**女博士7年不肯毕业，终一战成名！获理论计算机界至高荣誉，她破解了“量子计算最基础问题”**

2018-10-21 11:40 来源:[DeepTech深科技](http://www.sohu.com/" \t "_blank) [公司](http://www.sohu.com/tag/77937) /[计算机](http://www.sohu.com/tag/59959) /[量子计算机](http://www.sohu.com/tag/69991)

原标题：女博士7年不肯毕业，终一战成名！获理论计算机界至高荣誉，她破解了“量子计算最基础问题”

在今年于巴黎举行的理论计算机科学领域的最顶级会议——计算机科学年度基础论坛（FOCS）上，一位来自加州大学伯克利分校的博士后“一战成名”：乌尔米拉·马哈德（Urmila Mahadev）的成果被**会议授予“最佳论文”和“最佳学生论文”奖。这是理论计算机科学家梦寐以求的殊荣。**

曾经与马哈德合作的加州理工计算机科学家托马斯·温迪克（Thomas Vidick）在博文中表示，**“这是近年来理论计算机科学和量子计算交叉领域中最杰出的成果。”**

被德州奥斯丁大学的计算机科学家斯科特·阿伦森（Scott Aaronson,）认为，马哈德这一被统称为“盲计算”的工作，**将使其成为量子计算理论领域的新星。**马哈德的博士生导师乌尔什·瓦斯拉米（Umesh Vazirani）也表示，她学生的论文非常出色。



图 | 马哈德在计算机科学年度基础论坛获奖（来源：FOCS）

如此成果的背后，是这位女科学家“顽固”的 7 年博士生涯：到了马哈德 28 岁的时候，她已经在加州伯克利研究生院度过 7 个年头——大多数研究生根本不会待这么久。然而，**马哈德并没有考虑毕业，因为她认为自己的工作还没完成。**

直到 2017 年春季，她才终于确认，**自己已经解决了量子计算中的核心问题之一：如何证明量子计算机的输出结果确实对应于用户指令，而不是对应于与用户指令无关的随机的量子现象。**

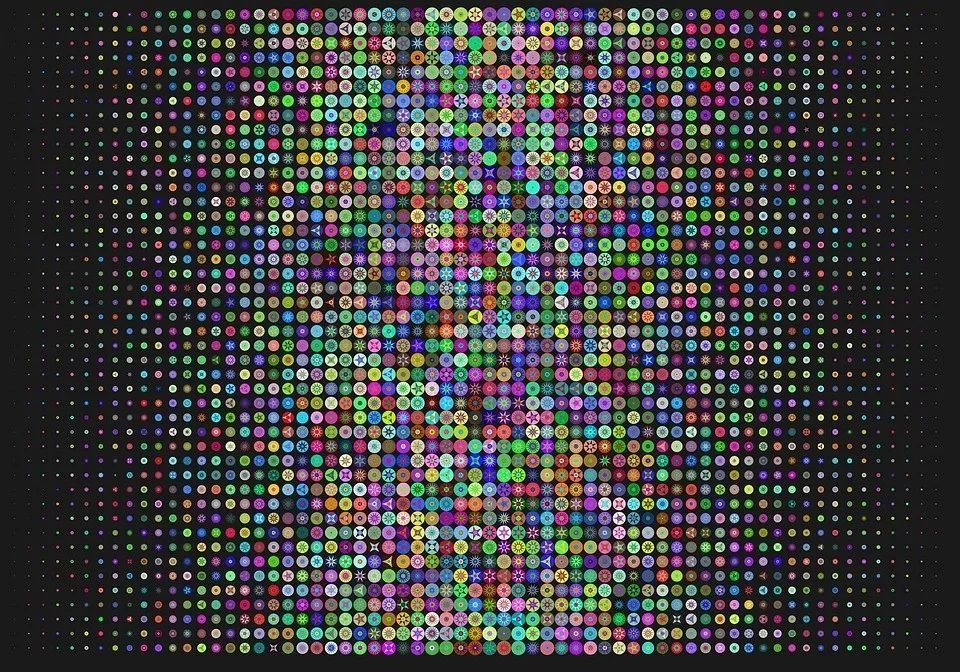


图 | 乌尔米拉·马哈德（来源：加州大学伯克利分校）

**量子计算领域最基础的问题**

马哈德花了 5 年时间研究被阿伦森称为“量子计算领域最基础的问题”：你如何知道一台量子计算机的输出结果确实来自于你输入的指令，而不是某种跟指令无关的随机量子现象的体现？

**这个问题可绝不仅仅是一个象牙塔学术问题。**如果不能证明量子计算机的输出结果确实对应于用户指令，那么不管是仿真黑洞行为还是计算蛋白质构型，结果都不可信。量子计算机的速度确实令经典计算机望尘莫及，但是，经典计算机能忠实执行用户指令，量子计算机可以么？



（来源：Pixabay）

用来证明经典计算机输出结果符合用户指令的方法，无法用来证明量子计算机的计算结果可靠性。至少在理论上，经典计算机的每一步计算结果都可以被用户复查。然而，物理原理决定，对量子系统不可能进行这种核查。量子计算的过程复杂到连将其表述出来都在技术上不可行：**对于只有数百个量子比特的量子计算机，要想把其内部状态完整表达出来，需要一块比整个可见宇宙还大的硬盘**。

就算人类能制造出足够大的硬盘，能完整描述量子计算机内部状态，从理论上也不可能测量这个内部状态。量子计算机的内部状态是无数状态的同时叠加，一经测量，马上坍缩到某个经典状态——经典的“确定态”和量子的“叠加态”完全是两回事。

瓦斯拉米表示，量子计算机非常强大，但是其运算结果的可靠性难以核查。

计算机科学家一直以来都在寻找对量子计算结果进行检验的方法。耶路撒冷希伯伦大学计算机科学家多瑞特·阿伦诺夫（Dorit Aharonov）表示，问题的核心在于首先证明：量子世界和经典世界的结果中间有足够强的联系，下一步才是基于这种联系，来证明量子计算的可靠性。

**马哈德在读研究生第 2 年的时候被这个问题深深吸引，尽管她甚至不能说清这个问题为何有这么大吸引力。**多年来，她尝试了一种又一种方法。“我提出了很多我认为可行的方法，但是一次又一次，它们被证明无效，要么很快，要么花上 1 年功夫。”

然而她没有放弃。瓦斯拉米说：“马哈德表现的决心无人能及——从这个意义上，她非常出色。”

8 年之后，马哈德成功了。她提出了一套协议，基于这套简单协议，用户无需复杂的技术，就可以对量子计算机施加一定的约束，然后输入指令，即可拿到符合自己指令的输出。**至此，量子计算机终于成为不仅“高速”，而且“可靠”的计算工具。**

阿伦森表示，一个研究生做出如此成果“极其惊人”。

量子计算专家不仅对于最终提出的准则给予高度评价，更对马哈德采用的创新性方法兴趣浓厚。将这种基于经典密码学的方法利用到量子领域是个“全新的点子”，未来可望产生更多的成果。

**漫长的道路**

马哈德出生于洛杉矶的的一个医生家庭，在南加州大学读本科，尝试过多个领域。最初，她只是知道，自己不想成为一名医生。不过，在听过计算机科学家，RAS 公钥加密算法发明人勒纳德·阿德曼（Leonard Adleman）的课之后，对于理论计算机科学产生了浓厚的兴趣。**她在提交给伯克利的研究生申请中表示，她对理论计算机科学的任何方向都感兴趣，“除了量子计算”，因为这听上去太过遥远，她不怎么了解**。

然而，在伯克利，导师瓦斯拉米的教导很快使马哈德改变了主意。瓦斯拉米说：“我引导马哈德接触了量子计算可靠性问题，这个问题激发了她无穷的想象。”

马哈德说：“协议就像猜谜。我觉得它比其他的问题简单一些，因为你可以立即在脑子里思考和分析协议，并搞清协议的工作原理。”马哈德将量子计算可靠性作为博士课题，瓦斯拉米导师称“这是一条非常漫长的路。”

当然，量子计算机“计算结果难以核查”的特性并不是绝对的。比如，对大数进行因数分解的问题，量子计算机能以经典计算机望尘莫及的速度解决。但是，量子计算机输出结果，经典计算机很容易核查这个结果是否正确：只需要做一次乘法。

然而，计算机科学家相信，大多数只有量子计算机可以解决的问题没有这么好的特性。也就是说，**对于这些问题的量子计算结果，经典计算机无法检验其正确与否**。而这一特性直到最近才被部分证明。2004 年，滑铁卢大学周界研究所的的理论物理学家丹尼尔·古斯曼（Daniel Gottesman）提出问题：是否能设计一款协议，根据该协议，量子计算机的输出结果可以被非量子观察者核查，以确定量子计算结果确实符合用户的目的？

4 年后，量子计算研究者取得了一些进展。2 个研究团队证明，如果借助一台拥有少量量子比特的量子计算机，那么核查量子计算输出结果就是可能的——但是只依靠经典计算机仍然不行。随后，研究者又证明，只要检查者可以 1 次测量 1 个量子比特，那么核查就可以做到。

2012 年，瓦斯拉尼所在的一个研究团队证明，如果使用 2 台独立的量子计算机对同一个问题进行计算，那么经典计算机可以通过比对 2 个量子结果来验证量子计算的可靠性。但是这个方法一直无法被拓展到更多的应用中，研究人员普遍认为，这条路继续探索的价值不大。



（来源：Quanta Magazine）

**此时，马哈德进入了这个领域。**起初，她试图直接做出一个终极结果，即“对量子计算机能做什么和不能做什么不加任何假定”。然而，碰壁之后，瓦斯拉尼建议，尝试一下**“后量子”密码学方法**。计算机科学家猜测（尚未严格证明），“后量子”密码算法甚至能在量子计算机的破解下保持足够的安全性，而类似于 RAS 算法的基于大数分解的经典加密算法，在量子计算机面前不堪一击。

2016 年，马哈德和瓦斯拉尼在另一个问题上取得了突破，这个成果在日后被证明是通向最终答案的关键。两人与 OpenAI 公司的的计算机科学家保罗·克里斯塔诺（Paul Christiano）合作，发明了一种利用密码学来让量子计算机创造“秘密状态”的方法。“秘密状态”对于经典计算机是不可知的，但是对于量子计算机本身是可知的的。

他们的核心工具是**“陷门函数”——该函数很容易正向计算，但是反向计算几乎不可能，除非拥有密钥**。此外，陷门函数还必须是 2 对 1 的映射，即每 1 个输出对应于 2 个不同的输入。类似于 4 等于 2 的平方和-2 的平方。研究团队成功构建了陷门函数。

有了陷门函数，就可以令量子计算机创建“秘密状态”：首先，令计算机构建一个陷门函数所有可能输入的叠加态——这远远没有听起来那么难。接着，令计算机用陷门函数处理这个叠加态，产生一个新状态，这个新状态是函数所有可能输出的叠加。输入叠加态和输出叠加态之间存在耦合，即对其中一个的测量会影响另外一个。

随后，令计算机测量输出叠加态，然后输出结果。这个测量过程会让输出叠加态坍缩到一个输出结果上，同时（由于耦合）输入叠加态也同时坍缩到对应的输入上。比如，如果陷门函数是“平方”，输出态是“9”，那么观察后结果会马上坍缩到“3”和“-3”。

由于用户手中有陷门函数的密钥，因此可以轻易区分构成输入叠加态的 2 个输入，但量子计算机做不到。更进一步地，量子计算机甚至不能通过测量输入叠加态来确定其构成，因为这种测量会导致输入叠加态进一步坍缩，留下的只是 2 个可能输入中的一个，但是永远不可能确定另外一个输入是什么。



（来源：Pixabay）

2017 年，马哈德提出，用一种被称为“试错方法”的加密方法构建陷门函数，是“秘密状态”方法的核心。“试错方法”作为一种加密方法被广泛应用于云计算领域，可以令云端服务器无法读取用户未授权的数据，即使它正在处理用户的数据。不久，马哈德、瓦斯拉尼、克里斯塔诺、温迪克和以色列魏茨曼科学研究所的斯维卡·布拉克斯基（Zvika Brakerski）进一步推动了陷门函数的研究，成功利用“秘密状态”方法构建了一种能证明量子计算机输出的随机数确实是随机数的方法。

马哈德此时完全可以毕业，但是他决心继续工作，直到彻底解决量子计算可靠性问题。**“我根本没考虑过何时毕业，因为我的目标从来不是拿学位。”**

她承认，探索未知领域有很大压力。不过，“我想通了，**花时间学习我感兴趣的东西不算浪费时间**。”

**一成不变**

马哈德尝试了各种办法，希望基于“秘密状态”方法设计出可靠性证明协议，但是很长时间没有进展。

直到某天她想到：研究人员已经证明，如果检查者可以测量量子比特，那么就可以检验量子计算结果；经典计算机无法测量量子比特，因此无法利用这个方法检验计算结果。然而，如果检查者能强迫量子计算机自己来测量量子比特，然后报告自查结果呢？

这个思路的核心前提在于：**在检验者发出测量指令之前，量子计算机不能知道检验者要做什么测量，否则计算机很容易愚弄检验者。**“秘密状态”方法简直就是解决该问题的天赐工具：马哈德令量子计算机首先创立一个“秘密状态”，然后将该秘密状态和待测状态耦合。只有在这个时候，量子计算机才会知道，要执行什么测量。计算机不知道秘密状态的内容，而检验者知道。马哈德证明，量子计算机不可能欺骗检验者而不留下痕迹。温迪克进一步解释，待测量子比特是“整个方法的基石”。最终，如果检验结果看上去是正确的，那么检查者就大可放心。

温迪克：“这个点子太惊人了，每次乌尔米拉解释的时候，我都会被震惊。”

马哈德的检验协议，以及随机数生成器和盲加密算法，都依赖于这样一个假定：量子计算机无法破解“试错方法”。目前，“试错方法”被认为是首屈一指的后量子加密方法，有望被美国国家标准和技术研究所认定为新的加密标准，来取代那些面对量子计算机不堪一击的加密方法。古斯曼表示，目前还不能说“试错方法”可以万无一失地克制量子计算机的解密，但是至少现在它足够可靠，没有谁发现这个算法有什么弱点可利用。

反过来，如果要愚弄马哈德提出的检验协议，那么就必须找出破解“试错方法”的办法，这同样会是一个惊人的成就。

**当然，马哈德的协议不太可能马上被应用，原因之一是执行该协议需要的计算量大得惊人**。不过，当量子计算机更加强大，算法得以优化之后，该协议仍有很大的应用希望。

虽然马哈德的协议不大可能在 5 年内得以应用。但是阿伦森表示，如果一切顺利，这将是量子计算下一轮技术革命的起点。

温迪克还补充，5 年前，计算机科学家普遍认为，量子计算机想要解决任何经典计算机解决不了的问题还要很多年。现在，科研界普遍认为：**“只要 1-2 年就够了”。因此马哈德协议的应用可能比想象的要快。**

对于马哈德，她承认自己的成就令自己有点迷茫，她个人希望找到一个新的问题来研究。

不过，在理论计算机科学圈看来，**马哈德一统量子计算和加密算法的工作远远不是终点，而是一个有望通向更多丰硕研究成果的起点。**