量子通信

杨易轩 罗昶凯 张质源

主要内容

绪论（罗昶恺）

- 基于纠缠的隐形量子传态
  - 二维（罗昶恺）
  - 三维（杨易轩）
- 基于测量的BB84协议
  - 无噪声（罗昶恺）
  - 有噪声（张质源）

绪论：简史篇

1917年G.vernam提出了“一次一密”密码体制，C.E.Shannon于1949年用信息论证明了该密码体制是无条件安全的，这是目前唯一被证明是绝对安全的密码体制。然而该密码体制要求通信双方Alice和Bob事先共享与明文等长的密钥，并且密钥只能使用一次。这样就需要极大数量的密钥供保密通信的双方使用。安全并且高效地密钥分配问题限制了“一次一密”密码体制的应用。量子密钥分配技术有效地解决了“ 一次一密”密码体制所需要的安全而且高效地密钥分配问题。通过量子密钥分配与“一次一密”密码体制相结合，就可以实现理论上无条件安全的信息传输。

绪论：应用篇

量子通信已逐步在国家政务、金融信息等安全领域开始发挥作用， 如2004年，奥地利银行成为世界上首个采用量子通信的银行，利用该技术，2007年，瑞士全国大选的选票结果传送时也采用了量子保密通信技术，以保证结果的绝对安全；2012年，党的十八大会议部署了量子加密电话网、量子加密数据传输设备，为大会顺利召开提供了安全通信技术保障。

截止2009年，点对点的两方量子通信技术已经比较成熟,科学家和技术人员利用光量子态已经能够实现几十公里到百公里级的两方量子密钥分发系统。

绪论：应用篇

2014年11月15日，中国研发的远程量子密钥分发系统的安全距离扩展至200公里，刷新世界纪录。

欧洲日内瓦大学和康宁玻璃公司合作建造的量子通信光纤网络全长为307公里。

2017年9月29日，世界首条量子保密通信干线“京沪干线”正式开通。当日结合京沪干线与“墨子号”量子卫星，成功实现人类首次洲际距离且天地链路的量子保密通信。干线连接北京、上海，贯穿济南和合肥全长2000余公里，全线路密钥率大于20千比特/秒可同时供上万用户密钥分发。

绪论：特性篇

与量子计算不同，量子通信区别于经典通信方式的优越性不在于通信效率，当然也不可能超光速传递信息（实际上接下来我们会看到，即便量子通信也离不开经典通信的辅助），而在于通信的保密性

量子通信融合了现代物理学和光通信技术研究的成果，由物理学基本原理来保证密钥分配过程的无条件安全性：单光子不可再分；测量塌缩原理；量子不可克隆定理。

一般而言，量子通信传递的不是信息本身，而是**密钥**（一次一密）

下面隆重请出组员张质源介绍量子不可克隆原理

绪论：分类篇

一般而言，量子通信分为两种主要方式：

基于测量型（e.g. BB84）— Alice制备已知量子态，传给Bob测量

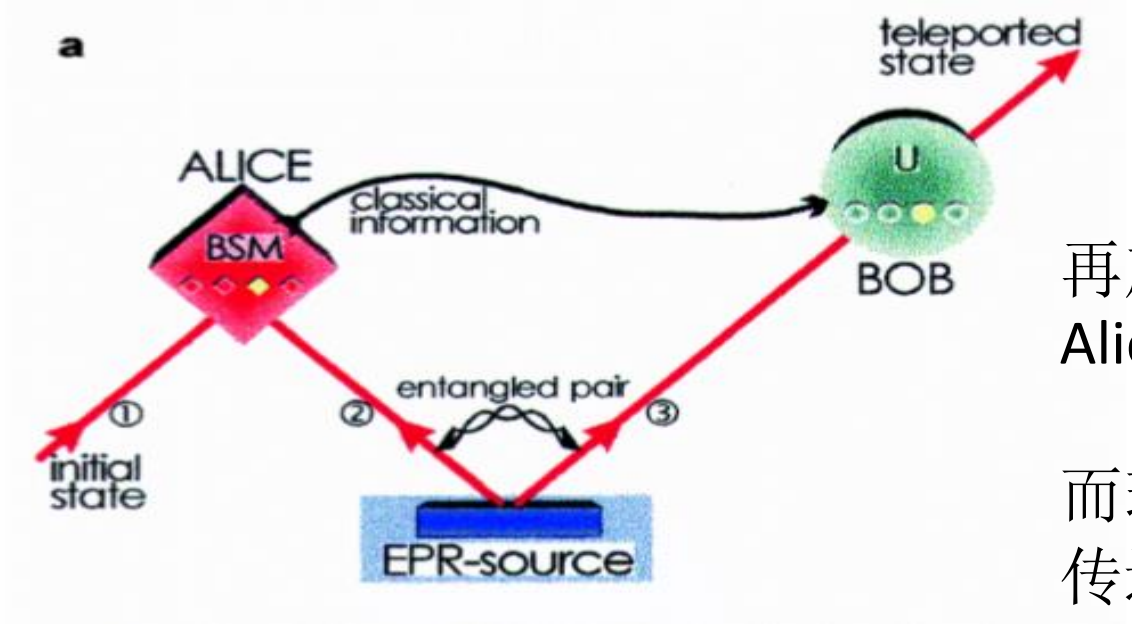
基于纠缠型（e.g. 墨子号）— Alice利用量子纠缠向Bob隐形传态

基于测量型物理实现较简单，多见于信科paper、图书、博客……

基于纠缠型一般有比较深厚的物理背景，往往是密密麻麻的纠缠光路，令人头秃……

我们这次报告以后者为主，有时间的话也会讲一下前者

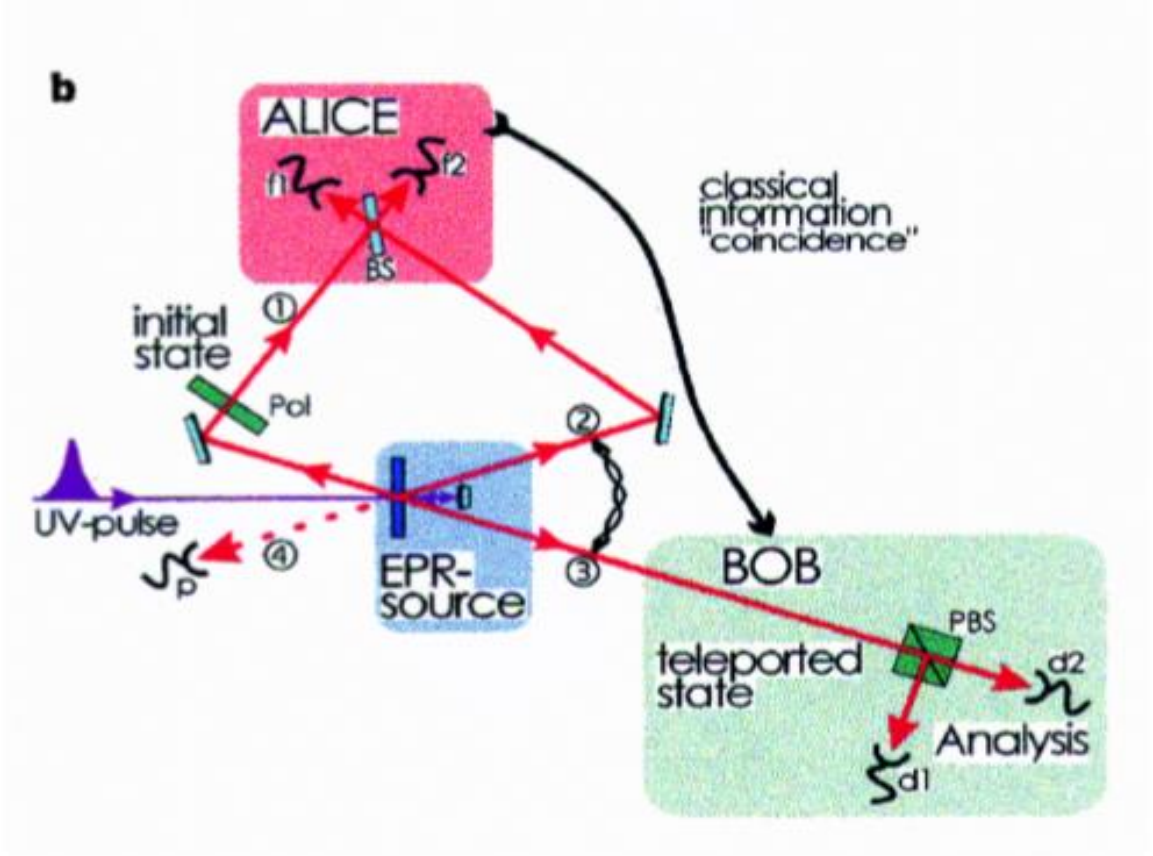
二维量子隐形传态（一般装置）



如图，Alice经由EPR纠缠源产生一对纠缠光子，再产生一个任意的量子态，利用纠缠光子的特性，Alice得以在Bob处复现她产生的量子态。

注意：整个过程Alice**无需**向Bob发送光子。因而理论上，无论Alice与Bob相距多远，量子态的传送都是顺时完成的（地面参考系下）。但这并不违背信息传递速度的上限，因为没有经典信道的辅助，Alice实际上无法传递任何信息，这一点将在接下来的具体实现中得到体现。

二维量子隐形传态（具体实现）



三维量子隐形传态

接下来我们介绍这次讨论班最重要的内容——潘建伟院士在今年8月份新鲜出炉的成果，对于本部分我们三位组员进行了大量深入探讨，不过我就来上来打一下酱油而已。。。

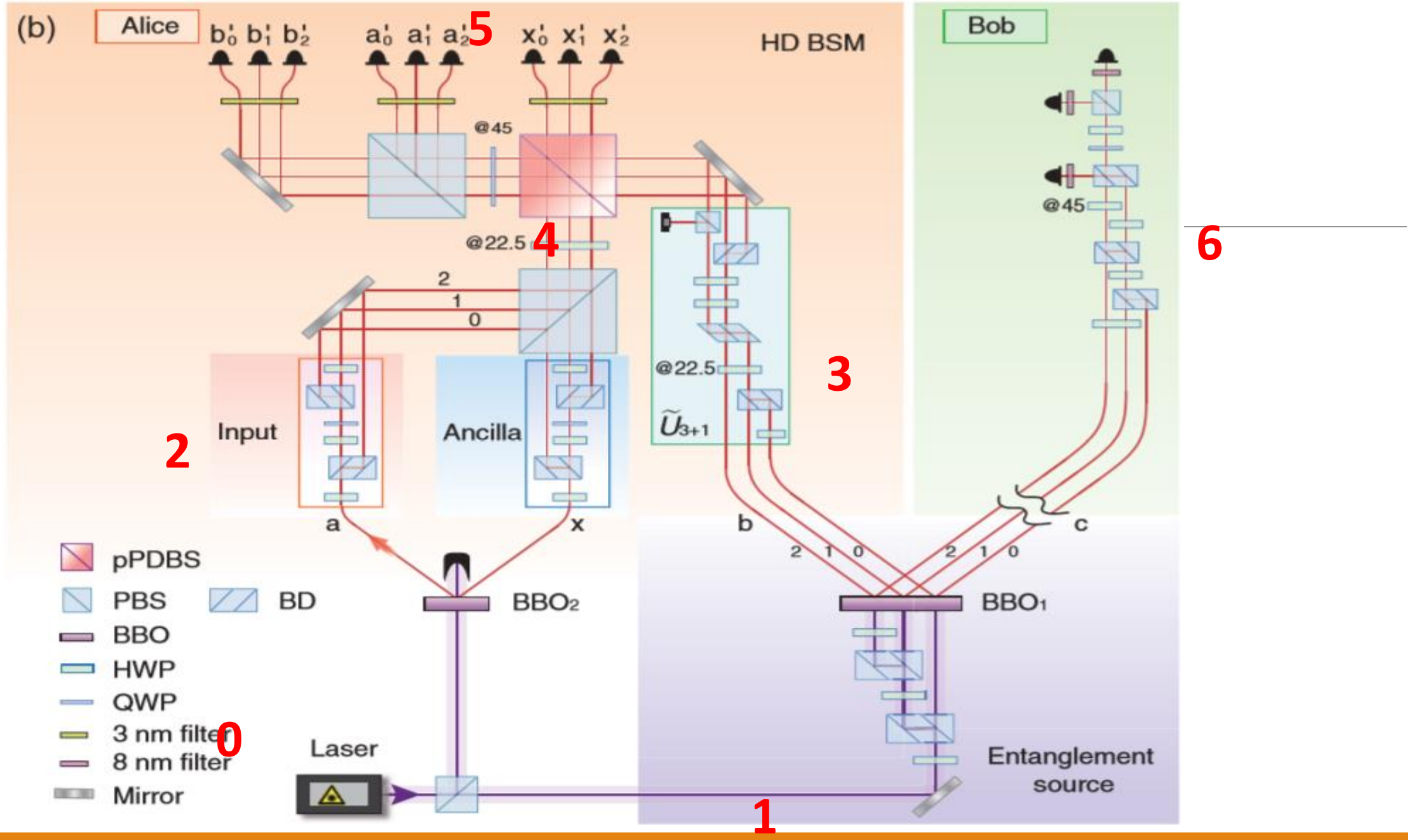
根据潘教授的说法“The ability of coherent control of high-dimensional quantum states is important for developing advanced quantum technologies. Compared to the conventional two-level systems, HD states can offer extended possibilities such as both higher capacity and noise resilience in quantum communications, more efficient quantum simulation and computation.”


美好生活之路 进步与您同步
中外科学家合作实现高维度量子隐形传态
2019-08-21 07:47:59 来源：科技日报
记者从中国科学技术大学获悉，该校潘建伟小组与奥地利维也纳大学塞林格小组合作，在国际上首次成功实现高维度量子体系的隐形传态。这是自1997年实现二维量子隐形传态实验以来，科学家第一次在理论和实验上把量子隐形传态扩展到任意维度，为复杂量子系统的完整态传输以及发展高效量子网络奠定了坚实的科学基础。研究论文以编
中华人民共和国中央人民政府
www.gov.cn
国务院 总理 新闻 政策 互动 服务 数据 国情
我科学家首次实现高维度量子隐形传态
2019-08-19 07:11 来源：光明日报
中国科学技术大学潘建伟、陆朝阳、刘乃乐等和奥地利维也纳大学塞
系的隐形传态。这是自1997年实现二维量子隐形传态实验以来，科学
打印
成功实现高维度量子体
态扩展到任意维
1026惊魂躲猫猫
中外科学家联手首次实现高维度量子隐形传态
中新社合肥8月18日电 (记者 吴兰)中国科学技术大学18日消息，该校潘建伟、陆朝阳等和奥地利维也纳大学塞林格小组合作，在国际上首次成功实现高维度量子体系的隐形传态。
相关推荐
中科院
近年来，中科院在社会各界的大力支持下，在全院科研人员的共同努力下，重大科技成果不断涌现。为进一步增进公众对中科院亮点工作的了解，同时促进院属各单位进一步加强对重大成果的传播推广，特启动“中科院科技创新亮点成果筛选”活动。
中科院相关职能部门现已推荐候选条目，欢迎大家积极参与投票，相关得票数将作为正式当选条目的重要参考依据。感谢对中科院科技创新工作的鼓励和支持！
亮点成果筛选
2019年第3季度
实现高维度量子隐形传态
CCTV.com 央视网 新闻
我国取得量子研究重大进展 世界首次实现
形传态
央视新闻客户端 2019-08-18 14:45
国内 国际 经济 军事 生活 文娱 教育 图片 评论
量子隐
央视新闻客户端
中科大首次实现高维度量子隐形传态
2019年08月19日
版次：01
本报讯（记者 桂运安）记者8月18日从中科大获悉，该校潘建伟、陆朝阳、刘乃乐等与奥地利维也纳大学塞林格小组合作，在国际上首次成功实现高维度量子体系的隐形传态。这是自1997年实现二维量子隐形传态实验以来，科学家第一次在理论和实验上把量子隐形传态扩展到任意维度，为复杂量子系统的完整态传

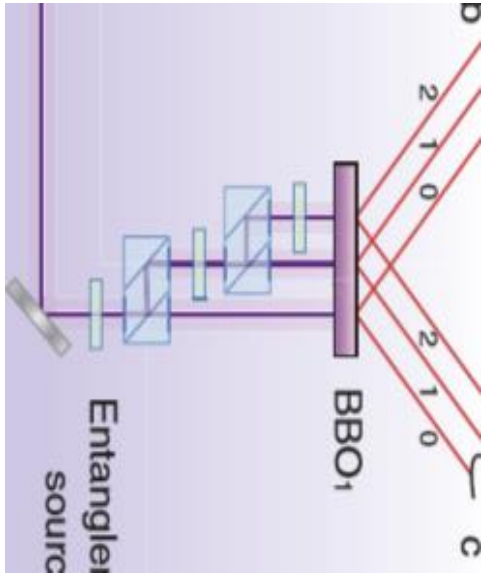
三维量子隐形传态

如前文所述，以下内容可视作paper reading：
《Quantum Teleportation in High Dimensions》

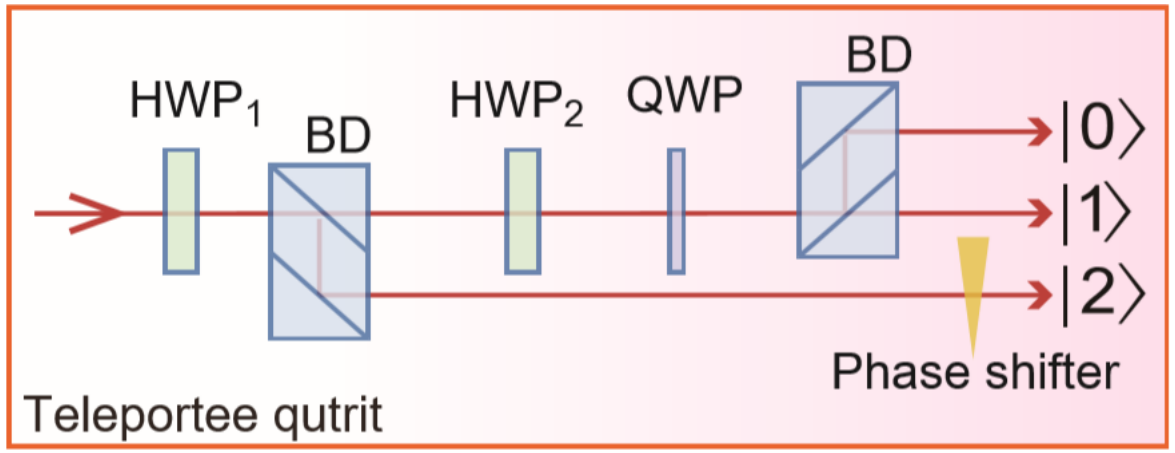
——PHYSICAL REVIEW LETTERS 123, 070505 (2019)


(b)
Alice
$b_0' b_1' b_2'$
$a_0' a_1' a_2'$
5
$x_0' x_1' x_2'$
HD BSM
Bob
@45
@45
@22.5
4
2
1
0
@22.5
3
$\tilde{U}_{3+1}$
Input
2
Ancilla
a
x
b
c
2 1 0
2 1 0
pPDBS
PBS
BD
BBO
HWP
QWP
3 nm filter
8 nm filter
Mirror
BBO_2
BBO_1
0
Laser
Entanglement source
1
6

Part 1： 制备纠缠态bc



Part 2：制备任意态a

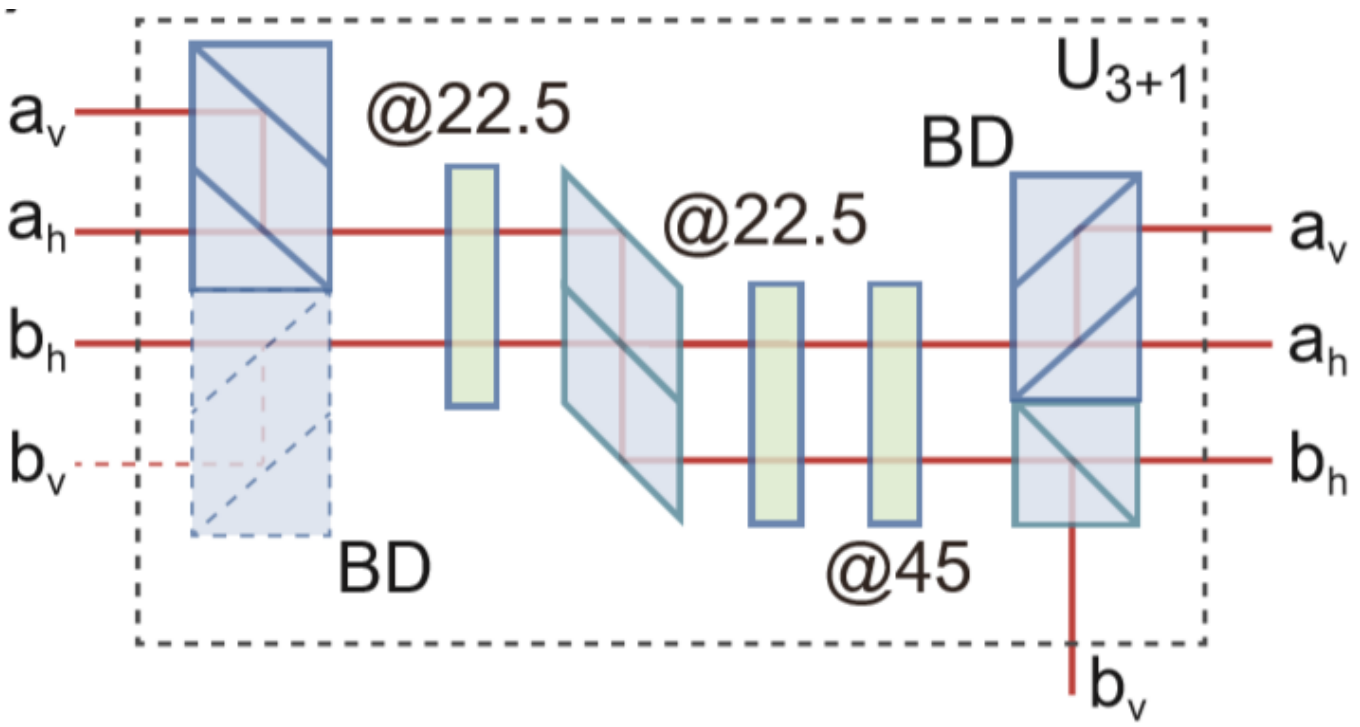


Part3：U_{3+1}

1.物理直观

2.光学实现

3.矩阵表述



Part3： U_{3+1}

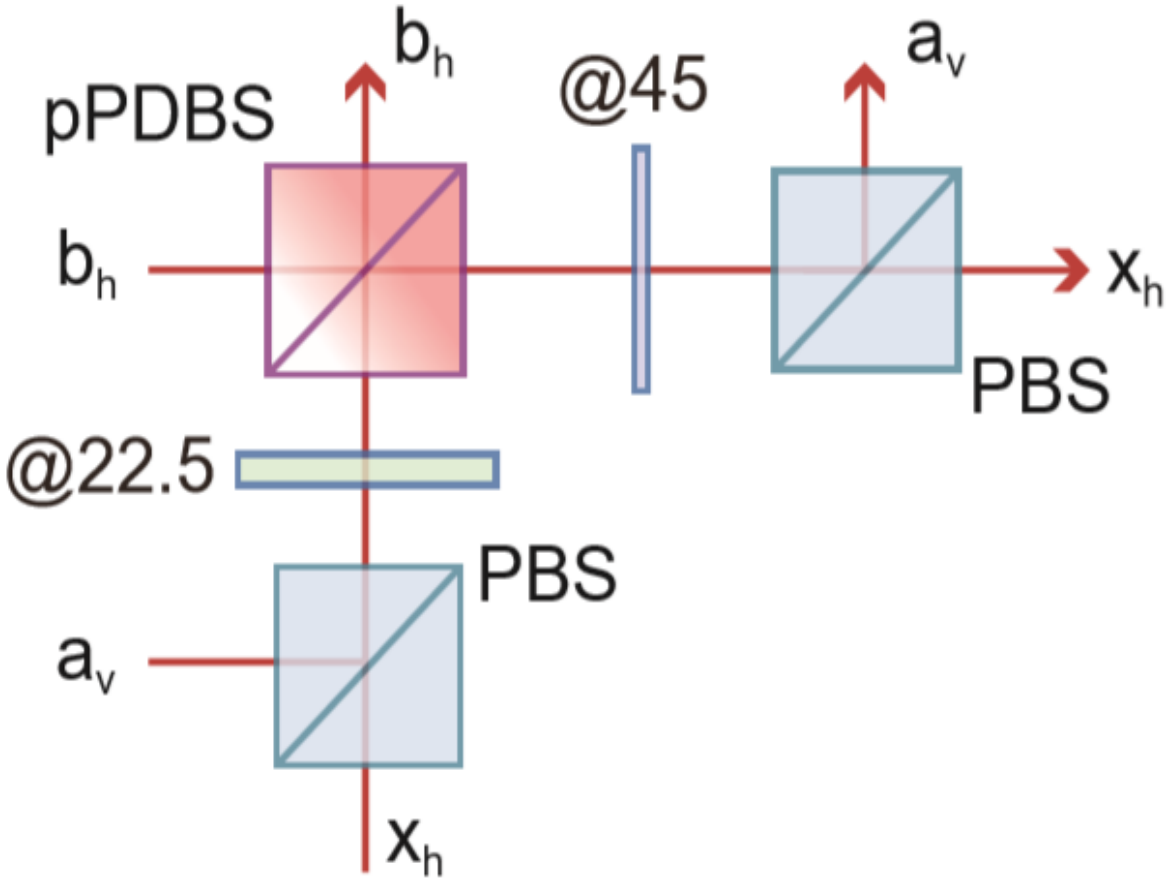
$$\frac{1}{2}\begin{bmatrix} -a_v & a_h & b_h \\ a_v & -a_h & b_h \\ a_v & a_h & -b_h \\ a_v & a_h & b_h \end{bmatrix} = \frac{1}{2}\begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \begin{pmatrix} a_v \\ a_h \\ b_h \\ 0 \end{pmatrix}$$

Part4： QFT(Quantum Fourier Transform)

~~1.物理直观~~

2.光学实现

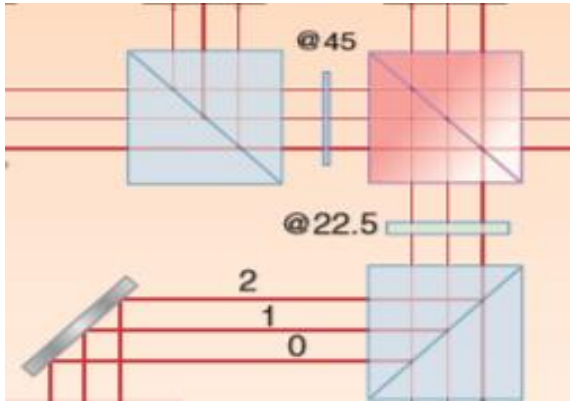
3.矩阵表述



Part4： QFT

此前的一切元件均作用在同一光子的不同光路上。

而QFT作用在同一光路的不同光子上。



Part4： QFT

在数学上这分别表现为——

$$|0\rangle_a \xrightarrow{U_{3\mp1}} |0\rangle_a + |1\rangle_a + |2\rangle_a$$

$$|0\rangle_a \xrightarrow{QFT} |0\rangle_a + |0\rangle_b + |0\rangle_x$$

Part4： QFT

QFT3 = T(QWP45) T(pPDBS) T(HWP22.5)

$$= \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}$$

Part5：观测

$$T_3|\chi\rangle_{\mathrm{abcx}} \propto (\alpha|0\rangle_{\mathrm{a}} + \beta|1\rangle_{\mathrm{a}} + \gamma|2\rangle_{\mathrm{a}}) \otimes (|0\rangle_{\mathrm{x}} + |1\rangle_{\mathrm{x}} + |2\rangle_{\mathrm{x}}) \otimes$$

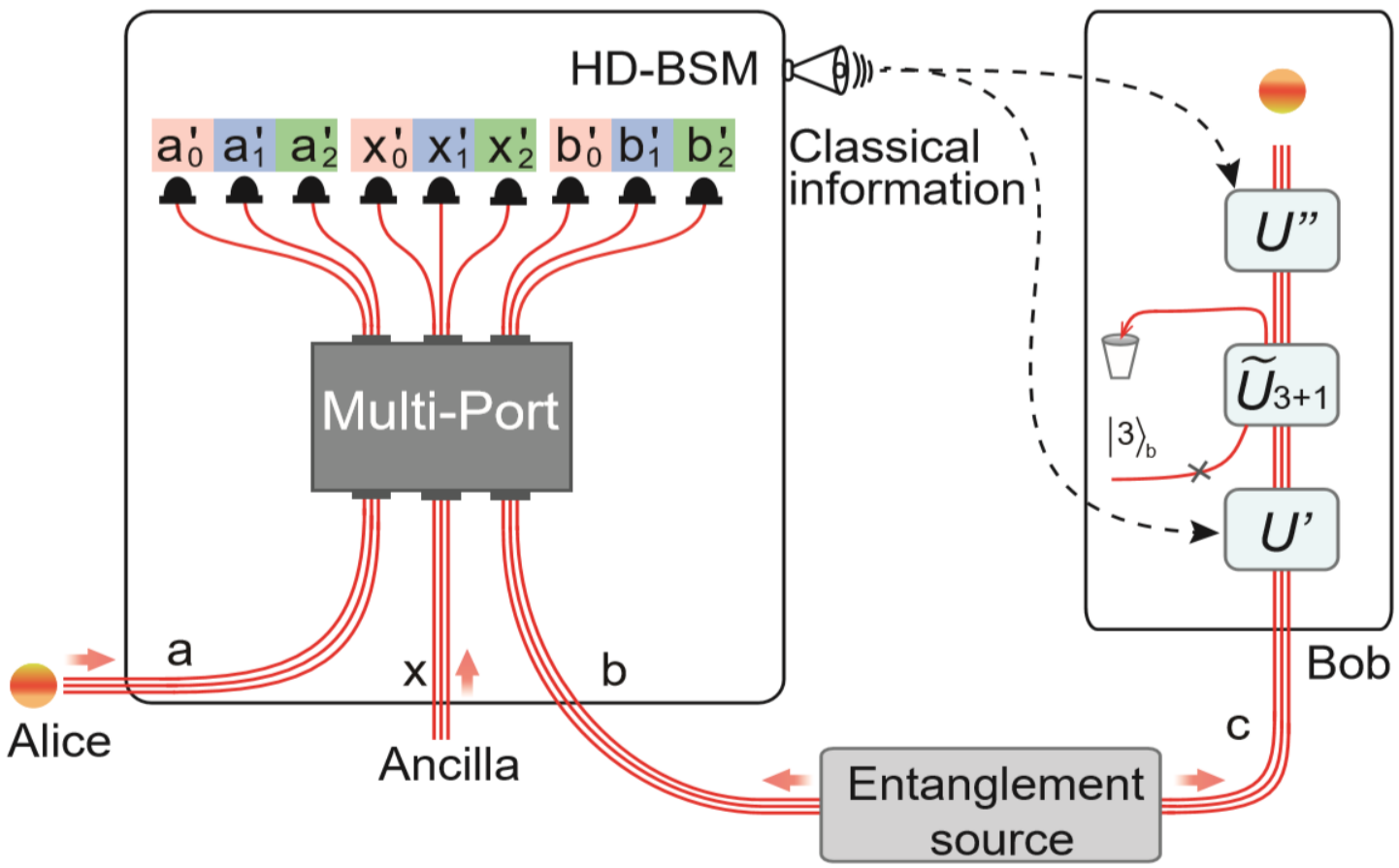
$$\left[\ |0\rangle_{\mathrm{b}}(-|0\rangle_{\mathrm{c}} + |1\rangle_{\mathrm{c}} + |2\rangle_{\mathrm{c}}) + |1\rangle_{\mathrm{b}}(|0\rangle_{\mathrm{c}} - |1\rangle_{\mathrm{c}} + |2\rangle_{\mathrm{c}}) + |2\rangle_{\mathrm{b}}(|0\rangle_{\mathrm{c}} + |1\rangle_{\mathrm{c}} - |2\rangle_{\mathrm{c}})\ \right]$$

$$\langle P|_{\mathrm{abx}} = \langle 0|_{\mathrm{a}}\langle 1|_{\mathrm{a}}\langle 2|_{\mathrm{a}}\mathbf{QFT} \ \propto\ (\langle 0|_{\mathrm{a}} + \langle 0|_{\mathrm{b}} + \langle 0|_{\mathrm{x}})(\langle 1|_{\mathrm{a}} + \langle 1|_{\mathrm{b}} + \langle 1|_{\mathrm{x}})(\langle 2|_{\mathrm{a}} + \langle 2|_{\mathrm{b}} + \langle 2|_{\mathrm{x}})$$

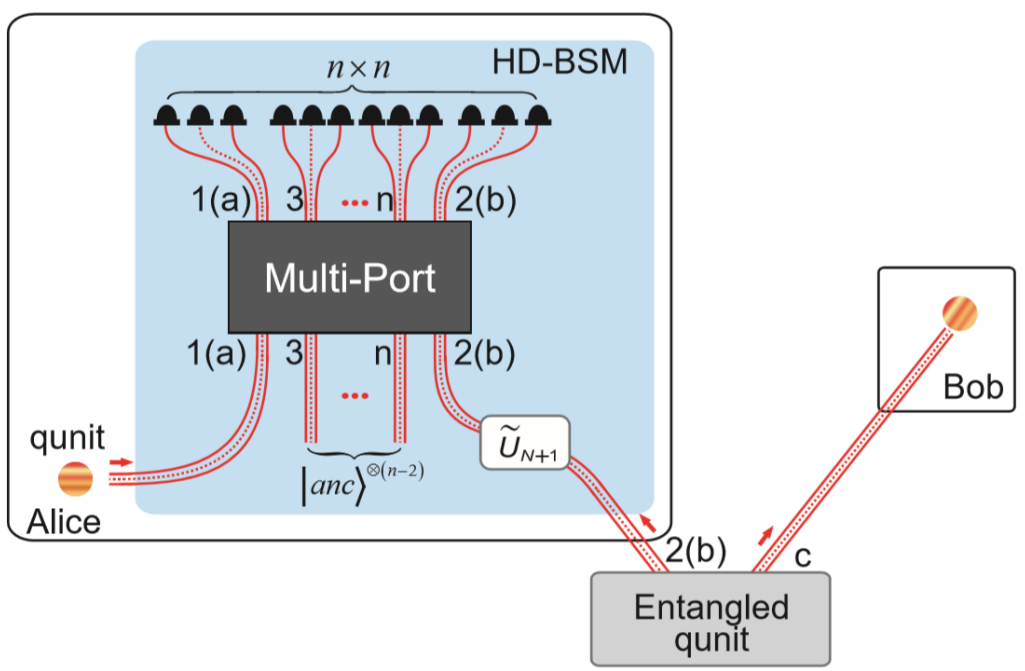
$$\langle P|_{\mathrm{abx}}|\psi\rangle_{\mathrm{abcx}} \ \propto\ \alpha|0\rangle_{\mathrm{c}} + \beta|1\rangle_{\mathrm{c}} + \gamma|2\rangle_{\mathrm{c}}$$

Part Extra： feed-forward

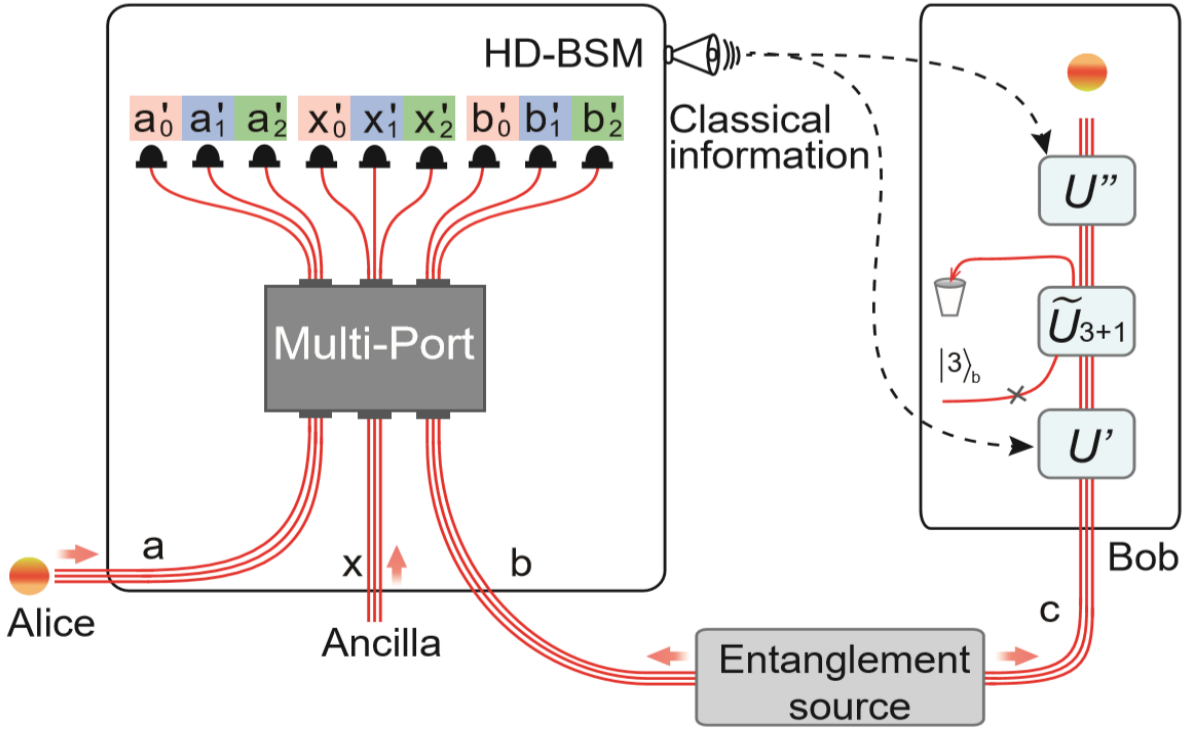
将成功率从1/81提升至1/9



Part Extra： feed-forward



1/81



1/9

Part Extra： feed-forward

$$\langle P| = (\omega^{y+2z}\langle 01| + \omega^{2y+z}\langle 02| + \omega^{x+2z}\langle 10| + \omega^{2x+z}\langle 12| + \omega^{x+2y}\langle 20| + \omega^{2x+y}\langle 21|)/\sqrt{6}$$

$$\langle P|_{\mathrm{ab}}(\alpha|0\rangle_{\mathrm{a}} + \beta|1\rangle_{\mathrm{a}} + \gamma|2\rangle_{\mathrm{a}})(|00\rangle_{\mathrm{bc}} + |11\rangle_{\mathrm{bc}} + |22\rangle_{\mathrm{bc}})$$

$$\propto \alpha(\omega^{y+2z}|1\rangle_{\mathrm{c}} + \omega^{2y+z}|2\rangle_{\mathrm{c}}) + \beta(\omega^{x+2z}|0\rangle_{\mathrm{c}} + \omega^{2x+z}|2\rangle_{\mathrm{c}}) + \gamma(\omega^{x+2y}|0\rangle_{\mathrm{c}} + \omega^{2x+y}|1\rangle_{\mathrm{c}})$$

$$= \omega^{2x+2y+2z}[\alpha\omega^{-2x}(\omega^{-y}|1\rangle_{\mathrm{c}} + \omega^{-z}|2\rangle_{\mathrm{c}}) + \beta\omega^{-2y}(\omega^{-x}|0\rangle_{\mathrm{c}} + \omega^{-z}|2\rangle_{\mathrm{c}}) + \gamma\omega^{-2z}(\omega^{-x}|0\rangle_{\mathrm{c}} + \omega^{-y}|1\rangle_{\mathrm{c}})]$$

Part Extra： feed-forward

$$U'(x,y,z) = \omega^x|0\rangle\langle 0| + \omega^y|1\rangle\langle 1| + \omega^z|2\rangle\langle 2|$$

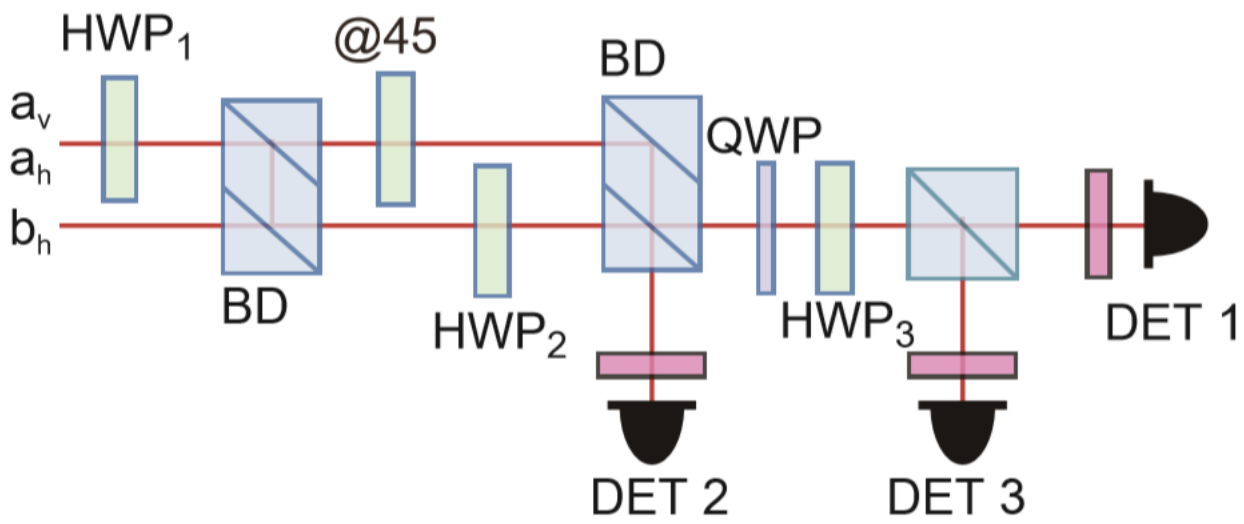
$$U''(x,y,z) = \omega^{2x}|0\rangle\langle 0| + \omega^{2y}|1\rangle\langle 1| + \omega^{2z}|2\rangle\langle 2|$$

Part 6：接收

即Bob如何测量自己接受到的光子。

事实上这很trivial，毕竟粒子已经制备完成。

因此并不详细描述。



ending

事实上，paper中还有很多的实测数据用于作证模型的正确性，限于篇幅不在此列举。

BB84

截至目前，我们的讨论局限在基于纠缠的量子通信，下面我们不妨以BB84协议为例，简要展示一下基于测量的量子通信是如何工作的。（最难的结束了，这部分比较欢乐和谐）

首先注意到Alice与Bob之间经典通信的信道无论如何都存在被窃听的可能性（一次成功的窃听，必须满足的重要条件之一就是不能被Alice或Bob中的任何一员察觉）

基于量子比特的测量坍缩和不可克隆性，我们考虑Alice经由量子信道向Bob传送二进制信息

Alice和Bob的困境

不过，如果Alice向Bob发送的量子态为$|\uparrow\rangle$（表示1）或者$|\rightarrow\rangle$（表示0），那么Eve完全可以拦截光子，而后用某个方向的检偏器进行测量（窃听），再原样复制给Bob，Bob和Alice却浑然不知。

所以，这么naive的思路是会泄密滴！

注意：与基于纠缠的隐形传态不同，这里我们确实要将某个偏振态的光子从Alice直接发送到Bob那里，所以完全有可能半路上被拦截。

Solution of Alice

既然这样，Alice灵机一动，把|↑⟩和|↗⟩两种偏振态的光子（都表示1，与它们正交的偏振态自然就表示0）随机发送，让Eve晕头转向，无从测量。

不过，这样似乎Bob也被搞懵了。。。

没关系，Bob也随机选用+和×两种坐标系来乱测一通，坐标系选的不对的话正确率自然就只有50%，然后用经典信道禀明Alice，让Alice来评定对错

邪恶天才Eve

难道这样安全了？别忘了Alice和Bob还要经过经典信道来回通信，妥妥被（无处不在的）Eve窃听

但没用啊，Eve只是知道了Alice用每一次用哪个坐标系来编码，又不知道编码内容是0还是1

（不死心的）Eve想：要不我学着Bob对那些光子乱测一通&窃听Alice和Bob的经典通信，这样不就行了？

Alice和Bob的反击

于是，针对Eve的一系列邪恶想法，Alice和Bob决定启用终极武器——经典信道校验，Bob的测量行为必然会导致光子坍缩，从而无法通过校验。

具体而言是这样： Alice和Bob从原密钥**Bob测量基矢设置正确**的那一半比特中，随机选择一个序列公开比较，从而验证是否被窃听。（这个序列既然已经公开，Eve怎么可能放过，所以之后的通信作废就好了）不考虑噪声的话，不被窃听的比特Bob测量结果应该与Alice的编码完全一致，但是Eve的窃听会使得正确率降低到75%。

当然，由于通信噪声的存在，校验正确率不会是100%，因而Alice和Bob要适当容忍阈值内的错误，做人疑神疑鬼会活得很累

一个问题

Alice和Bob就算通过校验发现了Eve，但机密都泄露了，亡羊补牢还来得及吗？？？

机密没有泄露，泄露的只是密钥，密钥被窃听了换一套呗，真正的机密还没发出去呢

如果Alice把密钥成功地保密传输给了Bob，香农证明了，根据一次一密的原理，接下来就算Alice光明正大地传输加密后的文件，Eve窃听到了也只能抓耳挠腮干着急

量子纠错码

刚刚的讲解中，我们提到了噪声问题但没有深究

接下来我们聊聊如何克服技术手段的限制，使量子编码以任意接近于1的概率正确传递信息

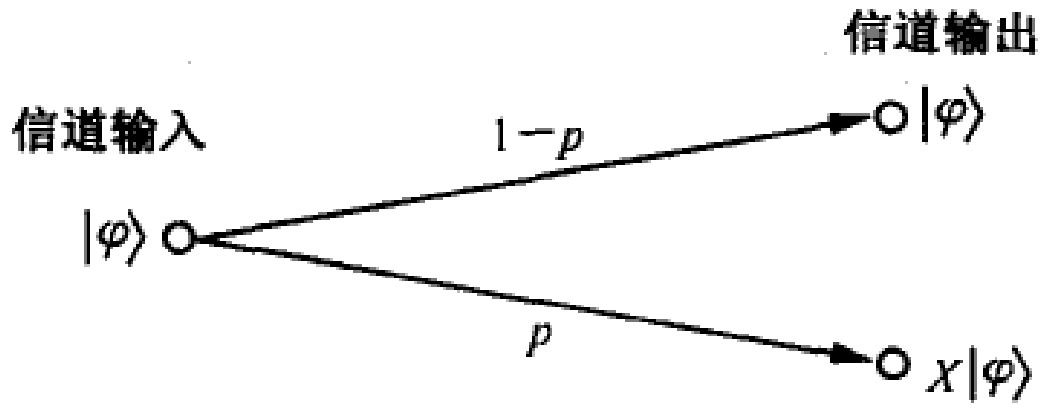
我们会尽量跳过数学上的细节

bit反转信道的量子纠错编码

输入 $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

以1-p概率原样输出，以p的概率作X-Gate演算（反转演算）

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$



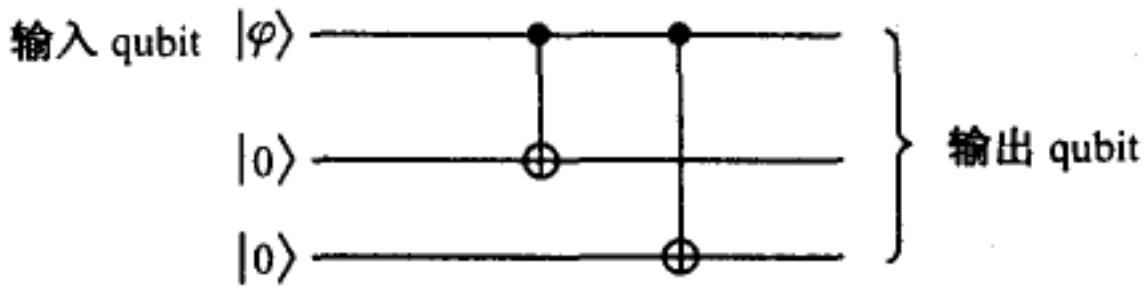
编码

类似经典编码

qubit		编码
$\|0\rangle$	$\longrightarrow$	$\|0\rangle\|0\rangle\|0\rangle = \|000\rangle$
$\|1\rangle$	$\longrightarrow$	$\|1\rangle\|1\rangle\|1\rangle = \|111\rangle$

假设编码保持线性　　$|\varphi\rangle = \alpha|000\rangle + \beta|111\rangle$

实际的编码器



解码方式D

接收到的信息		解码结果
|000⟩	$\xrightarrow{D}$	|000⟩
|001⟩		
|010⟩		
|100⟩		
|110⟩	$\xrightarrow{D}$	|111⟩
|101⟩		
|110⟩		
|111⟩		

解码操作保持线性 $D(\alpha|\varphi\rangle+\beta|\varphi'\rangle)=\alpha D|\varphi\rangle+\beta D|\varphi'\rangle$

第2个qubit出现bit反转错误，受信者接收到 $\alpha|010\rangle+\beta|101\rangle$

通过D变换得到纠正后的正确信息：

$$D(\alpha|010\rangle+\beta|101\rangle)=\alpha(D|010\rangle)+\beta(D|101\rangle)$$

$$=\alpha|000\rangle+\beta|111\rangle$$

与经典纠错编码的解码方式完全对应

量子纠错编码的性能比经典更难评估！

特定的叠加状态 $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$

2个bit反转错误 $\frac{1}{\sqrt{2}}(|101\rangle+|010\rangle)$

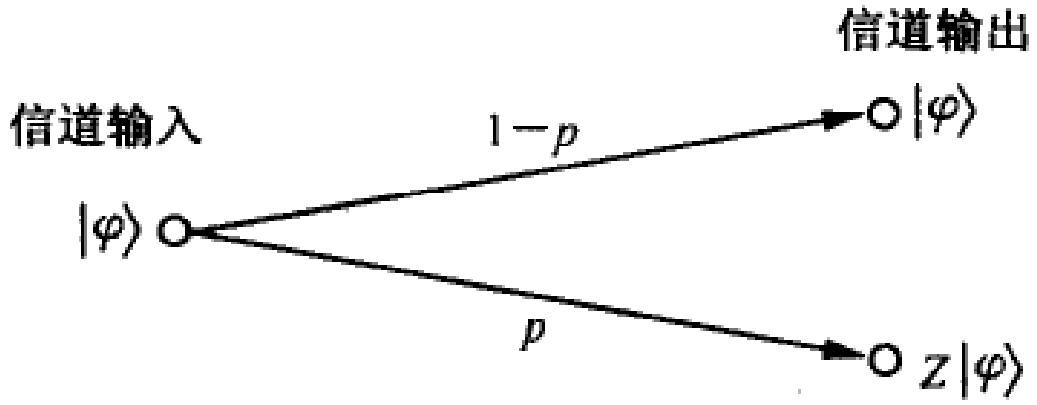
解码后得到正确结果 $\frac{1}{\sqrt{2}}(|111\rangle+|000\rangle)$

位相翻转信道的量子纠错编码

输入 $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

以1-p概率原样输出，以p的概率作Z-Gate演算

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$



非经典编码

Hadamard变换

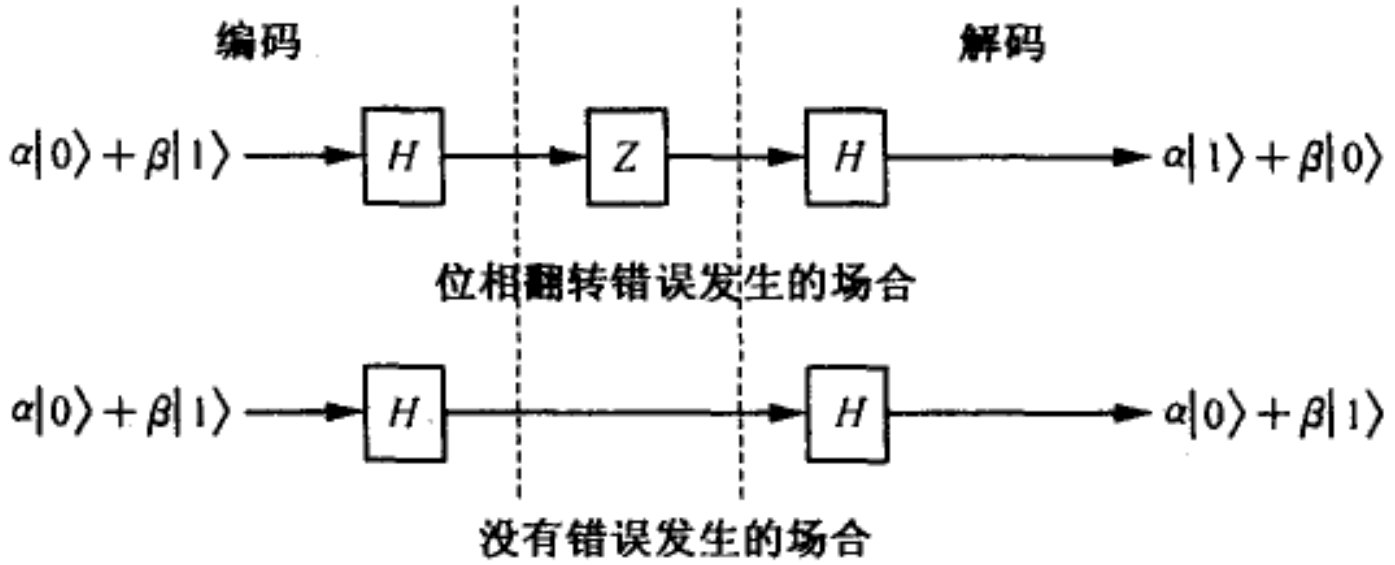
$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

简单计算

$$\begin{aligned}HZH &= \frac{1}{2}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\\ &= \frac{1}{2}\begin{bmatrix}1 & -1\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\\ &= \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\\ &= X\end{aligned}$$

将位相翻转错误转换成bit反转错误

对输入系统和输出系统添加Hardmard变换



$$|+\rangle = H\,|\,0\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$$

定义H变换后的状态

$$|-\rangle = H\,|\,1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

对各位qubit实施Hadamard变换

$$\begin{aligned}
&\alpha H\,|\,0\rangle H\,|\,0\rangle H\,|\,0\rangle + \beta H\,|\,1\rangle H\,|\,1\rangle H\,|\,1\rangle\\
&= \alpha\,|+\rangle\,|+\rangle 1+\rangle + \beta\,|-\rangle\,|-\rangle\,|-\rangle\\
&= \alpha\,|+++\rangle + \beta\,|---\rangle
\end{aligned}$$

对位相翻转信道输出的编码再次进行Hadamard变换后解码纠错

输入经过变换后编码 $\alpha|+++\rangle+\beta|---\rangle$

第2个qubit上发生位相翻转错误

$$Z|+\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix}=|-\rangle$$

$$Z|-\rangle=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{-1}{\sqrt{2}}\end{bmatrix}=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}=|+\rangle$$

接收到qubit列 $\alpha|+-+\rangle+\beta|-+-\rangle$

再次经过Hadamard变换

$$H\,|+\rangle = H(H\,|\,0\rangle) = |\,0\rangle$$

$$H\,|-\rangle = H(H\,|\,1\rangle) = |\,1\rangle$$

最终得到叠加态

$$\alpha|010\rangle + \beta|101\rangle$$

一般性的量子纠错编码

解决所有bit反转错误、位相翻转错误以及二者同时发生错误中任一种出现在某一位时的纠错编码

Shor编码：将上述两种编码结合起来

状态$|0\rangle$编码得到 $\frac{(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)(|000\rangle+|111\rangle)}{2\sqrt{2}}$

状态$|1\rangle$编码得到 $\frac{(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)(|000\rangle-|111\rangle)}{2\sqrt{2}}$

更一般性的错误纠正

一般性的量子错误能够用一个酉矩阵表示

纠一位错：Shor编码

纠多位错：经典线性编码→CRSS量子码、Goppa码等

更多实际问题：编码效率、解码难度……