浙江工商大学
ZHEJIANG GONGSHANG UNIVERSITY

量子信息技术

Quantum Information Technology

陈小余

目录


0
从电子信息到量子信息

01 优势： 电子信息，基于电子电荷（易于控制），基于电子的脱出功（不离开导体，即使是任意形状）。电子信息不使用电子自旋， 不考虑电子波动性。

02 基尔霍夫定律（欧姆定律）是什么历史地位？ 电流与电压成正比，速度与力成正比，亚里斯多德？ 牛顿第一运动定律，在电学中就是超导或者永久电流。介观实验。Aharonov-Bohm 效应

03 芯片的制造方式，对比于建筑学相当于挖窑洞。对碳纳米管，石墨烯还能这样做吗？

04 量子技术：我们用过吗？是的。比如核磁共振，激光，原子弹，超导，…。

量子：我们能看见吗？1902年的实验。

05 量子力学：迄今为止被实验验证得最精确的物理理论。

电子磁矩（g因子）的测量值： $(g-2)/2=0.00115965218073(28)$

量子电动力学的计算值： $(g-2)/2=0.00115965218178(77)$

难以置信的正确：没有与任何实验相违背。

06 难吗？很强的思辨性。容易吗？线性代数就够了。

07

量子纠缠 （1935-1985）惨淡50年

(1)EPR 1935　　(2)离散形式的纠缠态 1952

(3)贝尔不等式 1964，　为什么是贝尔？　(4)Aspect的实验 1982

08

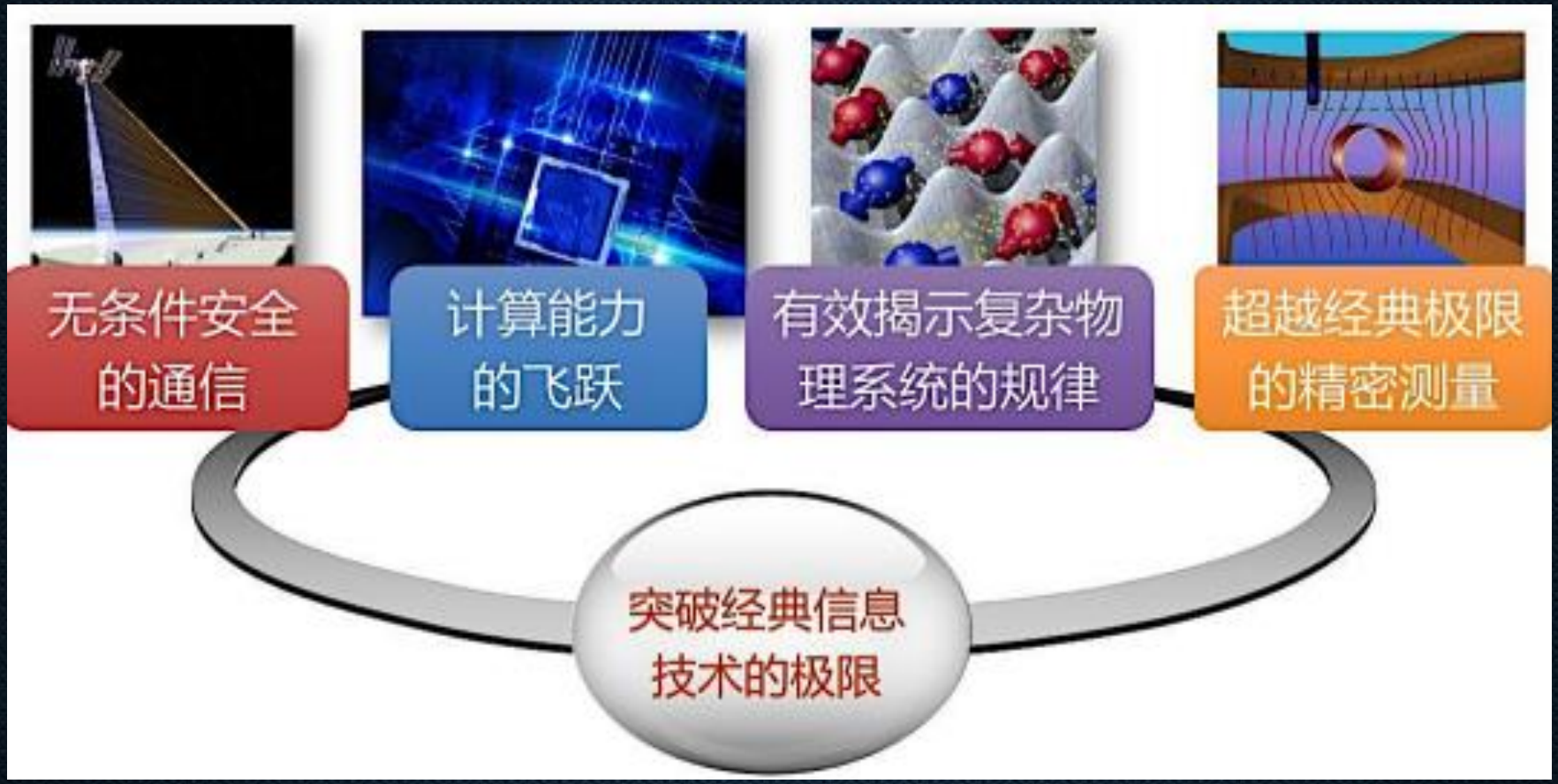
80年代　(1)费曼的量子计算机设想 1982　　(2) Deutch 算法 1985

(3)BB84协议　1984　(4)不可克隆定理 1982

09

90年代 (1) Shor算法 1996 (2)Grover算法 1996 (3) 量子编码 1995 (4)无噪量子信道编码定理 1993 (5)噪声量子信道编码定理 1996 -2003 (6)Teleportation 1993

第二代量子技术的主要内容



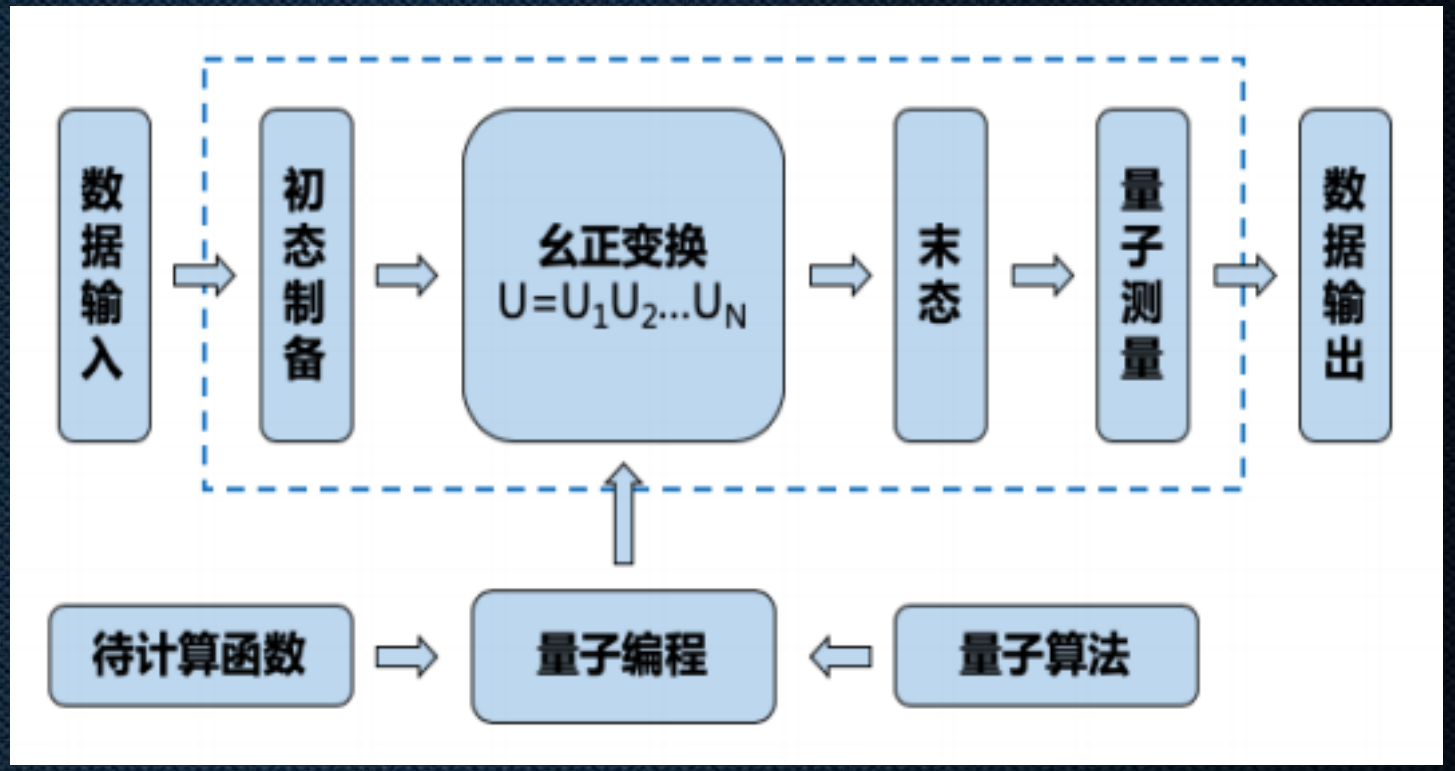
1 量子计算

01 量子计算模型

02 量子计算机的物理实现

03 量子计算的发展路径

量子计算机工作原理流程图



量子计算来源：可逆计算、并行计算

01：量子计算模型

量子线路模型

准经典法：其使用的语言和构造方法都和经典计算相似，只需要将经典的逻辑门换成量子逻辑门即可

One-way量子计算模型

量子法：一种通过制备量子纠缠态，然后经过简单的单比特测量来实现普适的量子计算方法

绝热量子计算模型

量子法：基于量子绝热定理，将问题映射到求解某个哈密顿量的基态问题上

拓扑量子计算模型

量子法：通过交换不同的任意子来实现免除噪音影响的普适量子计算

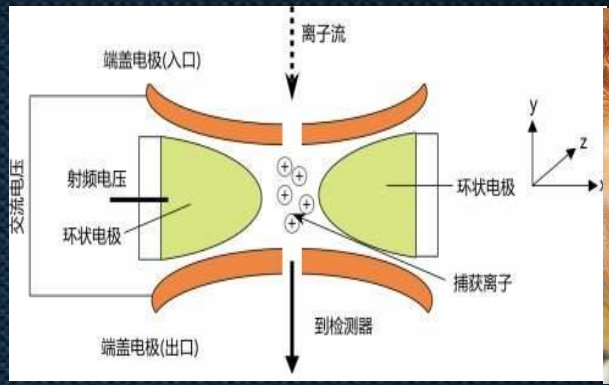
量子随机行走模型

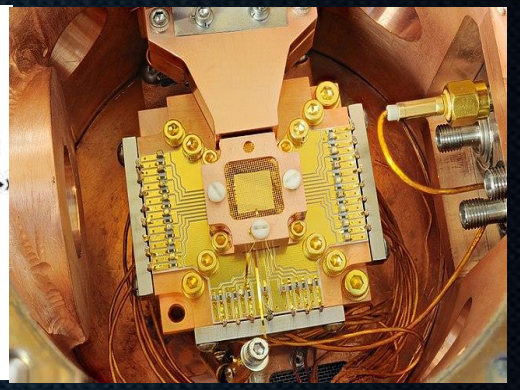
量子法：基于连续和离散时间量子随机行走来实现通用量子计算

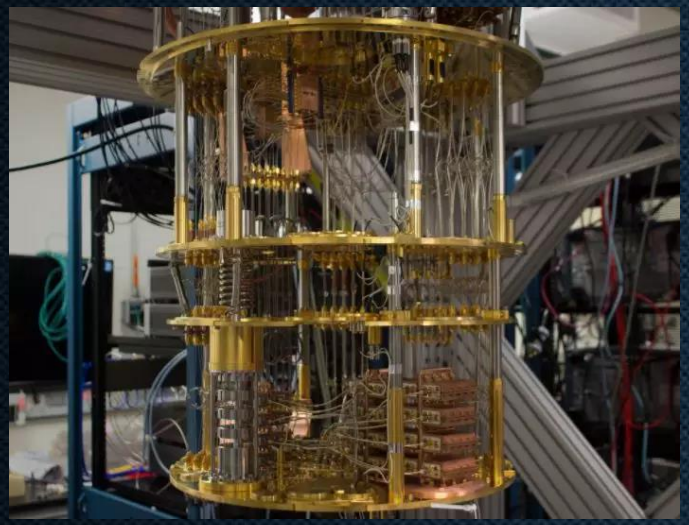
02：量子计算的物理实现

离子阱

1）：扩展性较为困难；
2）：单比特的初态制备实验误差 $<10^{-3}$
3）：比特操作的误差已经超过了实现普适容错量子计算的阈值；
4）：离子阱中状态读出误差很低（$<10^{-4}$）；
5）：可实现静止比特和飞行比特（光子）间的量子态转换。







超导线路

1）：有很好的可扩展性；
2）：利用反馈控制的比特初始化可以获得很好的效果；
3）：比特操作的保真度很高（99%）；
4）：相干时间能达到百毫秒量级；
5）：可实现高保真度的量子态读出（99%）。
6）：初步实现超导比特可以和飞行比特（光子）间的转换。

半导体量子点、光学量子计算、拓扑量子计算

03：量子计算的发展路径

量子霸权(Quantum supremacy)

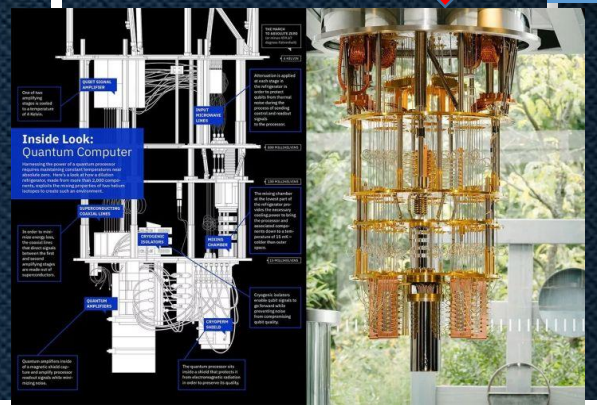
量子模拟机(Quantum simulation)

通用 量子计算(Universal Quantum Computation)

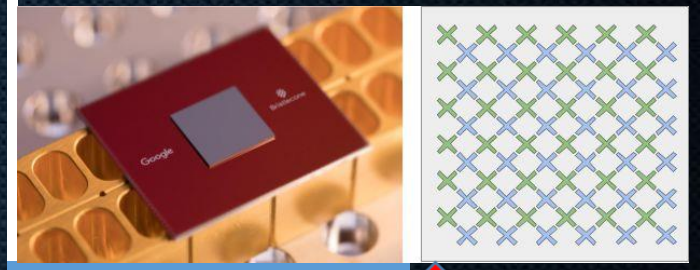
所谓“量子霸权”就是指：到底量子比特数到了什么程度，在某些特定问题上量子计算机就拥有了超越经典计算机的计算或者模拟能力。

加州理工学院的量子计算权威John Preskill 首先提出“量子霸权”的概念。初步估计需要50个量子比特。

中科大潘建伟和陆朝阳团队在二维光波导阵列上实现了10个光子比特的“玻色采样”。



IBM 推出了50个超导量子比特的量子计算原型机。



Google公布了具有72个量子比特的通用量子计算芯片Bristlecone。

Google宣布了量子霸权

2012 2017-05 2017-11 2018-03 2019


2
量子通信

01 量子离散变量密钥分配 (DV-QKD)

量子”数字通信”

（1）BB84协议、E91协议
（2）诱骗态协议
（3）双向量子通信
（4）设备无关协议

02 量子连续变量通信密钥分配 (CV-QKD)

量子”模拟通信”

（1）相干态编码
（2）压缩态协议
（3）CV-MDI-QKD

03 量子网络

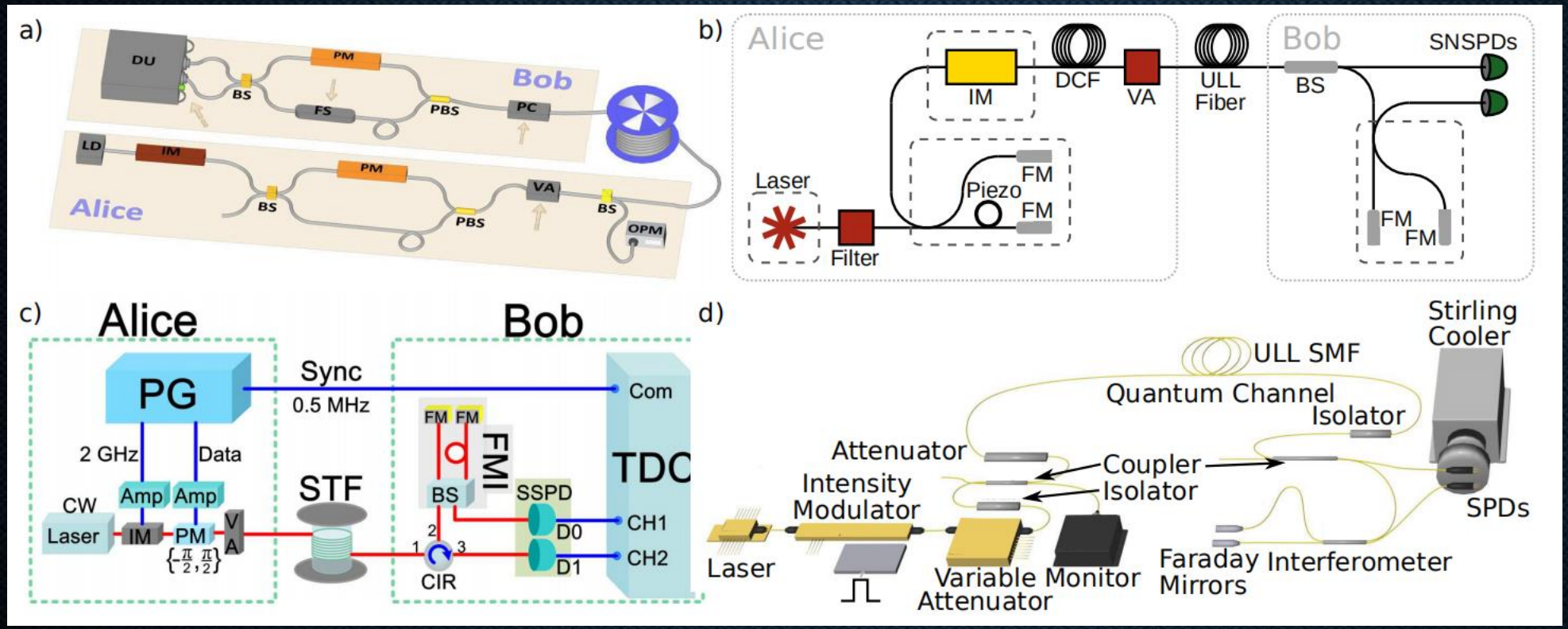
量子卫星、量子中继

04 量子信道编码定理

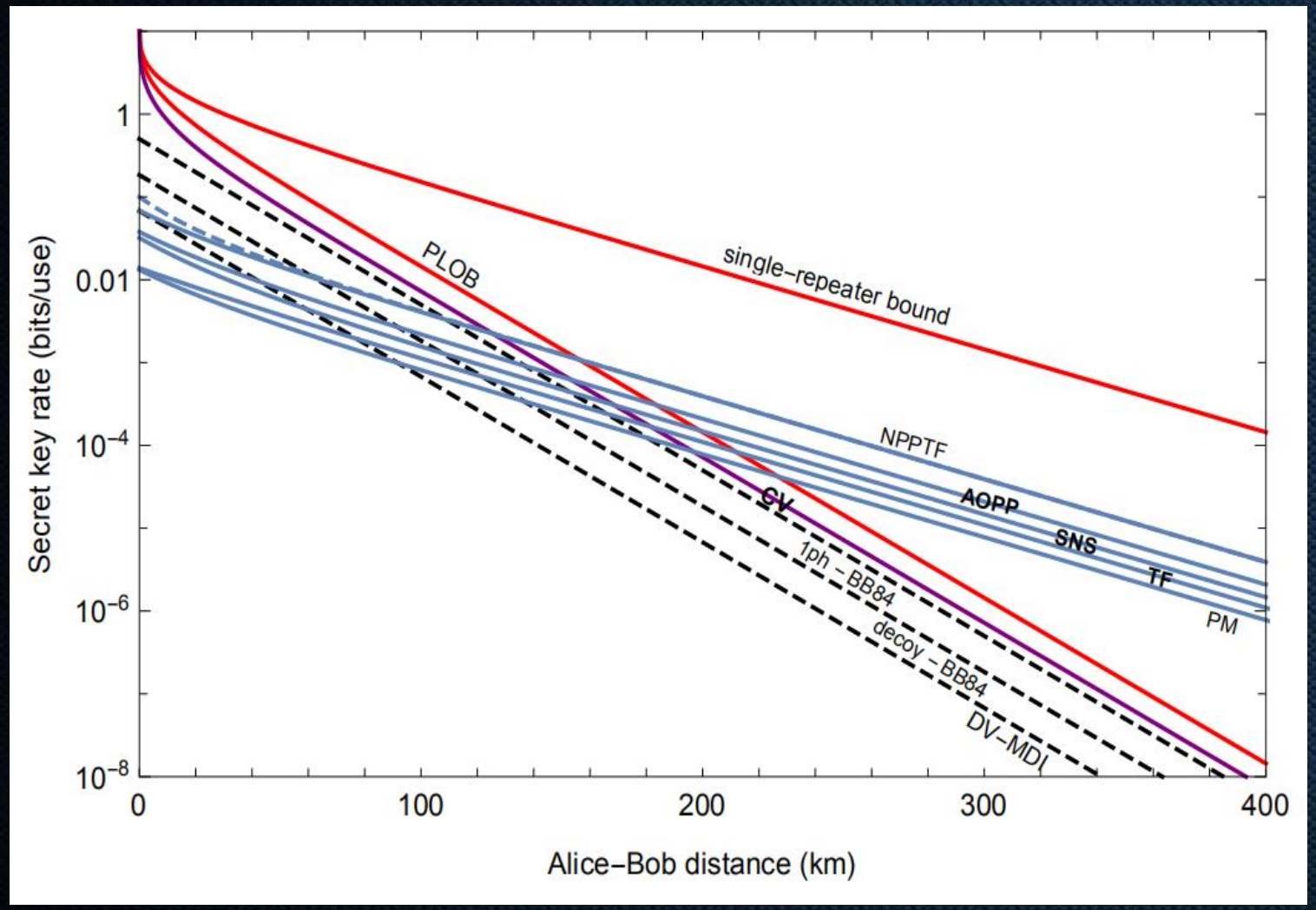
（1）经典保密容量、经典容量、纠缠辅助经典容量
（2）量子容量

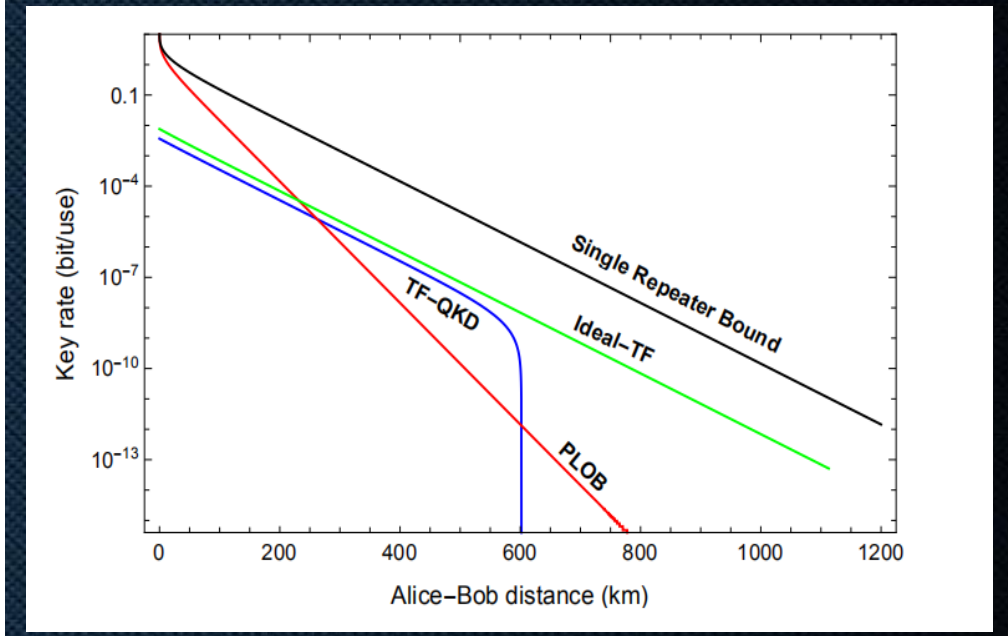
量子离散变量密钥分配 (DV-QKD)

- a) 双诱骗态BB84协议，1550nm，相位编码；
- b)单诱骗态BB84协议，1550 nm，421km，时隙编码；
- c) 差分相移编码，260km, 2GHz 码率，标准通信光纤； 超导单光子探测器；
- d) 相干单向协议，307km, 625MHz



量子密钥分配的性能界


Secret key rate (bits/use)
1
0.01
10^{-4}
10^{-6}
10^{-8}
0
100
200
300
400
Alice–Bob distance (km)
PLOB
single–repeater bound
NPPTF
AOPP
SNS
TF
PM
CV
1ph – BB84
decoy – BB84
DV–MDI


Key rate (bit/use)
0.1
10^{-4}
10^{-7}
10^{-10}
10^{-13}
0
200
400
600
800
1000
1200
Alice–Bob distance (km)
Single Repeater Bound
TF–QKD
Ideal–TF
PLOB

QKD渐近码率

Alice, Bob, Eve 分别具有变量 α, β, γ

单独攻击

$$R_{DR} = I(\alpha:\beta) - I(\alpha:\gamma)$$

$$R_{RR} = I(\alpha:\beta) - I(\beta:\gamma)$$

联合攻击

$$R_{DR} = I(\alpha:\beta) - \chi(\alpha:E)$$

$$R_{RR} = I(\alpha:\beta) - \chi(\beta:E)$$

$\chi(\alpha:E)$为Holevo 信息

纯衰减信道的私密密钥容量 $K = -\log_2(1-\eta)$,

η为透射率. (PLOB界,点对点);

单个中继容量: $K = -\log_2(1-\sqrt{\eta})$,

编码定理: $R \le K$

量子网络

- 网络上任意未知量子态从一点传到另一点有两种方案：
- (1) Teleportation, 转化为纠缠在网络上的分发。
- (2) QEC, （比特错误，相位错误，擦除错误） 需要量子计算组件。

- 两种方案都依赖量子中继平台。
- 纠缠交换和贝尔态测量是量子中继的要素.
- (1)概率量子中继 (2)确定性量子中继(用纠缠蒸馏或量子纠错) (3)无记忆量子中继(要求很高)

- 卫星量子通信

量子信道描述

- 量子态ρ用矩阵表示，称为密度矩阵，是正定的迹为1的矩阵。

- 信道将输入的量子态ρ映射为输出的量子态ρ’，信道用**超算符**表示.
- 一种等价的信道表示方法是**算符求和表示**，例如泡利信道ε

$$\rho' = \varepsilon(\rho) = p_0\rho + p_x X\rho X + p_y Y\rho Y + p_z Z\rho Z$$

- 量子信道必须将正定矩阵影射为正定矩阵，且保证迹为1不变。但这远远不够。它必须是完全正定的且保迹的，即对ρ的任意Spinespring 扩张ρ_{AB} 有 $\rho_{AB}'=(I\otimes \varepsilon)\,\rho_{AB}$ 保持正定。

- 量子信道是cptp (completely positive and trace preserving)

量子信道容量

- 双向量子容量Q_2，私密密钥容量K.

$$Q_2(\varepsilon) \le K(\varepsilon).$$

- 相干信息

$$I(\rho\rangle\varepsilon) = S[\varepsilon(\rho)] - S[(I_A \otimes \varepsilon)(\left|\Psi_{A\rho}\right\rangle\left\langle\Psi_{A\rho}\right|)]$$

$\left|\Psi_{A\rho}\right\rangle = \sum_i \sqrt{\lambda_i}\left|\xi_i^A\right\rangle\left|\psi_i\right\rangle$. 其中$\lambda_i, \left|\psi_i\right\rangle$是$\rho$的本征值和本征矢量。$\left|\xi_i^A\right\rangle$是辅助系统$A$的正交基。

ψ_i

- 量子容量Q

$$Q = \lim_{n\to\infty}\frac{1}{n}\max_{\rho_n} I(\rho_n\rangle\varepsilon^{\otimes n}).$$

- 可退化信道，图态编码


3
量子编码

量子编码（QEC）

为什么需要量子编码

量子态会受到环境的影响，导致系统的退相干。参考经典编码，可以将退相干看作是量子计算出错，也可以利用编码来解决。

如何实现容错

量子容错增加了实验实现量子计算机需要的量子比特规模。因此物理体系的可扩展性是关键！

量子容错计算的提出

除了环境外，量子操作、量子态制备和测量也都存在操作误差。 只要量子操作的出错率低于某个阈值，都可以通过适当增加量子比特把出错的量子态纠正回到它的理想状态去。

与经典编码的区别

1) 单个量子态的出错方式有比特翻转，相位翻转，比特相位都翻转，而经典计算的单比特出错是比特翻转；
2) 经典比特可以通过测量来判断错误是否发生，而一般的量子测量会导致量子态的塌缩，进而破坏整个计算过程。

还有一种方法是动力学去耦（dynamic decoupling）

离散系统量子编码——图态码

- 逻辑量子比特用多个物理量子比特以图的方式编码
- 图是点和边(连线)的集合， 每点赋以量子比特态 $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}$
- 对n点图，有量子态 $|+\rangle^{\otimes n}$
- 对每条边赋以控制非门

$$U_{ab} = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}; \quad U_{ab}|c\rangle|t\rangle = |c\rangle|t\oplus c\rangle.$$

- 则图态是 $|G\rangle = \prod_{ab\in E} U_{ab}|+\rangle^{\otimes n}$
- 图态基 $|G_{k_1k_2\ldots k_n}\rangle = Z_1^{k_1}Z_2^{k_2}\ldots Z_n^{k_n}|G\rangle$
- 例子： 贝尔态

- 例子：多体GHZ态， n点全连通图
- 用于量子容量的逼近计算

连续变量系统量子编码-----二项式码

Nature Physics 15, 503-508 (2019); Phys. Rev. X 6, 031006 (2016).

- 保护L 个光子丢失， 错误集 $\varepsilon_L = \{\hat{I},\ \hat{a}, \hat{a}^2, ..., \hat{a}^L\}$
- 单光子丢失码：错误集 $\varepsilon_1 = \{\hat{I},\ \hat{a}\}$
- 逻辑量子比特

$$|0_L\rangle = \frac{|0\rangle + |4\rangle}{\sqrt{2}};\ {}^{a}|1_L\rangle = |2\rangle.$$ 其中$|n\rangle$表示光子数为*n*的量子态

- 注意到

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle$$

- 有

$$\hat{a}(u|0_L\rangle + v|1_L\rangle) = u\sqrt{2}|3\rangle + v\sqrt{2}|1\rangle$$

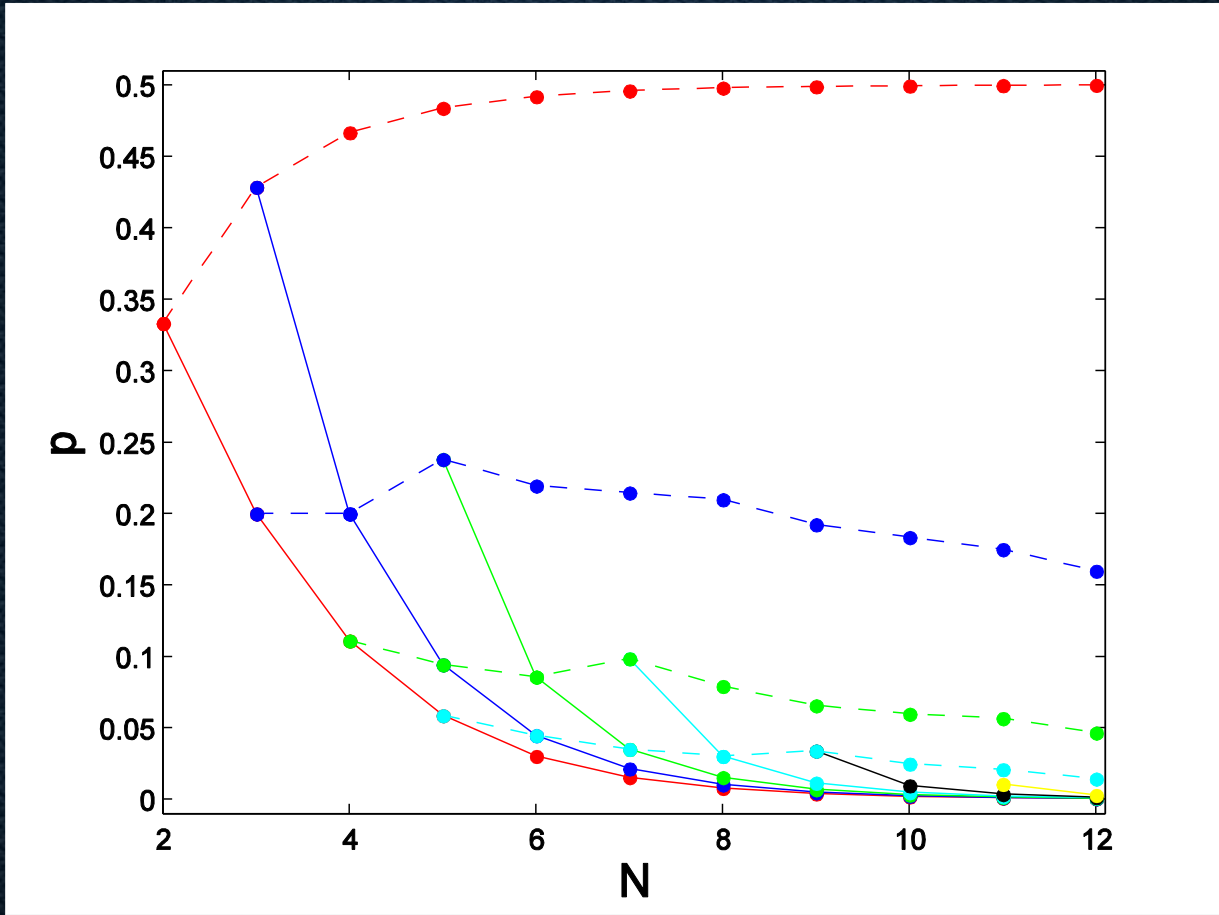
- 量子信息（复数u,v)没有改变。

4 量子纠缠

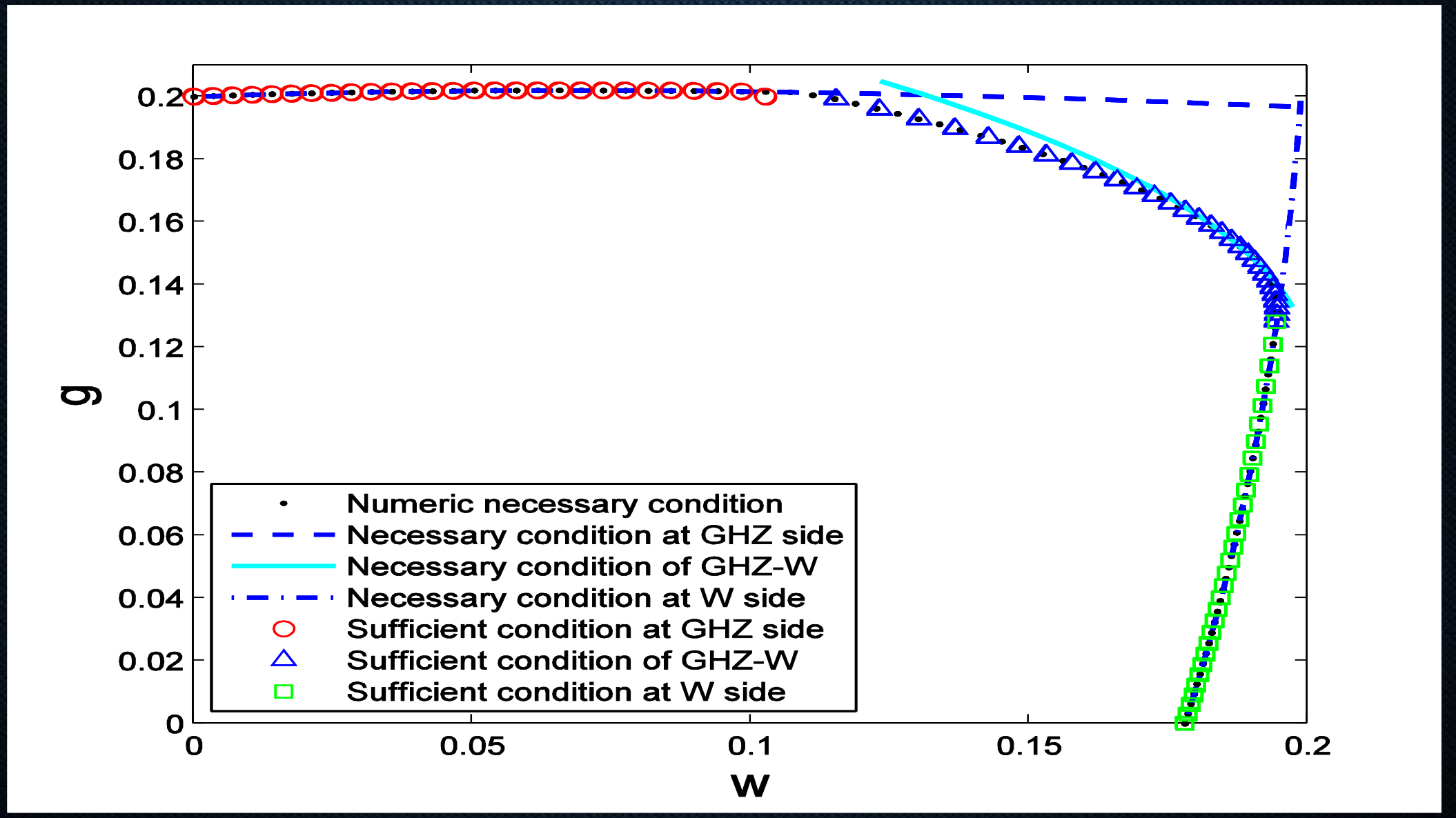
量子纠缠的判定

- 双量子比特：完全解决。双模高斯态：完全解决。两体问题：PPT
- 多体纠缠问题：NP hard
- 实验出现的多是特定态，几种不同的信道，用纠缠见证者方法。
- 多体纠缠的一些研究结果：

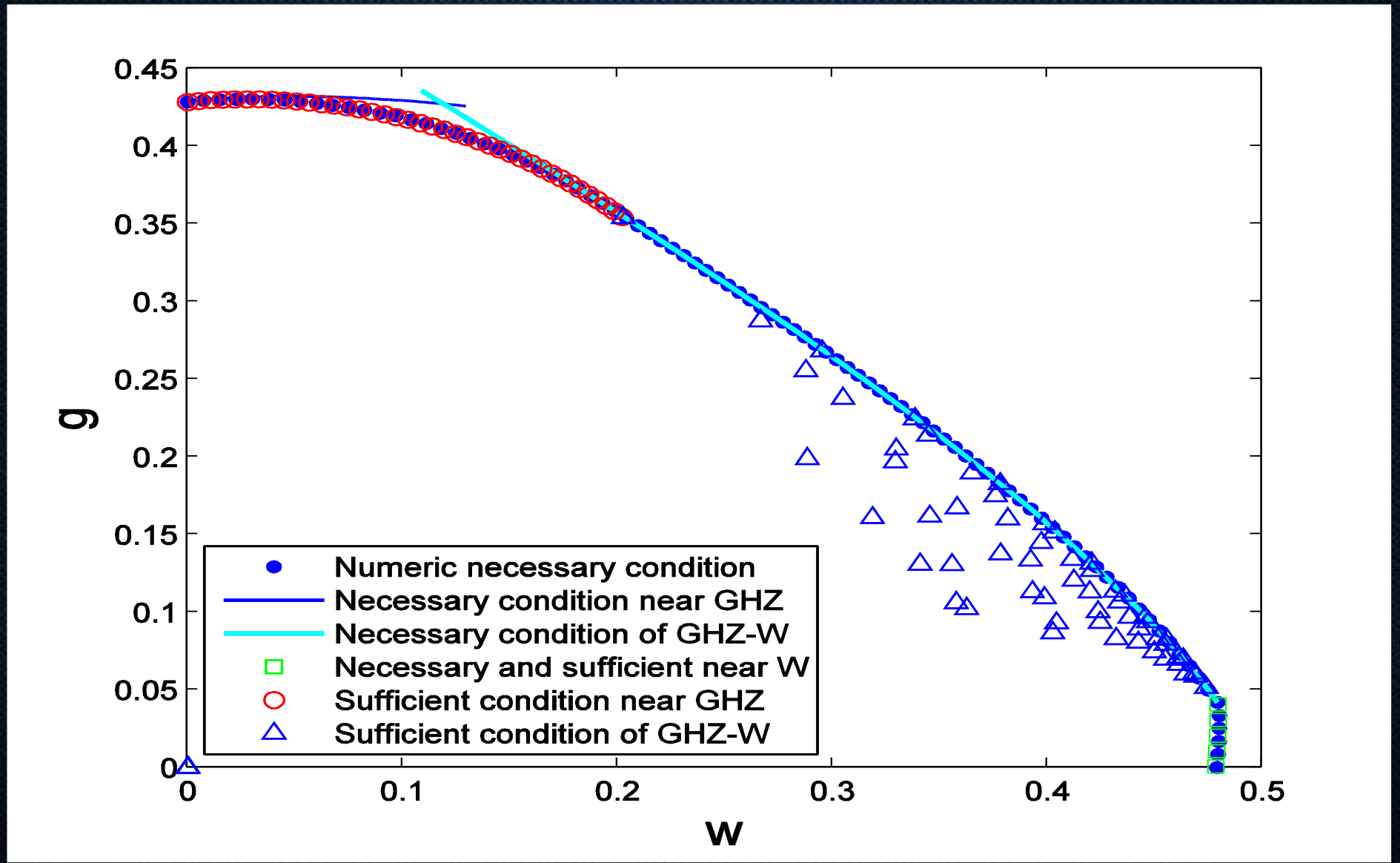
N qubit GHZ态与白噪声混合



3 qubit GHZ-W (完全可分)



3 qubit GHZ-W (2可分)




谢　谢　！