隐秘量子计算机在实验室诞生

隐秘计算(blind computing)是一种安全的远程计算.用户可以使用放在远处的计算机服务器进行计算,但是他的输入、计算过程或者输出结果不会泄露给任何其他人,包括服务器的提供商.现在具有这种特点的隐秘量子计算机在实验室诞生了,维也纳大学的 Philip Walther 及其同事在实验室里演示了一个小型隐秘量子计算机[1].

量子力学原理使得量子计算机具有比经典计算机更加强大的信息处理能力,而量子通信具有抵御窃听的安全性.隐秘量子计算结合了量子计算和量子通信的优点,具有重要和广泛的应用前景.牛津大学的 Vlatko Vedral 评论说,"隐秘量子计算可能是近十年来量子计算中最激动人心的想法".

隐秘量子计算机实验演示的方案是 2009 年由 Anne Broadbent (加拿大滑铁卢大学), Joseph Fitzsimons (当时也在滑铁卢大学,现在是在新加坡国立大学), 以及 Elham Kashefi (爱丁堡大学)提出的[2].量子计算有几种模式:量子线路、绝热量子计算和单向量子计算.Broadbent 的方案基于单向量子计算模式.单向量子计算是对所有量子计算先准备好纠缠度很高的团簇态,然后进行一系列单比特的测量,这些测量结果再经过经典计算机处理后得到计算的结果.

在 Broadbent 提出的方案中,为了能进行隐秘保密计算,首先从终端输入只有自己知道相位为 θ_i 的态,并且要求计算机使用角度 δ_i 进行测量.然后计算机将输入的量子比特纠缠起来,进行测量,最后返回计算的结果.由于不知道 θ_i 的大小,计算机和窃听者都不能从 δ_i 和测量结果推测出计算的结果.

与以前提出的保密计算机协议不同,Broadbent 等人的方案所要的操作都是现有技术上能够提供的.甚至在远程计算机方面所做的事(包括将输入量子比特成对地纠缠,然后再一个一个地进行测量),也能在小型系统中进行,正如 Walther 等人已经做到的那样.Walther 组用的量子计算机有 4 个光子比特.虽然这样大小的量子计算机还不能进行太多的计算,但是他们成功地实现了单比特量子门以及两比特的量子门.而这些量子门是最终构造更大量子计算机的基本构件.他们还完成了两个小规模的量子计算,包括量子搜索算法.量子搜索算法比经典搜索算法有更高的效率.并且他们发现,为了实现保密,并不需要计算机对所有的量子比特都隐秘.在他们的四比特系统中,只需要 2 个比特(θ_2 和 θ_3,在图中为黄色和绿色,见《物理》网刊彩图)隐秘未知就可以了.该发现有助于将来更容易地实现更大规模的隐秘计算(见图 1).

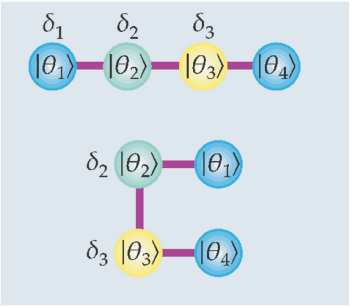

图 1 单向量子计算中的单比特门(上)和两比特门(下).量子比特的初始态为 $|\theta_i\rangle$,成对地纠缠在一起,然后从左向右用 δ_i 进行测量(不一定按数目顺序).最右边的比特是门的输出比特,在更复杂的量子计算中,它们还可以成为另一个量子门的输入.当 θ_2 和 θ_3 是保密的时候,计算是隐秘的,计算机和窃听者都不能推测出里面进行的计算(内容来自文献[1])

参考文献

[1] Barz S *et al*. Science, 2012, 335: 303

[2] Broadbent A, Fitzsimons J, Kashefi E. In: Proceedings of the 50th Annual Symposium on Foundations of Computer Science. IEEE Computer Society, Los Alamitos, CA (2009), p. 517; available at http://arxiv.org/abs/0807.4154

(清华大学 龙桂鲁 编译自 Johanna Miller. *Physics Today*, 2012, (3): 21, 原文详见 http://ptonline.aip.org)