\langle 90^\circ|0^\circ\rangle = |0^\circ\rangle - |90^\circ\rangle \cdot 0 = |0^\circ\rangle \\ \hat{M}_+ |90^\circ\rangle &= |0^\circ\rangle\langle 0^\circ|90^\circ\rangle - |90^\circ\rangle\langle 90^\circ|90^\circ\rangle = |0^\circ\rangle \cdot 0 - |90^\circ\rangle = -|90^\circ\rangle \end{aligned} \quad (9)$$

结果并不太令人惊讶——当在+基础中测量垂直或水平状态时，我们会检索到状态本身。注意，可观察到的 \hat{M}_+ 是要测量的量，而特征向量（即 $|0^\circ\rangle$ ， $|90^\circ\rangle$ ）是系统的可能状态。

⁵特征值（即 ± 1 ）表示测量的可能结果。在这里，+1对应于光子的透射，而-1对应于反射（反过来，这可以解释为由于反射而发生的相位跳跃）。

⁵提醒：当方程 $\hat{M}|x\rangle = x|x\rangle$ 对于一个状态 $|x\rangle$ 和一个算子成立时，我们称 $|x\rangle$ 为具有特征值 x 的算子的特征向量。

当在对角线基上测量时，对角线极化状态表现出相应的行为：

$$\begin{aligned}\hat{M}_x |45^\circ\rangle &= |45^\circ\rangle\langle 45^\circ|45^\circ\rangle - |-45^\circ\rangle\langle -45^\circ|45^\circ\rangle = |45^\circ\rangle \\ \hat{M}_x |-45^\circ\rangle &= |45^\circ\rangle\langle 45^\circ|-45^\circ\rangle - |-45^\circ\rangle\langle -45^\circ|-45^\circ\rangle = -|-45^\circ\rangle\end{aligned}\quad (10)$$

特征值-1并不对应于我们的设置中的反射（因为状态 $|-45^\circ\rangle$ 对应于传输，因此，位0）。这可以通过注意来理解，我们不是在对角线基上倾斜分束器，而是通过接收单元上的入/2波板旋转入射极化。

然而，当一个在+基上测量的 45° 偏振光子时，会发生什么呢？在式(7)中表明，该光子通过 0° 偏振器的传输概率可以计算为50%。计算状态得到 $|0^\circ\rangle$ 和 $|90^\circ\rangle$ 状态的叠加：

$$\begin{aligned}\hat{M}_+ |45^\circ\rangle &= |0^\circ\rangle\langle 0^\circ|\left(\frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle\right) - |90^\circ\rangle\langle 90^\circ|\left(\frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle\right) \\ &= \frac{1}{\sqrt{2}}|0^\circ\rangle\langle 0^\circ|0^\circ\rangle + \frac{1}{\sqrt{2}}|0^\circ\rangle\langle 0^\circ|90^\circ\rangle - \frac{1}{\sqrt{2}}|90^\circ\rangle\langle 90^\circ|0^\circ\rangle \\ &\quad - \frac{1}{\sqrt{2}}|90^\circ\rangle\langle 90^\circ|90^\circ\rangle = \frac{1}{\sqrt{2}}|0^\circ\rangle - \frac{1}{\sqrt{2}}|90^\circ\rangle \\ \hat{M}_+ |-45^\circ\rangle &= \frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle\end{aligned}\quad (11)$$

同样，在对角线基上测量垂直或水平偏振光子可以得到：

$$\begin{aligned}\hat{M}_x |0^\circ\rangle &= \frac{1}{\sqrt{2}}|45^\circ\rangle - \frac{1}{\sqrt{2}}|-45^\circ\rangle \\ \hat{M}_x |90^\circ\rangle &= \frac{1}{\sqrt{2}}|45^\circ\rangle + \frac{1}{\sqrt{2}}|-45^\circ\rangle\end{aligned}\quad (12)$$

现在我们知道了光子态是如何变化的了。下面，我们可以用数学方法描述Alice、Bob和Eve的测量和状态，如前面的描述。⁶我们从一张桌子开始，描述了没有夏娃的情况。然后，显示一个显示包括Eve在内的描述的表。

⁶请注意，所有的计算也可以在向量表示中执行。该表的代表人数如上所述。算子的表示形式是矩阵，即 $\hat{M}_+ = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ 和 $\hat{M}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ 。

艾丽斯		鲍勃		
状态	基础, 比特	选择的 基础	状态	测量位
$ 0^\circ\rangle$	+, 0	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$	0
		×	$\hat{M}_\times \frac{1}{\sqrt{2}} 0^\circ\rangle_- = 45^\circ\rangle_- - -45^\circ\rangle \frac{1}{\sqrt{2}}$	0或1
$ 90^\circ\rangle$	+, 1	+	$\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	1
		×	$\hat{M}_\times \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} 90^\circ\rangle_- = 45^\circ\rangle_- + -45^\circ\rangle$	0或1
$ 45^\circ\rangle$	×, 1	+	$\hat{M}_+ 45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle \frac{1}{\sqrt{2}} 90^\circ\rangle$	0或1
		×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$	1
$ -45^\circ\rangle$	×, 0	+	$\hat{M}_+ -45^\circ\rangle = - 0^\circ\rangle_- + 90^\circ\rangle \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}}$	0或1
		×	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	0

Alice & Bob相同的→位可以作为关键位

Alice & Bob不相同的→测量的基础被丢弃

艾丽斯		夏娃			鲍勃		
基础 ， 位	状态	基础	状态	状态 已发送	基础	状态	测量位
+, 0	$ 0^\circ\rangle$	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$	$ 0^\circ\rangle$	+	$\hat{M}_+ 0^\circ\rangle = 0^\circ\rangle$	0
		×	$\hat{M}_\times 0^\circ\rangle = \frac{ 45^\circ\rangle -45^\circ\rangle}{\sqrt{2}\sqrt{2}}$	$ 45^\circ\rangle$ 或 $ - 45^\circ\rangle$	×	$\hat{M}_\times\frac{1}{\sqrt{2}} 0^\circ\rangle = 45^\circ\rangle - -45^\circ\rangle\frac{1}{\sqrt{2}}$	0或1
		×	$\hat{M}_\times 0^\circ\rangle = \frac{ 45^\circ\rangle -45^\circ\rangle}{\sqrt{2}\sqrt{2}}$	$ 45^\circ\rangle$ 或 $ - 45^\circ\rangle$	+	$\hat{M}_+\frac{1}{\sqrt{2}\sqrt{2}} 45^\circ\rangle = 0^\circ\rangle - 90^\circ\rangle$ 或 $\hat{M}_+ -45^\circ\rangle = 0^\circ\rangle + 90^\circ\rangle\frac{1}{\sqrt{2}\sqrt{2}}$	<div>0 或 1</div> <div>0 或 1</div>
		×	$\hat{M}_\times 45^\circ\text{ Subur} = 45^\circ\text{ Suburb}$ 或 $\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$		×	$\hat{M}_\times 45^\circ\text{ Subur} = 45^\circ\text{ Suburb}$ 或 $\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	1 0
+, 1	$ 90^\circ\rangle$	+	$\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	$ 90^\circ\rangle$	+	$\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	1
		×	$\hat{M}_\times 90^\circ\rangle = \frac{ 45^\circ\rangle -45^\circ\rangle}{\sqrt{2}\sqrt{2}}$	$ 45^\circ\rangle$ 或 $ - 45^\circ\rangle$	×	$\hat{M}_\times\frac{1}{\sqrt{2}\sqrt{2}} 90^\circ\rangle = 45^\circ\rangle + -45^\circ\rangle$	0或1
		×	$\hat{M}_\times 90^\circ\rangle = \frac{ 45^\circ\rangle -45^\circ\rangle}{\sqrt{2}\sqrt{2}}$	$ 45^\circ\rangle$ 或 $ - 45^\circ\rangle$	+	$\hat{M}_+\frac{1}{\sqrt{2}\sqrt{2}} 45^\circ\rangle = 0^\circ\rangle - 90^\circ\rangle$ 或 $\hat{M}_+ -45^\circ\rangle = 0^\circ\rangle + 90^\circ\rangle\frac{1}{\sqrt{2}\sqrt{2}}$	<div>1 或 0</div> <div>1 或 0</div>
		×	$\hat{M}_\times 45^\circ\text{ Subur} = 45^\circ\text{ Suburb}$ 或 $\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$		×	$\hat{M}_\times 45^\circ\text{ Subur} = 45^\circ\text{ Suburb}$ 或 $\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	1 0
×, 1	$ 45^\circ\rangle$	+	$\hat{M}_+ 45^\circ\rangle = -\frac{ 0^\circ\rangle 90^\circ\rangle}{\sqrt{2}\sqrt{2}}$	$ 0^\circ\rangle$ 或 $ 90^\circ\rangle$	+	$\hat{M}_+ 0^\circ\text{ Subur} = 0^\circ\text{ Suburb}$ 或 $\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	0 1
		×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$	$ 45^\circ\rangle$	×	$\hat{M}_\times\frac{1}{\sqrt{2}\sqrt{2}} 0^\circ\rangle = 45^\circ\rangle - -45^\circ\rangle$ 或 $\hat{M}_\times\frac{1}{\sqrt{2}\sqrt{2}} 90^\circ\rangle = 45^\circ\rangle + -45^\circ\rangle$	<div>1 或 0</div> <div>1 或 0</div>
		×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$	$ 45^\circ\rangle$	+	$\hat{M}_+ 45^\circ\rangle = 0^\circ\rangle - 90^\circ\rangle\frac{1}{\sqrt{2}\sqrt{2}}$	0或1
		×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$		×	$\hat{M}_\times 45^\circ\rangle = 45^\circ\rangle$	1
×, 0	$ -45^\circ\rangle$	+	$\hat{M}_+ -45^\circ\rangle = +\frac{ 0^\circ\rangle 90^\circ\rangle}{\sqrt{2}\sqrt{2}}$	$ 0^\circ\rangle$ 或 $ 90^\circ\rangle$	+	$\hat{M}_+ 0^\circ\text{ Subur} = 0^\circ\text{ Suburb}$ 或 $\hat{M}_+ 90^\circ\rangle = - 90^\circ\rangle$	0 1
		×	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	$ - 45^\circ\rangle$	×	$\hat{M}_\times\frac{1}{\sqrt{2}\sqrt{2}} 0^\circ\rangle = 45^\circ\rangle - -45^\circ\rangle$ 或 $\hat{M}_\times\frac{1}{\sqrt{2}\sqrt{2}} 90^\circ\rangle = 45^\circ\rangle + -45^\circ\rangle$	<div>0 或 1</div> <div>0 或 1</div>
		×	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	$ - 45^\circ\rangle$	+	$\hat{M}_+ -45^\circ\rangle = 0^\circ\rangle + 90^\circ\rangle\frac{1}{\sqrt{2}\sqrt{2}}$	0或1
		×	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$		×	$\hat{M}_\times -45^\circ\rangle = - -45^\circ\rangle$	0



爱丽丝和鲍勃和夏娃的基地相同的→Eve没有被注意到



爱丽丝和鲍勃的基础不相同的→测量被丢弃，无论如何，爱丽丝和鲍勃的基础相同；



比特偶然是相同的，夏娃没有注意到爱丽丝和鲍勃的基础相同；比特偶然不同的→Eve



被发现

第6章示例

6. 1. 没有Eve的加密协议（两个字母）

第一步：爱丽丝和鲍勃随机选择他们的基地，爱丽丝也选择她的位Alice

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
比特	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

鲍勃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
比特																		

第二步： Alice在选择的基中发送位，Bob记录他测量的位。在鲍勃的测量过程中，他使用了他随机选择的碱基。然后，Bob将用下面的例子来解释爱丽丝的传输。请注意，在基不匹配的情况下，随机选择0位或1位结果。

鲍勃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
比特	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1

第三步： Alice和Bob交换他们的碱基（“我有+”或“我有x”）。Alice和Bob都会注意到哪些传输的位是使用相同的基础发送的（见下文）：

艾丽斯

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
比特	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

鲍勃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
比特	1	0	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	1

由它们两个生成的结果密钥是：“0 1 1 0 0 1 0 0 0 1”。他们都知道这个键，即使他们只交换了基地。

步骤4： Alice用刚刚生成的密钥加密两个字母。从字母表中读取Q和M的二进制表示，然后对第一行和第二行执行二进制加法，参考表见第9章。

Letter	Q					M				
Data Bit	1	0	0	0	0	0	1	1	0	0
Key Bit	0	1	1	0	0	1	0	0	0	1
Encrypted Bit	1	1	1	0	0	1	1	1	0	1

步骤5a： Alice使用+基础发送加密的消息（0° 表示0, 90° 表示1）。因此，她在下面的顺序中选择以下角度设置：

90° , 90° , 90° , 0° , 0° , 90° , 90° , 90° ,
0° , 90°

步骤5b： Bob也使用+基接收Alice的透射光（反射光=1，透射光= 0）。Bob将记录以下接收到的位：

收到的位	1	1	1	0	0	1	1	1	0	1
------	---	---	---	---	---	---	---	---	---	---

步骤6： Bob然后使用加密密钥来解码消息（第一行和第二行的二进制加法）

收到的位	1	1	1	0	0	1	1	1	0	1
键位	0	1	1	0	0	1	0	0	0	1
数据位	1	0	0	0	0	0	1	1	0	0
信	Q					M				

. 2. 6与Eve的加密协议

生成密钥的过程在这里再次讨论，但这次是与被窃听的伊芙有关。通过比较测试位元，我们发现了她的存在。

第一步：爱丽丝，Bob和Eve随机选择他们的基地，爱丽丝也随机选择要发送的比特。

艾丽斯

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
比特	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

鲍勃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
比特																		

夏娃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	x	x	+	+	x	+	+	+	x	x	x	x	+	x	+	x	+	+

第二步：然后Alice会用她选择的基发送比特，Bob会记录他测量的比特。然而，在这个场景中，Eve在爱丽丝和鲍勃之间，并随机选择她的基础（0° 和45° ）。如果Eve的基础与爱丽丝选择的基础相匹配，那么Eve将传输正确的位。如果Eve选择了不正确的基，她将根据她对爱丽丝信号（0或1）的解释传输一个随机位。然而，鲍勃会记录下他从伊芙那里收到的片段。由Eve和Bob进行的测量将出现在下表中所示（Eve的测量显示是为了解释性的原因，但通常对Alice和Bob都是隐藏的⁷）：

夏娃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	x	x	+	+	x	+	+	+	x	x	x	x	+	x	+	x	+	+
比特	1	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1

鲍勃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
比特	1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

在下表中，显示了相同的数据测量集，但所有事件都由随机确定，用绿色突出显示。第一个表中的绿色测量值表示Alice和Eve之间产生的随机事件，而第二个表中的绿色测量值表示Eve和Bob之间产生的随机事件。

在任何一种情况下，伊芙和鲍勃都不知道他们的测量结果是否是随机产生的。

夏娃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	x	x	+	+	x	+	+	+	x	x	x	x	+	x	+	x	+	+
比特	1	0	0	0	1	0	0	1	1	0	0	1	1	1	0	1	0	1

鲍勃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
比特	1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

⁷ 与没有Eve的实验类似，碱基不匹配的测量值是随机的。

第三步：此时，Alice和Bob交换了用于传输和接收的基地（“我有+”或“我有x”）。它们突出了碱基匹配的测量值。

艾丽斯

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	x	x	+	x	+	+	+	x	x	+	x	x	x	+	+	x	+	x
比特	1	0	0	1	1	0	0	1	1	1	0	1	0	0	0	1	0	1

鲍勃

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础	+	x	x	x	+	+	+	x	+	x	x	+	+	x	+	+	+	x
比特	1	0	1	1	0	0	0	0	1	0	0	0	1	1	0	0	0	0

第四步：现在Alice和Bob比较他们的基匹配的位（用红色圈出的）

爱丽丝： 0 1 1 0 0 1 0 0 0 1

如上图所示，这两个位序列之间存在差异——这些位序列是用蓝色圈起来的。十个错误发生了三次，接近预期的25%。⁸这个测试字符串中出现的错误会提醒Alice和Bob有窃听者的存在，此时协议将被放弃。

⁸ 在这里所选择的数字背后没有任何系统。因此，鲍勃有这么多零的事实纯粹是机会。此外，错误对的“*Alice*=1, *Bob*=0”组合是随机的。当绿色标记的随机事件被选择的不同时，*Alice*和*Bob*比较的位也会相应变化。

第七章系统的设置和调整

. 1. 7组件组件

将RDF1英尺的螺钉到所有的面包板上。为此，请使用1/4 “-20x1/2” (M6 x 12 mm) 螺钉将4英尺固定在每个面包板的底部。

<p>. 5取一个BA1 (/M) 底座，使用1/4 “-20x3/8” (M6 x 10 mm) 螺钉将一个PH1 (PH40/M) 柱架拧到底座上。插入TR1 。5 (TR40/M) 立柱，然后将KM100拧紧（见下图）。将CPS635R-C2激光器插入AD11NT适配器环中</p>	<p>取下一个BA1S (/M) 底座，然后将一个PH2 (PH 50/M) 支柱支架拧紧。插入TR2 (TR50/M) 柱，并拧紧AT1 (/M) 调整辅助装置。</p>	<p>取下一个BA1 (/M) 底座，然后拧紧其中一个PH2 (PH5 0/M) 护柱架。插入TR2 (TR 50/M) 柱。使用十六进制键从TR2 (TR50/M) 柱上拆下固定螺钉。然后使用螺纹适配器将传感器单元（见下图）拧到柱上</p>
		

KM100.

Carry out these steps for all 4 sensors.



Figure 5 Mounting a KM100 to a Ø1/2" Stainless Steel Post

现在设置两个分束器：使用UPH2（UPH50/M）通用支架，并插入TR2（TR50/M）柱。用十六角键从螺杆上拆下固定螺钉。用内盖螺钉连接KM100PM/M。连接PM3（/M）支撑臂，如图6所示。使用防护手套拾起PBS201，并将其插入下图所示的方向。它是通过拧紧支撑臂上的螺钉来固定的。确认正确的方向（底部的字母，边缘正确）。



图6将PBS201分束器安装到运动学平台



ATTENTION



Avoid touching the $\lambda/2$ plates with bare hands. Wearing gloves during assembly is strongly recommended. Only grasp the edge of optical components in order to avoid touching the surface with bare fingers.

安装入/2板。首先，将PH1.5（PH40/M）支柱支架固定在BA1（/M）底座上。

将TR1.5（TR30/M）阀柱拧入RSP1X225（/M）-ALICE索引旋转安装（请参见右侧图像）。

使用附带的SPW606拧下固定环

活动扳手插入入/2型板，并将其锁紧到固定环。对所有4个旋转安装程序重复上述步骤。

其中两个底座上刻有0°和45°的标记

而另外两个旋转支架则刻有四个标记（-45°、0°、45°和90°）。对齐程序

这些旋转安装的描述在

第7.3节。



7. 2. 电子产品

. 2. 1. 7电源

本套件中所包含的电源设备被设计用于提供一个稳定的5V。选择正确的插头为您的位于区域，并将其插入到电源设备上的千斤顶中。



. 2. 2. 7激光电子

除了连接电源外，激光电子盒⁹只有一个关于激光器的输入。一个适配器电缆包括用于连接激光电子与CPS635R-C2激光模块。



激光电子控制单元的特点是一个火灾，但用于在脉冲模式之间切换连续波模式（见右图）。H点火按钮关闭2秒钟，以切换到洛杉矶到连续波模式。压火，但是短暂地结束了连续波模式脉冲被发送。激光的输出可见在激光器前放着一张纸。一个gr LED侧的激光电子控制表示它已准备好使用。

ton
and
old
ser
ton
ort
ien
en
init



⁹ 使用所提供的电源进行操作。用户提供的电源单元必须是具有5V和最小电压的稳定电源。
0.5 A (2.5瓦), 5.5/2.1 mm的电源插座 (内部为正极端子)。

2.3.7 传感器电子

传感器电子设备有一个连接电源和两个传感器输入端。A 传感器可以插入到两者之一传感器端口。确保传感器是连接到电子盒之前插入电源。

传感器电子箱内装有一个绿色按钮，用于在两者之间切换“调整模式”和“测量模式”。

这些模式决定了传感器的led如何工作
当一个激光脉冲被接收到时，就会进行响应
两个传感器同时。

在调节模式下，指示灯在灯的侧面
盒子亮起黄色。等光时
强度由两个传感器接收，即
两个传感器上的蓝色led都会亮起来。

在测量模式下，LED在侧面
盒子亮起来了。等光时

强度由两个传感器接收，两个蓝色led中的一个（随机选择）亮起。这种效应模拟了在分束器上以50%的概率传输或反射的单个光子的“决策”。



7.3. 调整激光器和入/2型板

在进行实验之前，需要对准激光器的偏振平面和入/2板的方向。

首先，将激光器和分束器放在其中一个面包板上。

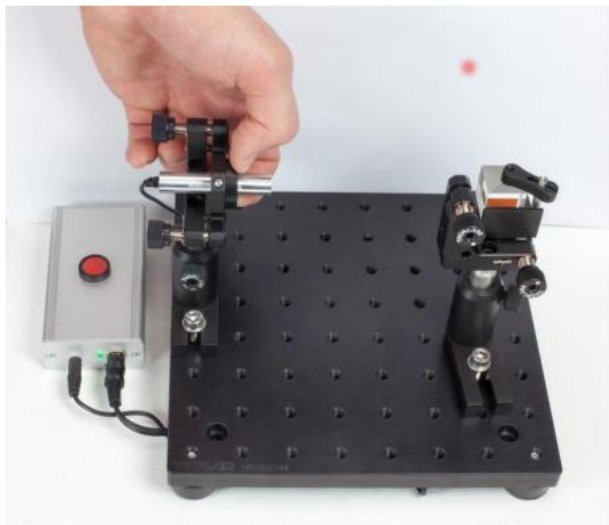
o 按住点火按钮2秒钟，使激光器切换到连续波模式。这使得调整更容易。



警告



激光器模块是一个2级激光器。虽然不需要防护眼镜
第2类激光器，不要直接观察光束或散射光。



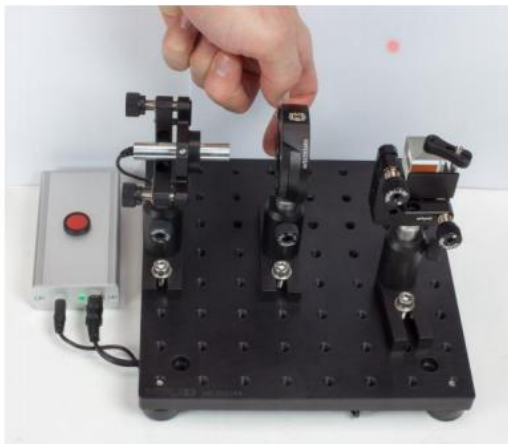
- o使用AT1/M高度调整工具，以确保激光器与桌面平行运行。必要时，使用KM100支架上的调整器调整激光尖端/倾斜。为了确保最佳对准，在对准过程中使用AT1/M调整工具交替距离激光近距离和远处。
- o定位激光器和分束器，使从分束器表面反射出来的光与入射光束成 90° 角。

现在激光器在支架上转动，旋转激光器的偏振。虽然激光器没有全线偏振，但它以方向为主。轻轻松开夹住运动学支架中的适配器环的螺钉。使用适配器环旋转激光器。为了防止它滑动，人们应该用两个手指从前面对适配器环施加压力。现在用一张纸来观察由分束器立方体反射的激光强度。在旋转过程中，它应该明显地减少和再次增加。您正在寻找在反射路径上强度最低的设置。

- o继续转动激光器，直到从分束器反射出来的光的强度最小，并将激光器固定在这个位置。
- o将整个组件（激光器和支架）从设置中退出，并使用其他激光器重复前面的步骤。在这个过程之后，两个激光器都应该是水平偏振的。

将旋转支架（项目#RSP1X225（/M））与入/2板放置在激光器和分束器之间，刻划盘面面向激光器。

- o松开旋转支架顶部的螺钉，以进行连续模式操作。



- o 旋转入/2板，观察反射强度。其强度会随旋转角度的变化而变化。寻找反射强度最低的方向。
- o 一旦你找到使反射光强度最小的角度，通过拧紧旋转安装架顶部的螺钉来启动索引模式。
- o 采取旋转安装从设置，并重新对齐拨号盘面。为此，请松开安装件表面上的两个螺钉。旋转表盘面，直到“0”标记与安装件的顶部中心部分的小标记对齐，如下图所示。在此步骤中，波板不得旋转。拧紧面板上的两颗螺钉，以固定表盘面。



- o 对所有旋转支架和波板重复上述步骤。

. 4. 7. 为爱丽丝和鲍勃做的设置

爱丽丝和鲍勃应该面对面，在大约60厘米的距离。为了获得最佳性能，将两个面包板尽可能平行。

在小面包板上设置Alice（激光器和入/2板）。旋转支架应位于实验板的中心位置。支架上刻着“-45、0、45、90”的标记。将Alice的激光器设置为连续模式（按住红色按钮2秒钟）。

在另一个面包板（Bob）上，将另一个入/2板直接设置在面包板的边缘。这个波板架上刻有“0, 45”的标记。这些标记应该指向远离爱丽丝的地方。

将两个传感器中的一个放置在Bob的面包板的另一端（在波板支架的对面）。大致对齐传感器的位置，使激光器入射到探测器上。

将分束器放置在鲍勃的波板支架和探测器之间。它应尽可能接近于垂直于梁。

第二个传感器应放置为：

- o从爱丽丝号探测器中被分束器反射的激光入射到这个探测器上。传感器的放置应使入口垂直于入射光。

两个探测器和分束器之间的距离相等的。

现在设置如下：



图7 Alice和Bob

微调对齐

- 将传感器电子设备设置为调整模式（侧LED灯亮黄色）。
将两个偏振旋转器均设置为 0° ，然后按下点火按钮。激光器路径上传感器上的蓝色LED应亮起。如果不是如此，请检查：
- o表示该传感器实际上垂直于光束。
 - o该激光器入射在传感器中探测器前面的开口上。

o表示该传感器处在正确的高度上。

o: 激光以传感器模块中的孔为中心。如果遇到困难, 让一个用户继续用激光发送脉冲, 而另一个用户对齐传感器。

当此传感器配置正确时, 对准设置中的其他传感器:

将Alice的入/2板设置为 90° (Bob保持在 0°)。现在, 当从Alice发送脉冲时, 另一个传感器上的LED (从分束器反射) 应该会亮起来。

分束器立方体的尖端/倾斜度可以进行调整, 以使反射光束与该传感器对齐。使用其他极化旋转组合重复以下对齐步骤:

例如, 在Alice上使用 45° 和 -45° 的偏振器旋转设置, 在Bob上使用 0° 设置, 两个传感器led都应该亮起来。这是因为光被分束器分割, 总入射光的一半到达每个传感器。如果没有发生预期的行为 (如下表所述), 请继续对齐传感器。或者, 确认传感器处于调整模式, i. e., 传感器电子设备的侧LED灯亮黄色。

总的来说, 一个人需要测试8个案例, 所有这些案例都必须在开始实验之前工作:¹⁰

艾丽斯	鲍勃	哪个LED点亮	比特		艾丽斯	鲍勃	哪个LED点亮	比特
-45°	0°	都	随机的		-45°	45°	传输的	0
0°	0°	传输的	0		0°	45°	都	随机的
45°	0°	都	随机的		45°	45°	反射的	1
90°	0°	反射的	1		90°	45°	都	随机的

验证所有案例后, 将传感器电子设备设置为测量模式(LED从黄色变为绿色)。所有八个案例都必须正确执行, 否则实验将不会产生正确的结果。第11章包含一个故障排除指南, 以额外帮助调整传感器和激光。

重要提示: 在实验过程中不应该移动该设置。靠在桌子上可能会导致激光器和传感器发生错位。

¹⁰ 位值也被添加到表中以获得帮助。如果传感器电子设备处于调节模式, 随机事件将导致两个led都亮起。如果传感器电子设备处于测量模式, 则只有一个随机LED会点亮。

7. 5. 添加Eve

要将Eve作为窃听者添加到设置中，请将大面包板放在Alice和Bob的面板之间。在这个场景中，Eve的目的是拦截从Alice到Bob的传输，因此避免对Alice和Bob进行更改，并在设置中对齐。

- o 将BBH1把手固定在Eve的面板上。这使得快速添加和删除Eve成为可能。
- o 安装Eve的接收器。该设置与在第7.4节中描述的对准Bob的接收器相同。测试以验证所有8个案例都正确对齐。然后将传感器电子设备从调整模式设置回测量模式。
- o 设置了伊芙的发射机。伊芙的发射激光应该对准鲍勃的每个传感器（取决于偏振）。使用Eve的激光器上的对准模式来帮助对准。验证所有8个传输案例都能在Eve的发射机和Bob之间工作，然后将Eve的激光器切换回测量模式。
- o 激光和传感器电子盒可以使用CL3/M夹连接到实验板上。这使得消灭夏娃变得更加容易。如图右图所示，每个夹具使用两个螺钉。1/4英寸-20x1.25英寸(M6 x 20x1.25英寸)帽螺钉使夹具适应所需的高度，而更接近的1/4“-20x2”(M6 x 45 mm)帽螺钉将夹具固定在面包板上。

Eve的完成设置如下：

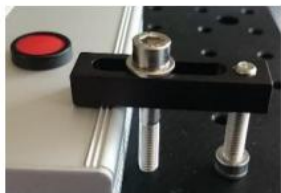


图8夏娃

第八章实验

实验分为三个部分：

第8.1节：生成一个长度至少为20位的密钥

第8.2节：一个4个字母的单词的加密和传输

第8.3节：安装Eve和检测窃听器

为了完成这些练习，用户应该熟悉第5章中概述的加密原则。第6章介绍了详细的例子，说明了有和没有Eve的整个过程。一个样本测量方案可以在第9章中找到。

. 1. 8密钥生成

练习1：设置Alice和Bob，让他们面对面的距离（留下足够的空间将Eve放在Alice和Bob之间）。使用第7章中的指南，对齐Alice和Bob，使所有8个传播病例都产生可重复的结果。在此步骤中，传感器电子设备应处于调整模式（LED指示灯为黄色）。

执行：安装说明见第7章。图3显示了一个基本的示意图，图7显示了一张完整的设置的照片。第7.4节概述了可能的传播病例。

练习2： Alice和Bob随机选择他们的基，Alice也选择随机位进行传输。第9章提供了一个52位的测量协议。填写Alice用于传输信号的位和基，以及Bob用于检测的基。

执行：这对应于第6.1节中描述的示例中的步骤1。这些协议可以在第9章中找到。

练习3：在练习2中选择的基础中传递Alice的位。鲍勃记下了他收到的那些片段。

执行：这对应于第6.1节中描述的示例中的步骤2。Alice和Bob必须生成一个至少有20位长的键。为此目的，我们建议使用至少52位的传输序列。由于在生成密钥时的随机组件，较长的传输更有可能实现加密密钥的20个匹配基。在此步骤中，传感器电子设备应处于测量模式（LED指示灯为绿色）。

总结一下在传输中使用的碱基的选择，如果Alice：

- 选择 0° ，然后她在“+”基础中发送一个0。
- 选择 90° ，然后她在“+”的基础上发送一个1。
- 选择 -45° ，然后她在“x”基上发送一个0。
- 选择 45° ，然后她在“x”基上发送一个1。

Alice和Bob根据练习2中准备的表传输这些位。爱丽丝发送了她的比特，鲍勃记录了他的测量值（反射=1，传输= 0）。

练习4：Alice和Bob公开交换了用于每个测量的基础。然后，它们会删除任何与碱基不匹配的测量值。其余的测量值/位构成了完整的加密密钥。

执行：这对应于第6.1节中详细介绍的示例中的步骤3。Alice和Bob交换他们的碱基（“我选择了+”或“我选择了x”），并用匹配的碱基标记任何测量值。相应的位构成了加密密钥。

如果52个测量不足以生成一个20位加密密钥，则应该使用更多的测量来重复传输，直到生成一个20位密钥。

. 2. 8加密和传输一个四个字母的Word练习5：使用生成的密钥加密Alice的信息（4个字母）。

执行：该过程在第6.1节的第4步和第5.2节中有描述。

练习6：将加密后的消息从Alice传输给Bob。

执行：实际消息的传输完全在一个基础上完成。Alice发送她的加密位（ 0° 表示0, 90° 表示1）。爱丽丝和鲍勃并没有改变基础

用于数据传输。这对应于第6.1节中的步骤5a和5b。练习7：解密Bob收到的

比特，以找到Alice的信息。

执行：此过程与第5.2节中所述的过程相同，并对应于第6.1节中的步骤6。

. 3. 8. 添加Eve和窃听检测

练习8：将Eve置于Alice和Bob之间，并将两个传感器电子设备设置为调整模式(LED亮黄色)。调整伊芙的接收器，使所有8个传输案例都能与爱丽丝一起工作。然后，调整Eve的发射机，使所有8个传输案例与Bob一起工作。返回到两个传感器电子器件的测量模式(LED亮起绿色)。

执行：按照第7章所述进行调整（也请参见图4和图8）。目标应该是在不干扰爱丽丝和鲍勃的设置的情况下调整Eve，因为窃听者对发送者和接收者没有影响。然后将传感器电子设备设置为测量模式。

练习9：填写Eve的表格，它决定了+或x基的随机选择。随机基也需要Alice和Bob，随机位应该由Alice选择进行传输。

执行：有两种方法可以实现此步骤。在一个理想的场景中，用户彼此隔离，Eve可以自发地选择一个基并传输测量结果。然而，由于用户在同一个房间，改变基础的物理行为导致非随机偏差

伊芙的操作员。在序列开始时选择随机的碱基可以防止这种偏差干扰实验结果。Eve使用的基础样本表可以在第9章中找到。请记住，夏娃的操作员不必记录任何数据。

在第6.2节的步骤1中还提供了一个示例。

练习10：使用前一个练习中选择的基础发送Alice的第一个位。 Eve选择了她的第一个基础（在练习9中随机选择）。她收到了一点，她中继给鲍勃使用同样的基础。鲍勃记录他收到的比特。这将对序列中的所有52位/碱基执行。

执行： Alice和Bob使用与练习3中相同的过程。Eve使用从练习9中随机选择的基础来接收来自Alice的信号。然后她传送她的测量结果（使用相同的基础）。此练习对应于第6.2节中的第2步。

练习11： Alice和Bob公开交换了每个测量的基础。然后，他们删除了与碱基不匹配的序列中的测量值。

执行： 与练习4类似，Alice和Bob比较他们的基，并消除所使用的基不匹配的位。其余的部分形成了用于测试窃听者的位序列。此练习对应于第6.2节中的第3步。

练习12：比较Alice和Bob的练习11得出的结果。

执行： 由于Eve使用随机基（不一定与Alice相同）进行窃听和传输位，由Alice和Bob记录的位序列应该包含错误（不匹配的位）。这些错误的存在使得爱丽丝和鲍勃能够检测到窃听者的存在。这与练习4的结果不同，其中Alice和Bob应该得到相同的结果。此练习对应于第6.2节中的第4步。

第9章测量协议

本节包含了爱丽丝、鲍勃和伊芙的测量协议。

为了便于打印，每一个都在一页纸上(该手册也可以在发现时免费下载。thorlabs.com)。然后你可以找到每个字母使用5位的字母编码的表。

密钥生成的测量协议-爱丽丝

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础 (+或x)																		
比特 (0或1)																		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
基础 (+或x)																		
比特 (0或1)																		

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
基础 (+或x)																
比特 (0或1)																

生成的密钥：

= = = = = - - - - -

角度设置 (提醒)	基础+	基准x
位0	0°	-45°
位1	90°	45°

消息的加密表-Alice

信																								
数据位																								
键位																								
加密位																								

数据位=字母，二进制形式，4 x 5位

密钥生成的测量协议-B0B

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础 (+或x)																		
比特 (0或1)																		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
基础 (+或x)																		
比特 (0或1)																		

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
基础 (+或x)																
比特 (0或1)																

生成的密钥：
= = = = = - - - - -

提醒	发射	反射的
基础+ (=0°)	0	1
基准x (=45°)	0	1

消息的解密表-B0B

收到的位																		
键位																		
数据位																		
信																		

基础选择-EVE

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
基础 (+或x)																		

	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
基础 (+或x)																		

	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
基础 (+或x)																

字母表的二进制表示

A	0	0	0	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	0	0	0	1	1
E	0	0	1	0	0
F	0	0	1	0	1
G	0	0	1	1	0
H	0	0	1	1	1
I	0	1	0	0	0
J	0	1	0	0	1
K	0	1	0	1	0
L	0	1	0	1	1
M	0	1	1	0	0
N	0	1	1	0	1
O	0	1	1	1	0
P	0	1	1	1	1
Q	1	0	0	0	0
R	1	0	0	0	1
S	1	0	0	1	0
T	1	0	0	1	1
U	1	0	1	0	0
V	1	0	1	0	1
W	1	0	1	1	0

X	1	0	1	1	1
Y	1	1	0	0	0
Z	1	1	0	0	1

二进制添加表

0	1	0	1
+ 0	+ 0	+ 1	+ 1
= 0	= 1	= 1	= 0

第十章教学技巧

随机数的产生是量子密码学中的一个基本问题。当实验中的碱基和位的选择是用腐相神经随机数进行的时，Alice和Bob可能有很多匹配，因为人类是一个糟糕的随机数生成器。这可以很容易地通过一个简单的练习来显示：

让学生们创建一个他们认为的0位和1位的随机序列

编写一个程序，使用位1分析其序列中任何链的数量和长度。例如，序列01110将是一个3位长的1s的单链。该程序应该计算在学生的序列中出现的长度为n的序列链的数量。概率（以发生的次数来衡量）应该随着 $1/2^n$ 对于一个真正的随机序列。

然而，当序列被人类选择时，偏见就会进入选择过程。学生很少会写出长度大于5的1（或0）链的序列，因为这样的序列看起来不是随机的。然而，给有足够的样本，如果随机选择，这样的序列确实会发生（尽管概率较低）。根据理论曲线绘制学生选择的序列，应该能迅速显示出与真实随机选择的偏差。

第8章的练习2指导学生为Alice和Bob随机选择碱基，也为Alice随机选择位。上面的一点说明了人类的偏见是如何使它们成为随机数生成器的糟糕选择的。

或者，一个可以产生随机选择的比特的设备将会产生更好的结果。这些例子包括商业设备，如IDQuacnce的数量或由光源、两个单光子探测器和分束器组成的设备。

一个简单的解决方案是使用一个带有几个骰子的透明盒子。掷骰子的偶数结果被解释为0位，而奇数结果被解释为1位。抛硬币或由计算机程序生成的伪随机数也提供了低成本的替代品。

第8章中描述的练习的结构是让学生首先设置Alice和Bob，生成一个密钥，然后传输一条消息。在初始传输之后，Eve被添加进来，并在生成第二个密钥的过程中被发现。这个过程并不完全符合第5.7节中提出的BB84协议。在BB84协议中，在发送消息之前对窃听者进行测试。不过，对于学生来说，密钥生成和数据传输是一个很好的起点。

第十一章故障排除

当测试爱丽丝和鲍勃（或爱丽丝和伊芙，伊芙和鲍勃）的入/2盘子的8个组合时，并不是所有的8个案例都有效。

两个传感器电子盒是否都设置为调整模式？这是由在侧面发出黄色光的LED来表示的。如果是绿色的，按绿色按钮切换到调整模式。测量模式由从LED发出的绿光表示。

RSP1X225/M支架中是否正确安装了所有入/2板？“快轴”必须与“0°”标记保持一致。此外，支架的固定机构（用支架顶部的螺丝松开并固定）必须固定在0°。

激光器插入正确，偏振轴正确？再次检查激光第一次通过0°设置的入/2板时，传输是否最小，然后通过90°设置的入/2板（“90°”与特殊比例！为此，支架本身只旋转45°增量），然后通过分束器。

分束器的方向是否正确？请与第7.1节中的照片进行比较。

爱丽丝和鲍勃（或者爱丽丝和伊芙，伊芙和鲍勃）的入/2盘子会面对对方吗？Alice的入/2板面对激光吗？

一切是否都尽可能地垂直设置？传感器是否垂直于入射激光束，透镜是否直接安装，反射光束的传感器是否距离入射光束90°？从上面检查设置通常很有帮助。

两个传感器与分束器的距离相同吗？有时，改变传感器/光电二极管与分束器之间的距离会有所帮助。例如，人们可以将两个传感器移动到更靠近分束器的地方。

你确定光电二极管排列正确吗？仅仅因为激光器大约通过传感器开口，这并不意味着对光电二极管的最佳击中

第十二章致谢

这个实验包是与各种致力于量子物理教学的讲师密切合作开发的。我们谨对以下几点表示诚挚的感谢：

莱布尼茨体育馆的施耐德，为联合实施实验，电子设备和传感器，在教学过程中进行测试，并分享他的教学文件。

安德烈亚斯·维特尔教授和教授。资料暂存器简-彼得·梅，埃尔兰根-纽伦堡大学，为他们的初步概念工作。他们两人建立了一个带有脉冲源和相应探测器的装置，并在他们的学生实验室中进行操作。见A. 维特，A. 斯特朗茨，P. 布朗纳和JP。.-梅：“现代社会的生活和生活。”自然实践：德国大学59(8) 1719 (2010)。

关于量子物理学的话题，我们特别推荐扬-彼得·梅的网站www.quantumlab。这也是前面几个部分指令的灵感来源。

海森堡大学。在慕尼黑的“2014学校量子物理”研讨会上建立了联系。

贾斯明·卡里姆，卡尔斯鲁厄理工学院，为她的狄拉克符号实验的量子力学描述草案。

你对已经实现的实验有想法吗

还是想要实现？请联系我们；我们很高兴能建立合作伙伴关系！

第十三条监管

根据欧洲共同体的WEEE（废物电气和电子设备指令）和相应的国家法律的要求，索拉布斯为欧洲共同体的所有最终用户提供了在不收取处置费用的情况下返回“生命结束”单元的可能性。

此优惠适用于Thorlabs电气和电子设备：
2005年8月13日以后出售
相应的“轮箱”标志（见右）
出售给欧盟委员会内的一个公司或机构
目前由欧共体内的一个公司或机构所拥有
仍然完整，未拆卸，未受污染

因为WEEE指令适用于独立的操作
电子和电子产品，这生命的终结收回
服务不指其他Thorlabs产品，如：

纯OEM产品，这意味着用户构建构建一个单元(例如。OEM)
沙痴公司组成部分
Subark力学与光学
用户拆卸的剩余部件（PCB、外壳等）。



如果您希望返回索拉斯单位废物回收，请联系索拉斯或您最近的经销商以获得更多信息。

废物处理是你自己的责任

如果你不把一个“生命终结”的单位归还给索尔拉布斯，你必须把它交给一家专门从事废物回收的公司。请勿将该设备处置在垃圾箱或公共废物处理场所。

生态背景

众所周知，WEEE在分解过程中会释放出有毒的产物，从而污染了环境。欧洲RoHS指令的目的是在未来减少电子产品中有毒物质的含量。

WEEE指令的目的是强制执行WEEE的回收利用。寿命结束产品的可控回收将因此避免对环境的负面影响。

第14章索尔拉布斯的全球联系方式

有关技术支持或销售查询，请访问我们的www。 [thorlabs](https://www.thorlabs.com). [联系我们最新的联系方式。](mailto:sales@thorlabs.com)



美国、加拿大和南美

胸实验室，Inc。

sales@thorlabs.com

techsupport@thorlabs.com

欧洲

胸实验室有限公司

europe@thorlabs.com

法国

Thor实验室SAS

销售的fr@thorlabs.com

日本

Thorlabs日本公司。

sales@thorlabs.jp

英国和爱尔兰

胸实验室有限公司。

销售的uk@thorlabs.com

techsupport.uk@thorlabs.com

斯堪的纳维亚

瑞典胸实验室

scandinavia@thorlabs.com

巴西

这是我的天堂。

brasil@thorlabs.com

中国

胸实验室中国

chinasales@thorlabs.com



THORLABS

www.thorlabs.com
