只能用于高斯玻色采样，它们做不了别的计算。

它们目前的主要意义，是为了验证和实现“量子优越性”，也就是在特定问题的计算能力上，量子计算要远远超过经典计算。“九章”的数据是：处理高斯玻色取样问题的速度比目前最快的超级计算机“富岳”快 100 万亿倍，且等效速度比谷歌的“悬铃木”快 100 亿倍左右。这已经实现了量子优越性。

用“九章”研制团队领衔人、中国科学技术大学教授潘建伟的话来说：现在的量子计算原型机更像是一个“玩具”，只能在玩某一个游戏方面击败经典计算机。在施郁看来，即使是这样的“玩具”，也是值得开发研究的，因为科学家需要通过这个过程进一步驾驭量子计算。

要攻克的难关是操纵更多的量子比特，而且在这个过程中保持它们的量子性质。量子状态是很脆弱的，要隔绝外界环境对它们的干扰，需要先进的技术来保障。验证量子优越性，需要操纵约 50 到 100 个量子比特，2019 年谷歌的“悬铃木”包含 53 个超导量子比特，2020 年中国的“九章”操纵了 76 个光子。

另一个有意义的研究方向是在经典计算机上模拟量子计算，演示量子比特如何对不同操作做出反应，为量子计算开发出适合特定科学领域的量子算法。

“这样的量子算法，现在还是不多的。”施郁向《新民周刊》记者表示。在他的研究团队里，有擅长经典计算机编程的，也有擅长相关物理领域的。

等到人们能操纵数百个量子比特，才可以解决某些经典计算机无法胜任的实用问题，例如量子化学、新材料设计、优化算法等。那时，量子计算机才开始从“玩具”变成“工具”。这是当前全球量子计算研究团队的主要任务，科学家们希望能在 5–10 年实现目标。

目前科学界认为量子计算能解决的实际问题，包括对密码的破解、大数据搜索、生物医学领域的一些模型构建等，就需要操纵至少几百万个量子比特才能实现，同时还要满足大于 99.9% 的操纵精度。做到这一步，也就是实现了可编程的通用量子计算机。学术界普遍认为，这个目标面临的挑战是巨大的，至少还需要 20–30 年的时间来攻关。

量子计算发展到可以解决实际问题的时候，是否会逐渐替代经典计算？换句话说，将来是否会由量子计算“一统天下”？施郁表示：这是不会发生的。因为量子计算和经典计算各有各的优势，人们当然是选择在对应的领域更合适、性价比更好的计算方式；两者不是谁取代谁的关系，而是互相补充的关系。那些经典计算机需要的时间太长、无法胜任，而量子计算费时

施郁多年来一直不遗余力地进行量子力学的科普宣传。

短的计算领域，才是量子计算机的用武之地；而且专用量子计算比通用量子计算现实得多，通用量子计算的实现难度要大得多，对量子比特个数、纠错和抗噪声的要求都更高。因此，量子计算具备有条件的“优越性”，但并没有超越一切的“霸权”。

“量子通信”到底意味着什么？

量子通信，是目前量子科技最“接地气”的一项应用领域。如果说墨子号量子通信卫星上天、“京沪干线”建成，还是让人们认为量子通信的“绝对安全”暂时只应用于军事、金融等高端特定领域的话；那么最近国内电信运营商推出的“量子密话”，就把量子通信与普通人的距离拉得更近。

这款移动通信产品宣称将 5G 通信与量子通信技术紧密结合，已成功在安徽试商用，用户只要更换为专用的安全通话 SIM 卡，再下载相应 App 就可实现安全通话，换卡的费用在 100 元以内。

这种“量子密话”，是利用量子随机数及量子密钥分发机制来生成认证密钥及通话密钥，其密钥具有“真随机性”。

“真随机性”是相对普通加密方式而言的。这些密钥只能用一次，用户每次发起“量子密话”时，系统会随机抽取 SIM 卡内的一个量子密钥与后台建立连接、校验身份信息；认证通过后，再另外实时生成一个新密钥作为会话密钥。认证密钥与会话密钥分离，用后会废弃。

当然，某次通话的密钥使用后，在理论上经过巨大的演算时间，有可能被破解；然而下一次通话又采用了新的密钥，所