Photo credit: Andrea Kane, Institute for Advanced Studies, Princeton, NJ, USA / Abel Prize

Avi Wigderson 传记

20 世纪 70 年代末，当 Avi Wigderson 开始他的学术生涯时，"计算复杂性"理论——本身与算法的速度和效率有关——这一理论仍处于起步阶段。可以说，他对扩大和深化该领域的贡献比其他任何人都大，曾经相对年轻的学科现已成为数学和理论计算机科学的成熟领域。计算复杂性也变得异常重要，为互联网安全提供了理论依据。

他于 1956 年出生于以色列海法。1977 年，他进入以色列理工学院学习，1980 年毕业，并获得计算机科学理学士学位。他转到普林斯顿大学攻读研究生，1983 年凭借论文《组合复杂性的研究》获得博士学位，Richard Lipton 是他撰写论文时的顾问。1986 年，Wigderson 返回以色列，在耶路撒冷的希伯来大学任教。第二年，他被授予终身教职，并在 1991 年成为正教授。

在 20 世纪 70 年代，计算机理论家对计算的本质，特别是 P 和 NP 的概念提出了一些基本观点。P 指计算机在几秒钟内就能轻松解出的一组问题，而 NP 也包含计算机认为难解的问题，这意味着已知的方法需要用数百万年才能找到答案。所有这些难题能否简化为简单的问题，即 P = NP 是否是计算复杂性的基本问题。事实上，它现在被认为是所有数学中最重要的待解问题之一。

通过研究随机性在辅助计算中的作用，Wigderson 在这一领域取得了令人瞩目的进步。利用计算机在计算过程中抛硬币的算法，一些难题可以变得简单。但是，如果一种算法依赖于抛硬币，那么解中总有可能出现错误。Wigderson 先后与 Noam Nisan 和 Russell Impagliazzo 一起证明，对于任何能够通过抛硬币来解难题的算法，只要满足某些条件，总是存在一种速度几乎一样但却不用抛硬币的算法。

Wigderson 对复杂性理论中的每一个主要的开放性问题都进行了研究。在许多方面，这个领域已经在围绕着他而演变，这不仅是因为他的研究领域范围广泛，也因为他平易近人的人格魅力和对共同协作满怀热情。他与 100 多人共同撰写了论文，并指导了一大批年轻的复杂性理论家。"能够生活在这个时代，我认为自己非常幸运，"他说。"[计算复杂性]是一个年轻的领域。这是一个非常民主的领域。这是一个非常友好的领域，也是一个非常注重合作的领域，非常符合我的天性。当然，它充满了智力问题与挑战。

1999 年，Wigderson 加入了普林斯顿高等研究院 (IAS)，并在那里工作至今。2016 年，在一场庆祝 Wigderson 60 岁生日的活动中，IAS 院长 Robbert Dijkgraaf 说，他开创了该研究院在理论计算机科学领域的黄金时代。

Wigderson 以能够发现明显不相关的领域之间的联系而闻名。他深化了数学和计算机科学之间的联系。他与 Omer Reingold 和 Salil Vadhan 一起发展的之字形图积就是一个示例，该之字形图积将组合理论、图理论与复杂性理论相关联，并得到了惊人的应用，比如如何最好地走出迷宫。

密码学是复杂性理论目前最重要的应用，可用于保护互联网上的信息，如信用卡号和密码。例如，设计加密系统的人必须确保解码系统的任务是一个 NP 问题，即计算机需要数百万年才能解出的问题。在职业生涯的早期，Wigderson 对密码学领域的新概念——零知识证明——做出了根本性的贡献，30 多年后，这种概念现在正被用于区块链技术。在零知识证明中，两个人必须为主张提供证据，但除了主张的有效性之外，不透露任何额外信息，例如两个百万富翁的例子，他们想证明谁更富有，但两个人都不透露他们拥有多少财富。Wigderson 与 Oded Goldreich 和 Silvio Micali 一起证明，零知识证明可以用于秘密地证明任何有关秘密数据的公开结果。比如说，您想向某人证明您已经证明出了一个数学理论，但却不想透露证明过程的任何细节，零知识证明可以帮助您做到这一点。

1994 年，Wigderson 获得了罗尔夫 • 内万林纳计算机科学奖，该奖项由国际数学联盟颁发，每四年颁发一次。他的众多其他奖项还包括 2009 年哥德尔奖和 2019 年高德纳奖。

Wigderson 与在以色列理工学院求学时结识的 Edna 结婚，后者在高等研究院的计算机系工作。他们有三个孩子和两个孙子。

引文来源：Heidelberg Laureate Foundation Portraits，Avi Wigderson 访谈，2017 年。