**本文转自："亦仙亦凡"微信公众号**

# 量子通信的机会与挑战

杨义先 教授

北京邮电大学信息安全中心主任

2016 年，当媒体上的量子通信惊天动地，今天要手撕全球黑客，明天又要脚踏算法密码时，老夫横刀立马，狠狠地泼了一盆凉水（见文献[1]），希望能让那些"见神灭神，遇佛杀佛"的量子唐·吉诃德们清醒清醒。虽不知老夫的那盆凉水是否算杯水车薪，但几年过去了，曾经"只听楼梯响，不见人下来"的量子之神，不但始终没能露面，甚至干脆连楼梯都不响了！唉，唐吉诃德们集体失声了；这至少说明老夫的那盆凉水没泼错。

现如今，当量子界万籁俱寂时，老夫却又着急了。这不，现在又来赤膊上阵，改"泼水"为"浇油"了！准确地说，是来给量子界加油鼓劲了！（见文献[2]）为啥呢？唉，因为老夫又不得不给自己的本行，正如日中天的通信界泼凉水了，而且还是很大一盆冰凉冰凉的凉水！通信界若想躲过这盆凉水之劫，在很大程度上可能得求助于量子通信；而且，还需要量子界与通信界精诚合作。**请相信，无论是量子专家，还是通信专家，都不可能单独撑起量子通信这片天。**

原来，在晴空万里的通信蓝天，出现了两朵不祥的乌云。

一朵叫**"香农信道容量极限危机"，即，随着 5G 手机等为代表的通信技术的飞速发展，端到端通信的香农信道容量极限，即将被逼近。**啥意思呢？换句话说，端到端信道的信息传输能力，将再也没有巨大潜力可挖了，虽然还可以采用一些改进型的技术，从骨头里勉强再榨出些油来！若用科幻小说"三体"的俗话来说，端到端通信的理论，就被三体人的"智子"锁死了。更麻烦的是，如今包括通信网、互联网、物联网等在内的所有信息网络，都是借用诸如时分复用技术、频分复用技术、码分复用技术等，在"瞒过"人类生理感官极限的前提下，将许多"端到端信道"生硬地拼接而成的"假网络"。一旦这些"假网络"中的某些"端到端信道"的容量达到极限后，整个"假网络"就必然出现"心肌梗塞"。

另一朵乌云，名叫**“摩尔定律危机”，即，信息存储介质的增长速度，即将慢于“摩尔定律”的预期。**若不能及时清除通信蓝天的这两朵乌云，整个信息领域的发展，也就基本到头了，信息通信领域的专家们就可以准备“洗洗睡了”。

本文只涉及第一朵乌云。为此，先回忆一下**通信系统的三要素：发信方、收信方和信道。**如果只有一个发信方和收信方，那么，香农的信息论就精确给出了信道的容量极限，而且这个极限的潜力即将被 5G 或随后的 6G 等耗尽。幸好，在真正的网络通信（特别是互联网）实践中，人际之间的通信需求，大都是网络式的，而不是端到端的。但不幸的是，如今的信息网络却都是由端到端的信道拼接出来的。于是，就出现了这样的矛盾：一方面，用户的真实需求是低标准的、网络式的，即，有时可以与多人共享通信内容；但另一方面，在工程上满足用户需求时，却不得不采取高标准的端到端信道拼接，即，出现相同内容反复转发的情况，从而浪费了许多通信能力。**若信道容量的潜力足够大，那这种供需矛盾就可忽略不计；但若香农极限被逼近或达到后，该供需矛盾就会突然白热化。**

如何解决这种白热化的矛盾呢？主要思路有两条：**其一，搭建“真网络”；其二，寻求新的信息载体。**

当然，无论要想实现哪种思路，都相当困难，都甭指望能立竿见影，必须未雨绸缪。但无论是哪种思路，量子技术也许都能发挥其独特作用。

## （一）关于搭建“真网络”

**什么才是真正的“网络”呢？**这还真不好说清楚，但可以肯定的是，**除小规模局域网等小型网络之外，目前全球的所有大型网络都不是真网络，因为，它们都可能发生局部“心肌梗塞”。**幸好，从理论上看，控制论的创始人维纳，于 1950 年提出的对话网络（见文献[3]），以下称为“**维纳网络**”，不会发生局部“心肌梗塞”，所以暂且认为它是一种真正的网络；而且，好像再也找不到整体传输能力比“维纳网络”还大的网络了（神经网络除外，因为目前人类对其结构还不太清楚）。有关“维纳网络”的细节描述，此处就省略了，大家不妨将它粗略想象成“带权值的全联通网”；有关“维纳网络”及其信息传输容量极限，请见《安全通论》（见文献[4]）第八章“对话的数学理论”；而香农的端到端信道容量极限，只是维纳网极限的一种特例。

**如何搭建“维纳网络”呢？**

让我们用排除法来进行“地毯式搜索”吧。首先，“不能被重叠的信息载体”都派不上用场，所以，**“真网络”中的信息载体必须具有“可重叠性”；**而波和量子纠缠，才是少有的具有“可重叠性”的信息载体。再看波类载体，声波显然不行，它根本就传不远，因此只剩电磁波了。但受限于电磁波的频谱，无论多么精细的调频或调幅切割，都不可让全球用户同时共享一个频段的电磁波，只能采取诸如蜂窝网等现行策略；但是，一旦出现哪怕一个蜂窝，它就是潜在的局部“心肌梗塞”点，相应的网络就不再是“真网络”了。就算电磁波的高频或甚高频等还有潜力可挖，但也只是“战术级”的动作了，不可能搭建出全局性的维纳网络；当然，部分采用维纳网络的结构，也是一种过渡办法，也可以敲骨吸髓。**于是，根据人类现有的知识，好像最终唯一的备选，就只剩下以量子纠缠为代表的新希望了。**

**如何用量子手段来搭建维纳网络呢？**

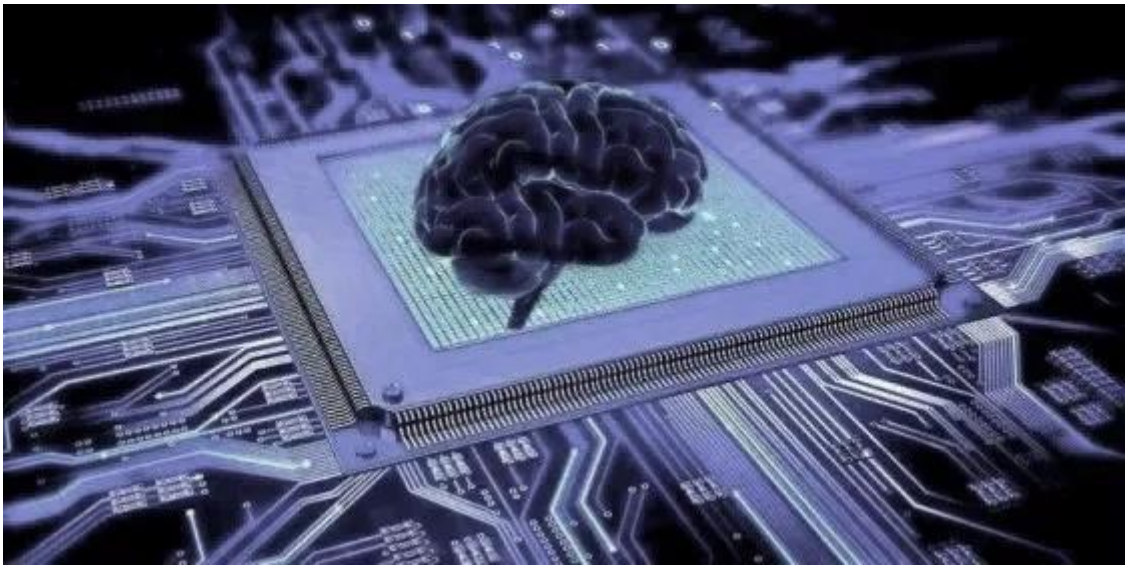
这绝对是一个相当艰难的问题，肯定需要长期研究；既不要轻易庆功，更不必过于悲观，特别**是要分清量子界和通信界中的许多东西，哪些是假设，哪些是结论。**比如，与欧氏几何类似，量子力学只是基于五个基本假设之上的理论，其中陷阱特多，甚至包括我自己的文章[1,2]和本文的描述，也难免有许多瑕疵；当然，量子力学中已被实验证实的东西（如不确定性原理和量子纠缠态等）肯定为真，而某些推导的结论则要认真挖掘，小心对待；比如，“量子不可克隆”其实是有条件的，需要搞清楚到底在哪些条件下有可能克隆，哪怕其条件相当苛

刻，也意味着一线希望。另外，从通信角度看，只要是能变化的东西，或只要是能区分出差别的东西，都能用于传递信息；因此，只需量子专家提供出能“区分差别”的东西就够了，而不管它们到底有多么玄幻或多么违背直觉。**特别需要注意的是，“不能超过光速”的限制，只对物质和能量有效；**没有任何人严格证明过“信息的速度不能超过光速”，当然更没有对此给出过证伪，因为过去压根儿就不必考虑这样的奇怪问题；此外，“信息必须有载体”只是一个过去认为“不证自明的公理”，而绝不是结论，但谁又能保证不会像“非欧几何”那样，被别的公理所替代呢？

伙计，上面这一大段绕口令式的陈述，到底在说什么呢？其实，只说了两点：**第一，过去媒体反复歌颂和宣传的所谓“绝对安全的量子通信”都是瞎扯；第二，不能轻易放弃量子纠缠的通信潜力。**

注意，此处没谈 BB84 等量子密码，它确实是一种“绝对保密”，但绝对不是“绝对安全”的密码手段，比如，至少不能防止鱼死网破式攻击；**从综合优势来看，它与现行的其它加密手段相比，并无绝对优势，更不可能替代所有其它密码，**绝不值得像前几年那样举国欢庆，当然确实是值得深入研究并大力推广。

当然，除了搭建维纳网络之外，**“模仿大脑神经网络”也是构建“真网络”的另一个途径。**可惜目前人类对神经网络还相当陌生，只知道它的传输效率奇高，能耗奇低，处理速度奇快。但是，大脑神经网络是维纳网吗？不知道！神经网络的通信奥秘到底是什么？仍不知道！不过，这不是本文的话题，故只点到为止。



## （二）关于寻求新的信息载体

从发明用火，到能将火用于通信载体，即，烽火通信，人类探索了至少一百万年！从公元前 2750 年发现电，到 1937 年能将电用于信息载体，即，电报通信，人类探索了约 5000 年！从公元前 3200 年左右发明文字，到公元 105 年蔡伦造出理想的文字信息载体（纸张），人类探索了三千多年！从 19 世纪末发现量子现象到如今，总共也不过区区 100 年；因此，大可不必责怪为啥量子还没成为通信信息载体！也许有“杠精”要质疑：为啥电磁波从发现到用于无线通信，只用了不到半世纪呢？其实，仔细分析一下就不难发现真相：原来，电与磁本来就是一体，电磁波真正传输的不是直接的信息，而承载了信息的电；而在电磁波之前，人类已能用电来传信息了，所以，电磁波其实只是信息载体的载体，它只是捡了一个便宜，所以很快就被用于通信了。

**从理论上看，任何物质和能量都能当成信息的载体，但前提是，人类必须对这种东西有相当的了解。**比如，若不能人为地生火或灭火，那就不可能有烽火通信；若不能人为地通电和断电，那就不可能有电报；若对电磁波的频率、振幅等内部结构不了解，那压根儿就不可能有今天随处可见的移动通信。但是，关于量子，人类又知道多少呢？除了“知其然不知其所以然”的所谓波粒二象性、不确定原理、量子纠缠态等极少数怪象外，剩下的东西就少得可怜了；甚至，除了不多的实验结果外，一般人都搞不清楚到底哪些是假设，哪些是结论。

**提高通信能力的另一种办法，是编制尽可能高效的码书。**为此，香农已在理论上给出了最佳的**“信源编码定理”**。但是，量子计算机却又开辟了另一种可能的信息编码渠道，虽不知该叫

啥名字。实际上，量子计算机确实能经过多项式级别的运算动作，完成诸如大数分解这样的、在普通计算机上需要指数级别运算的动作；**而计算与通信在本质上是相通的，即，通信就是计算，计算也是通信；**换句话说，整个通信网络完全可看成是一个大型的计算机，而任何计算机的内部其实也是各种元器件组成的小型通信网络；因此，只要充分利用好量子的叠加特性，就不排除这样一种可能性：用多项式级别的“量子比特”去承载指数级别的“电子比特”。如此一来，即使是利用现行的普通网络，只要有特殊的收发设备（比如，量子计算机），就能呈指数级地提高现行网络的通信能力，这也相当于在应用角度看，彻底度过了“香农信道容量极限危机”。

**注意：**这种高密度打包传输信息的做法，在每个人身上，每时每刻都在发生，它就是细胞分裂或生物遗传时的 DNA 信息传输！比针尖还小的一条 DNA，就浓缩了海量的生物生长和遗传信息。再用三体的俗话来类比，传输过程中用高维质子，收发双方再将该质子进行低维展开。

**总之，在可见的将来，量子通信问题，只是学术问题或技术问题，不是商业问题或新闻问题，更不是什么政治问题。**真心希望大家各就各位，该闭关的闭关，该下班的下班；该回家的回家，该找妈的找妈。反正，没必要围观看热闹，真的假不了，假的也真不了！

## 参考文献

[1] 杨义先，量子的安全笑话，科学网博客，

网址：http://blog.sciencenet.cn/blog-453322-1010441.html

[2] 杨义先，量子通信的价值到底在哪？科学网博客，

网址：http://blog.sciencenet.cn/blog-453322-1230628.html

[3] N.维纳著，陈步译，人有人的用处，北京：北京大学出版社，2014 年 6 月。

[4] 杨义先、钮心忻，安全通论，北京：电子工业出版社，2018 年。

[5] 杨义先，钮心忻，安全简史，北京：电子工业出版社，2017 年。

临菲信息技术港

临菲信息技术港公众号


临菲学堂